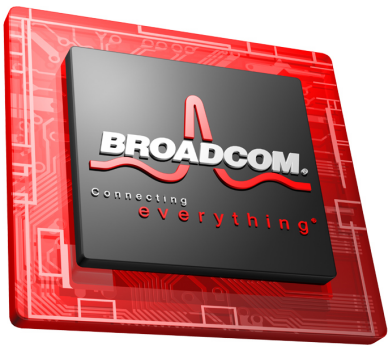
Architecting Next-Generation Networks

Don Jones



Produced Exclusivelv for Broadcom bv

realtimepublishers.com®

Chapter 1: Introduction

It's a term you're starting to hear more and more—*next-generation networks*. Depending on how long you've been in the industry, you might have heard it in the past, too: The move from coaxial 10Base-T and 2Base-T networks to modern 10Base-T twisted-pair networks (as well as Token Ring networks) was a major leap forward. As corporate networks began to roll out larger and larger Ethernet LANs, user productivity increased. Users had easier access to files, printers, and other resources; networks were easier to manage and troubleshoot; and connections, based on easier-to-wire CAT3 and CAT5 cabling, were more reliable. Another generation of networks was created when Ethernet switches hit the market, making networks faster and more efficient.

What came before, however, is no match for what's ahead. Forget about simple speed increases, lower latency, and a new type of infrastructure device. This time, *next-generation network* means a tenfold or better increase in network throughput. It also means an entirely new range of connectivity options, including wireless "disconnected connectivity." Next generation means intelligent devices capable of improving network performance and reliability. Finally, it means security built right into the infrastructure, for the first time ever. It's an exciting time to be a networking professional—provided you're ready.

Why Your Network Isn't Good Enough

Simply put, today's networks are barely sufficient for what companies are asking of them, and the networks are completely inadequate for the demands of the future. Think about it—many companies are running 100Base-T networks at best, perhaps with 11Mbps wireless connectivity for some users. These are more or less the same networks they've been running for half a decade or more, and yet the number of additional demands that have been placed on the network since then is truly staggering.

To appreciate the improvements provided by the next generation of networks, you need a firm grasp of how current networks and technologies developed to the present. In the following sections, we'll explore the Internet, voice and video technologies, business-to-business (B2B) e-commerce, handheld devices, and more. This background information will provide evidence of the need for the latest technologies and how they will address current networking concerns. We will then build on this foundation in the rest of the book:

- Chapter 2—The important elements of next-generation networks—specifically Gigabit Ethernet (GbE)
- Chapter 3—Strategies for wireless deployment and security
- Chapter 4—The importance of switching intelligence in the infrastructure
- Chapter 5—Server migration and optimization, paying special attention to return on investment (ROI)
- Chapter 6—How to secure your next-generation network

The Changes Add Up

Five years ago, the Internet was still just beginning to take off as a major vehicle for commercial communications and interaction. Nobody had a camera connected to a computer, very few people had anything like a handheld personal digital assistant (PDA), cellular phones did not have digital cameras and built-in General Packet Radio Service (GPRS) transmitters, and many companies still had users who didn't have email. In 5 short years, everything has changed.

The Internet

Today's users double the amount of data they work with every 18 months. Much of that data comes from the Internet. To date, companies have dealt primarily with maximizing the efficiency of their relatively low-bandwidth wide area network (WAN) connections; with the average company connecting to the Internet via a T1 line—even an old 10Base-T local area network (LAN) offers almost seven times the speed of a WAN connection. Companies have addressed the WAN bottleneck primarily by using both firewalls and proxy servers (see Figure 1.1) and by increasing pipe capacity through T3, OC3, OC12 and higher-speed connections.

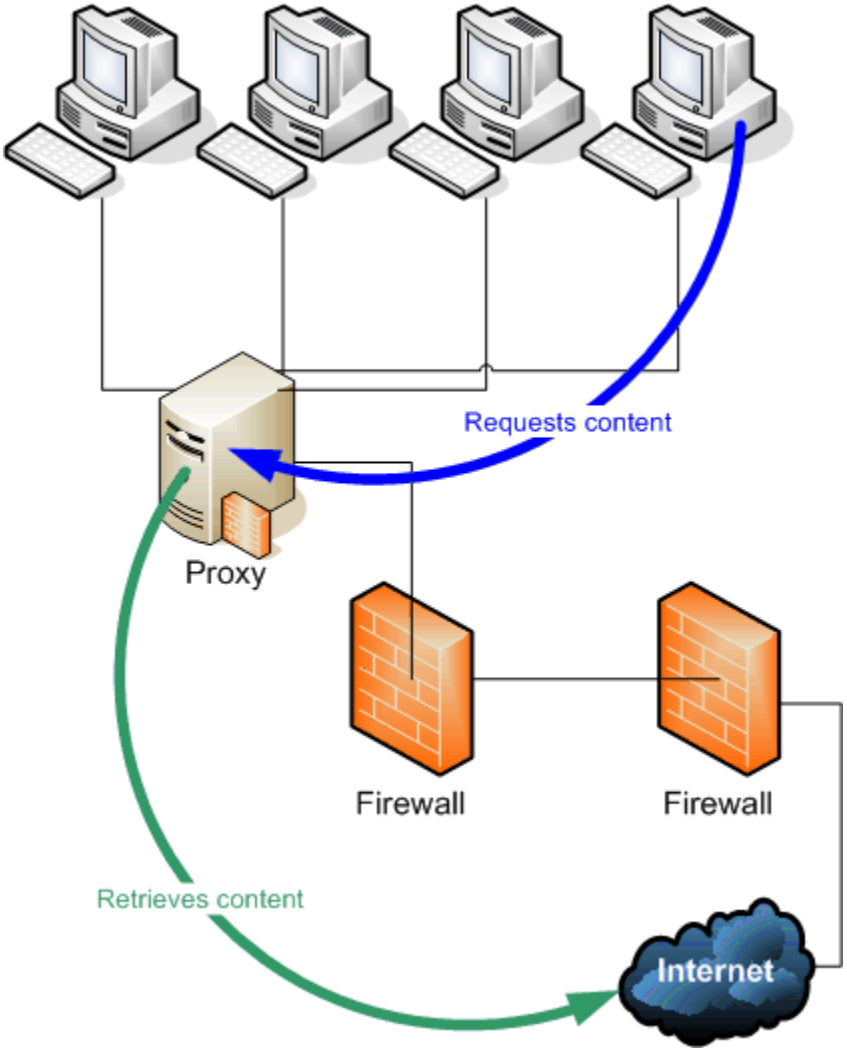


Figure 1.1: Maximizing Internet efficiency with proxies and firewalls.

