FOCUS

Networking Market Primer

Focus Research
Networking Group
May 2009

Introduction

Not sure where to start with networking? Building a local area network is a serious endeavor, and it can be difficult to know where to begin. Our Networking Market Primer is intended to provide CEOs, IT administrators and anyone else involved in making a first-time networking purchase with a fundamental understanding of network storage hardware and software.

In this Market Primer, you'll find:

Table of Contents

1 Networking Basics

Networking Defined

The largest network in the world is the Web, which creates a grid of thousands of PCs and servers all over the world. But a network can be as simple as just two or three computers connected so that users can share data and compute resources. Most modern business networks are built in the client/server model — PCs are the clients that make application requests to the server — and include routers and switches to connect PCs, laptops, printers and other peripherals. A network is made more useful by software, which includes performance and monitoring tools to keep network traffic moving smoothly and efficiently, NOSes (network operating systems) to get computers online, and security applications to protect it from the outside world. You can connect your business network to the Internet and other private networks.

- To share files, databases, printers and other hardware, as well as client/server applications within a building or between headquarters and a branch office
- To enable reliable backups across all the servers and PCs in an organization
- To move a company's business online, including an e-commerce Web site and individual email accounts for employees

There are two basic types of networks. The more common, especially for smaller companies that are building a network for the first time, is a LAN (local area network); a LAN is composed of the networked computing resources contained in a single room, in an entire building, or across a campus facility. The other type is a WAN (wide area network), which is more often used by large organizations that need to connect multiple LANs across several miles.

These days, many new networks are built with a combination of cables and wireless communications devices to enable the network connections. However, you can build a network just with cables running through the floor, ceiling, and walls, or you can make it entirely wireless. Ethernet is the most common LAN technology, and TCP/IP is the reigning data

transmission technology.

Prime Yourself: 10 Things to Know About Networking

When you build a network, you're laying the foundation for your company's growth. Many decisions must be made involved in planning and designing the network as well as building and maintaining it. Before you make the leap, here are 10 things that will inform your network construction and help you understand networking technologies:

1. Networks require some expertise. Networking technologies are established and many networking products are commodity items, but building and maintaining a network still requires a certain amount of specialized IT knowledge. You'll need a network administrator, either on your IT staff or via a consultant, who can troubleshoot performance issues and hardware malfunctions and generally keep the network running at full speed.

2. You don't have to start from scratch when you build your network. The computers you currently use can be connected to any network you build, assuming they run modern OSes (operating systems). All OSes, including Microsoft

10 Things to Know about Networking

1. You need a skilled network administrator to keep the network running at top speed.
2. Current PCs can be easily connected to a new network.
3. Running network cables is tough physical labor.
4. Your network should be built to support your company's growth.
5. You network should be flexible enough to support new features and technologies.
6. Network devices that are easy to use and manage are the best investment.
7. If your network is connected to the Internet, it will be vulnerable to new security risks.
8. Traffic must move quickly between every node on the network.
9. Performance management is an important aspect of network maintenance.
10. NAC tools can help authenticate approved users.

Windows, Apple MacOS and Linux are compatible with networking. Many existing printers, modems and other peripherals can also be added to your network.

3. Running network cables is hard work. Unlike many IT-related tasks, laying cable for a network is hard labor — it often requires climbing through drop ceilings, snaking them through walls, and running them under floor panels. Like the phone jacks, the network cables should end in neatly installed modular wall jacks in each cube.

4. Build your network for the future. Network building blocks, like the cables, routers and switches, generally have a much longer useful life than the PCs connecting to them. So even if you don't need it now, it's wise to invest in Category 5 cable, which supports networking at gigahertz speeds, and to purchase business-grade networking devices.

5. 5. Build flexibility into your network. You may want to start small with your network, but chances are your network will grow with your business. You want to be able to add new features and functionality as you need them, including VoIP, integrated messaging, wireless networking and video surveillance.

6. Choose easy-to-use network devices. Even if they cost a little more, opt for routers and switches that are easy to install and manage; for instance, choose devices that have in-line power (called Power over Ethernet or PoE) so that you don't have to worry about plugging them into an electrical socket as well as a network wall jack. Also, choose the devices with built-in redundancy — you don't want a hardware malfunction to take out your entire network.

7. Beware of security issues. If your network is connected to the Internet — and it probably should be — it will open your company to new risks like hacking, viruses, email attacks and more. It's therefore important to secure your network with at least a firewall, which may be built into a router or added via software. Additional security measures, including anti-virus software and an IPS (Intrusion Prevention System) may also be smart.

8. Traffic must move quickly across the entire network. Your network's design must send network traffic from node to node as quickly and efficiently as possible. In addition to routers and switches, you may need to add repeaters or bridges to your infrastructure.

9. Performance management is critical. To prevent serious network outages, you need to know what's happening on your network at all times. This means monitoring for error rates, taking response-time measurements, noting throughput and utilization metrics and knowing demand peaks and valleys.

