

The Three Faces of Networking

HIS CHAPTER examines backbone networks (BNs) that are used to link LANs together and to link BNs to WANs. We begin with the various types of devices used in BNs and discuss several backbone architectures. We then turn to two technologies designed primarily for use in the BN (ATM and gigabit Ethernet). The chapter ends with a discussion of how to improve BN performance and of the future of BNs.

OBJECTIVES

264

- Understand the internetworking devices used in BNs
- Understand several common backbone architectures
- Be familiar with ATM
- Be familiar with gigabit Ethernet
- Understand the best practice recommendations for backbone design
- Be aware of ways to improve BN performance

CHAPTER OUTLINE

INTRODUCTION

BACKBONE NETWORK COMPONENTS

Switches

Routers

Gateways

A Caution

BACKBONE NETWORK ARCHITECTURES

Backbone Architecture Layers

Routed Backbone

Collapsed Backbone

Virtual LAN

BACKBONE TECHNOLOGIES

Asynchronous Transfer Mode

THE BEST PRACTICE BACKBONE DESIGN

Architectures

Effective Data Rates

BACKBONE NETWORK COMPONENTS 265

Conversion between Protocols Recommendations IMPROVING BACKBONE PERFORMANCE Improving Computer and Device Performance Improving Circuit Capacity Reducing Network Demand IMPLICATIONS FOR MANAGEMENT SUMMARY

INTRODUCTION

Most business organizations realize that information must be stored, retrieved, analyzed, acted on, and shared with others at a moment's notice. Without an enterprisewide network or an Internet connection, moving information from one department LAN to another or to customers is difficult.

Interconnecting the organization's diverse networks is critical. A *backbone network* (*BN*) is a high-speed network that connects many networks. BNs typically use higher-speed circuits to interconnect a series of LANs and provide connections to other BNs, MANs, WANs, and the Internet. A backbone that connects many BNs spanning several nearby buildings for a single organization is often called a *campus network*. A BN also may be called an *enterprise network* if it connects all networks within a company, regardless of whether it crosses state, national, or international boundaries.

We begin this chapter by describing several commonly used devices in the BN and then showing how those can be used to create different backbone architectures with different performance capabilities. Next, we focus on the high-speed network technologies often used in BNs.

BACKBONE NETWORK COMPONENTS

There are two basic components to a BN: the network cable and the hardware devices that connect other networks to the BN. The cable is essentially the same as that used in LANs, except that it is usually fiber optic to provide higher data rates. The hardware devices can be computers or special-purpose devices that just transfer messages from one network to another. These include switches, routers, and gateways (Figure 8.1).

Switches

Most *switches* operate at the data link layer. They connect two or more network segments that use the *same* data link and network protocol. They understand only data link layer protocols and addresses. They may connect the *same or different* types of cable. These are

266

CHAPTER 8 BACKBONE NETWORKS

Device	Operates At	Packets	Physical Layer	Data Link Layer	Network Layer
Switch	Data link layer	Filtered using data link layer addresses	Same or different	Same	Same
Router	Network layer	Routed using network layer addresses	Same or different	Same or different	Same
Gateway	Network layer	Routed using network layer addresses	Same or different	Same or different	Same or different

FIGURE 8.1 Backbone network devices.

the same *layer-2 switches* discussed in Chapter 6 in that they use the data link layer address to forward packets between network segments (Figure 8.2). They learn addresses by reading the source and destination addresses.

Routers

Routers operate at the network layer. Routers connect two or more network segments that use the *same or different* data link protocols but the *same* network protocol. They may connect the *same or different* types of cable. Routers are the "TCP/IP gateways" that we first introduced in Chapter 5. Routers strip off the data link layer packet, process the network layer packet, and forward only those messages that need to go to other networks on the basis of their network layer address (Figure 8.3).

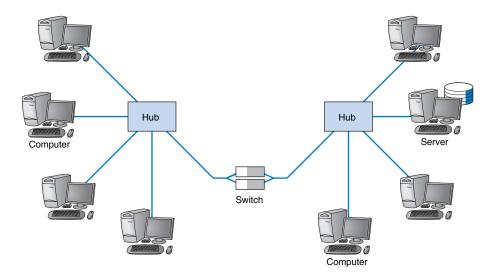


FIGURE 8.2 Use of switches to connect local area network segments.

BACKBONE NETWORK COMPONENTS 267

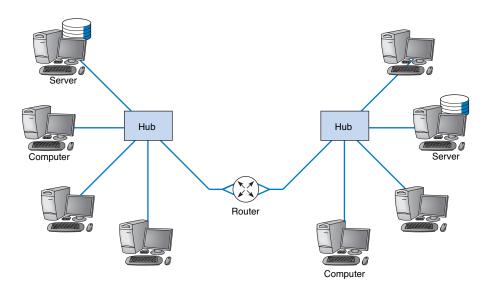


FIGURE 8.3 Use of routers to connect local area networks.

Routers may be "black boxes," computers with several NICs, or special network modules in computers or other devices. In general, they perform more processing on each message than switches and therefore operate more slowly.

One major feature of a router is that it can choose the "best" route between networks when there are several possible routes between them. Because a router knows its own location, as well as the packet's final destination, it looks in a routing table to identify the best route or *path*.