Proxy servers increase efficiency by aggregating multiple client connections. The proxy server retrieves content from the Internet, then saves it for future internal requests rather than retrieving the same content over and over. Some proxies and firewalls can improve efficiency by eliminating wasteful traffic, such as Web surfing to game sites and other non work-related sites.

This focus on the WAN pipe, however, has left the LAN, which is where bottlenecks are starting to appear, largely ignored. Users are working with a *lot* of data, and much of that data now originates on the LAN in the form of enormous data warehouses, databases, files, and more. Networks are becoming hard-pressed to transport all of that data.

Think about the average size of a Word, Excel, or PowerPoint document that contains pictures and graphics. File sizes continue to increase in most applications from version to version as users take advantage of new features to create more creative documents. Even the default image file from a 5 mega pixel digital camera is more than 3MB. The network—which isn't gaining speed as quickly as the files gain size—still has to move all the bits from the file server to client computers and back again.

Productivity is also affecting the network. Despite recent corporate restructuring and downsizing, most companies in the United States increased their overall output. How? Everyone is doing more with less. Thus, each worker has become more productive, and they didn't get to be more productive by dealing with *less* data; the corporate network bears the brunt of this increased productivity. Unfortunately, overburdened networks are easy to ignore. Users may complain that things are slow in the mornings, but they gradually begin to accept the status quo and the network remains a hidden efficiency problem.

Even worse for current network bandwidth is the trend towards collaborative computing. Products, such as Microsoft SharePoint Portal Server, which are designed to allow real-time collaborative computing between network users, cause not only an increased load on the network infrastructure but also highlight any latency problems, which become immediately noticeable and annoying to users.

Network bandwidth hogs can be many and varied including:

- Storage and backups—larger drives mean more to back up
- Educational training and videoconferencing—video being accessed by a large number of users
- Collaborative applications
- CRM tools
- Help desk software
- Richer content (voice, video, mp3)

Now consider the massive increase in data throughput that companies will see in the next 18 months to 3 years. Networks simply must become faster, more efficient, and much more intelligent in order to keep up. Raw speed is part of the answer, but more efficient and intelligent use of that speed is also an important component. Next-generation networks will provide this speed and intelligence.

Such networks are not a distant phenomenon; they are a current reality. For example, if you are building a network starting with a clean slate, you can use GbE to ensure that your network infrastructure is ready to benefit from emerging technologies. For existing networks, the migration to GbE means reduced wire time, less buffer congestion, and relieved flow control mechanisms—all of which add up to a better user experience and a less harried IT staff.

📖 We'll explore GbE in detail in Chapter 2.

Voice and Video

As companies seek to reduce travel expenses and improve employee productivity, network-based voice and videoconferencing have become more popular. Many companies are saving tens of thousands of dollars a year by piggybacking voice communications onto their data networks. Voice over IP (VoIP) is a popular suite of technologies that provides high-quality voice transmission over IP networks.

Unfortunately, voice and video, in particular, are harsh on the corporate network. Few networks are engineered to carry a normal share of data as well as decent streaming video. Network engineers and videoconferencing designers have been forced to make a number of concessions and compromises to make videoconferencing feasible. One primary technology is *multicasting*, enabling a conferencing server to send a single transmission for a video signal. Clients subscribe to the multicast's IP address and pick up the traffic sent to that address off the network. This technique is much more efficient than *unicasting*, in which the server must transmit an individual video feed to each client. With multicasting, multiple clients can receive the same transmission, conserving bandwidth. Even multicasting isn't always enough to make videoconferencing possible, however; some networks are so overburdened that the video traffic must be limited to a portion of the network. Figure 1.2 shows how routers can be programmed with *multicast boundaries*, creating a *multicast domain* that contains the videoconference traffic. Outside the multicast domain, users cannot subscribe to the feed.

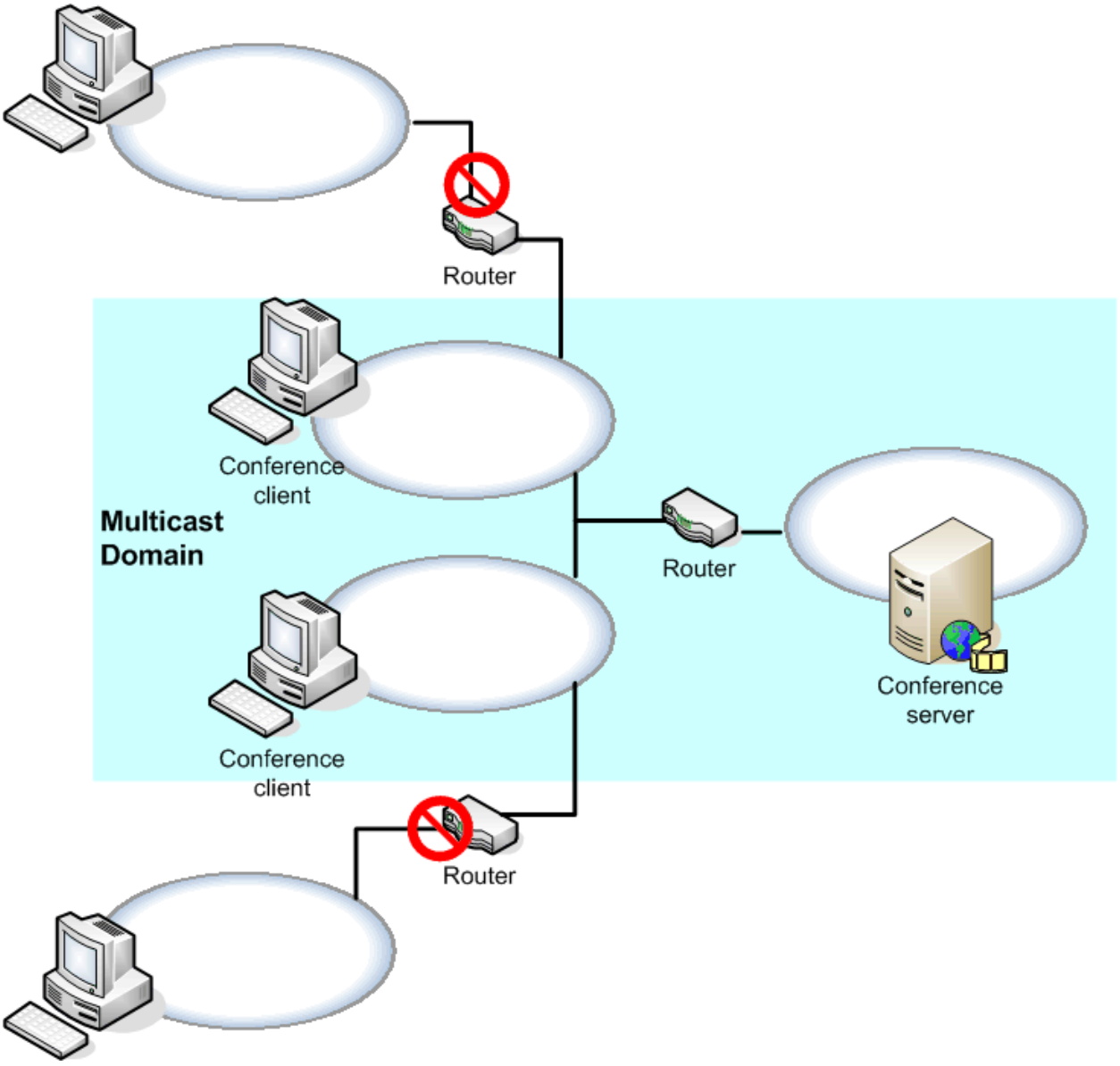


Figure 1.2: Creating a multicast domain with router multicast boundaries.