10. Only authorized users should be able to access your network. At worst, unauthorized users can steal proprietary information or, at best, install unapproved software. You can use NAC (Network Access Control) tools to authenticate approved users, find and isolate unauthorized users, grant guest access and spot any unauthorized devices or applications installed on your network.

2 Market Summary

Local area networks have become such a common aspect of the business technology scene, it's hard to remember a time when employees weren't connected through their computers. The challenge for modern companies is keeping up with users' expectations — delivering lightening-fast speeds, deploying easy-to-use solutions for mobile workers and maintaining 100 percent network uptime.

Market Evolution

The history of networking is almost as long as the history of PCs — it didn't take long for the scientists at Xerox PARC (Palo Alto Research Center) to see how advantageous it would be to connect those early 1970s PCs to PARC's first laser printer.

From 1973 to 1975, PARC researcher Robert Metcalfe developed Ethernet, which is now the primary standard used in LANs around the world. In 1976, several events laid the groundwork for LANs as we know them today: Metcalfe and David Boggs published their definitive paper, "Ethernet: Distributed Packet-Switching For Local Computer Networks," the White House and American universities started adopting personal distributed computing and the newly invented client/server architecture began to be commercialized. Xerex, DEC and Intel continued developing the new technology together and created the 10Mbps Ethernet (10Base-T) specification in 1980. It was published as the IEEE standard 802.3 in 1985 and continues to be widely deployed.

The most significant change in Ethernet is the speeds at which it sends data across the network. In 1995, Fast Ethernet (100Base-T), which sends data at 100Mbps, was developed, and in 1999, Gigabit Ethernet (1000Base-T), which sends data at 1000Mbps, was ratified by the IEEE standards body. Most recently, 10 Gigabit Ethernet standards became available in 2002 and 2006. Generally, fast Ethernet and faster standards are used for LAN backbone systems while the workstations on the network have Ethernet cards.

Ethernet may be key to a LAN, but it's not the only technology that makes networks work. The industry standard protocol TCP/IP (Transmission Control Protocol/Internet Protocol) is used to connect separate networks, including private networks to the Internet. First developed in the 1970s by DARPA (U.S. Department of Defense Advanced Research Projects Agency), TCP/IP version 4.0, which is still in use, was stabilized in 1978; TCP/IP was made widely available in 1983.

These early networks were inflexible and built on proprietary hardware, intended mainly to help co-workers share files and databases. But government officials joined forces with industry leaders to push for interoperability among networking products and protocols, and today you can build a best-of-breed LAN that mixes products from all networking vendors.

Two more important changes happened in the early 1990s that shaped modern LANs: Peripheral devices with built-in network cards, including printers and modems, started selling and the Internet became accessible by the general public.

In a short span of time, the networking industry made unbelievable gains in performance, reliability, interoperability and cost; today, users take for granted an always-on network connection that gives them access to various resources on the private LAN as well as the Web, and IT personnel think nothing of running out to a nearby electronics store to pick up a new router or a few cables.

As common as network technologies are, they aren't static. Innovations continue to be made in terms of wireless and mobile connectivity, ever faster data speeds, and increasingly sophisticated processors. Networks themselves continue to evolve as initiatives like cloud computing and grid networks become commercially viable.

Market Trends

The most recent networking trends are about extending the network to all users while making it more efficient. The three most significant are:

1. Freedom from the network: Wireless networks let employees work wherever they need to, whether they're roaming with their laptops between conference rooms, meeting with clients at their office or checking email at a coffee shop. Wireless networks can be a relatively simple way to add a LAN to a small or branch office because they don't require any cabling, and they're easy to expand as your needs grow. If you already have a wired network, you can add wireless capabilities by installing a wireless access point and connecting it to your router. Your end user devices need to support the wireless LAN protocol called wifi (or IEEE 802.11); many newer laptops and handhelds have built-in wifi support, but you can add adaptors if they don't.

2. One network for all: Until recently, data networks and voice networks were separate infrastructures. But network convergence uses emerging technologies and new network architecture designs to merge voice and data communications onto a single IP network that supports voice, video and data protocols. A converged network lets you consolidate support, maintenance and management to a single infrastructure while also cutting down the amount of space you need to house your network equipment. If you deploy VoIP on your converged network, you may be able to save money on long-distance calls that are made on the network rather than through long-distance calling over your phone lines.

3. Going green: Companies large and small are looking for ways to make their operations more environmentally friendly. Simply installing a network can dramatically reduce the amount of paper your business uses — email replaces paper memos on every desk. You can cut down energy consumption by choosing networking hardware that has optimized power supplies and power management. Also, a network supports green telecommuting practices by allowing workers to log in remotely and conduct videoconferences. The industry is working toward greener networking technologies, too; the new IEEE P802.3az project is trying to deliver major energy savings with a more energy-efficient Ethernet.

Vendor Landscape

The networking landscape has been dominated for a long time by a few industry titans, especially Cisco and Nortel, despite the latter's current financial troubles. Chances are good that you'd turn to these giants first when shopping for network equipment. According to CIO Insight's 2008 Vendor Value Survey, the top five network vendors are: Cisco, which had the most customers willing to continue doing business with them; Juniper Networks, which also enjoys a good degree of customer loyalty; 3Com, which is often chosen for its easy-to-manage, relatively inexpensive gear; and Motorola and Nortel.

