Getting Started with Networking and Security

FOR DUMMIES®

A Special Edition from Dell and Its Preferred Enterprise Partners

Discover ways to streamline and secure any network environment

A Reference for the Rest of Us!®

FREE eTips at dummies.com®

Brian Underdahl

Getting Started with Networking and Security FOR DUMMIES®

A Special Edition from Dell and Its Preferred Enterprise Partners

by Brian Underdahl

Based on *Networking All-in-One Desk Reference For Dummies,* 3rd Edition, by Doug Lowe

Wiley Publishing, Inc.

Getting Started with Networking and Security For Dummies®
A Special Edition from Dell and Its Preferred Enterprise Partners

Published by
Wiley Publishing, Inc.
111 River Street
Hoboken, NJ 07030-5774

Published by Wiley Publishing, Inc., Indianapolis, Indiana

ISBN: 978-0-470-61507-2

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Dell Acknowledgments

Dell is grateful for the efforts of individuals at the following companies: Aruba Networks, Blue Coat, Extreme Networks, NetScout Systems, and SonicWALL.

Each provided additional insights for this publication, as well as examples of how we work together to bring networking and security solutions to the real world.

Publisher's Acknowledgments

We're proud of this book; please send us your comments through our Dummies online registration form located at `www.dummies.com/register/`.

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Media Development

Project Editor: Carrie A. Burchfield

Editorial Manager: Rev Mengle

Custom Publishing Project Specialist: Michael Sullivan

Business Development Representative: Kim Shelly

Composition Services

Project Coordinator: Kristie Rees

Layout and Graphics: Samantha K. Cherolis

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary Bednarek, Executive Director, Acquisitions

Mary C. Corder, Editorial Director

Publishing for Consumer Dummies

Diane Graves Steele, Vice President and Publisher

Composition Services

Gerry Fahey, Vice President of Production Services

Debbie Stailey, Director of Composition Services

Table of Contents

Introduction

Are you trying to figure out how to set up a network that handles the needs of your business? Or are you trying to get up to speed so that you have some idea what your networking consultant is recommending? If so, this book is designed to help.

About This Book

Getting Started with Networking and Security For Dummies, A Special Edition from Dell and Its Preferred Enterprise Partners, shows you the basics of business networking along with case studies that show how Dell and its partners have been able to help people just like you to implement solutions that met the needs, saved the day, and made the world a better place.

How This Book Is Organized

This book is divided into seven chapters. Chapter 1 shows you the basics of networks, briefly discusses data centers, explains the types of network connections, and introduces a standard network model. In Chapter 2 you find out more about the OSI reference model and how it describes network traffic. In addition, you see the different flavors of Ethernet.

Chapter 3 gets into the meat (or more accurately, the hardware) of networking. Here you discover pieces of stuff that you can actually pick up and handle, and you see what they do for you. If you jump into Chapter 4, you get important elements that help keep your network secure. You see how to protect both your equipment and your data.

In Chapter 5, firewalls do more than keeping the bad guys from getting into your network; they also help you control what can get out from it. This chapter shows you what firewalls do and also explains the different types of firewalls that are available.

Wireless networks are covered in Chapter 6. You get the basics of wireless networking and see what it takes to make a wireless network secure. And Chapter 7 gives you the top ten things to consider when planning your business network.

We also include some case studies in this book for you to see real-word applications. Head to the case studies in the back of this book for more information.

Icons Used in This Book

This book uses the following icons to call your attention to information that you may find helpful in particular ways.

The information in paragraphs marked by the Remember icon is important and therefore repeated for emphasis. This way, you can easily spot the information when you refer to the book later.

The Tip icon indicates extra-helpful information.

This icon marks places where technical matters, such as pixels and whatnot, are discussed. Sorry, it can't be helped, but it's intended to be helpful.

Paragraphs marked with the Warning icon call attention to common pitfalls that you may encounter.

Chapter 1

Understanding Networks

In This Chapter

- Discovering why data centers exist
- Understanding the various types of networks
- Looking at network connections
- Viewing a network model

Rumor has it that the first computer network was invented when ancient mathematicians connected their abacuses (or is it *abaci*?) together with kite string so they could instantly share their abacus answers with each other. Over the years, computer networks became more and more sophisticated. Now, instead of string, networks use electrical cables, fiber-optic cables, or wireless radio signals to connect computers to each other. The purpose, however, has remained the same: sharing information and getting work done faster.

This chapter describes the basics of what computer networking is and how it works.

Why Data Centers Matter

With the advent of networks, sharing a lot of data became possible. For companies and other large organizations, this amount of data sharing also meant a lot of important information needed to be protected and controlled. *Data centers* arose as central points in the network where these functions could be conveniently performed using specialized computers called *servers*.

Dell makes many different types of servers to suit the needs of any size organization. For example, the PowerEdge T300 is perfect for a small business that wants a single server, and the PowerEdge M-series provides a rack mounted option for larger enterprises that need multiple servers.

Networks Big and Small

Networks come in all sizes and shapes. In fact, categorizing networks is common based on the geographical size they cover, as described in the following paragraphs:

- **Local area networks:** A local area network, or LAN, is a network in which computers are relatively close together, such as within the same office or building.
- **Wide area networks:** A wide area network, or WAN, is a network that spans a large geographic territory, such as an entire city, region, or even an entire country.
- **Metropolitan area networks:** A metropolitan area network, or MAN, is a network that's smaller than a typical WAN but larger than a LAN.

Network Topology

The term *network topology* refers to the shape of how the computers and other network components are connected to each other. Many different types of network topologies exist, each with advantages and disadvantages.

Bus topology

The first type of network topology is called a *bus,* in which nodes are strung together in a line, as shown in Figure 1-1.

Bus topology isn't used much today because each computer must be connected along a single line, and this connection may not be very convenient. More importantly, buses fell out of favor because a problem *anywhere* in the line took down everyone on that line.

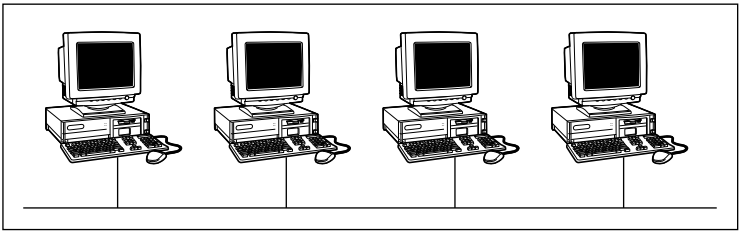

Figure 1-1: In a bus network, everything is spread out in a line.

Star topology

In a star topology, each network node is connected to a central device called a *hub* or a *switch,* as shown in Figure 1-2.

Star topology has a big advantage over other topologies because it's so flexible in terms of layout. It has a small disadvantage of requiring a hub or switch (covered in Chapter 3), but this disadvantage is also an advantage when it comes to layout.

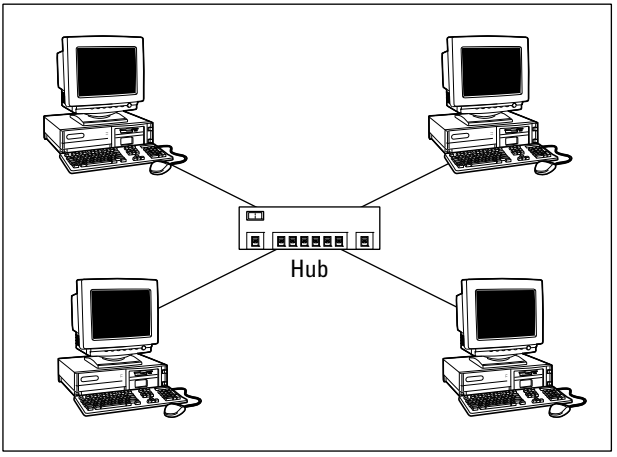

Figure 1-2: In a star network, a central switch controls network traffic.

Expanding stars

Physicists say that the universe is expanding, and network administrators know they're right. A simple bus or star topology is suitable only for small networks, with a dozen or so computers, but small networks inevitably become large networks as more computers are added.

One common way to expand a star topology is to use a technique called *daisy-chaining.* When you use daisy-chaining, a hub or switch is connected to another hub or switch as if it were one of the nodes on the star. Then, this device serves as the center of a second star.

Ring topology

A third type of network topology is called a *ring* (shown in Figure 1-3). In a ring topology, packets are sent around the circle from computer to computer. Each computer looks at each packet to decide whether the packet was intended for it. If not, the packet is passed on to the next computer in the ring. Ring networks have all but vanished from business networks.

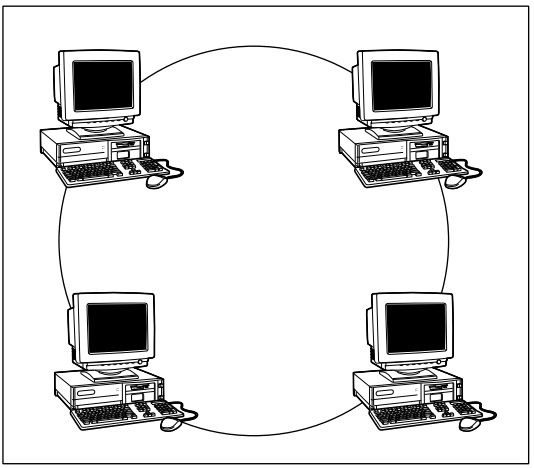

Figure 1-3: Ring topology.

Ring topology has a big disadvantage in that if the ring is broken, your network goes down.