In the world of networking, the inability of a network to handle its traffic load—particularly when the applications generating that traffic provide monetary savings and increases in productivity to the organization—is an unforgivable offense. Multicasting is an excellent technology that was designed to increase the efficiency of a network, but networks that can't even carry a share of multicast traffic across the entire corporation are clearly not engineered to serve the business' best interests. Next-generation networks need to offer the ability to extend cost-saving, productivity-boosting technologies to every corner of the corporate LAN. They will do so by providing additional raw bandwidth, more efficient routing of traffic, and better management of specialized traffic.

B2B E-Commerce

Networks built 5 years ago carried almost no B2B traffic. Such systems basically didn't exist; the closest systems to displaying B2B characteristics were the value-added networks (VANs) provided for electronic document interchange (EDI) customers—sort of a private equivalent of the Internet.

Today, there are few companies that *don't* run some form of B2B application on their networks, even if it is as simple as ordering office supplies from a Web site. Many companies rely heavily on B2B communications, placing an even greater burden on the corporate network. There is no denying the ways that B2B improves efficiency—inventory systems can place orders with vendors automatically, and entire classes of retailers now exist that don't even carry an inventory; they simply take orders from customers, pass those orders on to distributors through B2B systems, and process payments on both sides. Many companies utilize e-procurement systems for internal procurement of everything from office supplies to contractors.

The infrastructure required to support these B2B efforts is significant. Figure 1.3 shows a typical B2B infrastructure, including multiple firewalls, application servers, B2B processing platforms, database servers, internal and external clients, Web servers, and more.

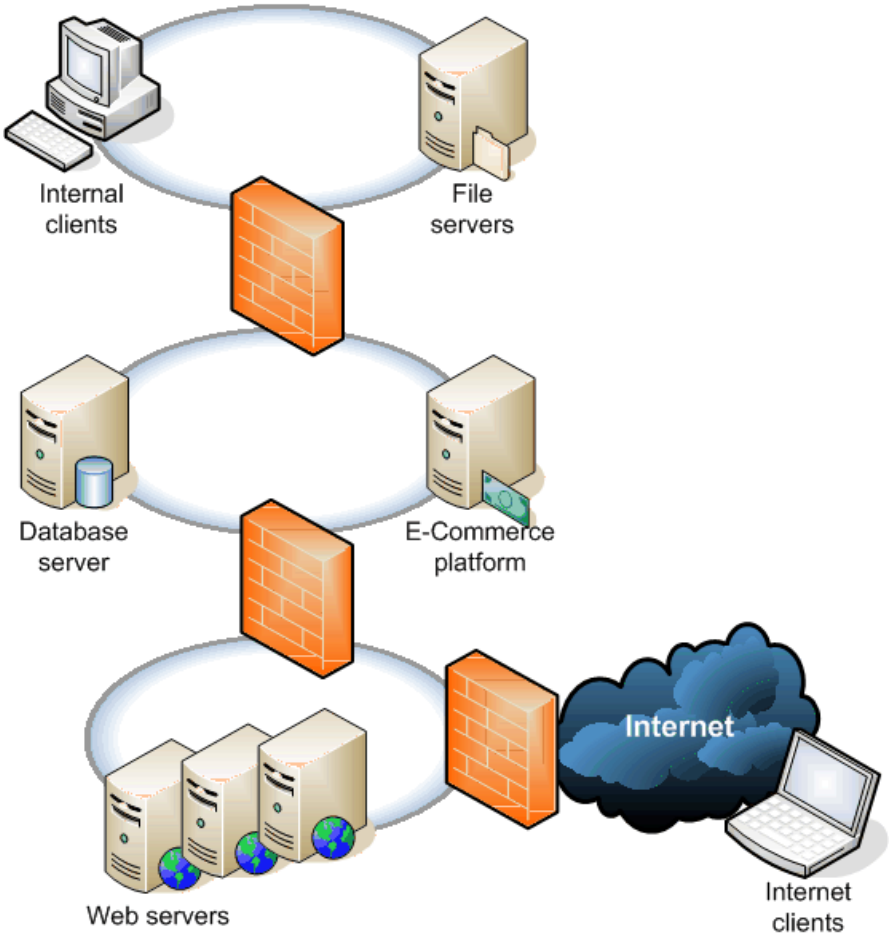


Figure 1.3: A typical B2B infrastructure.

What effect does this burden have on the network? Imagine that the population of the United States increased by a factor of ten over 2 or 3 years—how would the postal service feel the effect of this increase? Like a Los Angeles freeway at rush hour—which is pretty much how many corporate networks look these days. In addition, B2B functions aren't limited to server-to-server or external B2B connections. Internal clients will be using automated ordering, data entry, catalog management, and all sorts of high-bandwidth applications that deliver results to external clients or vendors but generate a great deal of activity between LAN clients and servers.

Next-generation networks need additional speed, intelligence, and security to segment and manage the traffic for these important B2B functions and to provide them with additional bandwidth.

More and More Users

The rapid pace of business growth also has an effect on networks. Obviously, networks must grow to support the business, but rapid change often means unplanned growth that lacks any cohesive, logical design. For example, consider the simple network that Figure 1.4 shows, which looks a lot like most networks that are just starting out. The network was over-engineered for the number of users it needed to support, providing plenty of room for growth—notice the router used to connect two segments, each containing a small number of users—or so it probably seemed at the time.