But these players aren't the only game in town — there are many network vendors that offer quality gear at competitive prices for small and large companies alike. Many hardware vendors also sell network management and performance software, but there are software vendors that specialize in this arena. You might also consider equipment from telecommunications vendors, particularly if you're considering a converged network that will run VoIP.

When you're building — or expanding — your LAN, expect to choose several vendors. Shop for the best deal on the equipment you need; after all, the point of network protocols is to make for a fully interoperable, best-of-breed network infrastructure.

Turn to the Network Equipment Vendor Universe appendix for an expanded list of current storage network vendors.

3 Product In-Depth

Local area networks have become such a common aspect of the business technology scene, it's hard to remember a time when employees weren't connected through their computers. The challenge for modern companies is keeping up with users' expectations — delivering lightening-fast speeds, deploying easy-to-use solutions for mobile workers and maintaining 100 percent network uptime.

Market Evolution

Whether you're building a simple LAN that will bring a handful of employees online, or you're designing a complex network that will connect all the buildings in a campus, you'll need to start with the same basic building blocks. The major difference is the amount of equipment you'll need to build the network.

When you're planning your LAN, you should familiarize yourself with three areas:

1. **Product features:** Network components
2. **Cost and benefits:** License fees and hardware costs
3. **Vendor:** Selling, implementation and support

Product Features

A network can be as complex as you want — you design and build it to fit your company's current and near-future needs. You may consider hiring a vendor to help with the design process, but ultimately you need to understand your business requirements in order to end up with the right infrastructure for your company.

Every network uses the same gear and standards, including routers and Ethernet, to make connections. A more sophisticated infrastructure might also include additional tools for optimizing performance, for example. Advanced LANs may have "extras" — features that some companies consider "must-haves," while others view as "nice-to-haves." When you're weighing your options, keep in mind where you expect your company to be in the next few years. Network equipment has a longer useful life by several years than your average PC or server, and you want to make sure your business doesn't outgrow it before its time is up.

The Basics

There are several essential building blocks that are at the core of every LAN. Without them, you won't have an efficiently functioning network that sends and receives data quickly and accurately.

Data transmission system: Whether wired or wireless, you need a system that carries the data travelling on your network. Most wired networks are built with twisted-pair cables, which are categorized based on the speeds they carry traffic. Networks should be built with at least Category 5 cables, which are rated for 100 Mbps performance; Category 6 cables are even better because they're rated for 1000 Mbps and faster performance. This will allow you to easily upgrade your network when the time comes.

For a wireless LAN (WLAN), you need a wireless access point, which connects wireless devices, like laptops and smart phones, to the wireless network and network peripherals, like printers. Most WLANs are connected to a wired network, such as to a wired router that allows access to the Internet.

Switch: A network switch connects multiple devices, such as computers, servers and printers, and creates a shared pool of resources. A switch dynamically makes point-to-point connections for the devices connected to it and eliminates most network traffic collisions by making the connections only when they're needed. Business-grade switches come in a variety of port and speed combinations; even switches designed for the SMB (small to medium-sized business) market often have eight to 48 ports with support for Ethernet, Fast Ethernet and Gigabit Ethernet speeds.

What Is a LAN?

A LAN (Local Area Network) connects two or more computers together to share data, peripherals (like printers) and a high-speed Internet connection.

The main reasons for implementing a LAN are:

- To enable greater collaboration among employees
- To bring your business online with a Web site and email addresses
- To make business data more secure

The essential features of any LAN infrastructure include:

- A network switch
- A network router
- Ethernet

You can choose between the two types of switches: managed and unmanaged. Unmanaged switches don't allow you to make changes and are typically suited just to home networks. Even a small company should choose a managed switch that you can remotely configure, monitor and troubleshoot. Look, too, at switches that have some built-in network security functions, such as a firewall, intrusion prevention and detection, VPNs (virtual private networks) and more.

Router: A router connects separate networks, such as your private LAN to the Internet, and it determines the best route for network traffic to travel. Like switches, business-grade routers have integrated security features, such as firewalls and VPNs, and support VoIP traffic. Some routers also have built-in wireless networking.

Server: On a network, a server can handle several different applications or be dedicated to a single purpose, accessible by all the users on the network. For instance, you might have a file server, a print server, a Web server, a mail server or a database server.

NIC (network interface card): Any computer on a LAN requires a NIC to make the network connection. If you're building an Ethernet-based LAN, your computers need Ethernet NICs. Most new computers ship with built-in NICs, but you can install them to older systems.

NOS (network operating system): This software, such as Microsoft Windows Server, Juniper JUNOS, Red Hat Enterprise Linux Server, Novell's SUSE Linux Enterprise Server 10 and Apple Mac OS X Server, enables computers on the network to access resources and services, including printer sharing, file system and database sharing, application sharing and basic network management functions.