Mesh topology

A fourth type of network topology, known as *mesh,* has multiple connections between each of the nodes on the network. Check out Figure 1-4 to see how it works.

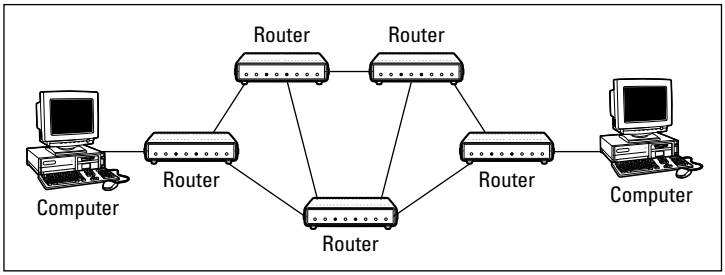

Figure 1-4: Mesh topology.

The advantage of a mesh topology is that if one cable breaks, the network can use an alternative route to deliver its packets. Mesh networks aren't very practical in a LAN setting. However, mesh networks are common for metropolitan or wide area networks.

A Network Model

Engineers and scientists sometimes like to create graphical representations to explain how systems function, so of course they have done so for computer networks. They even have a name for this — the *Open System Interconnection Reference Model,* or OSI Model for short. Figure 1-5 shows this model.

This model shows how data is communicated through the various layers of bits and pieces that make up a network. In reality, though, you can use a network for years without studying the OSI model (but knowing that it exists lets you throw around a fancy term when you want to impress your boss). More info on layers is covered in Chapter 2.

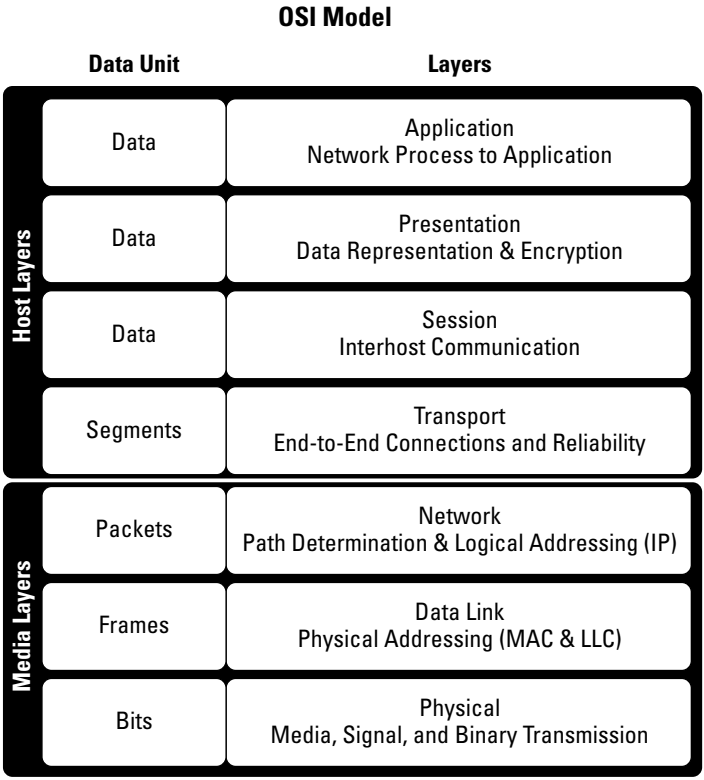

Figure 1-5: The OSI model shows how the network pieces work together.

Chapter 2

Understanding Network Protocols and Standards

In This Chapter

- Deciphering the layers of the OSI reference model
- Understanding an Ethernet

Imagine how chaotic your morning commute would be if everyone decided for themselves which direction to travel on the freeway, what the different colors on traffic lights meant, and which road lanes were for parking. Fortunately, traffic laws do exist to regulate those things so everyone knows what to expect. Just like road traffic networks, computer networks also have rules to control traffic, and this chapter provides a brief introduction to those rules.

Following a Packet through the Layers

Data flows through the layers of the network stack in an orderly fashion. In this section, you see how that happens.

Here's a brief explanation of the layers:

- **Physical layer:** Defines the electrical and physical specifications for devices
- **Data link layer:** Provides the means to transfer data between network entities

- **Network layer:** Performs network routing functions
- **Transport layer:** Controls the reliability of a given link
- **Session layer:** Controls the connections between computers
- **Presentation layer:** Establishes a context between Application Layer entities
- **Application layer:** Interacts with software applications that communicate

Figure 2-1 shows how a packet of information flows through the seven layers as it travels from one computer to another on the network.

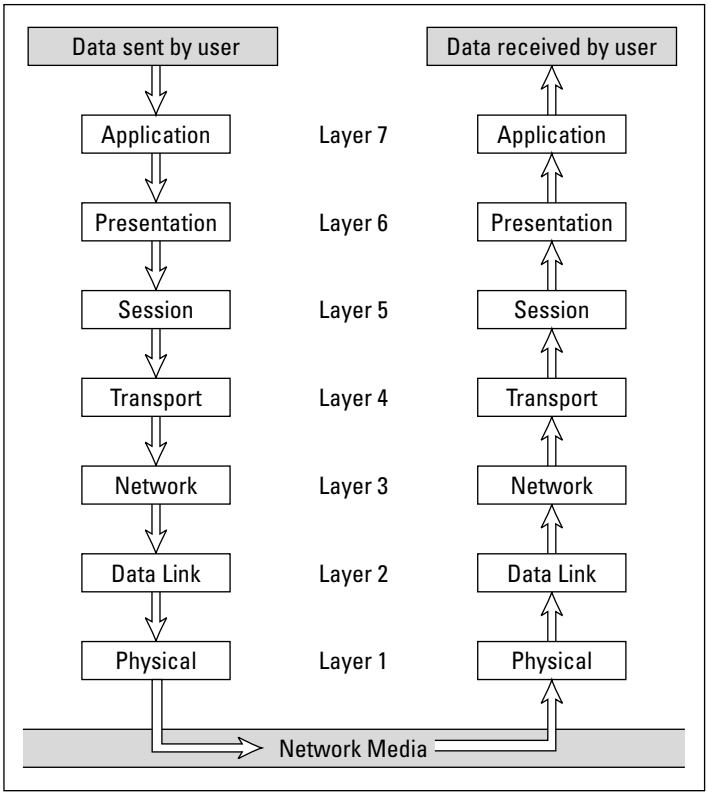

Figure 2-1: How data travels through the seven layers.

Here is the process:

1. **The data begins its journey when an end-user application sends data to another network computer.**

   The data enters the network through an Application layer interface.

2. **The data then works its way down through the protocol stack.**

   Along the way, the protocol at each layer manipulates the data by adding header information, converting the data into different formats, combining packets to form larger packets, and so on.

3. **When the data reaches the Physical layer protocol, it's actually placed on the network media (in other words, the cable) and sent to the receiving computer.**

4. **When the receiving computer receives the data, the data works its way up through the protocol stack.**

5. **Then, the protocol at each layer reverses the processing that was done by the corresponding layer on the sending computer.**

   Headers are removed, data is converted back to its original format, packets that were split into smaller packets are recombined into larger messages, and so on.

6. **When the packet reaches the Application layer protocol, it's delivered to an application that can process the data.**

The Ethernet Protocol

The first two layers of the OSI model deal with the physical structure of the network and the means by which network devices can send information from one device on a network to another. By far, the most popular set of protocols for the Physical and Data Link layers is *Ethernet.*

Ethernet has been around in various forms since the early 1970s. The current incarnation of Ethernet is defined by the IEEE standard known as 802.3. Various flavors of Ethernet operate at different speeds and use different types of media.

However, all the versions of Ethernet are compatible with each other, so you can mix and match them on the same network by using devices such as bridges, hubs, and switches to link network segments that use different types of media.

The actual transmission speed of Ethernet is measured in millions of bits per second, or Mbps. Ethernet comes in three different speed versions: 10 Mbps, known as *Standard Ethernet;* 100 Mbps, known as *Fast Ethernet;* and 1,000 Mbps, known as *Gigabit Ethernet.* Keep in mind, however, that network transmission speed refers to the maximum speed that can be achieved over the network under ideal conditions. In reality, the actual throughput of an Ethernet network rarely reaches this maximum speed.

Ethernet operates at the first two layers of the OSI model — the Physical and the Data Link layers. However, Ethernet divides the Data Link layer into two separate layers known as the *Logical Link Control (LLC) layer* and the *Medium Access Control (MAC) layer.* The two are generally considered sublayers rather than full layers. The LLC provides multiplexing and flow control, while the MAC provides addressing and channel access control.

Chapter 3

Identifying Network Hardware

In This Chapter

- Introducing servers
- Working with network interface cards
- Becoming familiar with network cable, network hubs, and switches
- Exploring repeaters, bridges, and routers

The building blocks of networks are network hardware devices, such as servers, adapter cards, cables, hubs, switches, routers, and so on. This chapter provides an overview of these building blocks.

Serving As The Network Centers: Servers

Server computers are the lifeblood of any network. Servers provide the shared resources that network users crave, such as file storage, databases, e-mail, Web services, and so on. Depending on your needs, you may have a single physical server which serves multiple purposes or you may use dedicated computers which each provide a single server function.

An *NAS device* is a self-contained file server that's preconfigured and ready to run. All you have to do to set it up is take it out of the box, plug it in, and turn it on. NAS devices like the Dell PowerVault units are easy to set up and configure, easy to maintain, and less expensive than traditional file servers.