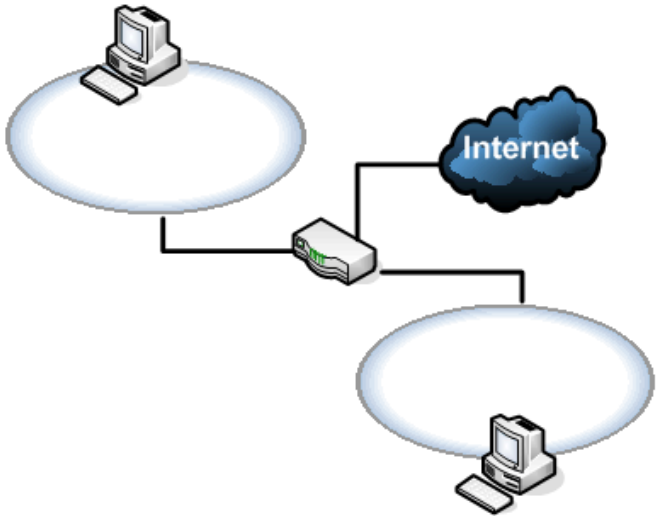


Figure 1.4: A typical network in the beginning.

As the business grows, users are added until the network can't support any more. Then the emergency growth patterns begin, with new segments added here and there, segments cascaded from one to the other, and so forth. Before long, the network is out of control—and the business is so busy growing that nobody has the time to redesign it. Figure 1.5 shows how a network's growth can be like that of a cancer cell—uncontrolled and ultimately detrimental to the host. Routers connect segments in a complex chain rather than through any logical topology. Segments are now more crowded with users and other devices, reflecting the network's rapid growth. Segments containing servers are at least dedicated to that task, but are haphazardly spread across the architecture rather than being centrally accessible to all segments containing client computers. In short, it is a mess.

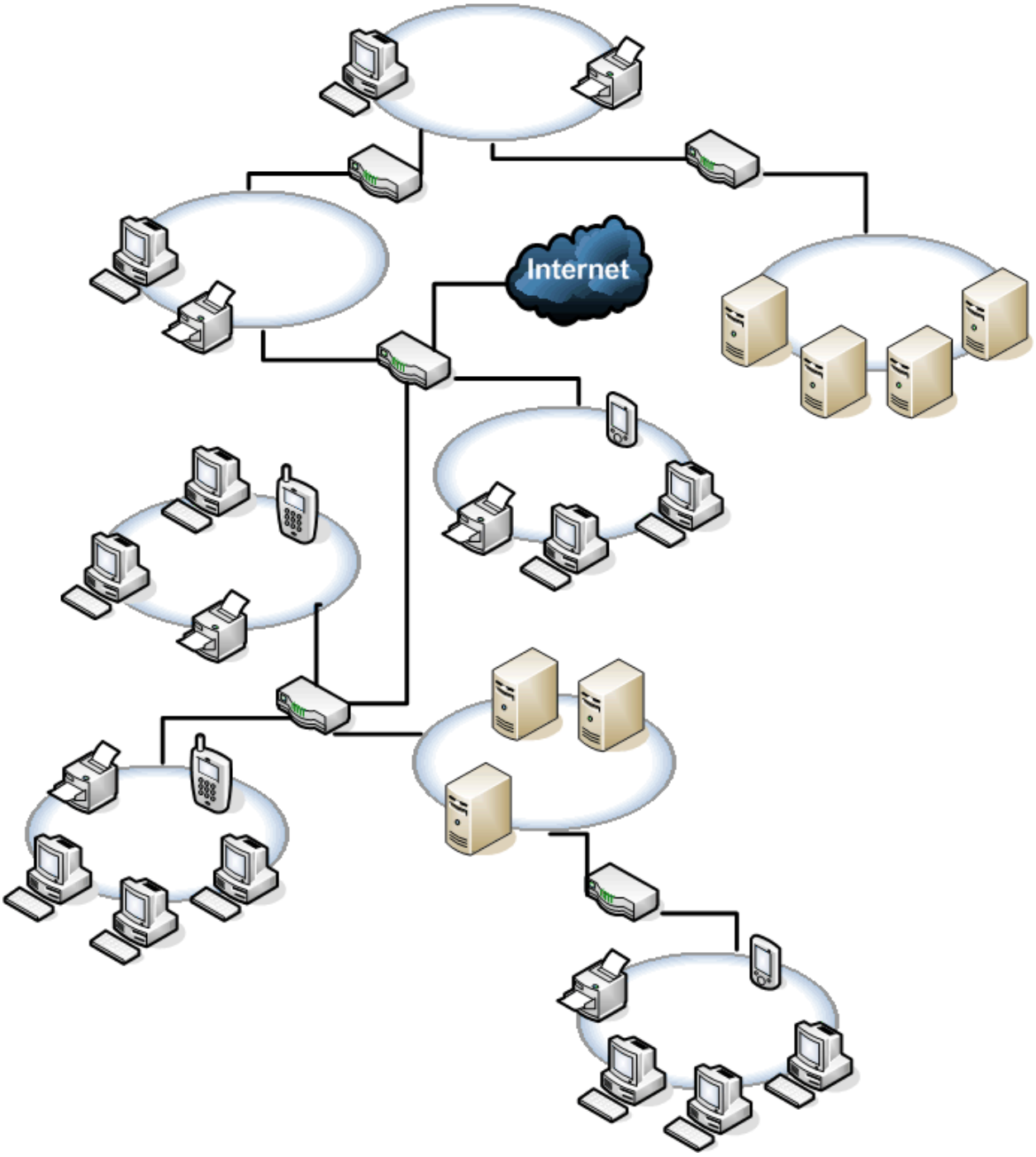


Figure 1.5: Uncontrolled growth is common in today's corporate networks.

Although this type of network "design" might not create huge performance issues, it definitely creates management issues. Problems, when they occur, are more difficult to troubleshoot. Managing change and finding bottlenecks is next to impossible. In short, the network works fine, but it is harder and harder to rein in. Next-generation networks must allow for easily controlled growth, making it so easy to expand the network in any direction that administrators don't need to think about it. In addition, such networks must ensure that manageability and security remain tight.

A Device in Every Pocket

We're used to thinking about networks in terms of users: How many users per segment? How many users on the LAN? How many videoconferencing users? But today's users are acquiring a staggering array of wired and wireless devices, meaning each user can easily represent three or four actual devices, as Figure 1.6 illustrates.