Directory services: This software organizes your resources on the network and makes them searchable so that you can discover where a folder, for instance, a printer or other service is located on the LAN. Directory services, such as Novell Directory Services, Microsoft Active Directory and LDAP (Lightweight Directory Access Protocol), also allow you to manage your network resources from a single platform.

Security services: These may already be present in your switch or router. Basic network security services include a firewall, DHCP (Dynamic Host Configuration Protocol) and NAT (Network Address Translation), which may perform content filtering, URL filtering and intrusion detection or prevention.

NAC (network access control): NAC allows you to control who — and what — can use your network. This means that you can prevent laptops or other devices from connecting to your network if they don't meet certain security requirements that you've set. Likewise, you can detect users who don't have permission to be online as well as grant guest access to temporary users.

Advanced Features

These are some of the more common network devices and software that are used to build out a larger LAN. Campus LANs, for instance, need to meet growing demands for tighter security and faster performance. To start meeting these demands, you might consider adding these to your network design:

Bridge: This device connects two LANs that are built on the protocol, such as Ethernet, and it intelligently sends data to its destination on the intended LAN.

Gateway: A server can function as a gateway, a network point that acts as an entrance to another network, like the Internet.

Network management tools: Most vendors offer their own management tools, some of which are specific to their hardware — and, for the larger LAN, they are essential for configuring, monitoring and troubleshooting the network. A basic network management system generally includes tools for monitoring availability, generating performance reports and troubleshooting problems with network devices via a Web-based UI. There are a wide range of additional network management tools, some of which are software while others are delivered as network appliances. They include image and configuration tools, which make large-scale device deployments easier to manage; network performance analyzers, which can improve application delivery; and unified management tools, which tie together the management of a vendor's routers, switches and sometimes, security devices.

IPS (Intrusion Prevention System): A larger network also has greater security needs, which may be met with an IPS. This device sits in-line on your network and inspects packets as the traffic passes through, stopping malicious packets before they can do any damage.

VPN (Virtual Private Network): A VPN uses software to create a private network connection over the Internet, so employees can securely log in to the company's LAN from any remote location with Web access.

VoIP and IP phones: If you build a converged network, you'll need a VoIP system that allows users to place their phone calls over the network. It includes VoIP software, management and optimization tools and IP phones, which are connected to the network like any other network device.

Unified messaging: Like VoIP, unified messaging is often associated with a converged network and requires specialized software. Unified messaging combines incoming voice, fax and email messages in a single mailbox, which users can access through their email clients or by phone.

QoS (Quality of Service): QoS lets you manage network resources so that business-critical applications have priority over less important applications. You can guarantee a specific amount of bandwidth to certain applications, so that streaming video or radio, for instance, don't slow down your payroll application at the end of the month.

Costs

Because there is no one-size-fits-all solution for building a LAN, there's no easy way to estimate the costs. You may have to include several variables that are specific to the network that fits your company's needs, including consultant fees if you use a contractor for design and installation, cables if your building is not already wired, monthly bandwidth fees for your Internet connection and the number of devices you need to install. The bottom line is that you want to design a cost-effective network that delivers consistently high performance.

Who Buys

The decision makers most often involved in deciding what kind of a network is best for a company are:

- CIOs
- CFOs
- IT directors
- Network administrators

Why Businesses Buy

A LAN is the best way to enable collaboration internally among employees and externally with clients and partners while also opening up new streams of revenue for your business:

1. A LAN is a cost-effective and efficient way to allow co-workers to share their data — they can email files, save them to a shared server that is accessible by all employees, and log on to common databases. Without a network, users can share data either by printing documents on personal printers or by swapping files copied to disks or USB jump drives.

2. When your network is connected to the Internet, it opens up a world of possibilities for cost-effectively interacting with clients and partners in real-time — team members can hold Web conferences with video and customer service reps can use text chats to solve customer problems, for instance.

3. With an online presence, your company can launch an e-commerce Web site to sell your products and services to customers around the world.

4. A LAN offers two overarching business benefits: It provides an economical way to make employees more productive and efficient, and it creates opportunities to reach new customers.

What They're Willing to Pay

According to networking giant Nortel, the average cost for a basic client/server network for 10 users is about $20,000; this total includes software, a small server, workstations and additional hardware, but not printers, faxes or modems. Of course, this is just a broad estimate — network-device costs vary widely, depending on how many routers, switches and servers you must buy, and second-tier vendors usually charge much less for their devices than the brand-name vendors. Depending on your company's requirements, you may spend as little as a few hundred dollars on a single wireless router to give employees Internet access, or you can spend several thousand dollars to install a campus-wide LAN.

In addition to purchasing network devices, you will need to buy networking software. You might also figure in the extra costs of network peripherals like printers, advanced network monitoring software, online collaboration applications or sophisticated security devices. Ongoing costs tend to include software updates and patches, monthly ISP fees — bandwidth can be a big-ticket item — and replacement hardware.

On-Premise Hardware Costs

If your office building isn't already wired for LANs, your hardware costs will start with the Ethernet cables. You can buy cables in bulk spools and in different increments, anywhere from one foot to 100 feet of patch cabling; for instance, a 1,000-foot spool of Cat5E UTP solid network cable costs about $65, RJ45 connectors cost about 10 cents each and compatible patch cables range from $3 for one foot of cable to $50 for a 100-foot cable.

