chapter 12

Advanced Networking Devices

"It followed from the special theory of relativity that mass and energy are both but different manifestations of the same thing. A somewhat unfamiliar conception for the average mind."

—Albert Einstein

In this chapter, you will learn how to

- **Discuss the four logical topologies as defined by CompTIA**
- **Configure and deploy VLANs**
- **Implement advanced switch features**

As we delve deeper into the world of networking in this book, the protocols and standards get more complex, but all of the hardware has stayed pretty much constant. Up to this point, we've dealt with nothing more than hubs, switches, and routers. The beauty of these three devices is that you can look at any one of them and instantly say at what layer of the OSI seven-layer model it operates. Hubs work at Layer 1, switches work at Layer 2, and routers work at Layer 3. Life is good, but a bit simplistic, because most of today's networking boxes take on more than one OSI layer.

Historical/Conceptual

Let's take a typical home router as an example. My router at home is really two devices in one: a four-port switch and a router. When you combine these features into a single box, you have more than just a switch and a router. By working together as a single piece of hardware, these features can do some truly amazing things that a single, separate switch connected to a single, separate router simply cannot do. This combination of features transforms a little home router into an advanced device that works at multiple layers of the OSI seven-layer model. It's not truly accurate to even call my little home router a router. Calling it a **multilayer switch** at least gives people a clue that it's more than just a router and a switch in the same box.

The world is filled with multilayer switches. These switches do hundreds of different jobs, and this chapter is designed to show you some examples of the jobs multilayer switches do so you can appreciate how and why we use them in the majority of networks.

To learn about these devices, you need to first understand the concept of what CompTIA calls logical network topologies—the way in which the many systems on a network are organized to send data between each other. Then I'll go into great detail about one of the four logical network topologies, VLAN, to demonstrate why any serious network uses this powerful feature (with the help of advanced switches) to administer a network. Last, I will give you a tour of a number of unique advanced devices, using the OSI seven-layer model as a tool to organize them.

Logical Network Topologies

Recall from Chapter 3, "Cabling and Topology," that the term "physical topology" describes the physical layout of the cabling and the term "signaling topology" refers to how the signals actually progress through the network. A star-bus topology, for example, has a physical star but a logical bus. These two terms work well for describing how data moves about a network—as long as you're working with a single broadcast domain. Just in case you don't remember your broadcast domains, let's do a quick review. Imagine a simple network with some number of computers connected to a single switch. When you send a piece of data to another single computer (a unicast), the switch creates a direct connection. When you send a broadcast message, every computer on the network receives the message (Figure 12.1).

Cross Check

Broadcast Domains and CSMA/CD

You learned about broadcast domains and the trouble with CSMA/CD back in Chapter 4, "Ethernet Basics," so check your memory now—or glance back at that chapter—to answer these questions. What function does CSMA/CD serve in an Ethernet network? How do collisions manifest within a single broadcast domain? What about between two broadcast domains? How does a switch affect things?

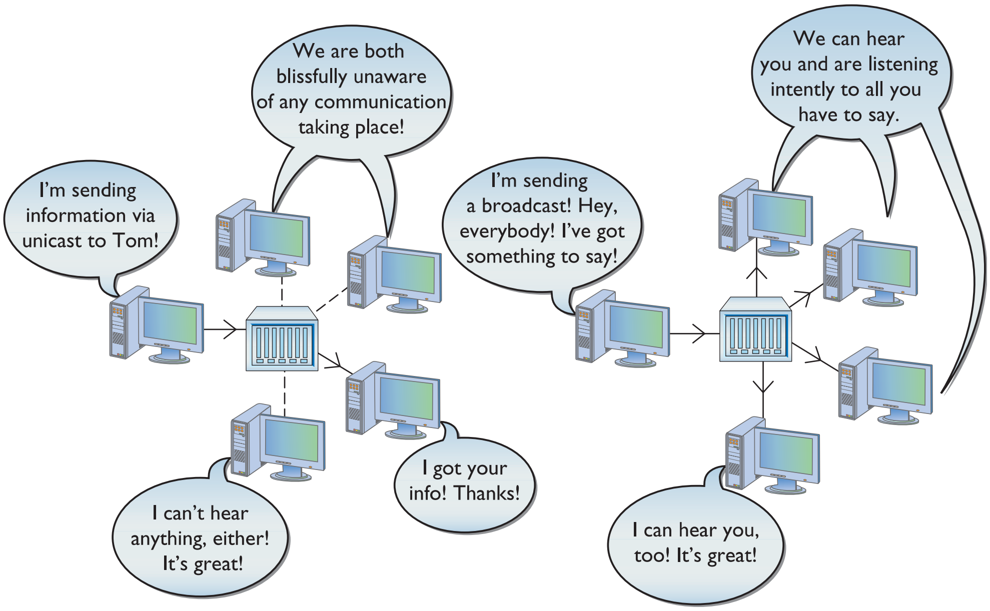

I'm sending information via unicast to Tom!
We are both blissfully unaware of any communication taking place!
I can't hear anything, either! It's great!
I got your info! Thanks!
I'm sending a broadcast! Hey, everybody! I've got something to say!
We can hear you and are listening intently to all you have to say.
I can hear you, too! It's great!

Figure 12.1 Unicast (left) and broadcast (right)

Tech Tip

CompTIA Terminology

While your humble author loves CompTIA, I need to warn you: outside of the CompTIA Network+ exam objectives, I don't think you'll ever see or hear these four terms lumped together: client/server, peer-to-peer, VPN, and VLAN. For the most part, the CompTIA Network+ exam objectives follow real-world terminology and examples, but lumping together this terminology is just a touch off the mark.

Routers block broadcasts and are used to connect broadcast domains. Figure 12.2 shows two broadcast domains separated by a single router.

But we're about to add some really interesting advanced features to your routers and switches, giving them the power to do things that go beyond the types of topologies thus far discussed. So we now need to talk about four topologies that go beyond the description of either physical or signaling topologies: peer-to-peer, client/server, VPN, and VLAN. CompTIA uses the name "logical network topologies" for these topologies.

CompTIA may like to use the term "logical network topologies" but the more common term heard out in the real world, at least to describe client/server and peer-to-peer, is "software architecture model." In common use, the terms refer to the role computers play in a network, as in which computers act as servers and which computers act as clients. I have some strong feelings about these terms—read on and see.

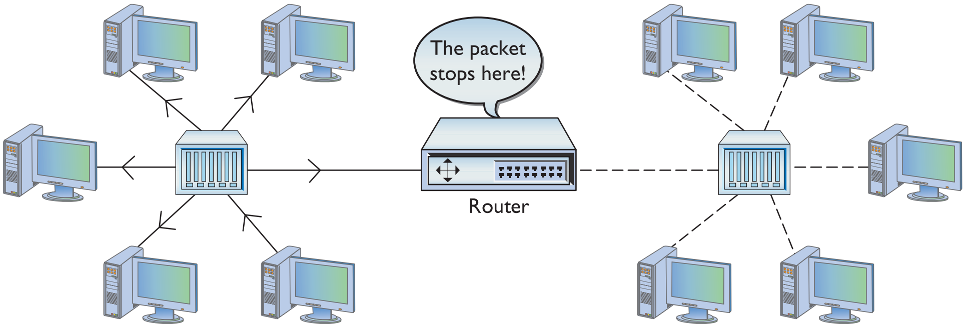
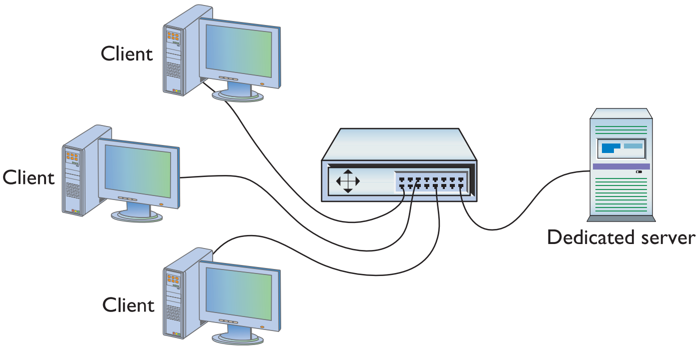


Figure 12.2 Two broadcast domains

Test Specific

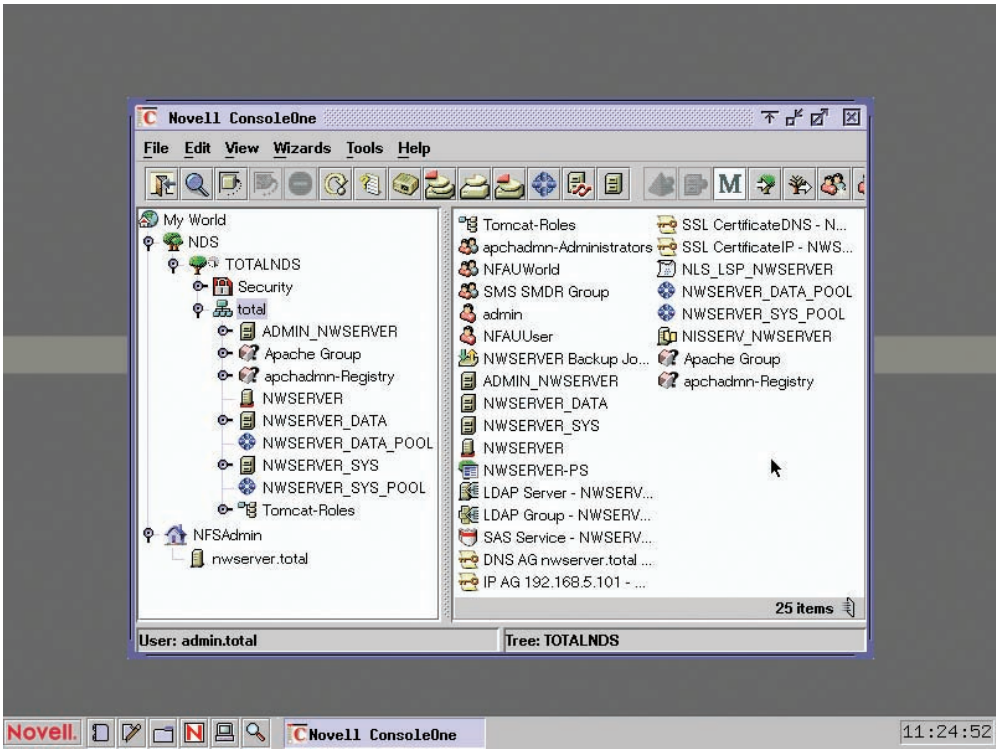
Client/Server



• **Figure 12.3** A simple client/server network

The earliest networks used a **client/server** model. In that model, certain systems acted as dedicated servers. Dedicated servers were called "dedicated" because that's all they did. You couldn't go up to a dedicated server and run Word or Solitaire. Dedicated servers ran powerful server network operating systems that offered up files, folders, Web pages, and so on to the network's client systems. Client systems on a client/server network never functioned as servers. One client system couldn't access shared resources on another client system. Servers serve and clients access, and never the twain shall . . . cross over . . . in the old days of client/server! Figure 12.3 shows a typical client/server network. As far as the clients are concerned, the only system on the network is the server system. The clients cannot see each other nor can they share data with each other directly. They must save the data on the server so that other systems can access it.

Back in the old days there was an operating system called Novell NetWare. Novell NetWare servers were true dedicated servers. You couldn't go up to a Novell NetWare server and write yourself a resume; there was no Windows, there were no user applications. The only thing Novell NetWare servers knew how to do was share their own resources, but they shared those resources extremely well! The Novell NetWare operating system was unique. It wasn't Windows, Macintosh, or Linux. It required you to learn an entirely different set of installation, configuration, and administration commands. Figure 12.4 shows a screen from Novell NetWare. Don't let the



User: admin.total

Tree: TOTALNDS

• **Figure 12.4** Novell NetWare in action passing resemblance to Windows fool you—it was a completely different operating system!

Dedicated servers enabled Novell to create an entire feature set not seen before on personal computers. Each dedicated server had its own database of user names and passwords. You couldn't access any of the resources on the server without logging in. The server's administrator would assign "permissions" to a specific user account, such as Write (add files to a directory), File Scan (see the contents of a directory), and Erase (delete files).

