ADVANTAGE: MANAGED

The power behind managed switches is software that simplifies the management of state-of-the-art network functions.

Keeping employees connected to the network means keeping them effective and productive. Managed switches can help by offering the added functionality that allows IT chiefs to remotely monitor and administer networks as well as switch functions.

Managed switches also provide smooth connectivity for advanced network requirements, while unmanaged switches are designed to serve plug-and-play environments.

"Unmanaged switches come with a fixed set of features that cannot be modified," says Doug Hyde, director of switching at HP. "Managed switches, in contrast, are customizable, allowing you to enable various features not available on unmanaged models."

By supporting the implementation of today's state-of-the-art technologies like virtual LANs (VLANs), unified communications, virtualization, Gigabit Ethernet and more, managed switches play a role in fully optimizing the network.

"That's huge," says Rihit Mehra, director of enterprise communications infrastructure research at the technology research and analyst firm IDC. "It's not just end users connecting to the network. The devices may not even be computing devices."

By way of example, he points to items such as IP video surveillance cameras, either attached directly to the network or coming in via a wireless access point. "Either way, there's an impact on the network," he adds.

Video over IP and voice over IP (VoIP) are both adding traffic at growing rates. That type of traffic requires special handling that high-end switches support. The traffic itself comes from devices that require

SWITCHES

Primary Functions

While managed switch capabilities will vary with vendors and models, even the most basic will offer the ability to select port parameters including accessibility, link speed and duplex settings. This is important for networks needing higher levels of security, optimized performance or 24x7 network uptime. It also is required when you want to monitor the network for status.

According to HP's Hyde, there are times when only managed switches will do. "For example, managed switches are recommended when you anticipate having more than a handful of switches or you need the switches to be doing any routing.

"The same holds true if you have temperamental applications running on the network," he adds. What's more, most business users prefer a managed switch to get stats on switch traffic, troubleshoot connections, and assess hard-code port speed and duplex settings.

The Switch Effect

To understand the need for fully managed switches, it's important to realize what's going on in the computing world. Those who follow the switch market point to the rising use of consumer and other nontraditional devices for accessing corporate networks.

Staffers want their smartphones and tablets to be both personal and enterprise application access devices. And that creates important security considerations for the network team.

power in locations not served by AC power or where it is impractical to extend electrical wiring.

Such devices include VoIP desk phones, for which no one wants power bricks to clutter cubicles, and Wi-Fi access points in ceilings or public areas where no AC plug is nearby. The result is a growing demand for Power over Ethernet (PoE).

Switches equipped with PoE are in high demand. In practice, the capability is as simple as it sounds. It consists of electrical power at configurable levels delivered to a device using standard CAT 5 Ethernet cabling.

In fact, PoE, governed by IEEE Standards 802.3af (15 watts) and 802.3at (for PoE+ at 30 watts) itself may be responsible for a switch refresh purchasing cycle, according to Mehra. Fully managed switches should be able to control the power, or even whether power is present, port by port.

Virtualization, or the separation of compute processing and storage from the user display device, is also changing the nature of network traffic. So is virtualization

moved to a second-party supplier, the phenomenon known as cloud computing.

In addition, faster strains of Ethernet are calling for managed switches. In addition, WAN acceleration, for example, and different security protocols call for careful control mitigation, which favors an architecture girded by fully managed switches.

Gaining Capability

So what are the key capabilities systems administrators look for in fully managed switches? First is the management capabilities of the switches themselves. In short, they offer the ability to configure, manage and monitor the LAN. This offers expanded control over how data travels over the network and who has access to it.

Equipped with Simple Network Management Protocol (SNMP) agents, command-line interfaces and communications via telnet or secure shell, these switches let systems administrators create centrally stored configuration files. These can then be broadcast to all of the switches on the network.

Some switches are equipped with an auto-configuration feature, says Geoffrey Sejourne, a group product marketing manager at Brocade. Upon reboot, the switch will automatically seek and install the latest configuration file from a remote server. "Large businesses need central management to apply policies all at once," Sejourne says.

Another capability of fully managed switches is centrally controlling the configuration of individual ports — as well as applying a given access policy to all ports simultaneously. "With port control, you can apply a lot of policies at ports and the processing of packets at the ports," explains Mark Hilton, director of product marketing at HP Networking. "You can lock a port when an attempt at accessing it is made without supplying the proper identification and authentication credentials."

Once the switch authenticates a user, it applies whatever policies are assigned by the access control list. This may include bandwith limitations and security settings, and what applications or databases are available to that user.

Hilton points out that some switch models come equipped with port-level detection of traffic, filtering out any traffic deemed to be malware and redirecting suspicious traffic to whatever intrusion detection system is in place. It is also possible to prevent access to (or from) certain IP addresses on a port-by-port basis.

A third capability is security related. Besides the ability to detect Media Access Control (MAC) addresses of connected devices, the latest managed switches support sFlow, a proposed standard for sampling network traffic packets and logging them for subsequent analysis.

Last but not least, managed switches support the highest speeds available for the most data throughout. In an age when high definition video must be delivered to all users, bandwidth requirements jump another order or magnitude.

It wasn't so long ago that 10BaseT, or 10 megabits per second, reflected the speed need for most corporate data. Today, high-end switches routinely support gigabit and 10-gigabit Ethernet. What's more, currently 40 and even 100 Gigabit Ethernet has been ratified, with corresponding products said to be available in mid-2011, according to estimates from the market intelligence firm IDC.