The purchase price for switches differs wildly based on the number of ports, the bandwidth speeds they support and the manufacturer. You can get an off-brand five-port 10/100 Mbps switch for as little as $10. Vendors like Cisco and

NETGEAR offer 24-port 10/100 Mbps switches for less than $100, but if you want gigabit Ethernet, expect to pay closer to $300 for a 24-port Cisco or NETGEAR switch. Naturally, enterprise-grade switches jump in price when you add features and ports. For instance, the Cisco Catalyst 4948 10/100/1000 Mbps switch has 48 ports, hot-swappable power supplies and fan trays and redundant fans. It retails for about $17,500.

Like switches, routers vary in price according to the size of the network they're designed to support. For around $100 you can buy a wireless router that includes QoS, a firewall and wireless security features suitable for a smaller office LAN. Wired routers that support the networks of medium and large companies, which might run VoIP and other advanced applications, cost much more. For example, Juniper's J-Series Services Routers cost between $2,000 and $9,000, and include Gigabit Ethernet ports, firewalls, QoS and more high-performance features.

Vendors that offer a wide range of server products nicely illustrate the range in prices. For instance, Sun Microsystems' bottom-of-the-line x64 Sun Fire X2100 M2 starts at about $1,200; mid-range servers cost between $3,000 and $12,000; and its enterprise-class servers can cost upwards of $40,000. When purchasing servers, you need to decide if you can repurpose existing computers and if you'll need the additional scalability and capacity of rack-mountable servers.

The final must-have hardware cost comes in the form of your connection to the Internet. A smaller company may be satisfied by contracting with an ISP that offers DSL broadband or cable connections. Larger companies, however, should consider contracting with an NSP (Network Service Provider) that provides T1 and faster connection speeds. Either way, take into consideration the provider's connection speeds, SLAs (service level agreements), additional services like Web hosting and installation and monthly fees. Look for discounts on multiyear agreements; for instance, AT&T's NxT1 6 Mbps connection costs $1,100 per month for a one-year contract, but only $900 per month for a three-year contract (in the San Francisco Bay Area). The slower 3 Mbps connection costs $40 a month.

On-Premise Software Costs

Essential on-premise software costs include your NOS (network operating system) and basic network management tools. Like operating system costs, NOS costs vary according to the number of clients you need to license, amount of advanced features you want and if you opt for a proprietary or an open-source solution.

For instance, the licensing model for Microsoft Windows Server 2008 consists of a server OS license and additional, incremental CALs (Client Access Licenses); the server OS plus five CALs costs $999, $1,199 for 10 CALs and $3,999 for 25 CALs. In comparison, the open source SUSE Linux Enterprise Server 10 starts at $350 for an annual basic subscription, which includes software updates and access to Web-based installation and configuration support; the $799 standard one-year subscription adds unlimited telephone and electronic support during business hours with four-hour response and previews to new product releases; and the $1,499 priority subscription adds one-hour responses to severe problems.

Some network hardware vendors, such as 3Com, also sell network management software. Much like enterprise-grade software, prices are quoted directly to the customer based on the number of users. If you're considering enterprise-scale software, download the free trial first. Network management software geared to smaller companies is easier to price; for example, NETGEAR's NMS100 ProSafe Network Management Software costs about $600, and 3Com's Network Director costs about $2,500.

Vendor

A list of vendors, current as of March 2009, is included in the back of this primer. The biggest vendors in the network industry include Cisco, Nortel and Juniper; most large networks are built on equipment from these titans. But there are several smaller vendors that offer equipment well-suited to smaller companies' LANs and are designed for limited IT budgets.

When you're evaluating your options, beware of vendor lock-in — know just how interoperable the network devices are with other devices as well as network software, and determine if your organization is comfortable with a single-vendor solution. Take into consideration the equipment you may already have that you want to add to the network, the vendor's road map for future products and the vendor's relationship with standards bodies such as the IEEE.

Implementation and Support

There's no such thing as a plug-and-play LAN — so the more complex your network, the more networking expertise will be needed to design, install and support it. It's important to honestly appraise your IT staff's ability to deploy a network. Even though network devices are relatively easy to install — switches are plugged into the electrical socket, then Ethernet cables are plugged into the switches — planning the network requires a good deal of knowledge about network design and technologies. It might make sense to seek outside help in the form of a consultant, integrator or professional services organization (often available through your network gear vendors), especially for labor-intensive network design services and cable installation. Server NOSes and clients must be configured properly to access the network and to run network services. Then, the LAN must be maintained, including real-time alerts, regular performance reports, hardware and software upgrades and additional functionality as your company grows.

Support for network hardware and software comes in a variety of flavors. Most vendors offer basic support, but others sell various levels of expanded support. Again, the level of support you opt for is based entirely on how technically competent you believe your IT staff to be. Some support offerings provide online help only; others have staff available 24 hours a day. Considering what's at stake if your network storage goes down, it's wise to partner with a vendor that will always be available to help in an emergency.