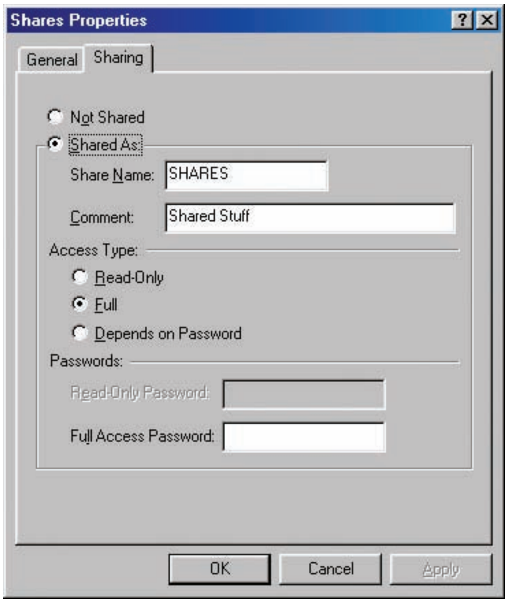
By keeping the server functionality separate from the client systems, the Novell folks made very powerful, dedicated servers without overwhelming the client computers with tons of software. (This was, after all, in the early days of personal computers and they didn't have anything near the power of a modern PC!) NetWare servers had tremendous power and great security because the only thing they did was run serving software. In the early days of networking, client/server was king!

Peer-to-Peer

Novell NetWare was the first popular way to network PCs, but it wasn't too many years later that Microsoft introduced the first versions of network-capable Windows. The way in which these versions of Windows looked at networking, called peer-to-peer, was completely different from the client/server view of networking. In a **peer-to-peer** network, any system acts as a server, a client, or both, depending on how you configure that system. PCs on peer-to-peer networks frequently act as both clients and servers. One of the most common examples of a peer-to-peer network is the venerable Windows 9*x* series of operating systems. Figure 12.5 shows the sharing options for the ancient Windows 98 operating system, providing options to share a folder and thus turn that computer into a server.

At first glance, it would seem that peer-to-peer is the way to go—why create a network that doesn't allow the clients to see each other? Wouldn't it make more sense to give users the freedom to allow their systems to both share and access any resource? The problem was a lack of security.

The early Windows systems did not have user accounts and the only permissions were Read Only and Full Control. So they made it easy to share, but hard to control access to, the shared resources. People wanted the freedom of peer-to-peer with the security of client/server.



Shares Properties

○ Not Shared
● Shared As:
Share Name: SHARES
Comment: Shared Stuff
Access Type:
○ Read-Only
● Full
○ Depends on Password
Passwords:
Read-Only Password:
Full Access Password:

• **Figure 12.5** Sharing options in Windows 98

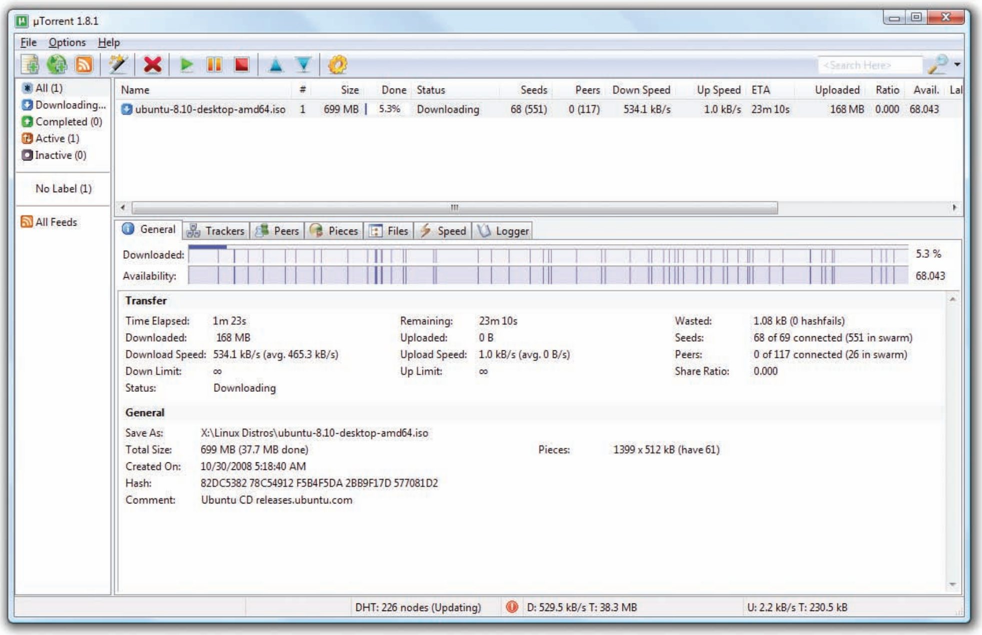
The "old school" client/server model means dedicated servers with strong security. Clients only see the server. In the peer-to-peer model, any system is a client, server, or both, but at the cost of lower security and additional demands on the system resources of each peer.

Client/Server and Peer-to-Peer Today

In response to demand, every modern operating system has dumped the classic client/server or peer-to-peer label. Windows, Linux, and Macintosh all have the capability to act as a server or a client while also providing robust security through user accounts and permissions and the like.

So why learn about classic client/server and peer-to-peer? Because CompTIA wants you to. Since the widespread adoption of TCP/IP and the Internet, however, client/server and peer-to-peer have taken on new or updated definitions, and refer more to applications than to network operating systems. Consider e-mail for a moment. For traditional e-mail to work, you need an e-mail client like Microsoft Outlook. But you also need an e-mail server program like Microsoft Exchange to handle the e-mail requests from your e-mail client. Outlook is a *dedicated client*—you cannot use the Outlook client as a mail-serving program. Likewise, you cannot use Microsoft Exchange as an e-mail client. Exchange is a *dedicated server* program.

Peer-to-peer applications, often referred to simply as P2P, act as both client and server. The best examples of these applications are the now infamous file-sharing applications based on special TCP/IP protocols. The applications, with names like BitTorrent, LimeWire, and DC++, act as both clients and servers, enabling a user both to share files and access shared files. BitTorrent is actually an entire protocol, not just a particular application. There are many different applications that use the BitTorrent standard. Figure 12.6 shows one such program, µTorrent, in the process of simultaneously uploading and downloading files.



Name	#	Size	Done	Status	Seeds	Peers	Down Speed	Up Speed	ETA	Uploaded	Ratio	Avail.	Lal
ubuntu-8.10-desktop-amd64.iso	1	699 MB	5.3%	Downloading	68 (551)	0 (117)	534.1 kB/s	1.0 kB/s	23m 10s	168 MB	0.000	68.043	

Downloaded: 5.3 %
Availability: 68.043

Transfer

Time Elapsed: 1m 23s
Downloaded: 168 MB
Download Speed: 534.1 kB/s (avg. 465.3 kB/s)
Down Limit: ∞
Status: Downloading
Remaining: 23m 10s
Uploaded: 0 B
Upload Speed: 1.0 kB/s (avg. 0 B/s)
Up Limit: ∞
Wasted: 1.08 kB (0 hashfails)
Seeds: 68 of 69 connected (551 in swarm)
Peers: 0 of 117 connected (26 in swarm)
Share Ratio: 0.000

General

Save As: X:\Linux Distros\ubuntu-8.10-desktop-amd64.iso
Total Size: 699 MB (37.7 MB done)
Created On: 10/30/2008 5:18:40 AM
Hash: 82DC5382 78C54912 F5B4F5DA 2BB9F17D 577081D2
Comment: Ubuntu CD releases.ubuntu.com
Pieces: 1399 x 512 kB (have 61)

DHT: 226 nodes (Updating)
D: 529.5 kB/s T: 38.3 MB
U: 2.2 kB/s T: 230.5 kB

Figure 12.6 µTorrent downloading an Ubuntu release

Talking about client/server or peer-to-peer when discussing classic networks or modern networking applications is great, but we can extend the idea of logical network topologies beyond the simple notions of client/server and peer-to-peer. Advanced networking devices enable the development of networks of amazing complexity, security, and power: virtual private networks and virtual LANs.

VPN

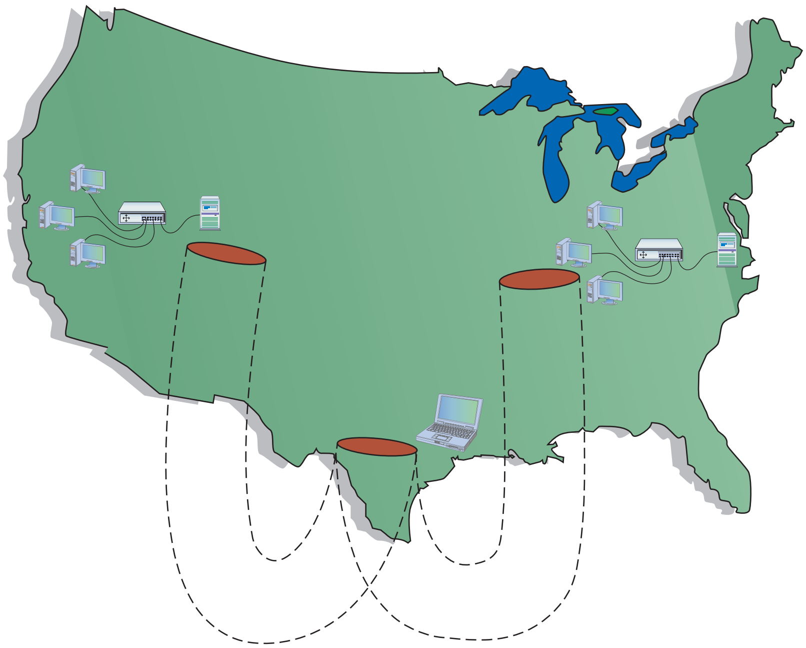
Remote connections have been around for a long time, long before the Internet existed. The biggest drawback about remote connections was the cost to connect. If you were on one side of the continent and had to connect to your LAN on the other side of the continent, the only connection option was a telephone. Or, if you needed to connect two LANs across the continent, you ended up paying outrageous monthly charges for a private connection. The introduction of the Internet gave people wishing to connect to their home networks a very cheap connection option, but there was one problem—the whole Internet is open to the public. People wanted to stop using dial-up and expensive private connections and use the Internet instead, but they wanted to be able to do it securely.

If you read the previous chapter, you might think we could use some of the tools for securing TCP/IP to help: and you would be correct. Several standards, many based on the Point-to-Point Protocol (PPP), have been created that use encrypted tunnels between a computer (or a remote network) and a private network through the Internet (Figure 12.7), resulting in what is called a **Virtual Private Network (VPN)**.

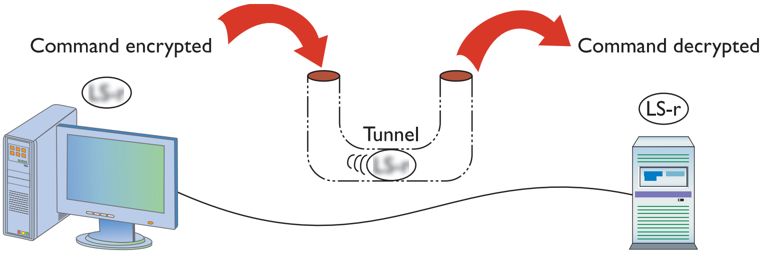
As you saw in the previous chapter, an encrypted tunnel requires endpoints—the ends of the tunnel where the data is encrypted and decrypted. In the tunnels you've seen thus far, the client for the application sits on one end and the server sits on the other. VPNs do exactly the same thing. Either some software running on a computer or, in some cases, a dedicated box must act as an endpoint for a VPN (Figure 12.8).

The key with the VPN is that all of the computers should be on the same network—and that means they must all have the same network ID. For example, you would want the laptop that you are using in an airport lounge to have the same network ID as all of your computers in your LAN back at the office. But there's no simple way to do this. If it's a single client trying to access a network, that client is going to take on the IP address from its local DHCP server. In the case of your laptop in the airport, your network ID and IP address come from the DHCP server in the airport, not the DHCP server back at the office.

If we are trying to connect two networks, we could make them each take on a subnet from a single network ID, but that creates all kinds of administrative issues (Figure 12.9).

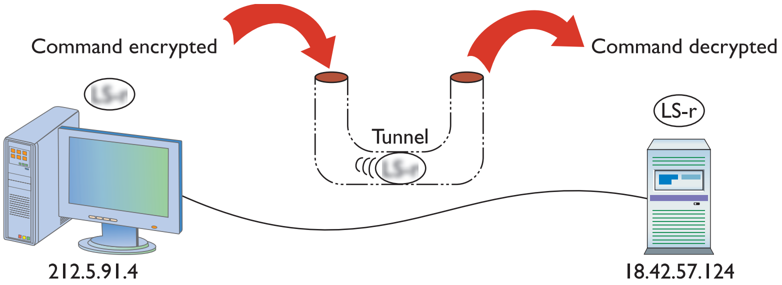


• **Figure 12.7** VPN connecting computers across the United States



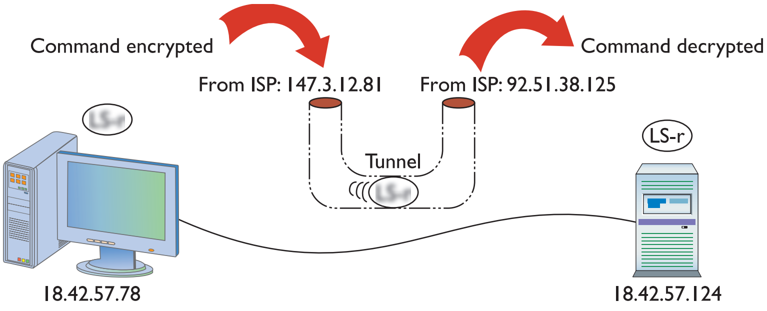
• **Figure 12.8** Typical tunnel

To make the VPN work, we need a protocol that will use one of the many tunneling protocols available but add the ability to query for an IP address from a local DHCP server to give the tunnel an IP address that matches the subnet of the local LAN. The connection will keep the IP address to connect



• **Figure 12.9** How do we get the same network IDs?

to the Internet but the tunnel endpoints must act like they are NICs (Figure 12.10). Two protocols fit our needs, PPTP and L2TP.