One other important difference between a router and a switch is that a router processes only those messages that are specifically addressed to it. Switches process all messages that appear on the network and forward them to the appropriate network on the basis of their data link layer address. Switches simply forward the message unchanged to the other network. In contrast, because routers operate at the network layer, the router's data link layer must first recognize that the incoming message is specifically addressed to the router at the data link layer level before the message is passed to the network layer for processing. The router will then process the message by building an entirely new data link layer packet, then transmit it to the other network.

The router attempts to make no changes to the network layer packet and user data it receives. (As noted previously, it creates a new data link layer packet.) Sometimes, however, changes are needed, such as when the maximum data link layer packet size on one network is different from another, which forces the router to split a message into several smaller messages for transmission.

Gateways

Gateways operate at the network layer and use network layer addresses in processing messages. Gateways are more complex than switches or routers because they are the interface

between two or more dissimilar networks. Gateways connect two or more networks that use the *same or different* (usually different) data link and network protocols. They may connect the *same or different* types of cable. Some gateways operate at the application layer as well. Gateways process only those messages explicitly addressed to them (i.e., using their data link layer address) and route those messages that need to go to other networks (Figure 8.4).

Gateways translate one network layer protocol into another, translate data link layer protocols, and open sessions between application programs, thus overcoming both hardware and software incompatibilities. More complex gateways even take care of such tasks as code conversion (e.g., converting from ASCII into EBCDIC) (see Chapter 3). A gateway may be a stand-alone computer with several NICs and special software or a front-end processor connected to a mainframe computer.

One of the most common uses of gateways is to enable LANs that use TCP/IP and Ethernet to communicate with mainframes that use other protocols. In this case, the gateway converts the microcomputer LAN transmissions into a transmission that looks like it came from a terminal. The gateway provides both the basic system interconnection and the necessary translation between the protocols in both directions. Without this gateway on the LAN, each microcomputer would have to have its own hardware and software in addition to the TCP/IP and Ethernet hardware and software (e.g., software to make the microcomputer act like a terminal). The gateway eliminates the need for additional hard-

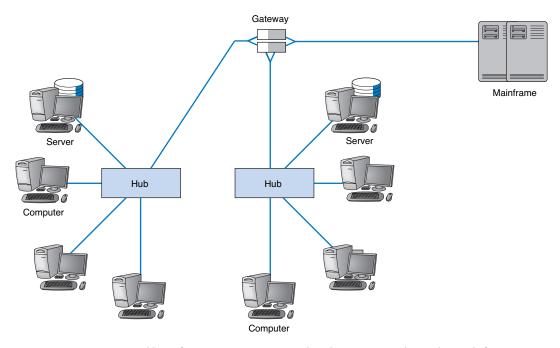


FIGURE 8.4 Use of gateways to connect local area networks and a mainframe.

268

BACKBONE NETWORK COMPONENTS 269

ware for the microcomputer, and it requires only one connection to the client computer because all data are sent through the LAN.

A Caution

One warning is in order. The terminology used in the marketplace may differ substantially from that in the preceding discussion. Many new types of switches, routers, and gateways are being developed, so that one vendor's "switch" may actually provide the functions of a "router." *Layer-3 switches* function in the same way as layer-2 switches discussed previously, but they switch messages on the basis of their network layer address (usually IP address). These switches provide the benefits of traditional layer-2 switches: much faster transmission and more simultaneously active ports than routers.

Multiprotocol routers can understand several different network layer protocols. If they receive a message in one protocol, they process it and send it out using the same protocol. Some vendors' multiprotocol routers translate between different network layer protocols (usually TCP/IP and IPX/SPX) so, technically, they are gateways.

MANAGEMENT

8-1 BUILDING A TCP/IP GATEWAY

FOCUS

Transco is the United Kingdom's largest utility company, responsible for gas transfer across a network of 200,000 miles of pipeline and serving the needs of more than 20 million commercial, industrial, and domestic consumers. Transco was formed from the merger of dozens of regional gas boards, and therefore inherited a network composed of a mixture of technologies, many of which were not compatible.

Transco concluded that its new network should be founded on TCP/IP. With many of the Transco sites being in remote outstation locations, the idea also emerged to create a satellitebased WAN carrying IP traffic, thereby removing the high costs and inflexibility of traditional telephone or cable systems.

The outstation locations had a large number of serial-based control and communications devices installed over the years. These were perfectly workable pieces of equipment for which there was no reason to replace. However, the equipment was serial-based with no Ethernet connection and was not compatible with IP. Therefore, an intermediate communications device was developed to translate the proprietary serial protocol into standard IP-based data. Engineers modified a matchbox-sized Lantronix industrial device server, the Micro IAP, which provides IP and a Web server, thus removing the need for the Transco engineers to write a TCP/IP driver. It simply plugged onto a connector designed as part of the Transco device, providing the unit with TCP/IP connectivity at a stroke.

After the Transco engineers had thoroughly tested the prototype device with the legacy outstations using the proposed protocol, the Micro IAP was added, making the unit Ethernet-enabled and so able to connect into the satellite WAN. Results over the Transco satellite IP system were "outstanding," according to Keith Hand, a Transco telemetry engineer.

SOURCE: "Case Study: Legacy Systems 1: Bringing Ethernet to the Outstations," www.ethernet.industrial-net-working.com, 2004.