4 Tools

To simplify a complex subject, we've included a set of tools that can help you understand the jargon used in networking, a breakdown of the vendors currently offering network products and a pair of lists that will help you evaluate whether your company is ready to build a LAN (Local Area Network), or if it could go without it for now.

10 Signs You Need a LAN

8 Benefits of Implementing a LAN

Glossary of Key Terms

Vendor Universe

10 Signs You Need a LAN

If your company has more than a few employees, if you want to encourage collaboration among co-workers and between your staff and your customers or if you want to move your business online, you need a LAN — or you soon will. There are very few modern businesses that can't benefit from networking. Here are 10 signs that it's time for you to make the leap:

1. **Employees need to access their data from remote locations.** With a LAN connected to the Internet, employees can work from home, a client's office or any other location with Internet access. When workers can connect with colleagues, partners, clients and customers no matter where they are, they can work for more efficiently and productively.

2. **You want to make company information more accessible via an intranet.** With a company intranet — a private network — different departments can disseminate their important information easily to all employees. For instance, the HR department can post updates to the benefits plans and employees can download forms. An intranet might also include job openings, employee policy changes, event calendars and shared scheduling applications. An intranet can be particularly helpful to a distributed work force who otherwise feels left out of the loop.

3. **You need to improve your data-protection measures.** Simply backing up data to disks doesn't sufficiently protect your company's valuable data. With a LAN, you can install a network storage device that will allow you to schedule regular backups of data and applications, will make your backups more secure and will increase the availability of your data.

4. **You need to connect separate offices in different locations.** If your company has more than one office location, you need a LAN to connect them. A secure connection between offices lets employees share databases and applications, and helps management keep everyone current with business practices and goals.

5. **You want to create effective business processes with partners.** A network allows you to establish secure and reliable online business process with partners, such as an ongoing order placed regularly with a supplier. Some large companies require their partners and customers to have secure networks in place before they'll do business with them.

6. **You want to make it easy for employees to work together**. Easy collaboration among co-workers and the people you do business with increases productivity and efficiency. With a LAN, employees can use emerging collaboration tools, such as interactive calendaring and unified communications.

7. **Employees want to conduct online meetings.** Co-workers can't always gather in the same conference room and conference calls can be difficult to follow. With an online meeting space, employees can quickly find out who's available to meet, share and access relevant data and give presentations that everyone can view from their own desks.

8. **You want to improve your company's customer service**. With a network, customer service reps can quickly

share information with each other and use a database of product information to deliver fast, informed service to customers. Also, with a network, you can add new customer service tools, such as a chat application, to your company's Web site.

9. You want to make IT more efficient. With a network, you can manage the servers and clients on your network from a single, centralized platform. For instance, you can streamline software updates by installing them just once on the server and pushing them out to clients, instead of installing them on each computer in the organization. A LAN also allows users to share network peripherals, such as printers and faxes, as well as the company's Internet connection.

10. Your company wants to increase revenue. When you launch a Web site, you make your business visible to potential new customers around the world. If you add e-commerce to the site, you can sell your products directly to the people who want them.

8 Benefits of Implementing a LAN

Having a network can become a competitive advantage when companies use it to increase employee productivity and open their business to new streams of revenue. Here's a list of the benefits a network brings; if three or four address pain points in your company, you're probably ready to deploy a network in your company.

1. **Centralized IT administration:** It's much easier and more efficient to manage the many computers that even a small company has from a single platform than it is to manage each of them individually. Also, IT administrators can remotely troubleshoot problems on computers across the network rather than doing it in person.

2. **Added IT security:** Most network devices, including routers, have built-in security features like firewalls, which make them a much safer way to get users online than a modem. Also, backups performed over the network add a dimension of data security, and servers that are in a locked room can't be stolen or otherwise accessed.

3. **Better performance:** Servers designed to support a network are usually optimized for better performance, which is particularly useful for Web servers and email servers. When optimized servers are used for file or database servers, they can increase application and data availability, ultimately leading to more productive employees.

4. **Centralized backups:** Data backups done over a network can be centrally managed and scheduled, which makes them more reliable (not to mention more likely to happen on a regular basis). They can also be saved to an off-site location. This means that your backups are secure and safe from any downtime or disasters at your office.

5. **Reduced operating costs:** A network lets co-workers share office equipment, like printers, faxes, and storage devices; for instance, this means you can buy just one or two shared printers for an entire office to use rather than individual printers for each employee who might need one. Similarly, an office can share high-speed Internet access.

6. **Better customer service:** With a network, customer service reps have easy access to all customer and product information at their fingertips. This lets them be more responsive and offer personalized services to each customer. When your reps are online, they can respond to customer queries by email, via Web-based forms, as well as through chat windows and phone calls.

7. **Universal access to business applications:** A network gives all users, whether they work in the main office, a remote office or from home, universal access to the same business applications and company information. When you build a network, you also open up the possibilities of deploying advanced communications applications, like VoIP or video conferencing.