Network Interface Cards

Every computer on a network, both clients and servers, requires a network interface card (or NIC) in order to access the network. A NIC is often a separate adapter card that slides into one of the computer's motherboard expansion slots. However, many newer computers have a built-in NIC, so a separate card isn't needed. Servers often have more than one NIC so they can connect to more than one network, such as your LAN and the Internet.

Stringing it Together

Your network won't be very useful unless it's somehow tied together. In the following sections, you see what pieces you need to make those connections.

Network cables

Nearly all modern networks are constructed using a type of cable called *twisted-pair* cable, which looks a little like phone cable but is subtly different. Older networks which use *coaxial* cable still exist. Here is a comparison of the two types of cable:

- **Coaxial cable:** A type of cable that was once popular for Ethernet networks is coaxial cable, sometimes called *thinnet* or *BNC cable* because of the type of connectors used on each end of the cable. Thinnet cable operates only at 10 Mbps and is rarely used for new networks.
- **Twisted-pair cable:** The most popular type of cable today is *twisted-pair cable,* or *UTP.* (The *U* stands for unshielded, but no one says *unshielded twisted pair.* Just *twisted pair* will do.) This type of cable is also known as Cat-5e or Cat-6.

Hubs and switches

The biggest difference between using coaxial cable and twisted-pair cable is that when you use twisted-pair cable, you

also must use a separate device called a *hub.* Years ago, hubs were expensive devices — expensive enough that most do-it-yourself networkers who were building small networks opted for thinnet cable in order to avoid the expense and hassle of using hubs.

Nowadays, the cost of hubs has dropped so much that the advantages of twisted-pair cabling outweigh the hassle and cost of using hubs. With twisted-pair cabling, you can more easily add new computers to the network, move computers, find and correct cable problems, and service the computers that you need to remove from the network temporarily.

A *switch* is simply a more-sophisticated type of hub. Because the cost of switches has come down dramatically in the past few years, most new networks are built with switches rather than hubs. If you have an older network that uses hubs and seems to run slowly, you may be able to improve the network's speed by replacing the older hubs with newer switches.

Here are some recommendations:

- When you purchase a hub or switch, purchase one with at least twice as many connections as you need. Don't buy a four-port hub or switch if you want to network four computers because when (not *if)* you add the fifth computer, you have to buy another hub or switch.
- For large networks, you may want to consider using a *managed switch* like the Dell PowerConnect series. A managed switch allows you to monitor and control various aspects of the switch's operation from a remote computer. The switch can alert you when something goes wrong with the network, and it can keep performance statistics so that you can determine which parts of the network are heavily used and which aren't. A managed switch costs a little more than an unmanaged switch, but for larger networks, the benefits of managed switches are well worth the additional cost.

For more information, see the sidebar, "Hubs and switches demystified."

Hubs and switches demystified

Both hubs and switches let you connect multiple computers to a twisted-pair network. Switches are more efficient than hubs, but not just because they're faster. If you really want to know, here's the actual difference between a hub and a switch:

- In a hub, every packet that arrives at the hub on any of its ports is automatically sent out on every other port. The hub has to do this because it is a Physical layer device, so it has no way to keep track of which computer is connected to each port. For example, suppose that John's computer is connected to port 1 on an 8-port hub, and Andrea's computer is connected to port 5. If John's computer sends a packet of information to Andrea's computer, the hub receives the packet on port 1 and then sends it out on ports 2 through 8. All the computers connected to the hub get to see the packet so they can determine whether the packet was intended for them.
- A switch is a Data Link layer device, which means it's able to look into the packets that pass through it to examine a critical piece of Data Link layer information: the MAC address. With this information in hand, a switch can keep track of which computer is connected to each of its ports. So if John's computer on port 1 sends a packet to Andrea's computer on port 5, the switch receives the packet on port 1 and then sends the packet out on port 5 only. This process is not only faster, but also it improves the security of the system because other computers don't see packets that aren't meant for them.

Repeaters

A *repeater* is a gizmo that gives your network signals a boost so the signals can travel farther. It's kind of like a Gatorade station in a marathon. As the signals travel past the repeater, they pick up a cup of Gatorade, take a sip, splash the rest of it on their heads, toss the cup, and hop in a cab when they're sure no one is looking.

Bridges

A *bridge* is a device that connects two networks so they act as if they're one network. Bridges are used to partition one large network into two smaller networks for performance reasons. Bridges also are useful when you have computer groups, which are physically separated because you only need a single cable between the bridges rather than long cable runs to each computer.

Routers

A *router* is like a bridge, but with a key difference. Bridges are Data Link layer devices, so they can tell the MAC address of the network node to which each message is sent and can forward the message to the appropriate segment. However, they can't peek into the message itself to see what type of information is being sent. In contrast, a router is a Network layer device, so it can work with the network packets at a higher level. In particular, a router can examine the IP address of the packets that pass through it. And because IP addresses have both a network and a host address, a router can determine what network a message is coming from and going to. Bridges are ignorant of this information.

One key difference between a bridge and a router is that a bridge is essentially transparent to the network. In contrast, a router is itself a node on the network, with its own MAC and IP addresses so messages can be directed to a router, which can then examine the contents of the message to determine how it should handle the message.

You can configure a network with several routers that can work cooperatively together. For example, some routers are able to monitor the network to determine the most efficient path for sending a message to its ultimate destination. If a part of the network is extremely busy, a router can automatically route messages along a less-busy route.

Chapter 4

Security 101

In This Chapter

- Physically securing your network equipment
- Figuring out user account security
- Hardening your network and securing your users

Before you had a network, computer security was easy. You simply locked your door when you left work for the day. You could rest easy, secure in the knowledge that the bad guys would have to break down the door to get to your computer.

The network changes all that. Now, anyone with access to any computer on the network can break into the network and steal *your* files. Not only do you have to lock your door, but also you have to make sure that other people lock their doors, too.

Physical Security: Locking Your Doors

The first level of security in any computer network is physical security. Physical security is important for workstations but vital for servers. Any hacker worth his salt can quickly defeat all but the most paranoid security measures if he can gain physical access to a server.

To protect the server, follow these suggestions:

- Lock the computer room.
- Give the keys only to people you trust.
- Keep track of who has the keys.
- Mount the servers on cases or racks that have locks.
- Disable the floppy drive and USB ports on the server.

Securing User Accounts

Next to physical security, the careful use of user accounts is the most important type of security for your network. Properly configured user accounts can prevent unauthorized users from accessing the network, even if they gain physical access to the network. Users who write their usernames and passwords on sticky notes on their monitors should be publically flogged — or at least educated about why this is such a bad idea!

Hardening Your Network

You should also take steps to protect your network from intruders by configuring the other security features of the network's servers and routers. The following sections describe the basics of hardening your network.

Using a firewall

A *firewall* is a security-conscious router that sits between your network and the outside world and prevents Internet users from wandering into your LAN and messing around. Firewalls are the first line of defense for any network that's connected to the Internet. For more information about firewalls, refer to Chapter 5.

Disabling unnecessary services

A typical network operating system can support dozens of different types of network services: file and printer sharing, Web server, mail server, and many others. In many cases, these features are installed on servers that don't need or use them. When a server runs a network service that it doesn't really need, the service not only robs CPU cycles from other services that are needed but also poses an unnecessary security threat.

When you first install a network operating system on a server, enable only those network services that you know the server requires. You can always enable services later if the needs of the server change.

Patching your servers

Hackers regularly find security holes in network operating systems. After those holes are discovered, the operating system vendors figure out how to plug the hole and release a software patch for the security fix. The trouble is that most network administrators don't stay up to date with these software patches. As a result, many networks are vulnerable because they have well-known holes in their security armor that should've been fixed but weren't.

Even though patches are a bit of a nuisance, they're well worth the effort for the protection that they afford. Fortunately, newer versions of the popular network operating systems have features that automatically check for updates and let you know when a patch should be applied.

Using network appliances

Another solution to hardening your network is to use a network appliance. Traditional Web antivirus gateways often lack scalability and performance for HTTP, HTTPS, and FTP scanning, leaving desktops to defend themselves. By using a network security appliance you get a proven record of enterprise robustness for effective virus scanning, plus complete visibility and control of enterprise Web communications.

The Blue Coat ProxyAV Security Appliance is a product that is used in conjunction with ProxySG to protect your entire network at the point where traffic crosses between your local network and the Internet.

Securing Your Users

Security techniques, such as physical security, user account security, server security, and locking down your servers, are child's play compared to the most difficult job of network security: securing your network's users.

The key to securing your network users is to create a written network security policy and stick to it. Have a meeting with everyone to go over the security policy to make sure that everyone understands the rules. Also, make sure to have consequences when violations occur.

Antivirus Programs

The best way to protect your network from virus infection is to use an antivirus program. These programs have a catalog of several thousand known viruses that they can detect and remove. In addition, they can spot the types of changes that viruses typically make to your computer's files, thus decreasing the likelihood that some previously unknown virus will go undetected.

The people who make antivirus programs have their fingers on the pulse of the virus world and frequently release updates to their software to combat the latest viruses. Because virus writers are constantly developing new viruses, your antivirus software is next to worthless unless you keep it up to date by downloading the latest updates.

If you're looking to deploy antivirus protection on your network, here are several approaches:

- **Install antivirus software on each network user's computer.** This technique is the most effective if you can count on all your users to keep their antivirus software up to date. Because that's an unlikely proposition, you may want to adopt a more reliable approach to virus protection.
- **Place antivirus client software on each client computer in your network.** Then, an antivirus server automatically updates the clients regularly to make sure they're kept up to date.
- **Use server-based antivirus software to protect your network servers from viruses.** For example, you can install antivirus software on your mail server to scan all incoming mail for viruses and remove them before your network users ever see them.
- **Limit Internet access:** Some firewall appliances include antivirus enforcement checks that don't allow your users to access the Internet unless their antivirus software is up to date. This type of firewall provides the best antivirus protection available.
- **Place appliances accordingly:** Place appliances responsible for catching Web-based threats, malware, and antivirus at the point where traffic crosses from your LAN to the Internet.