BACKBONE NETWORK ARCHITECTURES

The *backbone architecture* refers to the way in which the backbone interconnects the networks attached to it and how it manages the way in which packets from one network move through the backbone to other networks.

While there are an infinite number of ways in which network designers can build backbone networks, there are really only three fundamental architectures that can be combined in different ways. These four architectures are routed backbone (routers that move packets on the basis of network layer addresses), collapsed backbones (switches that move packets based on data link layer addresses), and virtual LANs (switches that move packets through LANs that are built virtually, not using physical location).

These architectures are mixed and matched to build sets of BNs. Before we discuss these architectures, we first must discuss the way in which network designers think about backbone designs and how to combine them; that is, the different layers of backbones that exist in most organizations today.

Backbone Architecture Layers

Network designers often think about three distinct technology layers¹ when they design BNs. The layer closest to the users is the *access layer*, the technology used in the LANs attached to the BN as described in the previous chapter (e.g., 100Base-T, wireless Ethernet) (Figure 8.5). Although the access layer is not part of the BN, the technologies used in the LANs (or access layer) can have major impacts on the design of the backbone.

The *distribution layer* is the part of the backbone that connects the LANs together. This is the part of the backbone that contains the "TCP/IP gateways" described in Chapter 5. It usually runs throughout one building.

The *core layer* is the part of the backbone that connects the different BNs together, often from building to building. The core layer is technologies used in the campus network or the enterprise network. Some small organizations are not large enough to have a core layer; their backbone spans only the distribution layer. Other organizations are large enough that they have a core network at several locations that are in turn connected by WANs.

In the sections that follow, we describe the four basic BN architectures and discuss at which layer they are often used. We will focus on TCP/IP networks when comparing these four architectures. We assume that you are comfortable with the material on TCP/IP in Chapter 5; if you are not, you may want to go back and review the last section of the chapter, entitled TCP/IP Example, before you continue reading.

¹Try not to confuse the five basic layers in the network model (application layer, transport layer, and so on) with the layers of backbone technology we are describing here. They are different. We would have preferred to use a different word than *layer* to describe these, but unfortunately, that is the term used in the industry.

BACKBONE NETWORK ARCHITECTURES 271

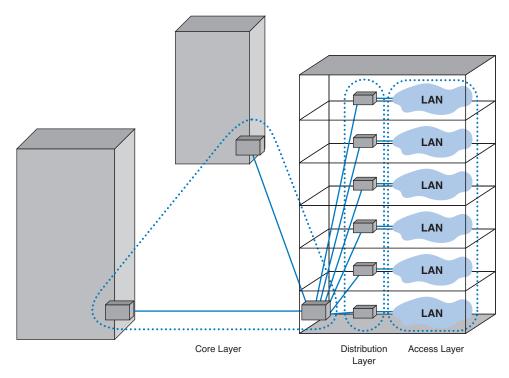


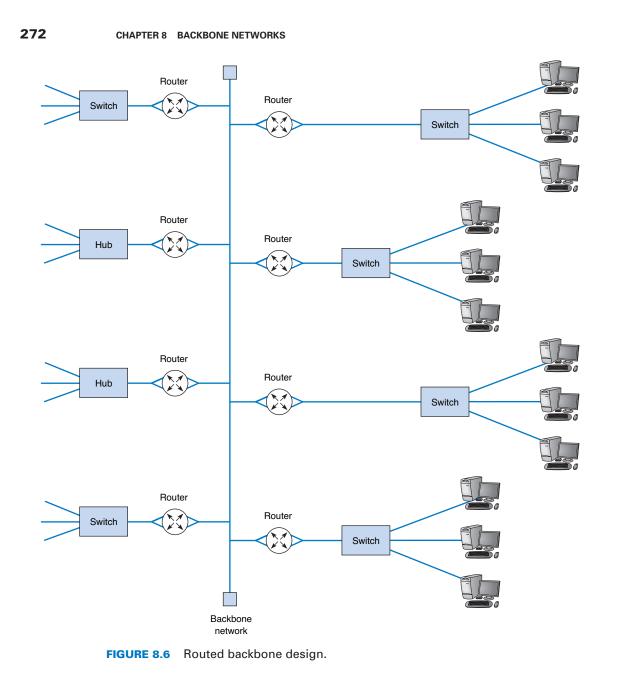
FIGURE 8.5 Backbone network design layers. LAN = local area network.

Routed Backbone

Routed backbones move packets along the backbone on the basis of their network layer address (i.e., layer-3 address). The most common form of routed backbone uses a bus topology (e.g., using Ethernet 100Base-T). Routed backbones are sometimes called subnetted backbones or hierarchical backbones and are most commonly used to connect different buildings within the same campus network (i.e., at the core layer).

Figure 8.6 illustrates a routed backbone used at the distribution layer (because it is simpler to explain how routed backbones work using the distribution layer than using the core layer). A routed backbone is the basic backbone architecture we used to illustrate how TCP/IP worked in Chapter 5. There are a series of LANs (access layer) connected by routers or layer-3 switches to a single shared-media BN. Each of the LANs is a separate subnet. Message traffic stays within each subnet unless it specifically needs to leave the subnet to travel elsewhere on the network, in which case the network layer address (e.g., TCP/IP) is used to move the packet.