• Figure 12.10 Endpoints must have their own IP addresses.

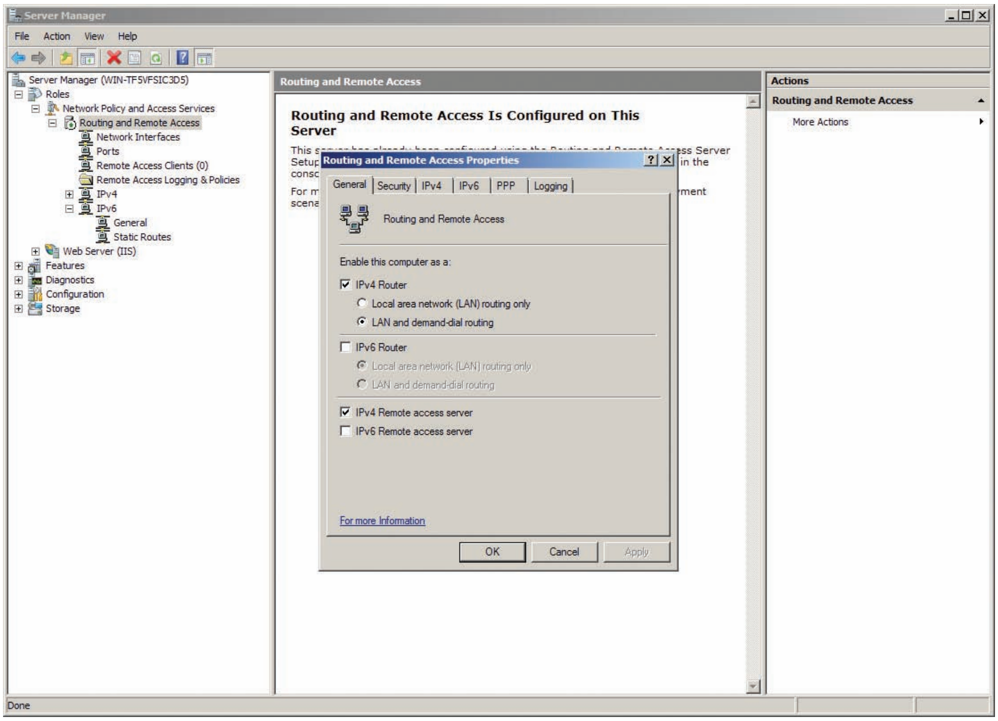
PPTP VPNs

So how do we make IP addresses appear out of thin air? What tunneling protocol have we learned about that has the smarts to query for an IP address? That's right! Good old PPP! Microsoft got the ball rolling with the **Point-to-Point Tunneling Protocol (PPTP)**, an advanced version of PPP that handles all this right out of the box. The only trick is the endpoints. In Microsoft's view, a VPN is intended for individual clients to connect to a private network, so Microsoft places the PPTP endpoints on the client and a special remote access server program, originally only available on Windows Server, called **Routing and Remote Access Service (RRAS)** on the server—see Figure 12.11.

On the Windows client side, you run Create a New Connection. This creates a virtual NIC that, like any other NIC, does a DHCP query and gets an IP address from the DHCP server on the private network (Figure 12.12).

When your computer connects to the RRAS server on the private network, PPTP creates a secure tunnel through the Internet back to the private LAN. Your client takes on an IP address of that network, as if your computer is directly connected to the LAN back at the office, even down to the default

A system connected to a VPN looks as though it's on the local network, but performs much slower than if the system was connected directly back at the office.



Routing and Remote Access Is Configured on This Server

This s… ss Server Setup … in the consc…

For m… ment scena…

Routing and Remote Access Properties

Routing and Remote Access

Enable this computer as a:

☑ IPv4 Router
○ Local area network (LAN) routing only
● LAN and demand-dial routing

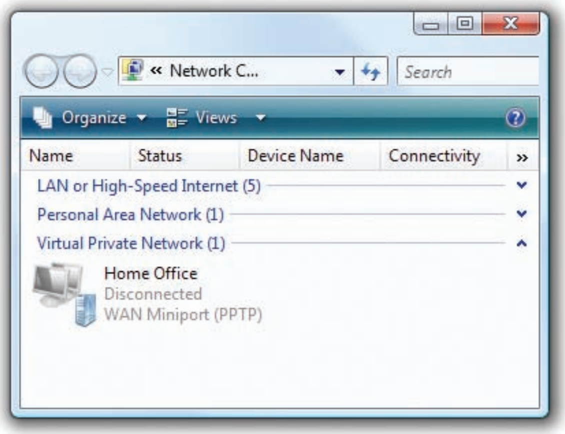
☐ IPv6 Router
● Local area network (LAN) routing only
○ LAN and demand-dial routing

☑ IPv4 Remote access server
☐ IPv6 Remote access server

• Figure 12.11 RRAS in action

gateway. If you open your Web browser, your client will go across the Internet to the local LAN and then use the LAN's default gateway to get to the Internet! Using a Web browser will be much slower when you are on a VPN.

PPTP VPNs are very popular. Every operating system comes with some type of built-in VPN client that supports PPTP (among others). Figure 12.13 shows Network, the Macintosh OS X VPN connection tool.



LAN or High-Speed Internet (5)

Personal Area Network (1)

Virtual Private Network (1)

Home Office
Disconnected
WAN Miniport (PPTP)

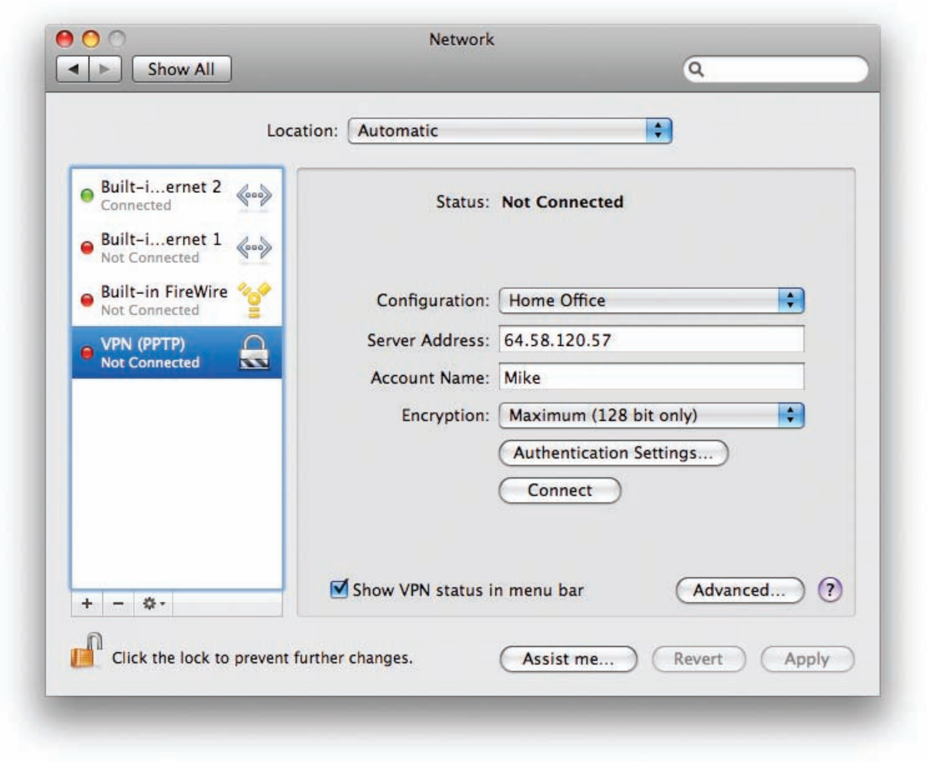
• Figure 12.12 VPN connection in Windows

L2TP VPNs

Microsoft pushed the idea of a single client tunneling into a private LAN using software. Cisco, being the router king that it is, came up with its own VPN protocol called **Layer 2 Tunneling Protocol (L2TP)**. L2TP took all the good features of PPTP and added support to run on almost any type of connection possible, from telephones to Ethernet to ultra-high-speed optical connections. Cisco also moved the endpoint on the local LAN from a server program to a VPN-capable router, called a **VPN concentrator**, such as the Cisco 2811 Integrated Services Router shown in Figure 12.14.

Cisco provides free client software to connect a single faraway PC to a Cisco VPN. Network people often directly connect two Cisco VPN concentrators to permanently connect two separate LANs. It's slow but it's cheap compared to a dedicated high-speed connection between two faraway LANs.

L2TP differs from PPTP in that it has no authentication or encryption. L2TP usually uses IPSec for all the security needs. Technically, you should call an L2TP VPN an "L2TP/IPSec" VPN.



Location: Automatic

Status: Not Connected

Configuration: Home Office

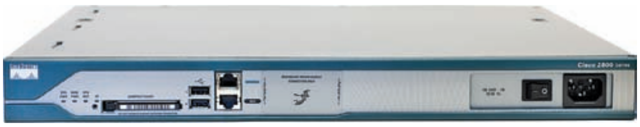
Server Address: 64.58.120.57

Account Name: Mike

Encryption: Maximum (128 bit only)

☑ Show VPN status in menu bar

• Figure 12.13 VPN on a Macintosh OS X system



• Figure 12.14 Cisco 2811 Integrated Services Router

L2TP works perfectly well in the single-client-connecting-to-a-LAN world, too. Every operating system's VPN client fully supports L2TP/IPSec VPNs.

Over the years there's been plenty of crossover between Microsoft and Cisco. Microsoft RRAS supports L2TP and Cisco routers support PPTP.

Alternatives to PPTP and L2TP

The majority of VPNs use either PPTP or L2TP. There are other options, some of them quite popular. First is OpenVPN, which, like the rest of what I call "OpenXXX" applications, uses Secure Shell (SSH) for the VPN tunnel. Second is IPSec. We are now seeing some pure (no L2TP) IPSec solutions that use IPSec tunneling for VPNs.

VLAN

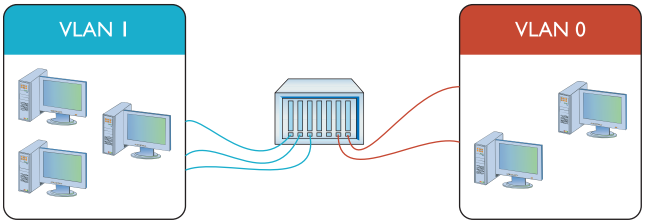
The last of CompTIA's logical network topologies is known as a **Virtual Local Area Network (VLAN)**. It's hard to find anything but the smallest of LANs today that do not use VLANs. VLANs are so important and so common that we need to spend a serious amount of time discussing them and how they work. Let's take some time to dive deeply into VLANs.

VLAN in Depth

Today's LANs are complex places. It's rare to see any serious network that doesn't have remote incoming connections, public Web or e-mail servers, and wireless networks as well as the basic string of connected switches. Leaving all of these different features on a single broadcast domain creates a tremendous amount of broadcast traffic and creates a security nightmare. You could separate the networks with multiple switches and put routers in between but that's very inflexible and hard to manage. What if you could segment the network using the switches you already own? You can, and that's what a VLAN enables you to do.

Creating a VLAN means to take a single physical broadcast domain and chop it up into multiple virtual broadcast domains. VLANs require special switches loaded with extra programming to create the virtual networks.