Chapter 5

Controlling Traffic with Firewalls

In This Chapter

- Understanding what firewalls do
- Examining the different types of firewalls

If your network is connected to the Internet, a whole host of security issues bubble to the surface. You probably connected your network to the Internet so your network's users could access the Internet. Unfortunately, however, your Internet connection is a two-way street. Not only does it enable your network's users to step outside the bounds of your network to access the Internet, but also it enables others to step in and access your network.

And step in they will. The world is filled with hackers looking for networks like yours to break into. They may do it just for fun, or they may do it to steal your customers' credit card numbers or to coerce your mail server into sending thousands of spam messages on their behalf. Whatever their motive, rest assured that your network will be broken into if you leave it unprotected.

This chapter presents an overview of a basic technique for securing your network's Internet connection: firewalls.

Firewalls — Network Traffic Cops

A *firewall* is a security-conscious piece of hardware or software that sits between the Internet and your network with a single-minded task: preventing *them* from getting to *us.* The firewall acts as a security guard between the Internet and your local area network (LAN). All network traffic into and out of the LAN must pass through the firewall, which prevents unauthorized access to the network.

Some type of firewall is a must-have if your network has a connection to the Internet, whether that connection is broadband (cable modem or digital subscriber line; DSL), T1, or some other high-speed connection. Without it, sooner or later a hacker will discover your unprotected network and tell his friends about it. Within a few hours, your network will be toast.

You can set up a firewall in two basic ways. The easiest way is to purchase a *firewall appliance,* which is basically a self-contained router with built-in firewall features. Most firewall appliances include a Web-based interface that enables you to connect to the firewall from any computer on your network using a browser. You can then customize the firewall settings to suit your needs.

Alternatively, you can set up a server computer to function as a firewall computer. The server can run just about any network operating system, but many dedicated firewall systems run Linux.

Whether you use a firewall appliance or a firewall computer, the firewall must be located between your network and the Internet, as shown in Figure 5-1. Here, one end of the firewall is connected to a network hub, which is in turn connected to the other computers on the network. The other end of the firewall is connected to the Internet. As a result, all traffic from the LAN to the Internet and vice versa must travel through the firewall.

The term *perimeter* is sometimes used to describe the location of a firewall on your network. In short, a firewall is like a perimeter fence that completely surrounds your property and forces all visitors to enter through the front gate.

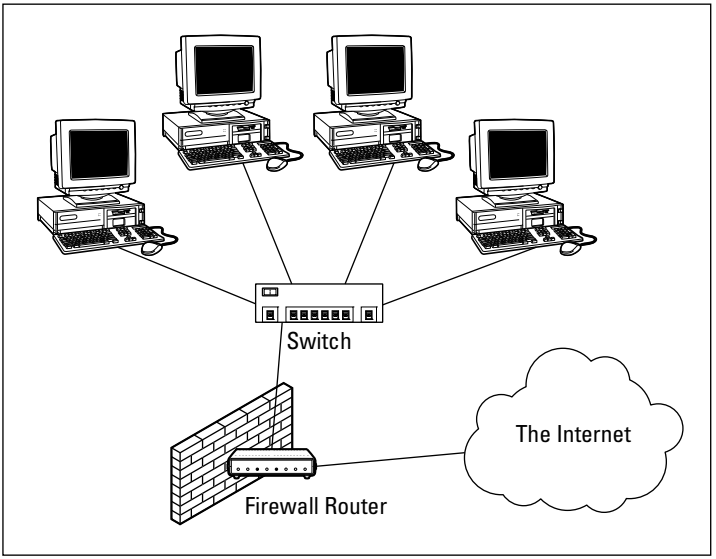

Figure 5-1: Using a firewall appliance.

Basic Types of Firewalls

Firewalls employ certain basic techniques to keep unwelcome visitors out of your network. The following sections describe the most common firewall techniques.

Packet filtering

A *packet-filtering* firewall examines each packet that crosses the firewall and tests the packet according to a set of rules that you set up. If the packet passes the test, it's allowed to pass. If the packet doesn't pass, it's rejected.

Packet filters are the least expensive type of firewall. As a result, packet-filtering firewalls are very common. However, packet filtering has a number of flaws that knowledgeable hackers can exploit. As a result, packet filtering by itself doesn't make for a fully effective firewall.

Packet filters work by inspecting the source and destination IP and port addresses contained in each Transmission Control Protocol/Internet Protocol (TCP/IP) packet.

TCP/IP ports are numbers that are assigned to specific services that help to identify for which service each packet is intended. For example, the port number for the HTTP protocol is 80. As a result, any incoming packets headed for an HTTP server will specify port 80 as the destination port.

Stateful packet inspection (SPI)

Stateful packet inspection (SPI) is a step up in intelligence from simple packet filtering (see the preceding section). A firewall with stateful packet inspection looks at packets in groups rather than individually. It keeps track of which packets have passed through the firewall and can detect patterns that indicate unauthorized access. In some cases, the firewall may hold on to packets as they arrive until the firewall gathers enough information to make a decision about whether the packets should be authorized or rejected.

Stateful packet inspection was once found only on expensive, enterprise-level routers. Now, however, SPI firewalls are affordable enough for small- or medium-sized networks to use.

Deep packet inspection

Another more comprehensive way to inspect the packets is *deep packet inspection* (DPI). In DPI, the actual content of the packets is inspected so viruses, spam, and other harmful content can be blocked.

DPI also allows practices, such as data mining, eavesdropping, and content censorship, which make its use a controversial subject.

Chapter 6

Setting Up and Securing a Wireless Network

In This Chapter

- Looking at wireless network basics
- Working with a wireless access point
- Enabling the security features of your wireless network

This chapter introduces you to the ins and outs of setting up a wireless network. With wireless networking, you don't need cables to connect your computers. Instead, wireless networks use radio waves to send and receive network signals. As a result, a computer can connect to a wireless network at any location in your office.

Wireless networks are especially useful for laptops. After all, the main benefit of a laptop is that you can carry it around with you wherever you go. At work, you can use your laptop at your desk, in the conference room, in the break room, or even out in the parking lot. With wireless networking, your laptop can be connected to the network, no matter where you take it.

Diving into Wireless Networking

A *wireless network* is a network that uses radio signals rather than direct cable connections to exchange information. A computer with a wireless network connection is like a cell phone. Just as you don't have to be connected to a phone line to use a cell phone, you don't have to be connected to a network cable to use a wireless networked computer.

The following summarizes some of the key concepts and terms that you need to understand in order to set up and use a basic wireless network:

- **A wireless network is often referred to as a *WLAN,* for *wireless local area network.*** Some people prefer to switch the acronym around to *local area wireless network,* or *LAWN.* The term *Wi-Fi* is often used to describe wireless networks, although it technically refers to just one form of wireless networks: the 802.11b standard.
- **A wireless network has a name, known as an *SSID.*** SSID stands for *service set identifier* — wouldn't that make a great *Jeopardy!* question? (I'll take obscure four-letter acronyms for $400, please!) Each of the computers that belong to a single wireless network must have the same SSID.
- **Wireless networks can transmit over any of several channels.** In order for computers to talk to each other, they must be configured to transmit on the same channel.
- **The simplest type of wireless network consists of two or more computers with wireless network adapters.** This type of network is called an *ad-hoc mode network.*
- **A more complex type of network is an *infrastructure mode network.*** All this really means is that a group of wireless computers can be connected not only to each other but also to an existing cabled network via a device called a *wireless access point* or WAP. (Discover more about ad-hoc and infrastructure networks later in this chapter.)

Wireless Access Points

Unlike cabled networks, wireless networks don't need a hub or switch. If all you want to do is network a group of wireless computers, you just purchase a wireless adapter for each computer, put them all within 300 feet of each other, and *voilà!* — instant network.

But what if you already have an existing cabled network? For example, suppose that you work at an office with 15 computers all cabled up nicely, and you just want to add a couple of wireless laptops to the network. Or suppose that you have a

conference room where executives want to meet, use their laptops, and not worry about crawling under the tables looking for network connections.

That's where a *wireless access point (WAP)* comes in. A WAP actually performs two functions:

- It acts as a central connection point for all your computers that have wireless network adapters. In effect, the WAP performs essentially the same function as a hub or switch performs for a wired network.
- It links your wireless network to your existing wired network so your wired computers and your wireless computers get along like one big happy family.

Infrastructure mode

When you set up a wireless network with an access point, you're creating an *infrastructure mode* network. It's called infrastructure mode because the access point provides a permanent infrastructure for the network. The access points are installed at fixed physical locations, so the network has relatively stable boundaries. Whenever a mobile computer wanders into the range of one of the access points, it has come into the sphere of the network and can connect.

An access point and all the wireless computers that are connected to it are referred to as a *Basic Service Set (BSS).* Each BSS is identified by a *Service Set Identifier (SSID).* When you configure an access point, you specify the SSID that you want to use. The SSID is often a generic name such as *wireless,* or it can be a name that you create. Some access points use the MAC address of the WAP as the SSID.

Roaming

You can use two or more wireless access points to create a large wireless network in which computer users can roam from area to area and still be connected to the wireless network. As the user moves out of the range of one access point, another access point automatically picks up the user and takes over without interrupting the user's network service.