Each LAN is usually a separate entity, relatively isolated from the rest of the network. There is no requirement that all LANs share the same data link layer. One LAN can use a hub for shared Ethernet, another could use switched Ethernet, whereas another



could use another technology altogether. Each LAN can contain its own server designed to support the users on that LAN, but users can still easily access servers on other LANs over the backbone as needed.

The primary advantage of the routed backbone is that it clearly segments each part of the network connected to the backbone. Each segment (usually a LAN or another back-

A DAY IN THE LIFE: NETWORK OPERATIONS MANAGER

The job of the network operations manager is to ensure that the network operates effectively. The operations manager typically has several network administrators and network managers that report to him or her and is responsible for both day-today operations as well as long-term planning for the network. The challenge is to balance daily firefighting with longer term planning; they're always looking for a better way to do things. Network operations managers also meet with users to ensure their needs are met. While network technicians deal primarily with networking technology, a network operations manager deals extensively with both technology and the users.

A typical day starts with administrative work that includes checks on all servers and backup processes to ensure that they are working properly and that there are no security issues. Then it's on to planning. One typical planning item includes planning for the acquisition of new desktop or laptop computers, including meeting with vendors to discuss pricing, testing new hardware and software, and validating new standard configurations for computers. Other planning is done around network upgrades, such as tracking historical data to monitor network usage, projecting future user needs, surveying user requirements, testing new hardware and software, and actually planning the implementation of new network resources.

One recent example of long-term planning was the migration from a Novell file server to Microsoft ADS file services. The first step was problem definition; what were the goals and the alternatives? The key driving force behind the decision to migrate was to make it simpler for the users (e.g., now the users do not need to have different accounts with different passwords) and to make it simpler for the network staff to provide technical support (e.g., now there is one less type of network software to support). The next step was to determine the migration strategy: a Big Bang (i.e., the entire network at once) or a phased implementation (several groups of users at a time). The migration required a technician to access each individual user's computer, so it was impossible to do a Big Bang. The next step was to design a migration procedure and schedule whereby groups of users could be moved at a time (e.g., department by department). A detailed set of procedures and a checklist for nettechnicians were developed work and extensively tested. Then each department was migrated on a one week schedule. One key issue was revising the procedures and checklist to account for unexpected occurrences during the migration to ensure that no data were lost. Another key issue was managing user relationships and dealing with user resistance.

With thanks to Mark Ross

bone) has its own subnet addresses that can be managed by a different network manager. Each segment off the backbone also can use different data link layer technologies.

There are two primary disadvantages to routed backbones. First, the routers in the network impose time delays. Routing takes more time than switching, so routed networks can sometimes be slower.

Second, routed networks require a lot of management. Establishing separate subnet addresses for each LAN is time consuming and requires a large set of TCP/IP addresses. Anytime a computer is moved from one LAN to another, it must be reconfigured (unless the network is using dynamic addressing, which imposes costs of its own).

Collapsed Backbone

Collapsed backbones are probably the most common type of BN used in the distribution layer (i.e., within a building); most new building BNs designed today use collapsed backbones. They also are making their way into the core layer as the campus backbone, but routed backbones still remain common.

Collapsed backbone networks use a star topology with one device, usually a switch, at its center. Figure 8.7 shows a collapsed backbone connecting the same series of LANs.

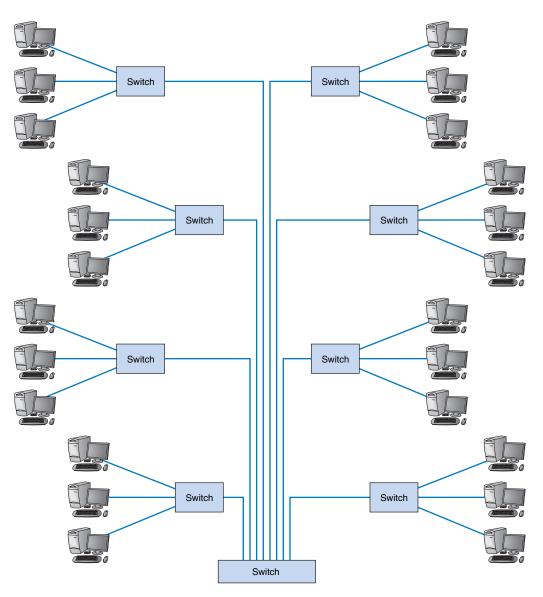


FIGURE 8.7 Collapsed backbone network design.

BACKBONE NETWORK ARCHITECTURES 275

Here, the backbone circuit and set of routers or bridges is replaced by one switch and a set of circuits to each LAN. The collapsed backbone has more cable but fewer devices. There is no backbone cable. The "backbone" exists only in the switch, which is why this is called a collapsed backbone.

There are two major advantages to collapsed backbones. First, performance is improved. With the routed or bridged backbone BN, the backbone circuit was shared among many LANs (eight LANs, in the case of Figure 8.7); each had to take turns sending messages. With the collapsed backbone, each connection into the switch is a separate pointto-point circuit. The switch enables simultaneous access, so that several LANs can send messages to other LANs at the same time. Throughput is increased significantly, often by 200 to 600 percent, depending on the number of attached LANs and the traffic pattern.

Second, there are far fewer networking devices in the network. In Figure 8.7, one switch replaces eight routers. This reduces costs and greatly simplifies network management. All the key backbone devices are in the same physical location, and all traffic must flow through the switch. If something goes wrong or if new cabling is needed, it can all be done in one place.