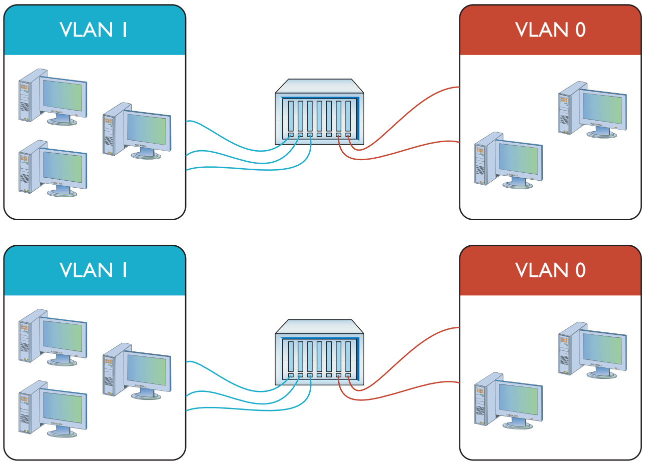
Imagine a single switch with a number of computers connected to it. Up to this point a single switch is always a single collision domain, but that's about to change. We've decided to take this single switch and turn it into two VLANs. VLANs typically get the name "VLAN" plus a number, like VLAN1 or VLAN275. We usually start at 0, though there's no law or rules on the numbering. We'll configure the ports on our single switch to be in one of two VLANs, VLAN0 or VLAN1 (Figure 12.15). I promise to show you how to configure ports for different VLANs shortly, but we've got a couple of other concepts to hit first.



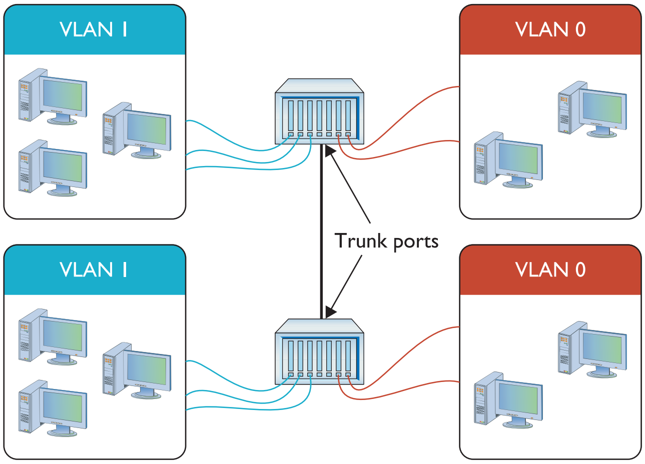
• Figure 12.15 Switch with two VLANs

Figure 12-15 shows a switch configured to assign individual ports to VLANs, but VLANs use more than just ports to define different VLANs. A VLAN might use the computer's MAC addresses to determine VLAN membership. A computer in this type of VLAN is always a member of the same VLAN no matter what port on the switch into which you plug the computer.

A single switch configured into two VLANs is the simplest form of VLAN possible. More serious networks usually have more than one switch. Let's say you added a switch to our simple network. You'd like to keep VLAN0 and VLAN1 but use both switches. You can configure the new switch to use VLAN0 and VLAN1, but you've got to enable data to flow between the two switches, regardless of VLAN. That's where trunking comes into play.



• Figure 12.16 Two switches, each with a VLAN0 and a VLAN1



• Figure 12.17 Trunk ports

Trunking

Trunking is the process of transferring VLAN data between two or more switches. Imagine two switches, each configured with a VLAN0 and a VLAN1, as shown in Figure 12.16.

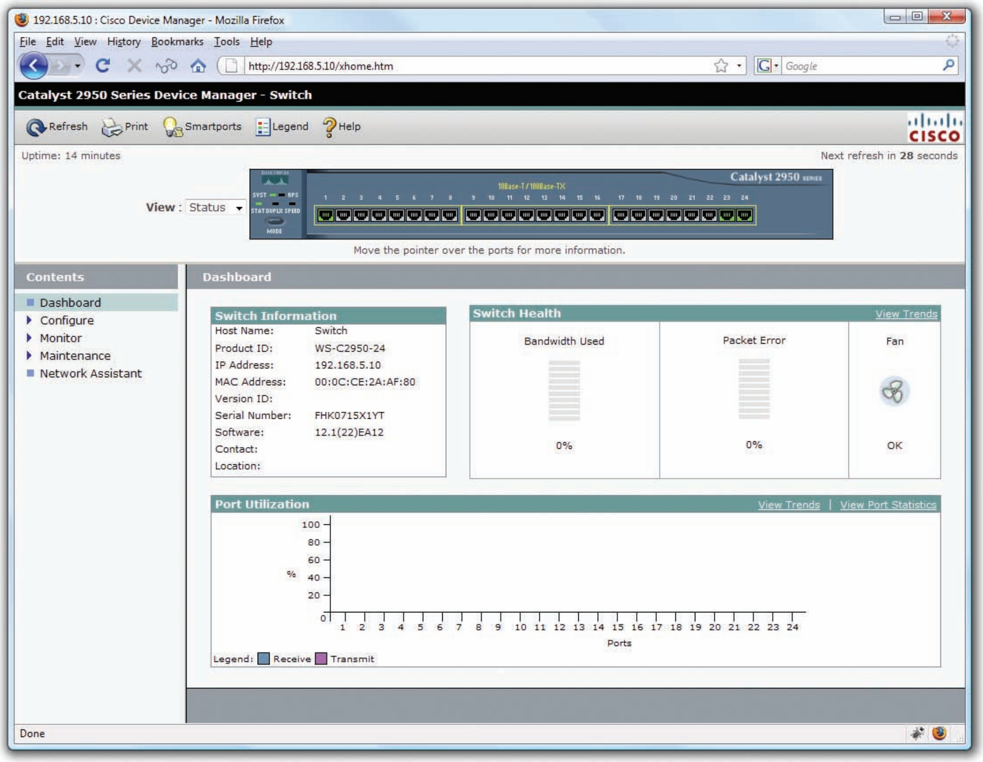
We want all of the computers connected to VLAN0 on one switch to talk to all of the computers connected to VLAN0 on the other switch. Of course we want to do this with VLAN1 also. To do this, a port on each switch must be configured as a **trunk port.** A trunk port is a port on a switch configured to carry all data, regardless of VLAN number, between all switches in a LAN (Figure 12.17).

In the early days of VLANs, every switch manufacturer had its own way to make VLANs work. Cisco, for example, had a proprietary form of trunking called Inter-Switch Link (ISL), which most Cisco switches still support. Today, every Ethernet switch prefers the IEEE 802.1Q trunk standard, enabling you to connect switches from different manufacturers.

Configuring a VLAN-capable Switch

If you want to configure a VLAN-capable switch, you must have a method to do that configuration. One method used to configure some switches is to use a serial port like the one described earlier in the book, but the most common method is to make the switch a Web server, like the one shown in Figure 12.18. Catalyst is a model name for a series of popular Cisco routers with advanced switching features. Any switch that you can access and configure is called a managed switch.

So if you're giving the switch a Web page, that means the switch needs an IP address—but don't switches use MAC addresses? They do, but managed switches also come with an IP address for configuration. A brand-new managed switch out of the box invariably has a preset IP address similar to the preset, private IP addresses you see on routers. This IP address isn't for any of the individual ports, but rather is for the whole switch. That means no matter where



Uptime: 14 minutes

Next refresh in 28 seconds

View : Status

Host Name: Switch
Product ID: WS-C2950-24
IP Address: 192.168.5.10
MAC Address: 00:0C:CE:2A:AF:80
Version ID:
Serial Number: FHK0715X1YT
Software: 12.1(22)EA12
Contact:
Location:

Bandwidth Used	Packet Error	Fan
0%	0%	OK

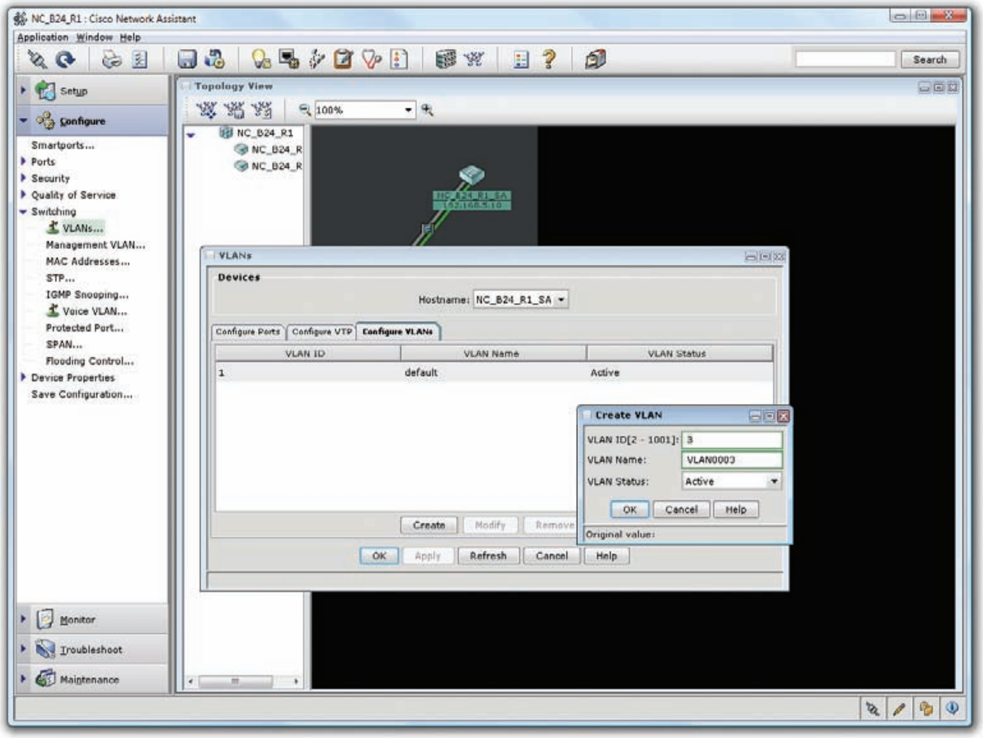
Legend: ▨ Receive ▨ Transmit

• Figure 12.18 Catalyst 2950 Series Device Manager

you physically connect to the switch, the IP address to get to the configuration screen is the same.

Every switch manufacturer has its own interface for configuring VLANs, but the interface shown in Figure 12.19 is a classic example. This is Cisco Network Assistant, a very popular tool that enables you to configure multiple devices through the same interface. Note that you first must define your VLANs.

After you create the VLANs, you usually either assign computers' MAC addresses to VLANs or assign ports to VLANs. Assigning MAC addresses means that no

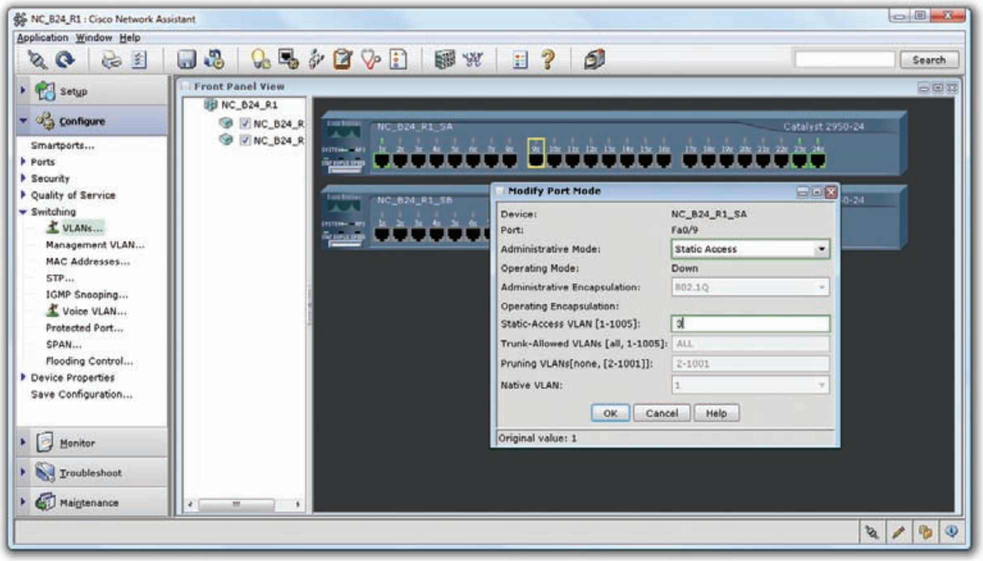


Hostname: NC_B24_R1_SA

VLAN ID	VLAN Name	VLAN Status
1	default	Active

VLAN ID[2 - 1001]: 3
VLAN Name: VLAN0003
VLAN Status: Active
Original value:

• Figure 12.19 Defining VLANs in Cisco Network Assistant

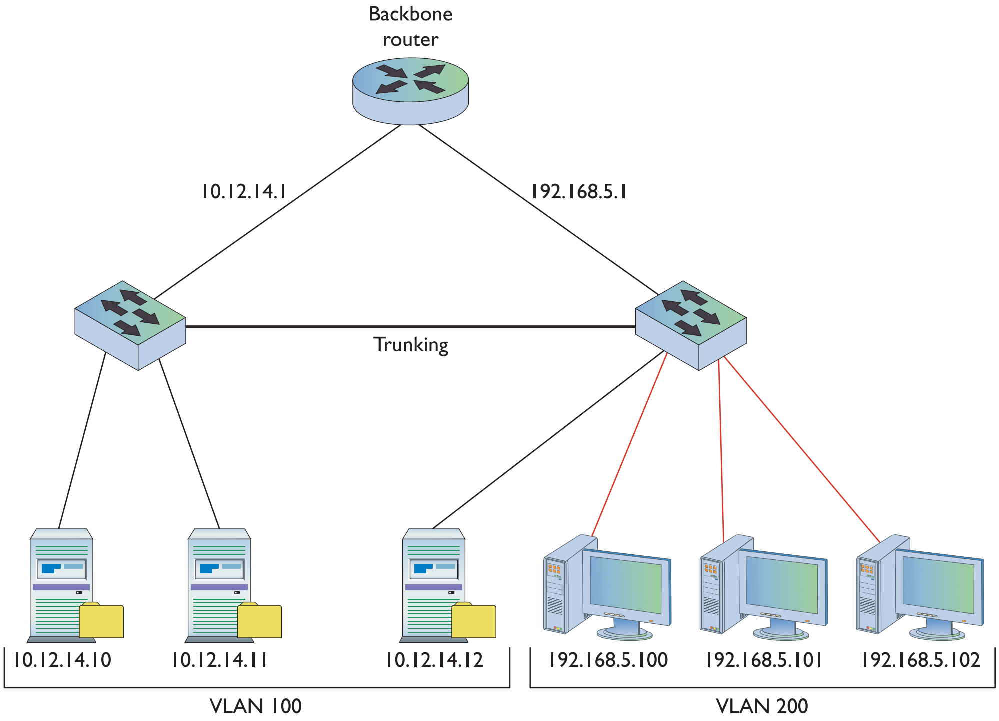


Device: NC_B24_R1_SA
Port: Fa0/9
Administrative Mode: Static Access
Operating Mode: Down
Administrative Encapsulation: 802.1Q
Operating Encapsulation:
Static-Access VLAN [1-1005]: 3
Trunk-Allowed VLANs [all, 1-1005]: ALL
Pruning VLANs[none, [2-1001]]: 2-1001
Native VLAN: 1
Original value: 1

• Figure 12.20 Assigning a port to a VLAN

matter where you plug in a computer, it is always part of the same VLAN—a very handy feature when you physically move a computer! Assigning each port to a VLAN means that whatever computer plugs into that port, it will always be a member of that port's VLAN. Figure 12.20 shows a port being assigned to a particular VLAN.

VLANs based on ports are the most common type of VLAN and are commonly known as static VLANs. VLANs based on MAC addresses are called dynamic VLANs.



• Figure 12.21 One router connecting multiple VLANs

InterVLAN Routing

Once you've configured a switch to support multiple VLANs, each VLAN is its own broadcast domain, just as if the two VLANs were on two completely separate switches. There is no way for data to get from one VLAN to another unless you use a router. In the early days of VLANs it was common to use a router with multiple ports as a backbone for the network. Figure 12.21 shows one possible way to connect two VLANs with a single router.

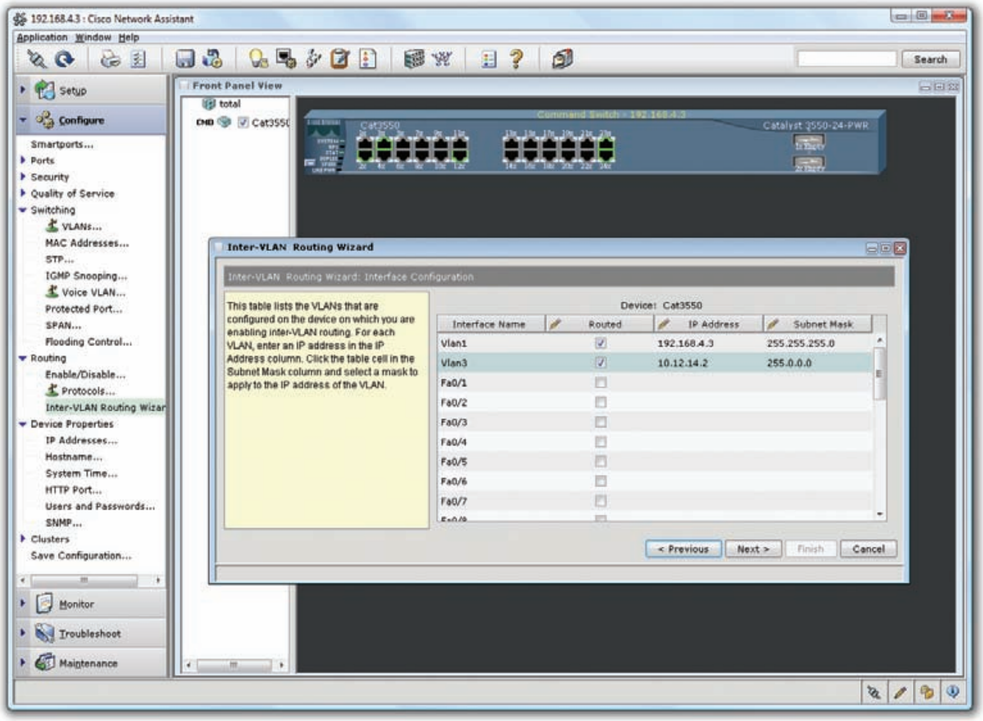
Adding a physical router like this isn't a very elegant way to connect

VLANs. This forces almost all traffic to go through the router, and it's not a very flexible solution if you want to add more VLANs in the future. As a result, all but the simplest VLANs have at least one very special switch that has the ability to make virtual routers. Cisco calls this feature **interVLAN routing**. Figure 12.22 shows an older but very popular interVLAN routing–capable switch, the Cisco 3550.

• **Figure 12.22** Cisco 3550

From the outside, the Cisco 3550 looks like any other switch. On the inside, it's an incredibly powerful and flexible device that not only supports VLANs, but also enables you to create virtual routers to interconnect these VLANs. Figure 12.23 shows the configuration screen for the 3550's interVLAN routing between two VLANs.

If the Cisco 3550 is a switch but also has built-in routers, on what layer of the OSI seven-layer model does it operate? If it's a switch, then it works at Layer 2. But it also has the capability to create virtual routers, and routers work at Layer 3. This isn't an ordinary switch. The Cisco 3550 works at both Layers 2 and 3 at the same time.



Inter-VLAN Routing Wizard: Interface Configuration

This table lists the VLANs that are configured on the device on which you are enabling inter-VLAN routing. For each VLAN, enter an IP address in the IP Address column. Click the table cell in the Subnet Mask column and select a mask to apply to the IP address of the VLAN.

Device: Cat3550

Interface Name	Routed	IP Address	Subnet Mask
Vlan1	☑	192.168.4.3	255.255.255.0
Vlan3	☑	10.12.14.2	255.0.0.0
Fa0/1	☐		
Fa0/2	☐		
Fa0/3	☐		
Fa0/4	☐		
Fa0/5	☐		
Fa0/6	☐		
Fa0/7	☐		

• **Figure 12.23** Setting up interVLAN routing

Multilayer Switches

That Cisco 3550 is an amazing box in that it seems to utterly defy the entire concept of a switch because of its support of interVLAN routing. Up to this point we always said a switch works at Layer 2 of the OSI model, but now you've just seen a very powerful (and expensive) switch that clearly also works at Layer 3. The Cisco 3550 is one example of what we call a *multilayer switch*.

At this point you must stop thinking that a switch is always Layer 2. Instead, think of the idea that any device that forwards traffic based on anything inside a given packet is a switch. A Layer 2 switch forwards traffic based on MAC addresses, whereas a Layer 3 switch (also called a router) forwards traffic based on IP addresses. From here on out, we will carefully address at what layer of the OSI seven-layer model a switch operates.

Multilayer switches are incredibly common and support a number of interesting features, clearly making them part of what I call advanced

Any device that works at multiple layers of the OSI seven-layer model, providing more than a single service, is called a *multifunction network device*.

networking devices and what CompTIA calls specialized network devices. We are going to look at three areas where multilayer switches are very helpful: load balancing, quality of service, and network protection (each term is defined in its respective section). These three areas aren't the only places where multiplayer switches solve problems but they are the most popular and the ones that the CompTIA Network+ exam covers. Let's look at these areas that are common to more advanced networks and see how more advanced network devices help in these situations.

Load Balancing

Popular Internet servers are exactly that—popular. So popular that it's impossible for a single system to support the thousands if not millions of requests per day that bombard them. But from what we've learned thus far about servers, we know that a single server has a single IP address. Put this to the test. Go to a command prompt and type `ping www.google.com`:

```
C:\>ping www.google.com

Pinging www.l.google.com [74.125.95.147] with 32 bytes of data:
Reply from 74.125.95.147: bytes=32 time=71ms TTL=242
Reply from 74.125.95.147: bytes=32 time=71ms TTL=242
Reply from 74.125.95.147: bytes=32 time=70ms TTL=242
Reply from 74.125.95.147: bytes=32 time=70ms TTL=242
```

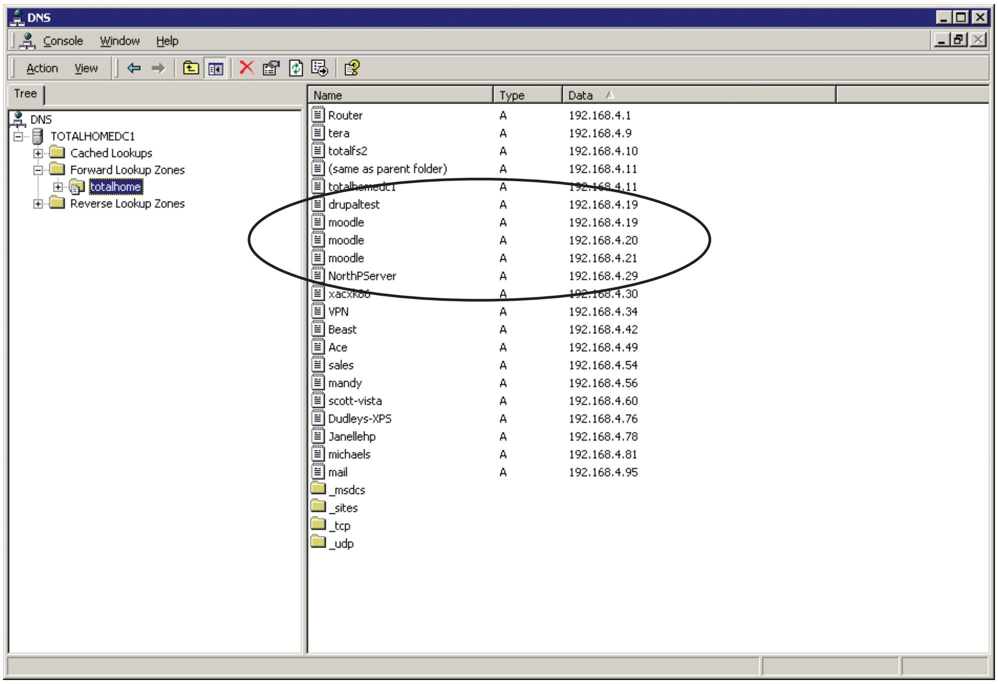
It's difficult to come up with a consensus on statistics like the number of requests/day or how many requests a single server can handle. Just concentrate on the concept. If some nerdy type says my numbers are way off, nicely agree and walk away. Just don't invite them to any parties.

It's hard to get a definite number but poking around on a few online Web site analysis Web sites like Alexa (www.alexa.com), it seems that www.google.com receives around 130 to 140 million requests per day; about 1600 requests per second. Each request might require the Web server to deliver thousands of HTTP packets. A single, powerful, dedicated Web server (arguably) handles at best 2000 requests/second. Even though www.google.com is a single IP address, there has to be more than one Web server to handle all the requests. Actually there are thousands of Google Web servers stretched across multiple locations around the world. So how does www.google.com use a single IP address and lots and lots of servers? The answer is in something called load balancing.

Load balancing means to take a bunch of servers and make them look like a single server. Not only do you need to make them look like one server, you need to make sure that requests to these servers are distributed evenly so no one server is bogged down while another is idle. There's a number of ways to do this, as you are about to see. Be warned, not all of these methods require an advanced network device but it's very common to use one. A device designed to do one thing really well is always much faster than using a general-purpose computer and slapping on software.