To set up two or more access points for roaming, you must carefully place the WAPs so all areas of the office or building that are being networked are in range of at least one of the WAPs. Then, just make sure that all the computers and access points use the same SSID and channel.

Two or more access points joined for the purposes of roaming, along with all the wireless computers connected to any of the access points, form what's called an *Extended Service Set (ESS).* The access points in the ESS are usually connected to a wired network.

One of the current limitations of roaming is that each access point in an ESS must be on the same TCP/IP subnet. That way, a computer that roams from one access point to another within the ESS retains the same IP address. If the access points had a different subnet, a roaming computer would have to change IP addresses when it moved from one access point to another.

Wireless bridging

Another use for wireless access points is to bridge separate subnets that can't easily be connected by cable. For example, suppose that you have two office buildings that are only about 50 feet apart. To run cable from one building to the other, you'd have to bury conduit — a potentially expensive job. Because the buildings are so close, though, you can probably connect them with a pair of wireless access points that function as a *wireless bridge* between the two networks. Connect one of the access points to the first network and the other access point to the second network. Then, configure both access points to use the same SSID and channel.

Ad-hoc networks

A wireless access point isn't necessary to set up a wireless network. Any time two or more wireless devices come within range of each other, they can link up to form an *ad-hoc network.* For example, if you and a few of your friends all have laptops with 802.11n wireless network adapters, you can meet anywhere and form an ad-hoc network. All computers within range of each other in an ad-hoc network are called an *Independent Basic Service Set (IBSS).*

Securing Your Wireless Network

Before you dive headfirst into the deep end of the wireless networking pool, you should first consider the inherent security risks in setting up a wireless network. With a cabled network, the best security tool that you have is the lock on the front door of your office. Unless someone can physically get to one of the computers on your network, she can't get into your network. (Well, I'm sort of ignoring your wide-open broadband Internet connection for the sake of argument.)

If you go wireless, an intruder doesn't have to get into your office to hack into your network. She can do it from the office next door, the lobby, or the parking garage beneath your office. In short, when you introduce wireless devices into your network, you usher in a whole new set of security issues to deal with.

When you first install a wireless access point, change its administrative password and then secure the SSID that identifies the network. A client must know the access point's SSID in order to join the wireless network. If you prevent unauthorized clients from discovering the SSID, you prevent them from accessing your network.

Using MAC address filtering

MAC address filtering allows you to specify a list of MAC addresses for the devices that are allowed to access the network. If a computer with a different MAC address tries to join the network via the access point, the access point will deny access.

MAC address filtering is a great idea for wireless networks with a fixed number of clients. For example, if you set up a wireless network at your office so a few workers can connect their laptops, you can specify the MAC addresses of those computers in the MAC filtering table. Then, other computers won't be able to access the network via the access point.

Unfortunately, it isn't difficult to configure a computer to lie about its MAC address. Thus, after a potential intruder determines that MAC filtering is being used, he can just sniff

packets to determine an authorized MAC address and then configure his computer to use that address. (This is called *MAC spoofing*.) So you shouldn't rely on MAC address filtering as your only means of security.

Using encryption

One big problem with wireless networking is simply that it's wireless. This means that anyone nearby with a wireless adapter in their PC has the potential to snoop on your wireless connection. Fortunately, there's a solution — encryption.

By using encryption the wireless signals are protected from snooping because no one else will be able to read their contents. If you don't use encryption on your wireless network, it's almost like leaving your credit cards on a park bench — you can hope everyone is honest, but it's not a good bet.

The first wireless networks used an encryption method called *Wired Equivalent Privacy (WEP),* which really didn't do much other than make users think that they were secure. Modern wireless networking equipment uses Wi-Fi Protected Access (WPA or WPA2), which actually does provide reasonable protection. WPA2 uses an AES (Advanced Encryption Standard)-based algorithm, CCMP, which is considered fully secure.

Chapter 7

Top 10 Strategies to Consider

In This Chapter

- Analyzing the needs
- Determining a fix
- Applying a solution

Choosing the correct networking equipment can be confusing, especially if you aren't sure which questions to ask. In this chapter, you see some questions which will help you focus your efforts.

What Type of Network Topology Should I Consider?

You need to create a new network or expand an existing one, and the answer to the question depends on many factors, but one of the most important is whether you need to work with existing infrastructure. Most modern networks use a star topology for the wired sections of the network, but if you are expanding an existing network, which uses bus topology, it may be cheaper to stay with what you have. Don't forget, though, that future expansion needs may dictate that you switch to UTP cabling or even wireless networking.

What's the Best Way to Connect Workstations to My Existing Network?

Say your company is considering buying a neighboring building for a call center and you want to connect workstations to your existing network. Well, carrier pigeons are probably out of the picture; they're too slow and you don't want to be responsible for cleaning up after them. So a better option may be to use a pair of bridges to extend the network between the two sites. That way you only need a single wired or wireless connection between the buildings.

What Types of Products Should I Consider?

Your company is spending a lot of money on bandwidth, and you've been tasked with improving the performance of legitimate business processes while reducing those costs.

If you suspect that a lot of bandwidth is being wasted on things like music downloads, you could announce a new company policy that anyone seen wearing earphones in their cube will be paraded naked around the building, but you may not want to contemplate how some employees would look in the buff. Rather, consider adding a firewall appliance, which offers comprehensive inspection so you can control which types of traffic are allowed into your network.

What Can I Do about Viruses and Poor Performance?

Even though you have installed anti-virus software on all your PCs, the occasional virus outbreaks still occur, and some users complain about poor performance.

Rather than relying upon AV software, it may be time to consider a network security appliance. By blocking the bad stuff before it ever enters your network, you'll stop most problems in their tracks. And you won't have to listen to that know-it-all in accounting who insists that his snot-nosed middle school nephew could make your PCs run faster.

What Should I Look for in Order to Make My Wireless Network Secure?

You have a very large building and your workers move around a lot with their laptops. A reasonable approach is to make sure that all wireless equipment supports the WPA2 encryption standard.

How Can I Detect and Contain Rogue APs and Other Wireless Threats?

You suspect that some users have added unauthorized wireless access points. The ability to detect unauthorized access points and accurately separate them from valid neighboring networks is critical. A state-of-the-art wireless LAN system not only can detect and classify rogues accurately but also stop rogue access points automatically and accurately point out the source of the threat as well.

An integrated policy enforcement firewall enables you to control the access privileges of each and every user, even if they move around in the network and use a multiple devices such as laptops, PDAs, and WiFi phones. An integrated policy enforcement firewall provides the highest level of security and trust necessary to deploy mission-critical applications wirelessly.

What Considerations Help Me Plan for Future Expansion?

You should be sure the system you buy today will support your future needs. Ask how many users a single system can accommodate, and be sure it can be centrally managed.

A good wireless system should eliminate the need for pre-deployment site surveys by configuring itself dynamically to provide best coverage and performance, and to fill coverage gaps in the event of an AP failure. In addition, location-enabled wireless systems accurately locate unauthorized access points and malicious users. Later, location functionality may be used to implement location-enabled applications.

What Do I Need to Ask?

You need to add new network capacity without disrupting day-to-day operations. So what should you ask?

WLAN architectures that don't require configuration changes and upgrades to the existing wired LAN infrastructure are superior to those that require hardware and software upgrades to achieve an "integrated wired and wireless solution." The cost of upgrading software, configuring VLANs everywhere and enabling mobility and management are too high not to be taken into account when purchasing a WLAN system just because they don't show up on the purchase order.

How Can I Identify the Actual Applications Consuming Bandwidth?

If you need to figure out what's eating up all your bandwidth and you want to monitor their behavior and quality, and set policy-based QoS controls to enable quality standards or manage bandwidth consumption, this is the section for you!

With certain types of network appliances, you can identify all the applications on the network and monitor response times and utilization at the application level. In addition, you can optimize application performance by using granular quality of service (QoS) controls to regulate traffic, ensuring business applications perform optimally.

How Can I Manage and Deliver Live, On-Demand Video?

To manage live and on-demand video to branch offices from internal and external sources most effectively, you can use a proxy server network appliance so multiple requests for the same stream are served locally. This type of appliance won't help a live feed, of course, but it can greatly enhance performance when many different people want to watch stored video, such as training materials (or even YouTube).

Case Study A

Aruba's Approach: Taking the Campus Wireless

In this case study, Aruba Networks worked with the California State University System (CSU) to move the network infrastructure on 23 campuses to modern wireless technology. With nearly 500,000 clients, this case was clearly not the place for someone who needed to learn on the job, so CSU brought in the experts. For more info on wireless networking, please see Chapter 6.

Analyzing the Situation

Facing a complicated and massive wired network refresh covering 23 university campuses from Humboldt to San Diego, the Technology Infrastructure Services (TIS) group of the CSU had few choices. While wireless technology seemed to hold great intrigue and promise, the CSU budget for wireless initiatives was limited. In the absence of wireless, individual CSU campuses were concerned that the need for Ethernet ports and switches would double.

"Our multi-campus network undergoes an equipment refresh every three to five years, depending on technology maturation," said Michel Davidoff, director of Cyberinfrastructure Services for the CSU System. "It quickly became evident that achieving our goal of providing one 10/100 Ethernet connection to 490,000 students, faculty members, and staff, as well as providing adequate capacity for classrooms, libraries, computer labs, common areas, and retail centers would be extremely complicated and cost prohibitive."