Collapsed backbones have three relatively minor disadvantages. First, they use more cable, and the cable must be run longer distances, which often means that fiber-optic cables must be used. Second, if the switch fails, so does the entire BN. However, if the switch has the same reliability as the routers in Figure 8.6, then there is less chance of a failure (because there are fewer devices to fail). For most organizations, these disadvantages are outweighed by benefits offered by collapsed backbones.

The third problem is broadcast messages. Because switches operate at layer 2, all networks connected to them are part of the same subnet. Broadcast messages (e.g., address requests) must be permitted to travel everywhere in the backbone. This means, for example, that a computer in one LAN attempting to find the data link layer address of a server in the same LAN will issue a broadcast message that will travel to every computer on every LAN attached to the backbone. (In contrast, on a routed backbone, such messages would never leave the LAN in which they originated.)

There are many different types of broadcast messages other than address requests (e.g., a printer reporting it is out of paper, a server about to be shut down). These broadcast messages quickly use up network capacity in a large bridged network. The result is slower response times for the user. In a small network, the problems are not as great because there are fewer computers to issue such broadcast messages. In larger networks, this can be a problem.

Rack-Mounted Collapsed Backbones Most organizations now use collapsed backbones in which all network devices for one part of the building are physically located in the same room, often in a *rack* of equipment. This form of collapsed backbone is shown graphically in Figure 8.8. This has the advantage of placing all network equipment in one place for easy maintenance and upgrade, but it does require more cable. In most cases, the cost of the cable itself is only a small part of the overall cost to install the network, so the cost is greatly outweighed by the simplicity of maintenance and the flexibility it provides for future upgrades.

The room containing the rack of equipment is sometimes called the *main distribution* facility (MDF) or central distribution facility (CDF). Figure 8.9 shows a photo of a MDF



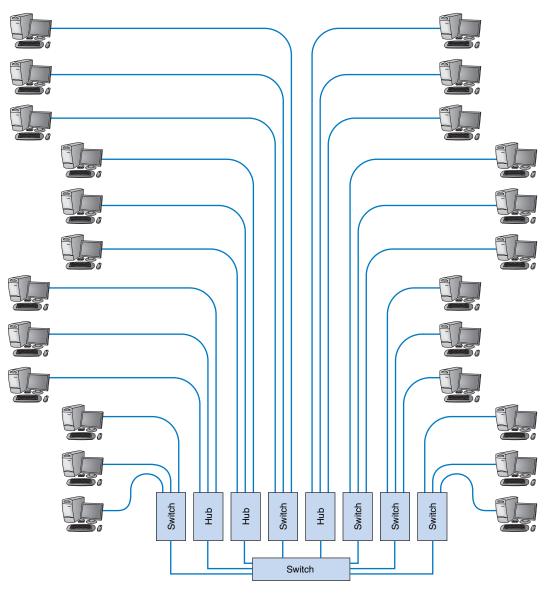


FIGURE 8.8 Rack-mounted collapsed backbone network design.

room at Indiana University. Figure 8.10 shows the equipment diagram of this same room. The cables from all computers and devices in the area served by the MDF (often hundreds of cables) are run into the MDF room. Once in the room, they are connected into the various devices. The devices in the rack are connected among themselves using very short cables called *patch cables*.

With rack-mounted equipment, it becomes simple to move computers from one LAN to another. In the traditional routed backbone design as shown in Figure 8.6, for

BACKBONE NETWORK ARCHITECTURES 277

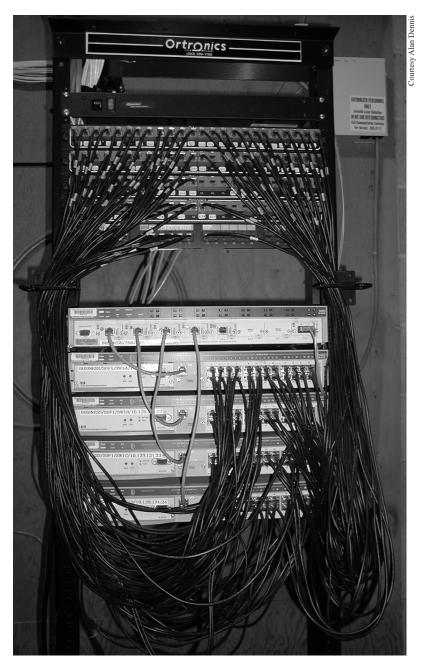
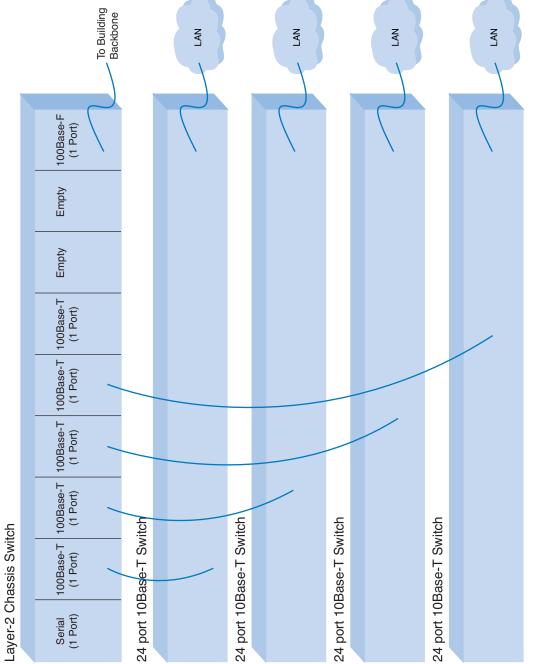


FIGURE 8.9 An MDF with rack-mounted equipment. A layer-2 chassis switch with six 100Base-T modules (center of photo) connects to four 24-port 10Base-T switches. The chassis switch is connected to the campus backbone using 100Base-F over fiber-optic cable. The cables from each room are wired into the rear of the patch panel (shown at the top of the photo), with the ports on the front of the patch panel labeled to show which room is which. Patch cables connect the patch panel ports to the ports on the switches.