DNS Load Balancing

Using DNS for load balancing is one of the oldest and still very common ways to support multiple Web servers. In this case, each Web server gets its own (usually) public IP address. Each DNS server for the domain has multiple "A" DNS records, each with the same fully qualified domain name (FQDN), for each DNS server. The DNS server then cycles around these



Name	Type	Data
Router	A	192.168.4.1
tera	A	192.168.4.9
totalfs2	A	192.168.4.10
(same as parent folder)	A	192.168.4.11
totalhomedc1	A	192.168.4.11
drupaltest	A	192.168.4.19
moodle	A	192.168.4.19
moodle	A	192.168.4.20
moodle	A	192.168.4.21
NorthPServer	A	192.168.4.29
xacxk86	A	192.168.4.30
VPN	A	192.168.4.34
Beast	A	192.168.4.42
Ace	A	192.168.4.49
sales	A	192.168.4.54
mandy	A	192.168.4.56
scott-vista	A	192.168.4.60
Dudleys-XPS	A	192.168.4.76
Janellehp	A	192.168.4.78
michaels	A	192.168.4.81
mail	A	192.168.4.95
_msdcs		
_sites		
_tcp		
_udp		

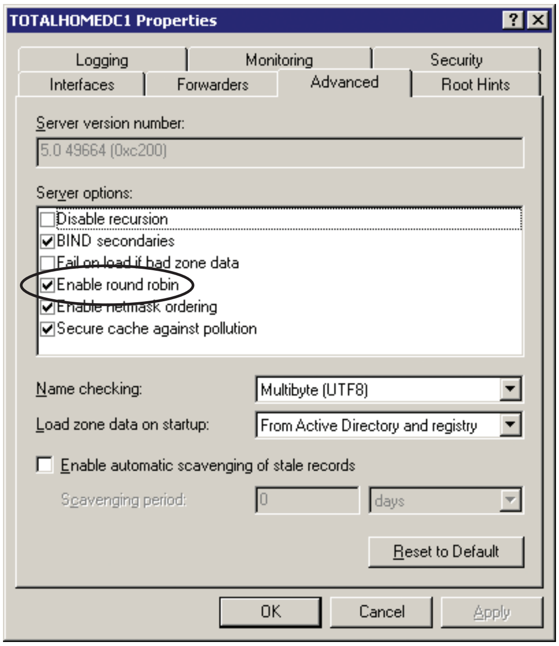
• **Figure 12.24** Multiple IP addresses, same name

records so the same domain name resolves to different IP addresses. Figure 12.24 shows a Windows DNS server with multiple A records for the same FQDN.

Now that the A records are added, you need to tell the DNS server to cycle around these names. With Windows DNS Server, there's a check box to do so, as shown in Figure 12.25.

When a computer comes to the DNS server for resolution, the server cycles through the DNS A records, giving out first one and then the next in a cyclic (round robin) fashion.

The popular BIND DNS server has a very similar process but adds even more power and features such as weighting one or more servers more than others or randomizing the DNS response.



Server version number:
5.0 49664 (0xc200)

Server options:

- □ Disable recursion
- ☑ BIND secondaries
- □ Fail on load if bad zone data
- ☑ Enable round robin
- ☑ Enable netmask ordering
- ☑ Secure cache against pollution

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

□ Enable automatic scavenging of stale records

Scavenging period: 0 days

• **Figure 12.25** Enabling round robin

Using a Multilayer or Content Switch

DNS is an easy way to load balance, but it still relies on multiple DNS servers each with its own IP addresses. As Web clients access one DNS server or another, they cache that DNS server's IP address. The next time they access the server, they go directly to the cached DNS server and skip the round robin, reducing its effectiveness.

To hide all of your Web servers behind a single IP, there are two popular choices. First is to use a special multilayer switch that works at Layers 3 and 4. This switch is really just a router that performs NAT and port forwarding, but also has the capability to query the hidden Web servers continually and send HTTP requests to a server that has a lower workload than the other servers.

Your other option is to use a **content switch**. Content switches must always work at least at Layer 7 (Application layer). Content switches designed to work with Web servers therefore are able to read the incoming HTTP and HTTPS requests. This gives you the capability to do very advanced actions, such as handling SSL certificates and cookies, on the content switch, taking the workload off the Web servers. Not only can these devices load balance in the ways previously described, but their HTTP savvy can actually pass a cookie to HTTP requesters—Web browsers—so the next time that client returns, they are sent to the same server (Figure 12.26).

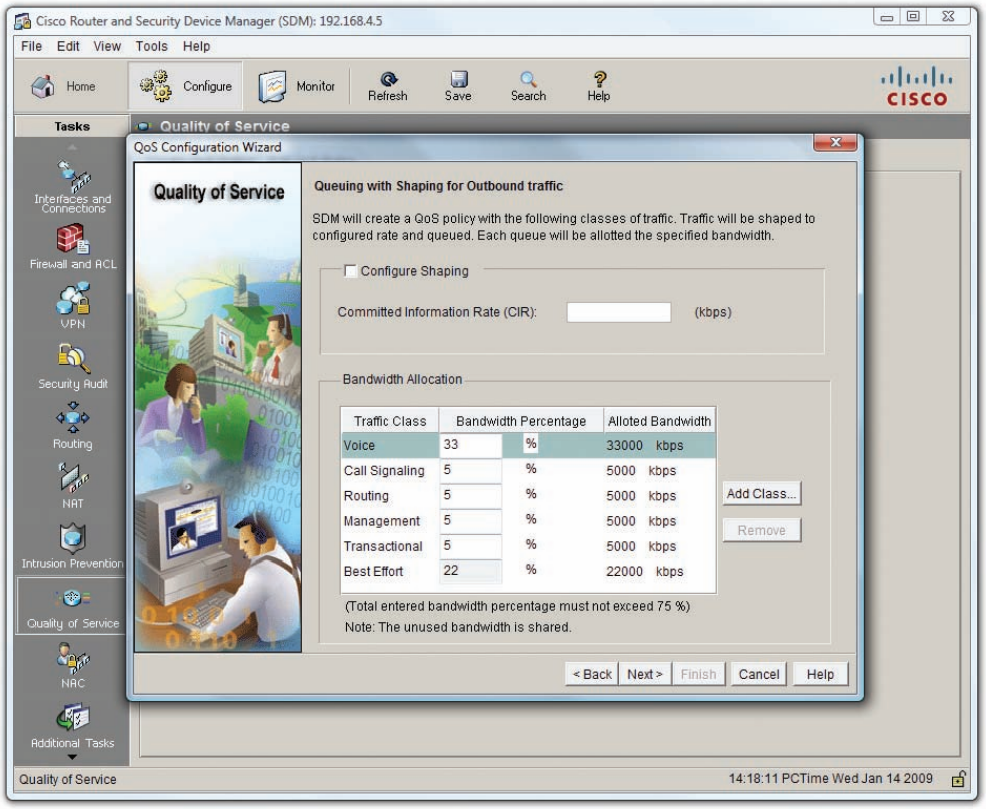
• Figure 12.26 Layer 7 content switch

Content switches are incredibly powerful—and incredibly expensive.

QoS and Traffic Shaping

Just about any router you buy today has the capability to block packets based on port number or IP address, but these are simple mechanisms mainly designed to protect an internal network. What if you need to control how much of your bandwidth is used for certain devices or applications? In that case you need **quality of service (QoS)**, policies to prioritize traffic based on certain rules. These rules control how much bandwidth a protocol, PC, user, VLAN, or IP address may use (Figure 12.27).

On many advanced routers and switches, you can implement QoS through bandwidth management such as **traffic shaping**, controlling the flow of packets into or out from the network according to the type of packet or other rules. Traffic shaping is very important when you must guarantee a device or application a certain amount of bandwidth and/or latency, such as with VoIP or video. Traffic shaping is also very popular in places such as schools, where IT professionals need to be able to control user activities, such as limiting HTTP usage or blocking certain risky applications such as peer-to-peer file sharing.



Queuing with Shaping for Outbound traffic

SDM will create a QoS policy with the following classes of traffic. Traffic will be shaped to configured rate and queued. Each queue will be allotted the specified bandwidth.

□ Configure Shaping

Committed Information Rate (CIR): (kbps)

Bandwidth Allocation

Traffic Class	Bandwidth Percentage		Alloted Bandwidth
Voice	33	%	33000 kbps
Call Signaling	5	%	5000 kbps
Routing	5	%	5000 kbps
Management	5	%	5000 kbps
Transactional	5	%	5000 kbps
Best Effort	22	%	22000 kbps

(Total entered bandwidth percentage must not exceed 75 %)

Note: The unused bandwidth is shared.

Quality of Service

14:18:11 PCTime Wed Jan 14 2009

• Figure 12.27 QoS configuration on a router

The term *bandwidth shaping* is synonymous with traffic shaping. The routers and switches that can implement traffic shaping are commonly referred to as *shapers*. On the CompTIA Network+ exam refers to them as *bandwidth shapers*.

Network Protection

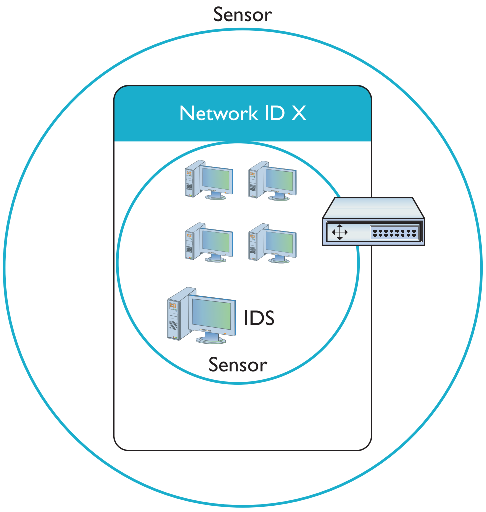
The last area where you're likely to encounter advanced networking devices is network protection. *Network protection* is my term to describe four different areas that CompTIA feels fits under the term specialized network devices:

- Intrusion protection/intrusion detection
- Port mirroring
- Proxy serving
- Port authentication

Intrusion Detection/Intrusion Prevention

Intrusion detection/intrusion prevention are very similar to the processes used to protect networks from intrusion and to detect that something has intruded into a network. Odds are good you've heard the term firewall. Firewalls are hardware or software tools that block traffic based on port number or IP address. A traditional firewall is a static tool: it cannot actually detect an attack. An intrusion detection system (IDS) is an application (often running on a dedicated IDS box) that inspects incoming packets, looking for active intrusions. A good IDS knows how to find attacks that no firewall can find, such as viruses, illegal logon attempts, and other well-known attacks. An IDS will always have some way to let the network administrators know if an attack is taking place: at the very least the attack is logged, but some IDSs offer a pop-up message, an e-mail, or even a text message to your phone.

Third-party IDS tools, on the other hand, tend to act in a much more complex and powerful way. You have two choices with a real IDS: network based or host based. A network-based IDS (NIDS) consists of multiple sensors placed around the network, often on one or both sides of the gateway router. These sensors report to a central application that in turn reads a signature file to detect anything out of the ordinary (Figure 12.28).



• Figure 12.28 Diagram of network-based IDS

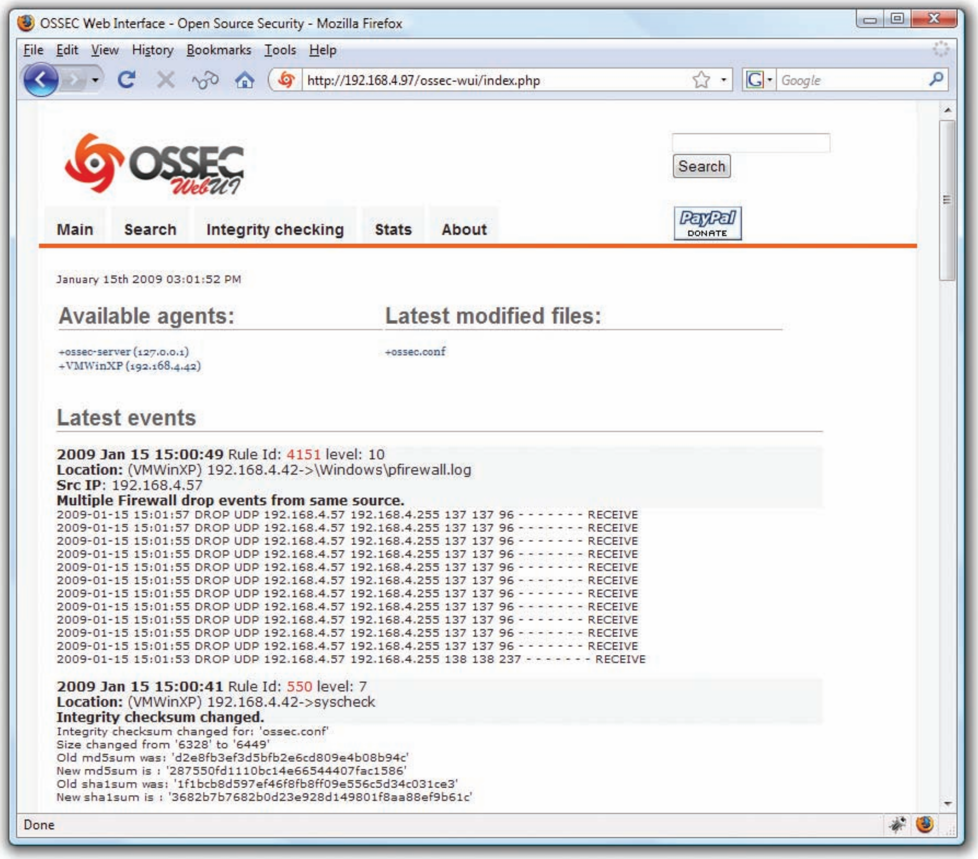
A host-based IDS (HIDS) is software running on individual systems that monitors for events such as system file modification or registry changes (Figure 12.29). More expensive third-party system IDSs do all this and add the ability to provide a single reporting source—very handy when one person is in charge of anything that goes on throughout a network.