Powerful Services

Fully managed switches allow the greatest degree of flexibility in dealing with competing requirements on the enterprise network. Heading the list is support for virtual LANs.

VLANs operate like regular LANs, but without the need for routers. Functionally, VLANs create channels that bring common traffic types together because user endpoints are not necessarily on the same physical switch.

With VLAN technology, a switch lets the systems administrator isolate, say, VoIP or video traffic with their need for low latency from file transfer traffic, which can operate fine at a lower priority, or quality of service. VLANs can also be set up to isolate traffic according to security settings or rights to network resources.

"As soon as you get voice over IP, you need VLANs," says Brocade's Sejourne. "You should use VLANs to define types of traffic." That means, for example, a separate VLAN for data, one for guests who might need Internet access but not access to the corporate intranet, another for remote employees, and still another for customers and trading partners.

Enterprise Benefits

Ultimately, a salient benefit of fully managed switches is their ability to give the network administrator policy-based, fine-grained control of the network. Control can be executed from any of several

Converged Infrastructures

The IT infrastructure is core to business functionality. Yet IT managers are currently challenged with a complicated, cumbersome and siloed infrastructure due to the rise of x86 architecture and virtualization, which can lead to physical and virtual machine sprawl.

To help, converged infrastructure (CI) brings together core network products into one solution set that allows businesses to manage their data center through a common framework of tools and technologies. This can translate into a more scalable, dynamic infrastructure that is more responsive to core business strategies including speed, agility and faster time to market.

Not All Switches Are Created Equal

Beyond sheer connection capacity, switches can be grouped into three main classes:

Unmanaged Switches

These are inexpensive and designed for small businesses or applications in which users share e-mail and traditional productivity applications such as spreadsheets and word processing documents. They can't be configured in any way. However, by the same token, they don't require tending. Unmanaged switches are useful for very small networks, such as conference rooms and when traffic is heterogeneous.

Web-managed Switches (Smart Switches)

These include a resident web server acting as the interface to software tools for managing the switch. Web-managed switches allow configuration to accommodate different types of traffic and security settings. But they can't be managed centrally.

Fully Managed Switches

In addition to supporting a range of services crucial to today's enterprise networks, they offer centralized management from a single console.

perspectives, such as by port, user, URL or application.

What's more, this control can be managed centrally from a single console. Using SNMP, switches and devices connected to them are visible to and alterable from the console.

Central control in a switched network environment bolsters enterprise security by enabling the network administrator to distribute software updates and patches automatically. Managed switches work through a web interface as well as through a command line for fast scripting of changes or configuration files.

Fully managed switches ensure network reliability by maintaining fallback routes among bridged network segments should a switch or other device, even a cable, fail. Networks can only tolerate single pathways — those that are free of loops that can cause network clogging.

Using the spanning tree protocol, first developed in the 1970s, a fully managed switch can calculate the next-best — least costly, in network terminology — data pathway according to preset parameters. This allows it to most effectively take data anywhere it is needed, on schedule.

Fully managed switches' centralized control also let administrators adjust quality of service, or traffic priority, according to applications that may be assigned their own virtual private networks. As more enterprises add VoIP and video (even post their marketing productions on YouTube), control over QoS becomes critical because the timing of voice and video packets is key to their coherence.

Scalability also ranks high in the benefits of fully managed switches, important to growing companies or those whose web applications receive increasing traffic. As Brocade's Sejourne points out, the trend in Layer 2 — or link layer — switches is to stack them via daisy chaining so that they act as a single logical switch. The benefit is fast and it allows scaling without an accompanying increase in management complexity.

Buying Considerations

Many switch parameters are governed by IEEE or Internet Engineering Task Force (IETF) standards. Many IT shops mix and match brands of switches, although aggregating buying among a short list of vendors can produce better pricing or terms and conditions.

When comparing switches, here are some considerations:

- **Performance.** Rated speed is a specification, but performance can depend on the internals of a switch. Compare so-called fabric speeds and how well the switch shuttles data among the ports internally. Also consider how fast, in terms of packets per second, the switches interact when stacked.
- **Price/performance ratio.** This is simply the dollars per unit of performance. Switches tend to be priced per port, ranging from hundreds of dollars per fully managed 10-gigabit port to less than $20 for unmanaged gigabit devices.
- **Construction and reliability.** Look for modules such as ports or electromechanical parts such as fans that can be switched out without shutting off and rebooting the switch. Also important from a reliability standpoint is whether the switch includes redundant critical parts and whether it incorporates automatic failover.
- **Modularity.** Look for interchangeable ports, letting you install individual ports with different speeds, depending on the requirements of the endpoint connected to the port.
- **Integration.** IDC's Mehra says to consider whether a switch that's going to be handling wireless access points will automatically configure the APs according to IT policy. "The trend is toward unifying wireless and wired as a single entity with respect to policies," he says.
- **Layer 2 or 3.** Lately there is differentiation between Layer 2 switches, prioritized for local traffic or within a sub-LAN, and Layer 3 for incorporating routing functions across sites or within a large corporate site.
- **Ease of management.** Switches have proprietary operating systems and management consoles. One is not necessarily superior or easier to learn than another. But consider the experience and certifications of the staff that will be managing them and whether they are trained on the brand you are considering. ◊