 \oplus

 ϕ



BACKBONE NETWORK ARCHITECTURES 279

example, all the computers in the same general physical location are connected to the same hub and thus share the capacity of the hub. Although this often works well, it can cause problems if many of the computers on the hub are high-traffic computers. For example, in Figure 8.6, if all the busy computers on the network are located in the upper left area of the figure, the hub in this area may become a severe bottleneck.

With an MDF, all cables run into the MDF. If one hub becomes overloaded, it is straightforward to unplug the cables from several high-demand computers from the overloaded hub and plug them into one or more less-busy hubs. This effectively spreads the traffic around the network more efficiently and means that network capacity is no longer tied to the physical location of the computers; computers in the same physical area can be connected into very different network segments.

Chassis-Based Collapsed Backbones Sometimes a *chassis switch* is used instead of a rack. A chassis switch enables users to plug *modules* directly into the switch. Each module is a certain type of network device. One module might be a 16-port 100Base-T hub, another might be a router, whereas another might be a 4-port 100Base-T switch, and so on. The switch is designed to hold a certain number of modules and has a certain internal capacity, so that all the modules can be active at one time. For example, a switch with five 10Base-T hubs, two 10Base-T switches (with 8 ports each), a 100Base-T switch (with 4 ports), and a 100Base-T router would have to have an internal switching capacity of at least 710 Mbps ($[5 \times 10 \text{ Mbps}] + [2 \times 8 \times 10 \text{ Mbps}] + [4 \times 100 \text{ Mbps}] + 100 \text{ Mbps} = 710 \text{ Mbps}$).

The key advantage of chassis switches is their flexibility. It becomes simple to add new modules with additional ports as the LAN grows and to upgrade the switch to use new technologies. For example, if you want to add gigabit Ethernet or ATM (discussed below), you simply lay the cable and insert the appropriate module into the switch.

MANAGEMENT

8-2 COLLAPSED BACKBONES AT INDIANA UNIVERSITY

FOCUS

At Indiana University we commonly use collapsed backbones in our buildings. Figure 8.11 shows a typical design. Each floor in the building has a set of switches and access points that serve the LANs on that floor. Each of these LANs and WLANs are connected into a switch for that floor, thus forming a collapsed backbone on each floor. Typically, we use switched 10Base-T or 100Base-T within each floor. The switch forming the collapsed backbone on each floor is then connected into another switch in the basement, which provides a collapsed backbone for the entire building. The building backbone is usually a higher speed network running over fiber-optic cable (e.g. 100Base-F or 1 GbE). This switch, in turn, is connected into a high-speed router that leads to the campus backbone (a routed backbone design).



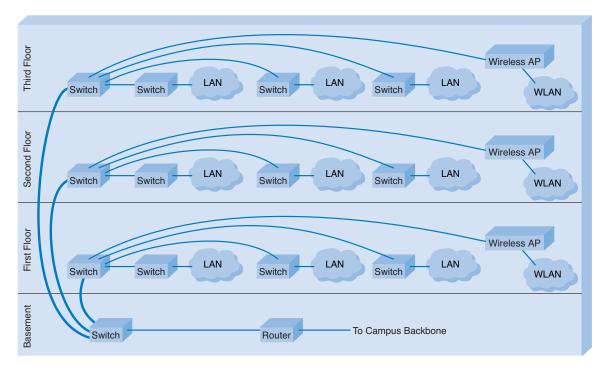


FIGURE 8.11 Collapsed backbones at Indiana University.

Virtual LAN

For many years, the design of LANs remained relatively constant. However, in recent years, the introduction of high-speed switches has begun to change the way we think about LANs. Switches offer the opportunity to design radically new types of LANs. Most large organizations today have traditional LANs, but many are considering the *virtual LAN (VLAN)*, a new type of LAN-BN architecture made possible by intelligent, high-speed switches.

VLANs are networks in which computers are assigned to LAN segments by software rather than by hardware. In the section above, we described how in rack-mounted collapsed BNs a computer could be moved from one hub to another by unplugging its cable and plugging it into a different hub. VLANs provide the same capability via software so that the network manager does not have to unplug and replug physical cables to move computers from one segment to another.

VLANs are often faster and provide greater opportunities to manage the flow of traffic on the LAN and BN than do the traditional LAN and routed BN architecture. However, VLANs are significantly more complex, so they usually are used only for large networks. There are two basic approaches to designing VLANs: single-switch VLANs and multiswitch VLANs.