A well-protected network uses both a NIDS and a HIDS. A NIDS monitors the incoming and outgoing traffic from the Internet while the HIDS monitors the individual computers.

An intrusion prevention system (IPS) is very similar to an IDS, but an IPS adds the capability to react to an attack. Depending on what IPS product you choose, an IPS can block incoming packets on-the-fly based on IP address, port number, or application type. An IPS might go even further, literally fixing certain packets on the fly.

IPS was originally called *Active IDS*, but that term is fading.

The CompTIA Network+ exam refers to intrusion detection and prevention systems collectively by their initials, IDS/IPS.


OSSEC Web Interface - Open Source Security - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.4.97/ossec-wui/index.php
Google
OSSEC WebUI
Search
Main
Search
Integrity checking
Stats
About
PayPal DONATE
Done

January 15th 2009 03:01:52 PM

Available agents:

+ossec-server (127.0.0.1)
+VMWinXP (192.168.4.42)

Latest modified files:

+ossec.conf

Latest events

```
2009 Jan 15 15:00:49 Rule Id: 4151 level: 10
Location: (VMWinXP) 192.168.4.42->\Windows\pfirewall.log
Src IP: 192.168.4.57
Multiple Firewall drop events from same source.
2009-01-15 15:01:57 DROP UDP 192.168.4.57 192.168.4.255 137 137 96 - - - - - - - RECEIVE
2009-01-15 15:01:57 DROP UDP 192.168.4.57 192.168.4.255 137 137 96 - - - - - - - RECEIVE
2009-01-15 15:01:55 DROP UDP 192.168.4.57 192.168.4.255 137 137 96 - - - - - - - RECEIVE
2009-01-15 15:01:55 DROP UDP 192.168.4.57 192.168.4.255 137 137 96 - - - - - - - RECEIVE
2009-01-15 15:01:55 DROP UDP 192.168.4.57 192.168.4.255 137 137 96 - - - - - - - RECEIVE
2009-01-15 15:01:55 DROP UDP 192.168.4.57 192.168.4.255 137 137 96 - - - - - - - RECEIVE
2009-01-15 15:01:55 DROP UDP 192.168.4.57 192.168.4.255 137 137 96 - - - - - - - RECEIVE
2009-01-15 15:01:55 DROP UDP 192.168.4.57 192.168.4.255 137 137 96 - - - - - - - RECEIVE
2009-01-15 15:01:55 DROP UDP 192.168.4.57 192.168.4.255 137 137 96 - - - - - - - RECEIVE
2009-01-15 15:01:55 DROP UDP 192.168.4.57 192.168.4.255 137 137 96 - - - - - - - RECEIVE
2009-01-15 15:01:55 DROP UDP 192.168.4.57 192.168.4.255 137 137 96 - - - - - - - RECEIVE
2009-01-15 15:01:53 DROP UDP 192.168.4.57 192.168.4.255 138 138 237 - - - - - - - RECEIVE

2009 Jan 15 15:00:41 Rule Id: 550 level: 7
Location: (VMWinXP) 192.168.4.42->syscheck
Integrity checksum changed.
Integrity checksum changed for: 'ossec.conf'
Size changed from '6328' to '6449'
Old md5sum was: 'd2e8fb3ef3d5bfb2e6cd809e4b08b94c'
New md5sum is : '287550fd1110bc14e66544407fac1586'
Old sha1sum was: '1f1bcb8d597ef46f8fb8ff09e556c5d34c031ce3'
New sha1sum is : '3682b7b7682b0d23e928d149801f8aa88ef9b61c'
```

• Figure 12.29 OSSEC HIDS

Port Mirroring

IDS/IPS often take advantage of something called **port mirroring**. Many advanced switches have the capability to mirror data from any or all physical ports on a switch to a single physical port. It's as though you make a customized, fully-configurable promiscuous port. Port mirroring is incredibly useful for any type of situation where an administrator needs to inspect packets coming to or from certain computers.

Proxy Serving

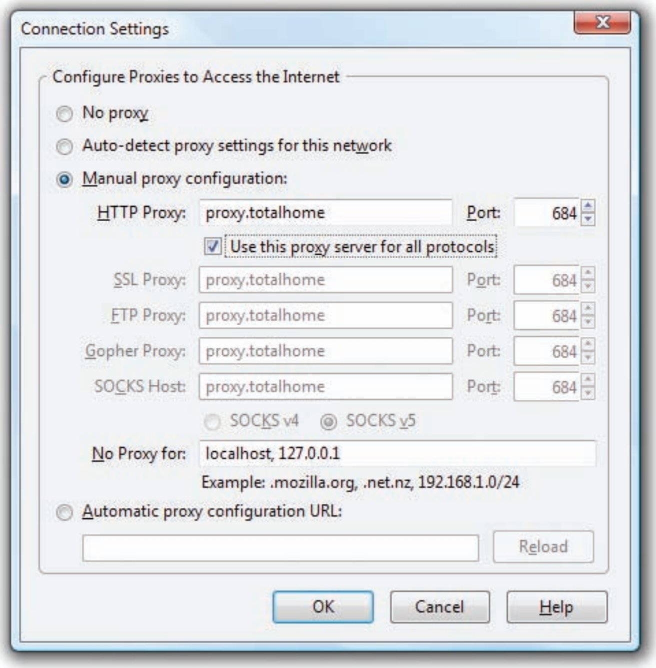
A **proxy server** sits in between clients and external servers, essentially pocketing the requests from the clients for server resources and making those requests itself. The client computers never touch the outside servers and thus stay protected from any unwanted activity A proxy server usually *does something* to those requests as well. Let's see how proxy servers work using HTTP—one of the oldest uses of proxy servers.

Since proxy serving works by redirecting client requests to a proxy server, you first must tell the Web client not to use the usual DNS resolution to determine the Web server and instead to use a proxy. Every Web client comes with a program that enables you to set the IP address of the proxy server, as shown in the example in Figure 12.30.

Once the proxy server is configured, HTTP requests move from the client directly to the proxy server. Built into every HTTP request is the URL of the target Web server, so the Web proxy knows where to get the requested data once it gets the request. In the simplest format, the proxy server simply forwards the requests using its own IP address and then forwards the returning packets to the client (Figure 12.31).

This simple version of proxy prevents the Web server from knowing where the client is located. This is a pretty handy trick for those who wish to keep people from knowing where they are coming from, assuming you can find a public proxy server that accepts your HTTP requests (there are plenty!). There are many other good reasons to use a proxy server. One big benefit is caching. A proxy server keeps a copy of the served resource, giving clients a much faster response. A proxy server might inspect the contents of the resource, looking for inappropriate content, viruses/malware, or just about anything else the creators of the proxy might desire it to identify.

HTTP proxy servers are the most common type of proxy server, but any TCP application can take advantage of proxy servers. Numerous proxy serving programs are available, such as Squid, shown in Figure 12.32. Proxy serving takes some substantial processing, so many vendors sell proxy servers in a box, such as the Blue Coat ProxySG 510.



Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

● Manual proxy configuration:

HTTP Proxy: proxy.totalhome Port: 684

☑ Use this proxy server for all protocols

SSL Proxy: proxy.totalhome Port: 684

FTP Proxy: proxy.totalhome Port: 684

Gopher Proxy: proxy.totalhome Port: 684

SOCKS Host: proxy.totalhome Port: 684

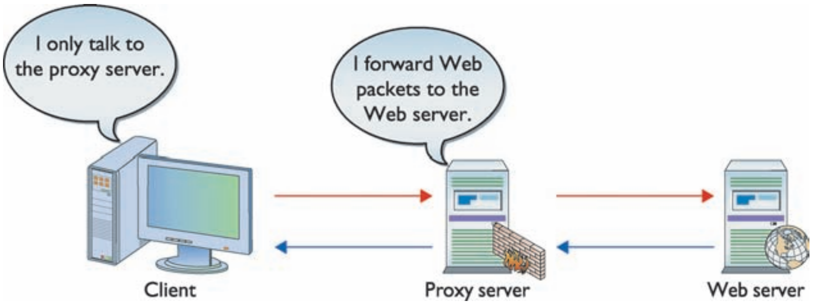
○ SOCKS v4 ● SOCKS v5

No Proxy for: localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

• **Figure 12.30** Setting a proxy server in Mozilla Firefox


I only talk to the proxy server.
I forward Web packets to the Web server.
Client
Proxy server
Web server

• **Figure 12.31** Web proxy at work

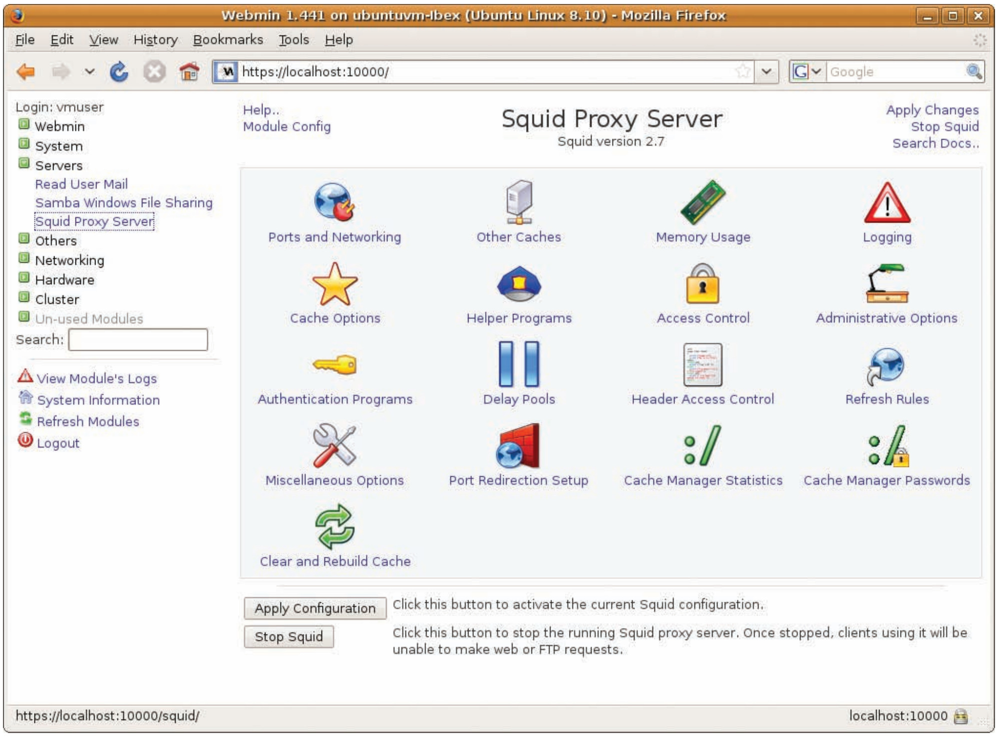
Port Authentication

The last place where you see advanced networking devices is in port authentication. We've already covered the concept in the previous chapter: **port authentication** is a critical component for any AAA authentication method, in particular RADIUS, TACACS+, and 802.1X. When you make a connection, you must have something at the point of connection to make the authentication, and that's where advanced networking devices come into play. Many switches, and almost every wireless access point, come with feature sets to support port authentication. A superb example is my own Cisco 2811 router. It supports RADIUS and 802.1X port authentication, as shown in Figure 12.33.

Try This!