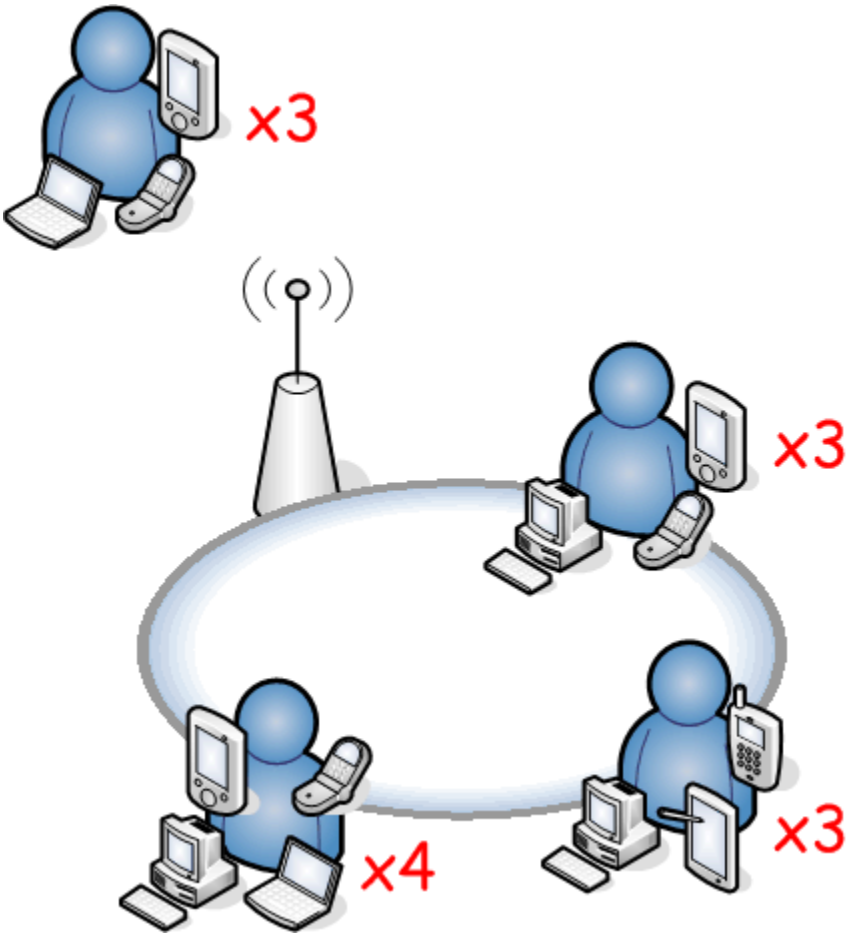


Figure 1.6: Users are beginning to represent multiple devices apiece.

Each device requires bandwidth, has security implications, and has network addresses. Multiply the number of users in your environment by even a conservative number like 1.5 devices, and you'll see that it is no wonder that networks are beginning to show a little strain. Next-generation networks must provide the raw bandwidth for these additional devices. They also need to support open protocols for management and security, allowing this vast range of devices to participate in the network in a secure, controllable fashion.

The Problems Pile On

All of these factors—the Internet, increased data processing, new voice and video services, B2B e-commerce, rapid growth, and a diversity of devices—tend to result in three problem areas: efficiency, management, and security.

Network Efficiency

Network engineers often speak of network utilization in percentages. "Our network runs at 70 percent utilization." What many don't realize, and even more don't discuss, is that networks can't achieve 100 percent efficiency. Ethernet networks, in particular, become less efficient the more traffic they carry, primarily as a result of the shared-medium, collision-detection nature of Ethernet.

To set up our discussion in later chapters, we'll quickly review switches to ensure a baseline vocabulary. Switches are the primary methodology used to improve network efficiency. They create an individual physical segment with each switch port while allowing IP addressing to remain the same—in effect creating a virtual subnet that spans many physical segments. As Figure 1.7 illustrates, switches can permit multiple simultaneous conversations because they separate the actual traffic.

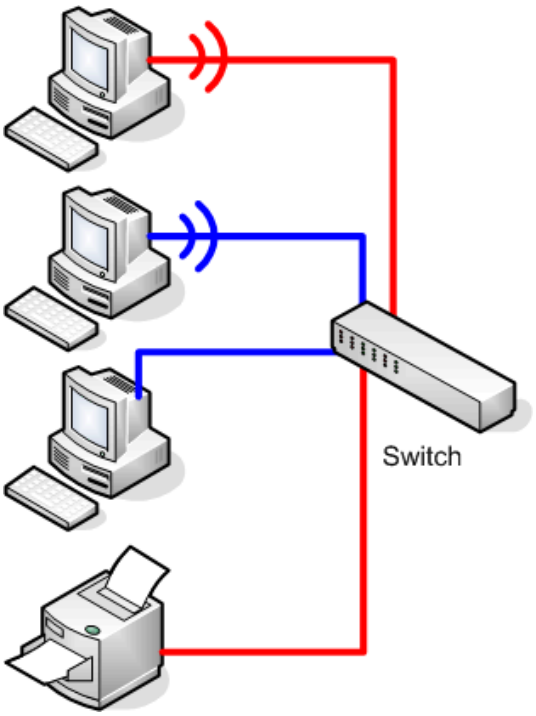


Figure 1.7: Switches make networks more efficient.

However, even switches have their limits. Switches can become saturated, at which point they simply can't carry any more traffic. Bargain-basement switches are the most likely to become saturated—even before they are carrying all the traffic that they should be able to handle—creating an instant bottleneck in your network.

Next-generation networks will help solve this problem by providing faster raw bandwidth, which will require a more robust switching fabric. If computers can transmit the information they have and then get off the line, another computer will be able to transmit much sooner. Next-generation switches will operate at higher speeds and will be able to handle the full load of traffic that the network can generate.

📖 We'll discuss these concepts, including switching fabric, in detail in Chapter 4.

Management and Design

As networks have become more complex to suit business needs, they have also become more difficult to manage. The sheer variety of devices—routers, switches, hubs, gateways, firewalls, proxies, servers, desktop and notebook computers, and other network-attached devices (such as printers)—has, in many cases, become a management nightmare. Pile on the complexity of application-specific management—managing VoIP, videoconferencing protocols and gateways, and so forth—and it is a wonder that administrators don't simply quit in frustration.

The next generation of networks needs to offer more intelligence and self-management capabilities. Switches must be able to talk to one another more effectively, allowing groups of devices to be managed as a single unit. Devices need to take more responsibility for handling today's special-purpose traffic, such as VoIP, videoconferencing, and next-generation applications including TCP/IP Offload Engine (TOE), Internet Small Computer System Interface (iSCSI), and Remote Direct Memory Access (RDMA).

📖 We'll discuss each of these emerging technologies in detail in Chapter 2.

The next generation of networks must also build on the intelligence in today's networks—particularly in regard to tolerating rapid growth. Networks must readily adapt to changing business conditions without requiring complex redesigns. For next-generation network topologies to succeed, there will need to be even more intelligence and performance built-in to the switches that control the flow of traffic on the network. The combination of better software combined with more advanced hardware is the key to making these critical network infrastructure components a success.