BACKBONE NETWORK ARCHITECTURES 281

Single-Switch VLAN A single-switch VLAN means that the VLAN operates only inside one switch. The computers on the VLAN are connected into the one switch and assigned by software into different VLANs (Figure 8.12). The network manager uses special software to assign the dozens or even hundreds of computers attached to the switch to different VLAN segments. The VLAN segments function in the same way as physical LAN segments; the computers in the same VLAN act as though they are connected to the

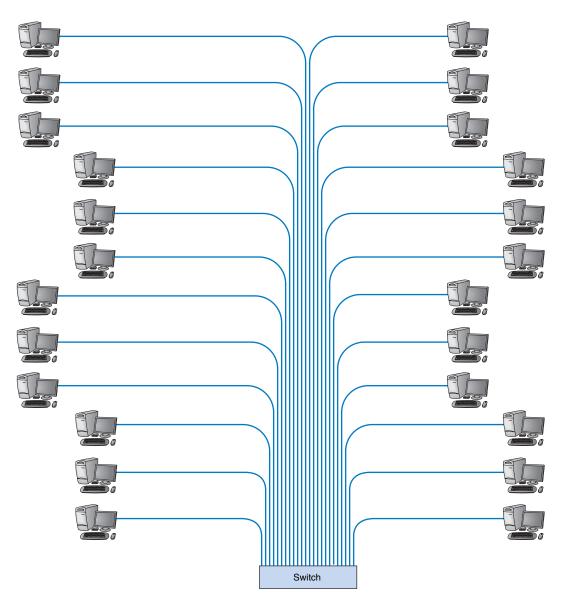


FIGURE 8.12 VLAN-based collapsed backbone network design.

same physical switch or hub. For example, broadcast messages sent by computers in a VLAN segment are sent only to the computers on the same VLAN. VLANs can be designed so that they act as though computers are connected via hubs (i.e., several computers share a given capacity and must take turns using it) or via switches (i.e., all computers in the VLAN can transmit simultaneously). Although switched circuits are preferred to the shared circuits of hubs, VLAN switches with the capacity to provide a complete set of switched circuits for hundreds of computers are more expensive than those that permit shared circuits.

We should also note that it is possible to have just one computer in a given VLAN. In this case, that computer has a dedicated connection and does not need to share the network capacity with any other computer. This is commonly done for servers.

There are four ways in which computers attached to VLAN switches can be assigned to the specific VLANs inside them. The first approach, used by *port-based VLANs* (also called *layer-1 VLANs*), uses the physical layer port number on the front of the VLAN switch to assign computers to VLAN segments. Each computer is physically cabled into a specific port on the VLAN switch. The network manager uses special software provided by the switch manufacturer to instruct the switch as to which ports are assigned to which VLAN. This means that the network manager must know which computer is connected to which port.

The second approach, used by *MAC-based VLANs* (also called *layer-2 VLANs*), uses the data link layer address (or physical address) to form the VLANs. The network manager uses special software to instruct the switch which incoming data link layer addresses are assigned to which VLAN segment. The advantage of a layer-2 VLAN is that they are simpler to manage when computers are moved. If a computer is moved in a layer-1 VLAN, then the network manager must reconfigure the switch to keep that computer in the same VLAN because the computer has moved from one port to another. With a layer-2 VLAN, no reconfiguration is needed. Although the computer may have moved from one port to another, it is the permanently assigned data link layer address that is used to determine which VLAN the computer is on.

The third approach, used by *IP-based VLANs* (also called *layer-3 VLANs* or protocol-based VLANs), uses the network layer address to form the VLANs. As before, the network administrator uses special software to instruct the switch as to which network layer addresses are assigned to which VLAN. Layer-3 VLANs reduce the time spent reconfiguring the network when computers move in the same way as layer-2 VLANs. Layer-3 VLANs tend to be a bit slower at processing each message than layer-2 VLANs because processing layer-3 protocols is slightly slower than processing layer-2 protocols.

The fourth approach, used by *application-based VLANs* (also called *policy-based VLANs* or *layer-4 VLANs*), uses the type of application indicated by the port number in the TCP packet in combination with the network layer addresses to form the VLAN groups. As before, the network administrator uses special software to instruct the switch as to which types of packets from which addresses are assigned to which VLAN. This process is very complex because the network manager must decide on a variety of different factors in forming the VLANs. The advantage is a very precise allocation of network capacity. Now VLANs can be formed to allocate a certain amount of network capacity for Web browsing to certain individuals, so much to Web browsing for others, so much to transac-

282

BACKBONE NETWORK ARCHITECTURES 283

tion processing, and so on. For example, a given user could be assigned to a switched 100Base-T VLAN for e-mail, but assigned to a shared 100Base-T VLAN for downloading MP3 files. In this way, the network manager can restrict the amount of network capacity used by potentially less productive applications (e.g., Web surfing) and thus provide much better allocation of resources.

Multiswitch VLAN A multiswitch VLAN works the same way as a single-switch VLAN, except that now several switches are used to build the VLANs (Figure 8.13). VLANs are most commonly found in building backbone networks (i.e., access and distribution layers) but are starting to move into core backbones between buildings.

The switches must be able to send packets among themselves in a way that identifies the VLAN to which the packet belongs. *IEEE 802.1q* is an emerging standard that inserts the 16-byte VLAN tag into the normal IEEE 802.3 Ethernet packet (see Chapter 5 for the Ethernet packet layout). When a packet needs to go from one VLAN switch to another VLAN switch, the first switch revises the incoming Ethernet packet to include the 16-byte VLAN tag. The VLAN tag is used to move the packet from switch to switch within the VLAN network. When the packet arrives at the final destination switch, the VLAN tag is stripped off and an Ethernet packet identical to the one with which it entered the VLAN is sent to the destination computer.