The TIS staff and campuses began to measure port usage, and wired ports across all 23 campuses were consistently underutilized. Armed with this data, the team decided to explore a different approach to its planned network refresh. The team identified the following requirements:

- Adequate network capacity for classrooms, libraries, computer labs, common areas, and retail centers
- Satisfy the hundreds of functional requirements defined in the RFP for the multi-campus wireless network
- Intuitive and feature-rich management interface, simplicity of configuration and monitoring, and ease of use

The Wireless LAN Technology Option

While wireless LAN technology was traditionally viewed as a "nice to have" service on some campuses, CSU's recent experience led them to conclude that wireless was a reliable, low-cost option for delivering pervasive campus connectivity. Several campuses had already deployed some Aruba wireless LAN equipment, mostly for coverage in selected high-usage areas, and San Diego State University had built a relatively large WLAN on its campus. It found the Aruba WLAN to be a highly-secure, scalable, and reliable enhancement to its wired network, allowing for a refresh approach that only replaced utilized wired ports.

The CSU team assembled a consortium of engineers to produce and issue an RFI to leading wireless LAN vendors. From the vendor respondents, three were selected to participate in a comprehensive technology evaluation. Additionally, the evaluation team analyzed the vendor proposals, looking at the eight-year costs associated with purchasing and refreshing the hardware, staff training, and overall maintenance.

The team determined that Aruba Networks provided the best value for fulfilling the needs of the CSU technology infrastructure while providing additional benefits. These benefits included the following:

- **Operational simplicity:** The Aruba WLAN infrastructure was easy to deploy and manage during the evaluation process.
- **Management:** The AirWave Management Platform delivers data that's used to quickly resolve helpdesk issues and lower support costs.
- **802.11n Future-Proofing:** Aruba delivers low-cost 802.11n-capable access points that can be software-upgraded to full .11n when needed. With thousands of access points deployed across the multi-campus system, this flexibility will save the CSU system significant capital in upgrade costs, as well as the labor required to physically replace access points.
- **Scale:** The Aruba architecture has the controller capacity and central RF intelligence to provide reliable access across large campuses in the CSU system like San Diego State that exceeds 1,000 access points.

Adding It Up

Determined to approach the opportunity analytically and impartially, the Technology Infrastructure Services staff created a database with every telecommunication room in CSU, the number of ports in each room, and the number of those ports that are actively used. They developed a formula to determine the refresh requirements of each campus based on this measurement. Applying this formula across all 23 campuses, CSU recognized a savings of approximately $30 million by reducing the scale of its planned wired network refresh and utilizing Aruba's wireless LAN technology.

While not yet directly measured, CSU is confident that other operational cost savings will be recognized from the transition of some wired ports to wireless, such as maintenance, cooling, power, and so on.

A corollary benefit is a reduced carbon footprint and improved environmental responsibility that further strengthen the University system's sustainability efforts.

Additionally, the team almost immediately began to see a marked increase in network usage as wireless was deployed.

Prior to the upgrade, faculty and university staff were the primary users of the wired network, but that majority shifted to the student body as wireless connectivity became available. With up to 5,000 faculty/staff and 36,000 students per campus, many campuses have seen a nearly fivefold increase in network usage with the implementation of pervasive wireless LAN.

With this explosion in network usage, plans are underway to utilize the wireless infrastructure for a plethora of new applications, including technology enhanced curriculum, mobile device access in university health centers, and campus safety enhancements, such as wireless video monitoring.

The Solution

In the end, the team decided on the following solution:

- 802.11n-capable indoor access points that can be software-upgraded to full .11n
- Outdoor access points to extend coverage beyond campus buildings
- Centralized Multiservice Mobility Controllers
- Policy Enforcement Firewall, Mesh, Wireless Intrusion Prevention, and Remote Access Point software modules
- AirWave Wireless Management Software

This solution provided these benefits:

- Operational simplicity to ease deployment and ongoing management
- Powerful wireless network management to quickly resolve helpdesk issues and increase network stability
- 802.11n Future-Proofing to save the CSU system significant capital and labor costs
- Controller capacity and central RF intelligence to provide reliable access on any size campus

Case Study B

Blue Coat's Approach: Making the Network Deliver

This case study shows how Blue Coat Systems allows architectural offices half a world apart to function as a single, efficient organization. Discover more about networking hardware in Chapter 3.

The customer, Woods Bagot, is a Sydney-based international architecture design firm, with over 1,000 employees at 16 studios in Asia, Australia, Europe, Middle East, and North America. Woods Bagot operates as one global studio, enabled by global technology solutions and a commitment to working without boundaries. Their clients have access to any of Woods Bagot's expert employees, while still benefiting from the project support provided by a local studio.

For you Google searchers out there, Woods Bagot designed Hong Kong University, Qatar Science and Technology Park, the Melbourne Convention & Exhibition Centre, and the Qantas first class lounges.

Defining the Problem

Due to the nature of their business, Woods Bagot studios work collaboratively on projects, not singularly. So Sydney and San Francisco would work together on a project that might require sharing 100 MB collaborative architectural files multiple times per day. On their intranet (local and WAN) they typically have 300 Gb of data — podcasts, videocasts, and

mission critical applications and data, with staff accessing these all the time. The WAN is also utilized for real time communications, such as voice, video, and video conferencing.

The main problem Woods Bagot faced was the slow delivery of applications and mission critical data. The primary applications and protocols impacted at Woods Bagot were:

- AutoCAD
- Email
- FTP
- Microsoft CIFS – File sharing
- Microsoft SharePoint
- SQL databases
- Symantec file replication
- Video conferencing
- VoIP
- Windows media streaming

A large file transfer (such as a 3D simulation) takes far too long to send, immediately creating issues with VoIP, and making video conferencing unusable. Such file sharing was only possible by burning the files to DVDs and sending via a courier.

A solution was needed — one that addressed the immediate issue of network utilization but one that allowed Woods Bagot to stay at the forefront of innovation while being responsive and competitive.

Examining the Options

To address the issues, Woods Bagot looked at several options:

- Increasing bandwidth was a logical choice, but was cost prohibitive and in several of their locations, would result in heavy tariffs. In addition, simply increasing bandwidth didn't address QoS issues either.

- A Multiprotocol Label Switching (MPLS) solution was considered, but again, was found to be cost prohibitive.
- Microsoft Windows Distributed File System (DFS) replication was another potential solution that was looked at, but it seemed to lack certain network efficiency features Woods Bagot was seeking.

Ultimately, the only approach that met expectations appeared to be deploying a WAN Optimization Controller (WOC) at each Woods Bagot location. Also, QoS and acceleration enabled by these appliances would bring visibility and control of the WAN. With this in mind, several vendors were considered best of breed and evaluated. In the end, Woods Bagot settled on Blue Coat Systems.

"Acceleration of CIFS (Common Internet File System) and HTTPS traffic, along with greater visibility of network, and the ability to manage video and do the best QoS, was what convinced us about their solution," said Nectarios Lazaris, Woods Bagot's group CIO. More importantly for Lazaris and his IT team, it was Blue Coat's availability and willingness to rise to the occasion with its own engineers and those of its SI's that really differentiated it from its competitors. Additionally, the branch office-based ProxySG appliances also enabled Woods Bagot to securely gain direct Internet access rather than backhauling inbound and outbound Internet traffic.

Creating a Solution

Woods Bagot recognized that WAN optimization solutions were rapidly evolving, but they could see immediate value in upgrading to implement an Application Delivery Network layer offered by the combination of Blue Coat ProxySG and Packet Shaper. By installing the Blue Coat products at their sites, Woods Bagot received all the benefits of the optimization and acceleration of applications and data across the WAN, with the added benefits of now being able to prioritize traffic, applying QoS to real time and mission critical applications and data. In addition, they could also now secure and accelerate more traffic utilizing SSL.

Gauging the benefits

Woods Bagot internal testing estimated that after implementing Blue Coat products, the following results occurred:

- CAD performance was 50x faster
- SharePoint was 300x faster
- FTP was 50x faster

In addition, Woods Bagot achieved other benefits, which are highlighted in the following sections.

Optimization and acceleration

With optimization and acceleration, you get 60 percent compression and caching of data that provides much faster application and data delivery. Woods Bagot estimates this faster delivery added up to an increased productivity of approximately five minutes per day for all staff and increased staff productivity by 83 hours a day.

Cost savings

A huge reduction in the daily link costs from Sydney and Dubai enabled Woods Bagot to pay for the entire Blue Coat deployment in four months. Afterwards this reduction produced pure operational savings.

Video conferencing

Enabling the use of high quality video conferencing over the existing WAN to replace in-person Board meetings produced travel savings of $200,000 per meeting and enabled a significant boost in productivity and efficiency.

Data replication

Woods Bagot's business uses a lot of large file transfers, SharePoint, CAD, and graphic-rich data containing all sorts of architectural content. This content may be produced in Australia or the U.S., reviewed and manipulated in Asia, and then presented to a customer in the Middle East. Being able to control the flow of this content based on regional peak usage times allowed Woods Bagot to further optimize bandwidth. Woods Bagot runs a lean IT operation, and operational efficiency is key.

Centralized management

Utilizing the Blue Coat management solution, Woods Bagot implemented centralized management, configuration storage, and deployment.

Application/data QoS

Blue Coat allows Woods Bagot to achieve a happy medium — prioritize work so people can still do recreational traffic while ensuring it doesn't interfere with mission critical applications and data.

SSL proxy

The SSL proxy accelerates the speed of encrypted data.

Video streaming QoS

Video streaming QoS reduces network traffic for better performance. For instance, if five staff members in Abu Dhabi watch a video streamed from the Sydney media server pre-ProxySG, the information would've traveled over the network five times and the service levels would decrease dramatically — potentially killing the link for mission critical applications. Now, the information travels over the network once and is stored in the Blue Coat box in Abu Dhabi for future viewings.