Security

A little more than 2 years ago, network security was something a few industry gurus preached, but nobody seriously practiced. Security was an add-on, something you implemented if you had some free time. And who has ever had free time? Today, security is an overriding concern in every field of information technology (IT) and communications. It is no longer sufficient to add security to a network by adding a monitoring tool or antivirus software—security has to be built-in starting at the physical network level.

Today's networks offer only a modicum of built-in security. For example, on wireless networks, the Wired Equivalent Privacy (WEP) standard provides little more than a veneer of security due to the ease with which the wireless network traffic can be probed and the availability of tools to crack the simplified encryption scheme used. In addition, wired networks are limited to transport-level encryption protocols such as IP Security (IPSec) to provide security. Practically no physical security exists, making it easy for intruders to simply plug-in to a spare LAN jack anywhere in an office to begin sniffing traffic from the network. Even when the network hardware supports the ability to route traffic only to an approved list of MAC addresses (thereby preventing a random LAN jack from allowing access to your entire network enterprise) few network administrators take the steps necessary to implement this degree of security.

Next-generation networks will include security in every aspect of their design. Already, network adapters with built-in IPSec capabilities are enabling all-encrypted networks that are transparent to the client and server operating system (OS). These adapters use high-speed onboard processors to reduce or eliminate additional overhead on the computer's CPU. Support for the 802.1x protocol is becoming available, requiring network devices to authenticate themselves before they're even allowed to pass other traffic—effectively stopping the plug-in attacker. In addition, support for new security standards that provide powerful authentication and data encryption functionality—such as Wi-Fi Protected Access™ (WPA) and Advanced Encryption Standard (AES)—are being built-in to next-generation wireless devices.

The Evolving Network

The next generation of networks promises, when properly designed and deployed, to solve most of today's problems, as well as, perhaps for the first time ever, look ahead to bypass future networking problems. Network engineers are thinking more about the future applications of networks and designing networks that support open protocols and standards to provide the best possible compatibility with technologies that don't yet exist. As Figure 1.8 shows, the next generation of networks will provide seamless connectivity for a range of devices, both wired and wireless, with built-in security, a diverse range of connection speeds, and more.

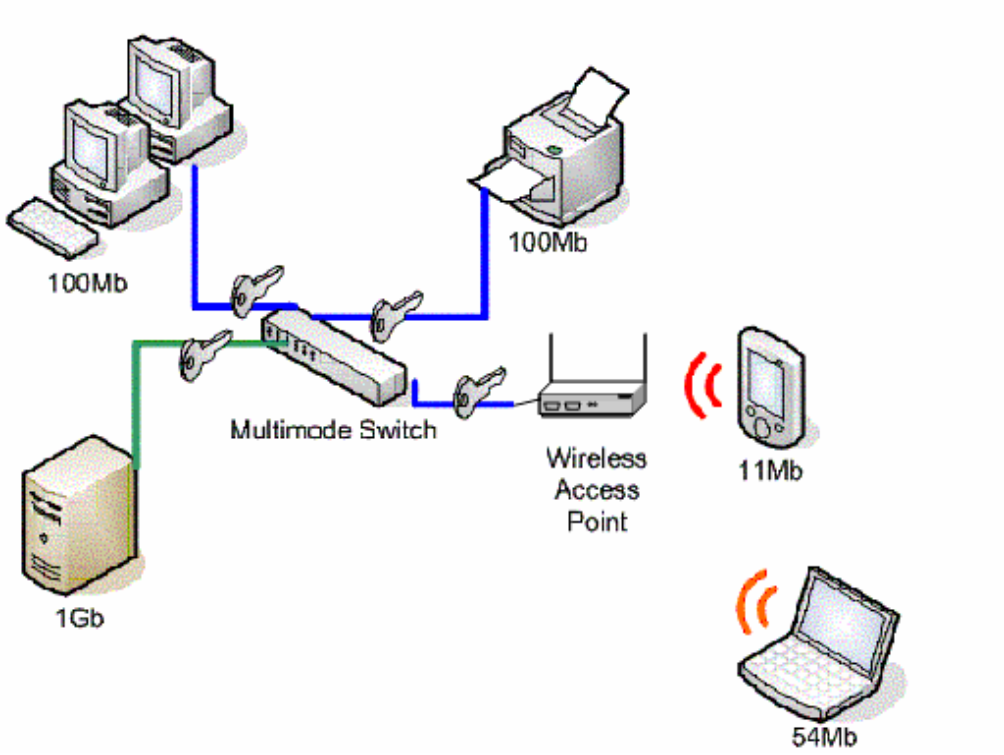


Figure 1.8: Next-generation networks focus on easy connectivity, security, and open standards and protocols.

Bigger, Better, Faster, More

Next-generation networks will provide better mid-range connectivity. Rather than relying on expensive, complex Synchronous Optical Network (SONET) connections—a form of high-speed connectivity generally used for WAN connectivity that provides speeds in excess of 2.8Gbps—metropolitan area networks (MANs) will be able to rely on massive 10GbE connections. As Figure 1.9 shows, these MANs will allow end-to-end Ethernet connectivity, providing better security (because the traffic won't have to pass thorough protocol gateways), design, and bandwidth. In addition, an Ethernet MAN provides the benefit of using only a single technology, Ethernet, rather than multiple technologies and the equipment necessary to bridge between many different protocols at every location (that is, you are not doing expensive protocol conversion; you are connecting an Ethernet LAN to an Ethernet LAN rather than converting to Frame Relay or ATM then back to Ethernet).