8. **Real-time insight into the business:** Data, including sales figures, incoming orders and more, can be immediately accessed when it's stored on a LAN. This gives management insight into what's happening across the business when it happens, leading to more effective and intelligent decision making.

Glossary of Key Terms

10Base-T: The specification for the 10 Mbps Ethernet speed.

100Base-T: The specification for the 100 Mbps Ethernet speed.

10-Gigabit Ethernet (10 GbE): The fastest Ethernet speed.

802.x: The specification for Ethernet networks. Both 802.2 and 802.3 are used.

ACL (Access Control List): A list of security permissions for the resources on a network, including files and directories.

Access rights: Controls what a user can and cannot do with the network resource named in the access right.

Account: Each user on the network must have an account to access the network and its resources; the user's account defines what the user is allowed to do.

AppleTalk: The networking protocols used with Apple Macintosh computers.

Application Layer: The seventh and highest layer in the OSI networking model (see OSI network model) that handles the communication between applications across the network.

Backbone: A high-speed cable that is shared be different network segments; usually a higher speed than the network segments because it carries traffic from all the network segments.

Bandwidth: The amount of data that can travel across a network. Bandwidth is usually described in terms of speed, often megabits per second (Mbps).

Client: Refers to the PCs and laptops connected to the network.

Client/server: The prevalent networking model that provides a way to connect distributed programs; multiple clients share the services provided by an application on a single server. Most business and Internet applications are developed to use the client/server model — a Web browser is a client program that sends a request to view Web pages on a Web server located on a different network.

Data-Link Layer: The second layer of the OSI networking model (see OSI network model) that handles error-free connections between two devices over a physical connection.

Directory: A container for files in the tree-shaped structure of a disk's filesystem.

Domain: The name of a network (or address) on the Internet, such as www.focus.com.

DNS (Domain Name System): A naming system for computers on the Internet that translates hostnames, such as www.focus.com, into the IP address, such as 69.25.138.122, that networking devices use to find locations on the Internet.

DHCP (Dynamic Host Configuration Protocol): A communications protocol that lets network administrators centrally manage IP addresses in the network.

DSL (Digital Subscriber Line): Provides high-speed digital data communications over a telephone line. It is an adequate Internet connection for small businesses.

Ethernet: A common network standard that can carry network data over different types of media at different speeds; it is frequently used on LANs. Ethernet also refers to the slowest Ethernet speed, 10 Mbps.

Fast Ethernet: Refers to the second Ethernet speed, 100 Mbps.

FTP (File Transfer Protocol): An Internet protocol for copying files from one computer to another.

Firewall: A network device or application that protects the network from outside intruders, including hackers and their attacks.

Gateway: A network device that connects two networks together, such as an email gateway that sends email from one network to another.

Gigabit Ethernet: Refers to the third Ethernet speed, 1000 Mbps.

IEEE: The Institute of Electric and Electronics Engineering, the organization that defines computing standards.

IP (Internet Protocol): The protocol used to send data from one computer connected to the Internet to another. It is part of the TCP/IP protocol suite.

IPv4: The current version of IP, which is running out of new IP addresses.

IPv6: The next-generation version of IP that uses 128-bit IP addresses to create additional IP addresses.

IP address: The number — currently a 32-bit number — that identifies each computer or other device on the Internet. Each IP address includes the indentified of a particular network on the Internet and the identified of the specific device on that network.

Network administrator: The IT staff member responsible for the network. He or she has permission to access any device on the network, perform all network tasks, set policies and grant permissions to other users.

NIC (Network interface card): A computer circuit board that is installed in a computer to allow it to access the network; most modern laptops and PCs ship with NICs installed.

Network Layer: The third layer in the OSI networking model (see OSI network model) that defines different packet protocols, including IP.

Network protocol: A set of rules that enable data communications over a network to complete varies network transactions.

Network topology: A schematic drawing of the arrangement of the network, including all the nodes and connecting lines. Common network topologies include bus, ring and star.

Node: Each computer or device on a network that is a separate entity, such as the CEO's laptop or HR's workgroup printer.

NOS (Network Operating System): The operating system that runs on network servers, such as Microsoft Windows Server or Novell's SuSe Open Enterprise Server.

Network segment: A single part of a network that connects two or more computers together.

OSI (Open Sessions Interconnections) network model: A description for layered communications and network protocol design that has seven layers: the Application, Presentation, Session, Transport, Network, Data-Link and Physical Layers.

Packet: A unit of data that is sent from one network node to another network node, often between nodes on the Internet.

Physical Layer: The first layer of the OSI networking model (see OSI network model) that defines the specifications for the physical wiring of the network.

Presentation Layer: The sixth layer of the OSI networking model (see OSI network model) that ensures that the communications passing through are in the correct form for the recipient device.

Protocol: A set of rules that two or more computers or devices use when they communicate over a network.

Remote access: The ability to log in to and access resources on a network from a location other than the office, usually via the Internet.

RJ-45: The connector attached to Ethernet cables that allows cables to plug into the Ethernet port; similar to telephone cable connectors.

Router: A network device that directs network traffic from one network to another.