Security

By simply adding the appropriate licenses to ProxySG, Woods Bagot has the ability to enable Blue Coat's security technology, eliminating Web-based threats and malware from the entire Woods Bagot network.

Checking the results

With PacketShaper appliances, Woods Bagot was able to deploy high-definition video conferencing over its existing network. The first use was to conduct a board meeting. This saved the company $200,000 in travel costs just for one meeting and more when time and productivity are taken into account. The meeting was so successful that the Board decided that all meetings would be via video conferencing and the frequency of meetings could be more often.

Drawing a conclusion

Woods Bagot exemplifies the value of adding Application Delivery Networking as a layer of intelligence and control to the existing packet network. The solution offered benefits that were both tactical and strategic.

Tactical gains included a dramatic reduction in bandwidth consumption, resulting in lower cost WAN links in places such as the Middle East. These lower costs resulted in a four-month payback and then created pure operational savings. The new ability to conduct high-quality video conferencing over the existing network also produced substantial cost savings.

The strategic advantage was Woods Bagot's ability to create a true "virtual studio" so clients in any location could be served by a global team of Woods Bagot experts on any particular project. This was accomplished by enabling the efficient sharing of very large files across the WAN for true collaboration. By achieving the virtual studio, Woods Bagot could better serve customers, make more effective use of its own resources and win new business more easily.

Case Study C

Extreme's Approach: Building a New Network

In this case study, you see how Virtual Wonders, a customer of Extreme Networks, replaced an outdated network with one that better suited their current and future needs.

Virtual Wonders had a core network built on a hodgepodge of switches of various different technologies — from several different vendors. Virtual Wonders needed to beef up their network performance, simplify management, and add redundancy.

Please refer to Chapter 3 for more of the basics on the network hardware.

The Challenge

Virtual Wonders specializes in stunning visual effects, combining artistic creativity with advanced technologies and organizational quality. Initially focused on the visual effects market for the motion picture industry, Virtual Wonders recently opened a new center dedicated to its international advertising customers.

The company now owns three locations connected by a fiber optic network and Gigabit links. The network supports 60 application servers, 32 image computing servers, and approximately 250 graphics workstations. Due to the immense size of the graphic images and videos, the storage requirements are approximately 20 terabytes.

An extreme need

Multimedia creation is an intense, time driven business that demands high performance and constant availability from a network. Virtual Wonders' customer deadlines are often very short, and the data network must perform without fail 24/7 to assure success.

To overcome the problems caused by its original network, which was no longer meeting the company's business requirements, Virtual Wonders launched a network migration initiative to support a more robust core network as well as a new SAN network.

An extreme solution

Virtual Wonders' IT team decided to break the network design into two separate projects:

- Phase 1, to address the core network
- Phase 2, to address the SAN/Server network

The IT team established the following requirements:

- All network switches must run the same operating system across all platforms.
- The switch operating system must be resilient and be capable of withstanding process faults without restarting the entire platform to avoid network downtime.
- All equipment must provide sub-second network convergence (system or link) capabilities.
- All equipment must have capability to automate tasks and create executable routines upon event recognition.
- Core equipment must be chassis based.
- Core equipment must be capable of In Service Software Update (ISSU).
- The roadmap should include upgrade to 40/100GbE technologies without chassis replacement.
- Low latency should support high performance SAN/Server equipment needs.

- SAN/Server equipment needs a plan for converting Gig SAN to 10GbE SAN in the future.
- SAN/Server equipment needs fault tolerant/highly available network architecture.

Project 1: Core Network

Virtual Wonders' staff was very happy with the performance of the existing Extreme Networks Summit series switches in place. Extreme Networks, a leader in converged Gigabit Ethernet network solutions, was already the network infrastructure of choice for Virtual Wonders. So Virtual Wonders looked to Extreme Networks to help them further. In addition, an evaluation revealed that Extreme Networks was competitively priced to the market.

After a detailed evaluation and in-house testing was completed, Virtual Wonders selected Extreme Networks BlackDiamond 8810 switches to replace its two existing core switches.

Extreme Networks BlackDiamond 8800 series switches deliver industry leading 3.8 Tbps of switching bandwidth, and over 2,840 Mbps Layer 2 – Layer 3 hardware forwarding rate, with 256 Gbps per slot bidirectional bandwidth and local switching on every I/O module. BlackDiamond 8810 supports up to 784 gigabit ports or up to 192 10-Gigabit Ethernet ports in a single chassis.

The BlackDiamond 8810 modular switch provided many hardware and software resiliency features to maintain business continuity for Virtual Wonders. High-availability features of the BlackDiamond 8810 include

- Redundant management modules (switch fabric and management) to deliver hitless failover
- Redundant load sharing power supplies
- Passive backplane with isolated control and data planes
- Redundant controller boards for power distribution
- Fan control and environmental monitoring to identify anomalies before they affect network availability

- Modular operating system that provides loadable software modules and true preemptive multitasking and memory protected process that can be restarted to enable non-stop operation
- Link level protection with Extreme's Ethernet Automatic Protection Switching, which can deliver sub-second network recovery

Project 2: SAN/Server Network

Virtual Wonders examined the two primary designs of Top of Rack (ToR) and End of Row (EoR) and chose to implement the ToR design. Simplicity and reduction of cable plant were the two primary business drivers. Today, all of the SAN connections are Gigabit connected but Virtual Wonders knew that in the near future SAN controllers would be available with 10GbE network connections. Therefore, they strove to accommodate both Gigabit and 10GbE technologies without replacement of the SAN/Server infrastructure during any future migration to the higher speed.

Virtual Wonders chose the Extreme Networks Summit X450a and Summit X650 switches for their common operating system, common stacking system, high performance, and ability to create a distributed stack or virtual chassis across the racks. By creating a distributed stack across racks, the SAN environment appeared as a single network with low latency, sub-second failover with the EAPS protocol, and the ability to connect both Gigabit and 10GbE connections today.

Each top switch in a rack is connected to each other through a high speed stacking cable creating the distributed stack. Each bottom switch is a member of another distributed stack. The dual stack model provides protection against faults which potentially could take the entire stack out of production. Multiple high speed 10GbE connections across the stack can be aggregated across the racks to the core providing resiliency, redundancy, and higher throughput using 802.1d Link Aggregation. The SAN environment is separated through VLAN and security technologies providing a common Layer 2 domain to all SAN devices.

Layer 3 routing provides the logical separation between the SAN and server domains. Sub-second convergence time between the server environment on the distributed stack and the core switches are achieved with the EAPS protocol.

Virtual Wonders needed to beef up the performance, simplify management, and add redundancy. Extreme Networks met the challenges with a solution of BlackDiamond 8810 chassis for core functionality and the Summit X450a/X650 with distributed stacking for the SAN/Server requirements.

Benefits realized included the following:

- **Infrastructure matched to SAN size:** An entire SAN group (16 arrays) can be serviced by two distributed stacks/virtual chassis.
- **Virtualization:** The SAN network infrastructure is virtualized like the SAN and server moves and their associated network parameters (for example, QoS, ACLs, VLANs, and so on) can be tracked and moved via the Dynamic Virtualization Mobility widget.
- **Performance:** Gigabit and 10GbE technologies are delivered today without needing a future upgrade as the SAN technology matures and very low latency ensures efficiency of iSCSI SAN traffic.
- **Server Environment:** Server traffic is distributed across the distributed stack/virtual chassis, high speed 802.1D Link Aggregation is distributed across each stack for redundancy and resiliency, and convergence grade resiliency is provided by EAPS.
- **Simplification:** Several factors also contributed toward making this a simpler solution:
  - **Infrastructure Management:** The architecture is managed as a single switch with management redundancy and the distributed stack/virtual chassis are functionally equivalent to a chassis.
  - **Infrastructure Resiliency:** The SAN communicates over the high-speed stacking backplane eliminating the requirement for a resiliency protocol (for example, spanning tree).
  - **Cable Management:** The only cables leaving a rack are the stacking cables and 10G links.

In the near future, Virtual Wonders plans to renew networking equipment at a different location. For the upcoming project, the company has chosen to consult with Extreme Networks in order to maintain a homogeneous network environment and deliver the same performance, availability, and reliability to which its networks users have grown accustomed.

Case Study D

NetScout's Approach: Network Planning and Troubleshooting

In this case study, you see how NetScout helped Dell conduct effective capacity planning and accelerate network troubleshooting. This help reduced costs and increased productivity while contributing to an improved customer experience. Chapter 3 explains more about networking hardware.

The Dell global IT network group monitors all the network traffic flowing through more than 10,000 switches, routers, load balancers, and firewalls and among the company's 83,000 employees, numerous worldwide data centers, and hundreds of thousands of customers. The group needs to ensure that traffic flows smoothly, and when it isn't, the group plays an essential role in solving any problems that develop — problems that could negatively affect worker productivity, manufacturing processes, and customer interactions.

Defining the Challenge

Dell needed to accelerate troubleshooting and facilitate effective capacity planning by deploying a robust network monitoring solution that provided detailed information about network traffic.

For several years, the Dell team used network analysis appliances along with a combination of freeware software utilities to monitor the network. But those tools provided only rudimentary network information. "Our primary software tool

could only show historical trends of network traffic volumes," says Kyle Robertson, senior network engineer at Dell. "To solve problems effectively, we needed more information on the type and volume of network traffic and the identity of the users on the network. We needed to see who was using what application, how much bandwidth they were using, and what response times they were experiencing."