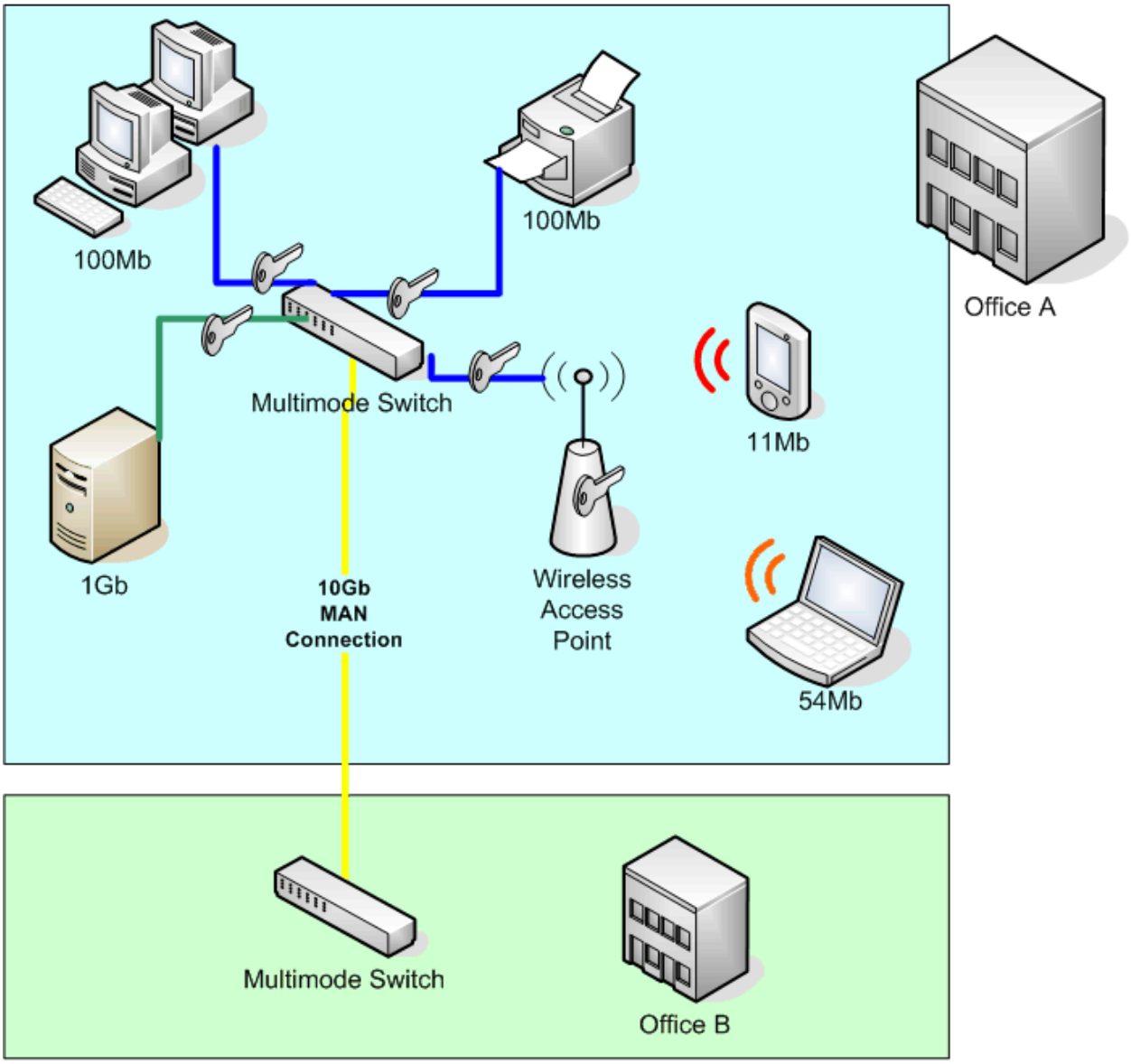


Figure 1.9: 10GbE provides an exciting new opportunity for MANs.

Internal server I/O has always been measured in mega*bytes* per second, while network I/O has always been measured in mega*bits* per second. Hard disk I/O has continued to grow, however, GbE is the first major jump in network performance in recent memory. Thus, while GbE is now capable of reducing the performance bottleneck on servers (especially when multiple NICs are being aggregated), the introduction of 10GbE will take us to the point at which the bottleneck between server and network begins to disappear. GbE clients will also see significant latency improvements as they will be able to take full advantage of the bandwidth and reduced latency that GbE promises. Hence, the real promise of next-generation network is to remove the network as a limitation to business.

> 🕮 Read more about 10GbE and its applications at http://searchstorage.techtarget.com/tip/1,289483,sid5_gci870890,00.html, as well as in Chapter 2 and Chapter 4.

Open Standards, Open Protocols

Past networking technologies have often relied on proprietary or complex protocols, such as SONET, Integrated Services Digital Network (ISDN), and others. As an open standard, Ethernet and wireless fidelity (Wi-Fi) offer a broader range of support and, thanks to the competitive marketplace for such devices, lower prices. Because next-generation networks will support open standards for security, traffic management, and device management, you will be able to easily mix and match devices to achieve exactly the type of network your company requires.

Designed for Mobility and Connectivity

The remaining limitation of the network is the wire—and that limitation will be short lived. Wireless technologies, such as 802.11b Wi-Fi, have already had a major impact, enabling "disconnected connectivity" everywhere from the office conference room to the neighborhood coffee shop. The next generation of that technology—802.11g Wi-Fi—is quickly becoming the new mainstream wireless LAN standard. Even advances in cellular technologies, such as 1X and 3G, promise ubiquitous wireless connectivity.

> 🕮 Read more about 802.11g at http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci783003,00.html, as well as in Chapter 3.

Now, full-size desktop and notebook computers are among the minority in the world of connected devices. Cellular phones, wireless PDAs, tablet PCs, and convergence devices such as the popular BlackBerry™ personal communicator all rely on cellular, GPRS, and Wi-Fi connections to access the Internet, corporate networks, and email—either through direct connection to the corporate net or VPN connections that use the Internet to reach back to the home office.

Even wired networks are seeing an enormous amount of growth in device diversity. Not that long ago, the network contained servers, client computers, and printers. Today, even the mailroom fax machine and copier are connected, allowing users to utilize these devices right from their desktops. Webcams allow parents to peek in on daycare centers while at work. Even the office soda machine may be Internet-connected, allowing 30 workers to check the available selections over the Web and to bill purchases to their company accounts.

Wired networks will also become a medium for storage area networks (SANs). Rather than using expensive, dedicated fiber-based connections, the iSCSI standard allows directly connected storage devices to be accessed by servers over 1GbE, 10GbE, and 100GbE connections. Microsoft's iSCSI implementation for Windows 2000 (Win2K), Windows Server 2003, and Windows XP Professional allows iSCSI use on any form of standard Ethernet, not just GbE and faster technologies. The LAN now provides an infrastructure for building out vast, fault-tolerant SANs at a lower cost than many fiber-based solutions, using reliable, well-understood Ethernet technologies.

> 🕮 Read more about iSCSI at http://whatis.techtarget.com/definition/0,,sid9_gci750136,00.html and in Chapter 2.

Next-generation networks will provide appropriate connectivity options for all of these devices—from slower 100Base-T wired connections to the fastest new Ethernet connections—as well as seamless roaming between wireless LAN and wireless WAN connections.

Embedded Security

Next-generation networks build security into every layer. 802.1x support, which includes embedded Extensible Authentication Protocol (EAP) capabilities, authenticates devices at the LAN port, disallowing unknown devices and locking down the physical network. Run wires—or wireless signals—anywhere you like; only authorized users will be able to attach. These networks will also include embedded IPSec capabilities, transparently encrypting traffic and preventing even authorized connections from eavesdropping on the network's traffic. Security won't be something you add to these networks, it will be something that is built-in from the very start, providing, for the first time in the history of networks, a truly integrated, secure infrastructure on which to build business applications and services. A highly secure OS will finally become a less important consideration as the underlying infrastructure begins to take responsibility for security.