Session Layer: The third layer of the OSI networking model (see OSI network model) that manages the setting up and taking down of network connections.

Server: A computer on the network that provides a network service, such as email, printing, file server, etc., to the clients on the network.

SMTP (Simple Mail Transfer Protocol): The Internet standard used to send email between systems on the Internet.

Switch: A network device that moves traffic between two or more network segments.

TCP/IP (Transmission Control Protocol/Internet Protocol): A standard network protocol that defines a set of rules used to send data from one node on a network to another; used on the Internet and on many private networks.

Transport Layer: The fourth layer of the OSI networking model (see OSI network model) that coordinates the packet exchange between nodes on the network.

Twisted pair: A type of network cable that uses small-gauge wires twisted together inside a sheath to carry network signals; Ethernet cables are twisted pair and they come in unshielded (UTP) and shielded (STP) types.

VPN (Virtual Private Network): A secure, virtual, private network made via an Internet connection, generally to allow employees to log in to the corporate network from home or other remote location.

Network Equipment Vendor Universe

The following summarizes the vendors serving various areas of the networking market. While we have tried to be comprehensive, there may be smaller network equipment vendors that we have not included. This list is current as of March 2009.

Vendors are broken into several categories according to the types of networking products they offer. The last category of vendors provides solutions for vertical-specific industries. Be aware that vendors may appear in multiple categories.

Vendors Offering Network Cables

ConnectZone
StarTech.com

Vendors Offering Network Software

Alcatel-Lucent
ConSentry Networks
Extreme Networks
Juniper Networks
Microsoft
Novell
Vyatta

Vendors Offering Network Management Products

3Com
Alcatel-Lucent
Anue Systems
Avaya
Brocade
CA
Cisco
Citrix
Coyote Point Systems
Enterasys Networks
Extreme Networks
F5 Networks
Fluke Networks
Hewlett-Packard
Juniper Networks
NETGEAR
NetQoS
NetScout Systems
nMetrics
OPNET Technologies
Riverbed Technology
Splunk
WildPackets
Xirrus

Vendors Offering Routers

3Com
Brocade
Cisco
D-Link Systems
Enterasys
Extreme Networks
Juniper Networks
MRV Communications
NETGEAR
Nortel
SMC Networks
TP-Link
TRENDnet
Vyatta

Vendors Offering Network Security Products

3Com
Alcatel-Lucent
Cisco
Citrix
D-Link Systems
Enterasys
Extreme Networks
F5 Networks
Hewlett-Packard
Juniper Networks
NETGEAR
Nortel
Palo Alto Networks
Radware
TippingPoint Technologies
Vyatta

Vendors Offering Switches

3Com
Alcatel-Lucent
Apcon
Blade Network Technologies
Brocade
ConSentry Networks
Cisco
D-Link Systems
Datacom Systems
Enterasys
Extreme Networks
Gigamon Systems
Hewlett-Packard
Juniper Networks
MRV Communications
NETGEAR
Nortel
SMC Networks
TP-Link
TRENDnet

Vendors Offering Network Security Products

3Com
Alcatel-Lucent
Belkin
Cisco
D-Link Systems
Enterasys
Extreme Networks
Hawking Technology
Hewlett-Packard
Intel
Motorola
MRV Communications
NETGEAR
NexAira
Nortel
SMC Networks
TP-Link
TRENDnet
Xir

Vendors Serving Specific Vertical Industries

CA	Communications service providers, education, financial services and government
Cisco	Media and entertainment
Citrix	E-commerce, education, financial services, government, health care manufacturing, media and content, retail and telecommunications
ConSentry	Education, financial services, health care and manufacturing
D-Link Systems	Education and government
Enterasys	Education and health care
Extreme Networks	Carrier Ethernet, education, health care, hospitality and gaming
Juniper Networks	Health care, financial services, government, research, education and service providers
Hughes Networks Systems	Government and service providers
NetScout Systems	Banking, consumer retail, energy, government, health care, insurance, investment services, life sciences, manufacturing, petroleum and natural gas and service providers
Nortel	Education, financial services, government, health care, hospitality, service providers, cable operators and wireless operators
Radware	E-commerce, education, financial services, government and insurance

About **FOCUS**

Our Mission

Our mission is to support business professionals' critical purchase decisions by creating and distributing the highest quality, most relevant purchase research and tool sets.

Our Approach

To ensure maximum insight and relevancy, Focus has designed a four factor approach to buyer-centric research. All research at Focus begins with defining the buyer factor. Categorized in our research as Buyer Types, the buyer factor identifies the buyer needs and preferences in a market that make a difference in selecting the right product and vendor. Buyer Types are studied and developed based on Focus' interaction with thousands of buyers across a category. The buyer factor in turn shapes Focus recommendations on how buyers approach three other critical factors: 1) product requirements, 2) cost considerations and 3) vendor relationships.

Buyer Feedback

In addition to speaking with industry experts and other participants, a critical priority is to integrate feedback from experienced buyers. We speak with thousands of buyers each month and conduct our formal buyer surveys throughout the year.

For more information on our research approach, please visit Focus.