Without that detailed information, troubleshooting was complex and cumbersome. "If users submitted trouble tickets about slow application performance, for example, we had to determine whether the problem was a software issue, a hardware issue, or a network issue before we could even begin to troubleshoot," says Robertson. "In some cases, it could take us a week to resolve those issues. That delay could cause a project to slip or a product shipment to be delayed."

The IT group also needed a better way to conduct network capacity planning. "You simply cannot do effective capacity planning unless you know who is using the network and how they are using it," says Robertson. "Both over-preparing and under-preparing can be costly to the business."

Evaluating a Solution

The Dell IT group evaluated several solutions for monitoring network traffic before selecting NetScout nGenius Performance Manager — an application that provides detailed network information for application and network monitoring, capacity planning, troubleshooting, fault prevention, and service-level management. nGenius Performance Manager integrates Sniffer Intelligence and Sniffer Analysis modules, analyzing packet flow information collected by NetScout nGenius Probes and InfiniStream appliances to provide a clear view of real-time and historical network and application performance.

"We tried a competing solution, but we had a terrible time trying to deploy it in our infrastructure," says Robertson. "When we evaluated the NetScout nGenius Performance Manager, the advantages were clear almost immediately. We launched it easily, and in the middle of our evaluation, we used it to solve a global application problem that might have taken us five days to resolve otherwise. We solved the problem within just 48 hours of receiving the trouble ticket."

Fixing the Problem

With help from NetScout, the Dell IT group deployed the NetScout nGenius Performance Manager solution across its global network. "The NetScout team helped us define applications, configure devices and probes, and develop methods for conducting analyses and creating reports," says Robertson. "Now we have an on-site engineer to answer questions and provide internal training. The NetScout team has been an invaluable resource."

The fact that the NetScout appliances use Dell PowerEdge servers as their hardware platform made the decision easy. "Our preference is to choose solutions that can run on Dell platforms," says Robertson. "With a Dell hardware platform, the NetScout appliances can provide the performance and reliability we need for these critical tasks."

Global solutions

To cover the entire network, Dell installed more than 150 nGenius Probes in remote locations and in Class 1 data centers in each geographic region. "We don't have IT network staff available in all of our global locations, so it can be very difficult to monitor the network in remote offices," says Robertson. "With the NetScout Probes in place, we can run a packet trace at a moment's notice and get a quick and detailed assessment of network problems. The end result is a reduction in network downtime, increased performance, and improved sustainability."

Accelerated troubleshooting

In some cases, the insight from global solutions (see preceding section) has accelerated troubleshooting by several hours. "At one point, there was a problem with the network links between two of our Asian data centers," says Robertson. "The local personnel spent about four hours troubleshooting but couldn't identify the problem. They contacted our group, and within 15 minutes, we were able to discover a single process that was consuming most of the bandwidth and saturating the links between the data centers. With access to detailed

information, we were able to resolve the issue rapidly. In this case, we spent about 90 percent less time working on the problem than the local team — and we had a much more successful result."

By facilitating effective capacity planning, NetScout can also help Dell avoid costly upgrades. "NetScout has helped us identify and eliminate non-production traffic," says Robertson. "As a result, we have been able to avoid the cost of upgrading our WAN circuits."

Specific solutions

The NetScout team helped Dell identify the specific pieces needed to implement the solutions to the problem. These pieces included

- Dell PowerEdge 2850 and R710 servers for the NetScout appliances
- NetScout nGenius Probes
- NetScout InfiniStream appliances
- NetScout nGenius Performance Manager
- NetScout Sniffer Intelligence and Sniffer Analysis modules

Case Study E

SonicWALL's Approach: Securing the 21st Century Network

As networks continue to evolve, so do security and access concerns. With the adoption of new Web 2.0 technologies and social networking, the abundance of mobile devices and the expansion of the perimeterless network, there has been a dramatic increase in the risk of threats penetrating the network. IT departments have to enable these productivity-boosting technologies while supporting new business requirements, such as telecommuting.

In this case study, you discover how a large school district implemented a SonicWALL Network Security Solution to secure the distributed enterprise, control application usage, connect remote users, and meet regulatory compliance requirements. You can find out more about firewalls in Chapter 5.

A Real Challenge

Serving the Little Rock, Arkansas metropolitan area, the Pulaski County Special School District (PCSSD) is an innovative education system dedicated to ensuring academic excellence for nearly 18,000 students. The district supports approximately 1,500 teachers and administrators at over 40 separate sites.

Their challenge was multi-faceted. Being an education institution, they needed best-in-class threat protection to secure their distributed network. They also needed to manage multiple firewalls and report on any security incidents for compliance purposes. Another issue was the student community was draining valuable bandwidth by accessing social media, video, and music sites. Finally, they needed to give anytime, anywhere remote access to the staff so they could connect to critical data and network resources. All of this had to be achieved without increasing IT staff or affecting network performance.

A Solution that Passed the Test

For comprehensive threat protection across the distributed network, PCSSD implemented a series of SonicWALL Network Security Appliances that delivered integrated Enforced Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Firewall technology.

The VPN features built into the firewall secured not only inbound traffic but also site-to-site VPN traffic between administrative offices and schools. The powerful application firewall enabled the district to control student access to inappropriate, time-wasting, and bandwidth draining Web sites and applications.

To manage security over the district's distributed network, the district uses the Global Management System. The GMS lets them manage over 40 SonicWALL appliances distributed at over 40 locations across 730 square miles. They're able to push firmware updates, back up configuration files, and manage each appliance and all their feature sets from one console. The GMS also provides a centralized reporting database that documents all firewall activity for regulatory compliance. The capability of managing all the firewalls from one console is priceless and saves countless staff hours.

Their business need for secure telecommuting was met with a SonicWALL Secure Remote Access (SRA) solution, allowing staff to access files when at home or out at conferences. Because this solution didn't require installation of software on remote computers, it lessened the load on support and provided them with a secure, easy-to-use means of access.

The SonicWALL Aventail SRA E-Class EX-1600 made sure any remote device had the latest updated protection before letting the user on the SSL VPN. And end-users see an easy interface that makes their desktop look like they're at work, without having to load extra applications or get IT help. Now IT managers just point users to a Web portal, and they can safely link to all the resources they need. It's letting them sleep a little better at night knowing they're secure.

The combination of the Network Security Appliance and the Secure Remote Access Solution produced a Clean VPN environment where all inbound traffic was scanned before entering the network, greatly improving their security. With this they could even apply the same inbound and outbound firewall features as if their users were on the local network.

Said Jimmy Hogg, Assistant Director of Network and Computer Operations, "I would definitely recommend SonicWALL solutions. The EX-1600 in particular worked very well for us, was very user friendly, and was up and running quickly without problems."

The Right Investment

In response to PCSSD's unique security needs, Mr. Hogg successfully addressed these issues with SonicWALL solutions, by adding a SonicWALL E-Class Network Security Appliance (NSA) E6500, a SonicWALL Aventail Secure Remote Access E-Class EX-1600, and a SonicWALL Global Management System (GMS) solution to their existing deployment of SonicWALL PRO and NSA Series firewalls.

- **SonicWALL E-Class Network Security Appliance (NSA) E6500:** This product is engineered to combat the evolving threats to the enterprise network by providing administrators with a high performance, scalable, multifunction threat prevention appliance. The NSA E6500 combines parallel traffic processing with SonicWALL's Reassembly free Deep Packet Inspection engine, which prevents viruses, prevents attacks/intrusions, does firewalling, anti-virus, anti-spyware, VPN functionality and content filtering.

- **SonicWALL Aventail E-Class Secure Remote Access (SRA) EX-1600:** SonicWALL Aventail E-Class SRAs provide complete application access with full security, control of the end point, and unified policy management. Easy to use and control, SonicWALL Aventail E-Class SRAs increase productivity by providing employees and partners with secure, clientless access to the resources they need from any device, anywhere, with unmatched security.
- **SonicWALL Global Management System (GMS):** The SonicWALL Global Management System (GMS) provides organizations, distributed enterprises, and service providers with a flexible, powerful, and intuitive solution to centrally manage and rapidly deploy SonicWALL appliances and security policy configurations. SonicWALL GMS also provides centralized real-time monitoring, and comprehensive policy and compliance reporting.

For the future, the district will be evaluating SonicWALL SonicPoint wireless access points for a Clean Wireless deployment. They are also considering other SonicWALL solutions to back up mobile laptops used by senior staff members and looking into SonicWALL Email Security.

Everyone seems happy with the solution except possibly those students who haven't found a way to bypass the security systems. Oh well, who says you have to please everyone?

Notes

Notes

Implement solutions that may save the day!

Do you and your company need to get a better understanding of networking basics?

Then this book is for you! Discover networking tricks of the trade and study five different case studies from some of Dell's Preferred Enterprise Partners — describing how they make networking and security work in a variety of environments. *Getting Started with Networking and Security For Dummies,* A Special Edition from Dell and Its Preferred Enterprise Partners, helps you on your way to being better connected.

Discover how to:

- *Handle network needs of your business*
- *Understand your network consultant*
- *Figure out the business networking basics*
- *Analyze real case studies in action*

THE DUMMIES WAY®

- *Explanations in plain English*
- *"Get in, get out" information*
- *Icons and other navigational aids*
- *Top ten lists*
- *A dash of humor and fun*

Get smart! @ www.dummies.com

- *Find listings of all our books*
- *Choose from many different subject categories*
- *Sign up for eTips at etips.dummies.com*

ISBN: 978-0-470-61507-2
Not resalable

For Dummies®
A Branded Imprint of
WILEY