Exploring Switch Capabilities

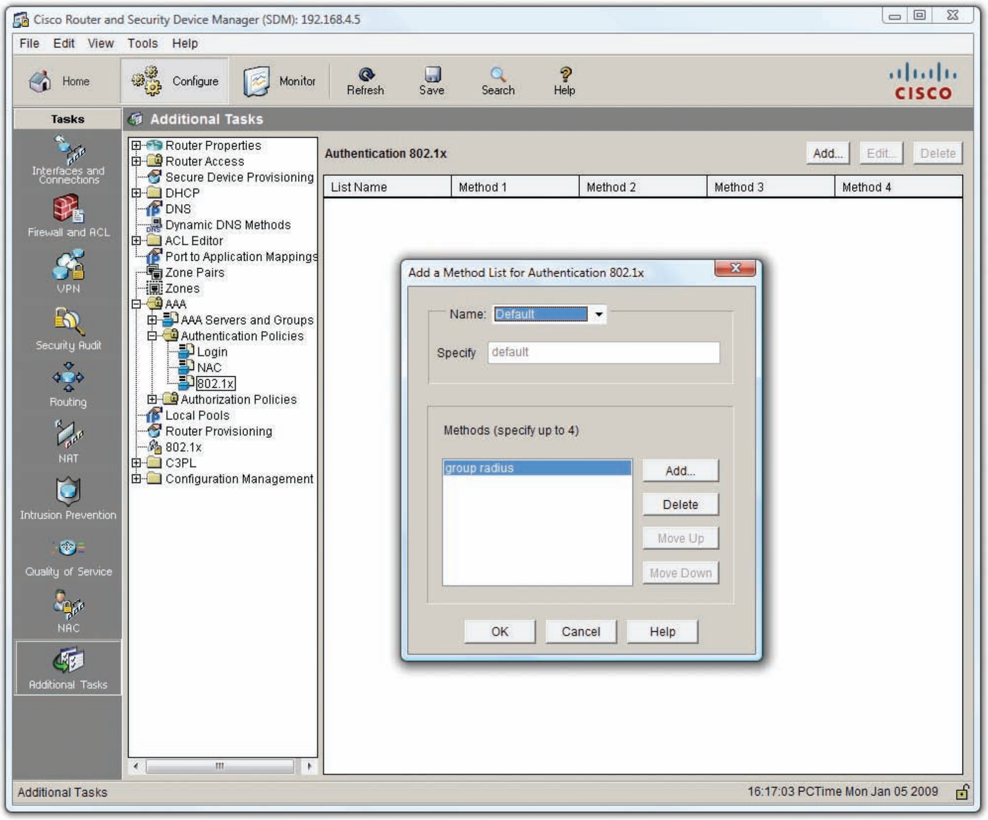
If you have access to a managed switch of any kind, now would be a great time to explore its capabilities. Use a Web browser of choice and navigate to the switch. What can you configure? Do you see any options for proxy serving, load balancing, or other fancy capability? How could you optimize your network by using some of these more advanced capabilities?



Apply Configuration — Click this button to activate the current Squid configuration.

Stop Squid — Click this button to stop the running Squid proxy server. Once stopped, clients using it will be unable to make web or FTP requests.

• **Figure 12.32** Squid proxy software



• **Figure 12.33** 802.1X configuration on a Cisco 2811

Chapter 12 Review

Chapter Summary

After reading this chapter and completing the exercises, you should understand the following about networking.

Discuss the four logical topologies as defined by CompTIA

- A physical topology describes the physical layout of cabling while a signaling topology refers to how the signals actually progress through a network.
- Logical network topologies include peer-to-peer, client/server, VPN, and VLAN. Client/server and peer-to-peer are more commonly referred to as software architecture models.
- In a client/server model, certain systems act as dedicated servers. A client never acts as a server, so one client can never access shared resources on another client.
- In a peer-to-peer network, any system can act as a client, server, or both. This model first became popular in the 1990s with Microsoft Windows.
- Today, the terms client/server and peer-to-peer refer more to applications than to network operating systems.
- A VPN creates a tunnel that enables users to connect to remote LANs across the Internet.
- RRAS, a program available only on Windows servers, allows VPN connections using PPTP. PPTP creates the secure tunnel through the Internet to your private LAN.
- L2TP is a Cisco VPN protocol that was built upon the best features of Microsoft's PPTP. Rather than requiring special server software (such as Microsoft's RRAS), L2TP places a tunnel endpoint directly on a VPN-capable router.
- L2TP provides no authentication or encryption. It usually relies on IPSec for this.
- The majority of PPTP and L2TP VPNs use either PPTP or L2TP. However, some use other options such as OpenVPN or IPSec.

Configure and deploy VLANs

- A VLAN takes a single physical broadcast domain and splits it into multiple virtual broadcast domains, thereby reducing broadcast traffic.
- Trunking allows multiple switches to assign individual ports to specific VLANs. This allows multiple computers on the same LAN, but connected to different physical switches, to be members of the same VLAN.
- A trunk port carries all data, regardless of VLAN number, between all switches on a LAN. Today, every Ethernet switch prefers the 802.1Q trunk standard, enabling you to connect switches from different manufactures.
- Many switches can be configured for VLANs via a serial port connection, but the most common method is via a Web server built into the switch.
- Once the VLANs have been created on the switches, the next steps include assigning computers' MAC addresses to VLANs (Dynamic VLANs) or assigning switch ports to VLANs (Static VLANs).
- A switch that has the ability to do Inter-VLAN Routing can act as a virtual router, connecting different VLANs.

Implement advanced switch features

- A multilayer switch is one that operates at multiple levels of the OSI model, such as the Cisco 3550 switch that functions at both Layer 2 and Layer 3.
- Any device that forwards traffic based on packet contents is a switch. Layer 2 switches forward packets based on MAC addresses while Layer 3 switches (also called routers) forward packets based on IP addresses.
- Load balancing involves configuring multiple servers to look like a single server, allowing multiple servers to handle requests sent to a single IP address. Additionally, load balancing spreads

the requests evenly across all the servers so that no one system is bogged down.

- With DNS load balancing, each Web server receives a unique IP address because the DNS servers hold multiple A records, each with the same domain name, for each Web server. The DNS server then cycles around these records so that the same domain name resolves to different IP addresses.
- DNS load balancing loses effectiveness when client computers cache the resolved IP address, bypassing the DNS server when connecting to a Web server.
- A content switch provides load balancing by reading the HTTP and HTTPS requests and acting upon them themselves, taking the workload off the Web servers.
- Quality of service (QoS) sets priorities for how much bandwidth is used for certain protocols, PCs, users, VLANs, IP addresses, or other devices or applications. This is often implemented through traffic shaping.
- Intrusion detection systems (IDSs) inspect incoming packets and actively monitor for attacks. A network-based IDS (NIDS) typically consists of sensors on one or both sides of the gateway router while a host-based IDS (HIDS) consists of monitoring software installed on individual computers.
- Intrusion prevention systems (IPSs) can react to attacks. An IPS proactively monitors for attacks, then reacts if an attack is identified.
- Port mirroring mirrors data from any or all physical ports on a switch to a single physical port, making it easy for administrators to inspect packets to or from certain computers.
- A proxy server intercepts client requests and acts upon them, usually by blocking the request or forwarding the request to other servers.
- Many switches support port authentication, a feature that requires network devices to authenticate themselves, protecting your network from rogue devices.

Key Terms

client/server *(315)*
content switch *(328)*
interVLAN routing *(325)*
intrusion detection/intrusion prevention *(329)*
Layer 2 Tunneling Protocol (L2TP) *(320)*
load balancing *(326)*
multilayer switch *(313)*
peer-to-peer *(316)*
Point-to-Point Tunneling Protocol (PPTP) *(319)*
port authentication *(331)*
port mirroring *(330)*
proxy server *(330)*
quality of service (QoS) *(328)*
Routing and Remote Access Service (RRAS) *(319)*
traffic shaping *(328)*
trunk ports *(322)*
trunking *(322)*
Virtual Local Area Network (VLAN) *(321)*
Virtual Private Network (VPN) *(318)*
VPN concentrator *(320)*

Key Term Quiz

Use the Key Terms list to complete the sentences that follow. Not all terms will be used.

1. _______________ is Cisco's VPN protocol that relies on IPSec for all its security needs.
2. In a(n) _______________ network, all computers can act in dual roles as clients or servers.
3. A(n) _______________ services client requests and forwards them to the appropriate server.
4. In a(n) _______________ network, client computers cannot share resources with each other or see each other. They can only connect to a server.
5. _______________ allows a VLAN to be defined across multiple switches.

6. Routers that enable you to set QoS often use _______________ to limit the amount of bandwidth used by certain devices or applications.

7. Creating a(n) _______________ helps to reduce broadcast traffic on any one network by separating the one large network into smaller ones, but requires the use of a special switch.

8. A(n) _______________ is a network created by a secure tunnel from one network to another remote network.

9. _______________ is a special program running on Microsoft servers that enables remote users to connect to a local Microsoft network.

10. Microsoft's _______________ enables computers on one end of a VPN to receive an IP address on the subnet of the remote network.

Multiple-Choice Quiz

1. Which network model uses only truly dedicated servers?
   - **A.** Client/server
   - **B.** Peer-to-peer
   - **C.** Virtual Private Network
   - **D.** Virtual Local Area Network

2. Marcy is home sick, but uses a VPN to connect to her network at work and is able to access files stored on the remote network just as if she were physically in the office. Which protocols make it possible for Marcy to receive an IP address from the DHCP server at work? (Select two.)
   - **A.** PPTP
   - **B.** IDS
   - **C.** L2TP
   - **D.** IPS

3. What is one benefit of a VLAN?
   - **A.** It allows remote users to connect to a local network via the Internet.
   - **B.** It reduces broadcast traffic on a LAN.
   - **C.** It can create a WAN from multiple disjointed LANs.
   - **D.** It provides encryption services on networks that have no default encryption protocol.

4. Rashan's company has multiple FTP servers, allowing remote users to download files. What should Rashan implement on his FTP servers so that they appear as a single server with a guarantee that no single FTP server is receiving more requests than any other?
   - **A.** Load balancing
   - **B.** Port authentication
   - **C.** Port mirroring
   - **D.** Trunking

5. Raul sits down at his computer, checks his e-mail, edits a document on the server, and shares a folder with other users on the network. What kind of network is Raul on?
   - **A.** Client/server
   - **B.** Peer-to-peer
   - **C.** PPTP
   - **D.** Trunked

6. Which of the following describes a VPN?
   - **A.** A remote connection using a secure tunnel across the Internet
   - **B.** Segmenting a local network into smaller networks without subnetting
   - **C.** A network that is protected from viruses
   - **D.** A protocol used to encrypt L2TP traffic

7. To enable computers connected to different switches to be members of the same VLAN, what do the switches have to support?
   - **A.** Content switching
   - **B.** Port authentication
   - **C.** Port mirroring
   - **D.** Trunking

8. What is true of a multilayer switch?
   - A. It can work at multiple OSI layers at the same time.
   - B. It can work with one of several OSI layers at a time, depending on its configuration mode. Working at a different layer requires making a configuration change and resetting the switch.
   - C. It can communicate with other switches that work at different OSI layers.
   - D. It has twice the ports of a standard switch because it contains two regular switches, one stacked on top of the other.

9. Which statement about L2TP is true?
   - A. It is more secure than PPTP.
   - B. It was developed by Microsoft and is available by default on all Microsoft servers.
   - C. It lacks security features and therefore relies on other protocols or services to handle authentication and encryption.
   - D. It ensures router tables are kept synchronized across VLANs.

10. What are the benefits of caching on a Web proxy? (Select two.)
   - A. Response time
   - B. Virus detection
   - C. Tracking
   - D. Authentication

11. Which are effective methods of implementing load balancing? (Select two.)
   - A. Content switching
   - B. DNS round robin
   - C. Traffic shaping
   - D. Proxy serving

12. Employees in the sales department complain that the network runs slowly when employees in the art department copy large graphics files across the network. What solution might increase network speed for the sales department?
   - A. DNS load balancing
   - B. Content switching
   - C. Traffic shaping
   - D. 802.1z

13. How does an IPS compare to an IDS?
   - A. An IPS is more secure because it uses IPSec.
   - B. An IDS is more secure because it uses L2TP.
   - C. An IPS is more robust because it can react to attacks.
   - D. An IDS is more robust because it can react to attacks.

14. A dynamic VLAN assigns VLANs to:
   - A. IP addresses
   - B. MAC addresses
   - C. Ports
   - D. Trunks

15. Novell NetWare is an example of what?
   - A. A dedicated client
   - B. A dedicated server
   - C. A multilayer VLAN switch
   - D. Intrusion Detection System software

Essay Quiz

1. Your boss is becoming increasingly worried about hacking attempts on the company Web server. Write a letter explaining the various options for protecting against, and reacting to, attacks.

2. A co-worker is constantly talking about VLANs and VPNs, but rarely uses the terms correctly. Educate your co-worker as to what VPNs and VLANs are, what they are for, and how they differ.

Lab Projects

• Lab Project 12.1

You have read quite a bit in this chapter about securing networks against attacks. Research at least three Intrusion Protection Systems and create a matrix comparing them. Include comparisons of features, cost, reliability, network/operating system support, and general user reviews.

• Lab Project 12.2

Your boss wants to reduce broadcast traffic and asks you to segment the network into multiple VLANs. Use your favorite e-commerce Web site for purchasing computer and networking devices and find at least three switches that support VLANs. Create a matrix comparing features and cost. Based on your research, which VLAN switch would you recommend to your employer and why?