> 🕮 Read more about 802.1x at http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci787174,00.html as well as in Chapter 6.

Next-Generation Networking

What are the technologies that will deliver on all of these wonderful new promises? Surprisingly, nothing new. Instead, the next generation of networking technologies builds upon the solid, reliable foundation of technologies that you've been using for years. Starting with this foundation enables lower upgrade costs, easier architecture design, and easier integration with your existing infrastructure—meaning you can "ease into" the next generation of networks without throwing away all of today's investment.

GbE

Described in the Institute of Electrical and Electronics Engineers (IEEE) 802.3ab standard, GbE is available now. Also named 1000Base-T, this new networking technology is ten times faster than 100Base-T Ethernet and backward-compatible with 10Base-T and 100Base-T networks. Also available, although still fairly expensive, is 10GbE, as specified in the IEEE 802.3ae standard. Currently designed primarily for trunking (between offices, for example) applications, 10GbE switches and other devices are on the market, allowing companies to create end-to-end Ethernet networks at lower acquisition and support costs than previous technologies permitted.

Wireless

Wireless access points (WAPs) now support a variety of protocols. In addition to bridging to 10Base-T, 100Base-T, and 1000Base-T wired networks, WAPs support wireless clients using 11Mbps 802.11b, 54Mbps 802.11g, and even 54Mbps 802.11a. 802.11a is currently being used primarily in areas of high user density, as it provides lower range than 802.11b and 802.11g. 802.11a operates in a higher frequency band (5GHz) than 802.11b/g (which operates at 2.4GHz), making the two sets of standards inherently incompatible.

> 🕮 Read more about the 802.11 family of wireless protocols at http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci341007,00.html as well as in Chapter 3.

> ✎ European networks are more likely to feature 5GHz-based HiperLAN technology, which is similar to the 802.11x family of protocols. A newer version, HiperLAN/2, offers as fast as 54Mbps operation in the same frequency.

Switches

Switches supporting 1000Base-T, 100Base-T, and 10Base-T connections are widely available, and switches offering 10GbE connections for office-to-office connections are also entering the market. Most of these devices are fully compatible with slower network devices, allowing you to deploy the central infrastructure of a faster network and slowly migrate individual devices—such as clients, servers, and other connection devices—as feasible or necessary within your organization. Switches have finally killed the hub—few companies are offering new Ethernet hubs, recognizing that a fully-switched architecture is a more efficient and practical way to build the next generation of networks.

Servers

Servers are already shipping with dual 1000Base-T network adapters integrated into their motherboards, and a variety of server-quality GbE adapter cards are available to upgrade older equipment. As you begin to purchase new computers, look for machines that offer a built-in or bundled GbE network adapter. Many hardware vendors include GbE NICs as standard in their business computing lines; if it isn't standard, you'll likely pay as little as $40 for the upgrade with a new computer (but you'll pay three or four times that amount to upgrade the computer later). Because of it's complete backward-compatibility with existing Ethernet standards (such as 100Base-T), trickling GbE into your environment is an affordable, slow-paced way to build the next generation of networks without a complete redesign of what you've got and without the need to throw away existing equipment. Upgrading existing server hardware to GbE when you have the box open for another upgrade, such as disk or memory, gives you a very inexpensive way to move your servers to GbE, because the cost is in the downtime, not the upgraded NIC.

Security

802.1x and IPSec are the latest rage in network security, and you'll find them available in higher-end network adapters and devices, such as wired switches and WAPs. IPSec is available in hardware network adapters for most major OSs, allowing you to completely offload the otherwise considerable burden of encrypting large quantities of network data onto a dedicated hardware processor, making network security completely transparent and easier to manage. Newer versions of the Windows OS include an 802.1x client, allowing those computers to participate in 802.1x-secured networks. WPA and AES are part of the upcoming IEEE wireless LAN security standard 802.11i, which will provide powerful wireless LAN security. Some vendors offer these technologies today: Microsoft offers support for WPA on a select subset of the available wireless hardware in a OS upgrade for Windows XP.

Getting Ready

The building blocks of the next-generation networks are available and prices are falling rapidly. You'll need to start planning to introduce them into your environment, but before you do, what steps should you take? What can you do today to prepare yourself, your peers and employees, and your equipment for the new network?

Education

Take the time to learn all you can about these new networking protocols—how they differ from past versions and how they'll affect your environment. Focus on the leading edge: 1GbE and 10GbE, 802.1x security, iSCSI SANs, and 802.11a/g wireless connections. Vendor white papers, magazine articles, and an increasing number of books are available to explain these new technologies and give suggestions for how to approach them in your environment.

Future-Proofing Your Network

How can you get your network ready to be a next-generation network? The following list highlights tips—we'll explore these topics in more detail throughout the rest of this book:

- Consider the next-generation network in all new hardware purchases. Provision new computers with 1GbE, and buy new switches that support 1GbE and potentially even 10GbE for MAN connections.
- Make all of your new wired NIC purchases 1000Base-T adapters. The backward-compatibility with your existing Ethernet technology makes the eventual transition to GbE completely transparent to users.
- Migrate server backbones to 1000Base-T infrastructure devices (switches, routers, and so on).
- Root out the old voice-quality CAT3 cabling that is hiding in your walls—1000Base-T is designed to run over existing CAT5 and CAT5e or better wiring. Use high-quality CAT5e, CAT6, or better cables, and ensure that cable runs don't run along electromagnetic sources such as ceiling lights and electrical lines. Check wall jacks to ensure cable terminations meet CAT5, CAT5e, or better standards; improperly terminated wall jacks are the leading cause of electromagnetic noise in high-speed networks. If you're running new wires, go with CAT6, which will provide the best long-term investment in your physical infrastructure.
- Take a hard look at where your network is going. Many next-generation networking technologies—such as GbE and iSCSI—are relying more on less-expensive copper wiring (CAT5, CAT5e, and CAT6) than on fiber. GbE over CAT5 and iSCSI will give you plenty of performance at a much lower cost than implementing a fiber networking technology.

Summary

The network that you've been working with for the past decade is likely showing its age. Fortunately, the next generation of networking technologies is here: GbE, solid wireless networks, smarter switches, and built-in security. These are the building blocks of the next-generation networks that companies will rely on to enhance productivity, lower costs, raise security, and improve connectivity. So how do you get started?

In the next chapter, we'll explore GbE, including network adapters and switches, introducing you to the key improvements in addition to the speed of this technology. We'll discuss how to migrate your current network to support GbE. In each subsequent chapter, we'll cover the additional technologies that form next-generation networks so that you have the resources in place to make decisions that will result in an optimized next-generation network in your environment.