Operating Characteristics VLANs offer two major advantages compared to the other network architectures. The first lies in their ability to manage the flow of traffic on the LAN and backbone very precisely. VLANs make it much simpler to manage the

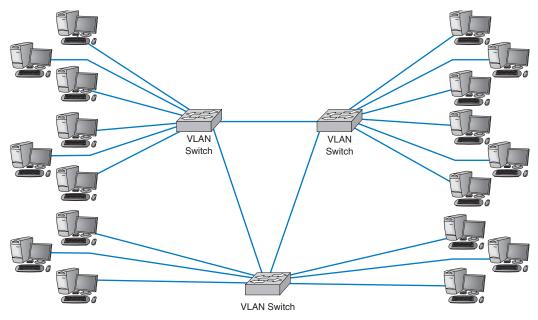


FIGURE 8.13 Multiswitch VLAN-based collapsed backbone network design.

284

CHAPTER 8 BACKBONE NETWORKS

broadcast traffic that has the potential to reduce performance seriously and to allocate resources to different types of traffic more precisely. The bottom line is that VLANs often provide faster performance than the other three backbone architectures.

The second advantage is the ability to prioritize traffic. The VLAN tag information included in the Ethernet packet defines the VLAN to which the packet belongs and also specifies a priority code based on the IEEE 802.1q standard. As you will recall from Chapter 4, the network and transport layers can use RSVP quality of service (QoS), which enables them to prioritize traffic using different classes of service. RSVP is most effective when combined with QoS capabilities at the data link layer. (Without QoS at the hardware layers, the devices that operate at the hardware layers [e.g., layer-2 switches] would ignore QoS information.) With the Ethernet packet's ability to carry VLAN information that includes priorities, we now have QoS capabilities in the data link layer.

The biggest drawbacks to VLANs are their cost and management complexity. VLAN switches also are much newer technologies that have only recently been standardized. Such "bleeding-edge" technologies sometimes introduce other problems that disappear only after the specific products have matured.

BACKBONE TECHNOLOGIES

Many of the same high-speed technologies used in LANs are often used in BNs (e.g., 100Base-T, 1000Base-T). Gigabit Ethernet is the newest technology for the backbone. Gigabit Ethernet was discussed in Chapter 6, but is worth mentioning again here because it is commonly found in the backbone. One gigabit Ethernet (1 GbE), 10 gigabit Ethernet (10 GbE), and the latest addition, 40 gigabit Ethernet (40 GbE), are usually run over fiber optic cable when used in the backbone because of the longer distances they must run (although twisted pair versions of these technologies are available).

MANAGEMENT

8-3 VLAN NETWORK AT IONA

FOCUS

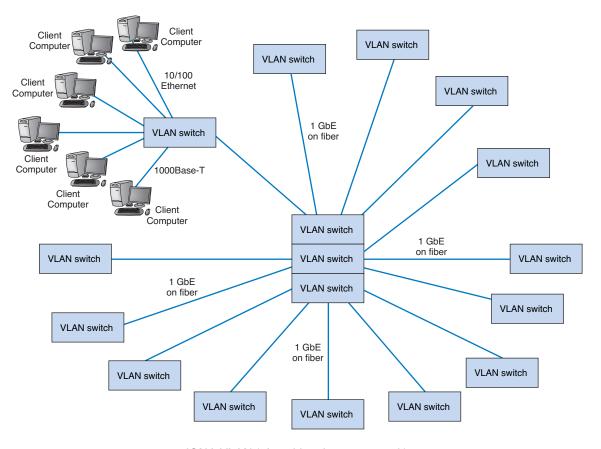
IONA Technologies, Inc., a 600person software developer of enterprise middleware, took advantage of its relocation to Waltham, Massachusetts, to redesign its network infrastructure. The new network, designed to support 230 users in one office complex, uses a multiswitch virtual local area network (VLAN) architecture.

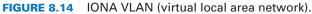
IONA has 27 access-layer VLAN switches located close to its users—built into their cubicle walls, to be exact. Up to 24 users are connected to each access-layer switch, using a mixture of 10/100 Ethernet and 1000Base-T over copper cables (e.g., category 5e) (Figure 8.14). Each of the first-level switches are connected via gigabit Ethernet over fiber to a central set of five VLAN switches that form the core of the network. IEEE 802.1q is used to communicate among the access-layer switches and the distribution-layer switches.

Because both the access-layer switches and distribution-layer switches are modular, it is easy for IONA to upgrade when technologies change.

SOURCE: "Middleware Maker Future-Proofs LAN Infrastructure," *Packet*, Cisco Systems, Inc., Second Quarter, 2000.







One technology originally developed for use in MANs and WANs has also been refined for use in BNs. ATM is still used but is slowly being displaced by gigabit Ethernet.

Asynchronous Transfer Mode

Asynchronous transfer mode (ATM) is a technology originally designed for use in WANs that is now often used in BNs. Because it is standardized, it is simple to connect ATM BNs into ATM WANs run by common carriers such as AT&T. ATM is sometimes called cell relay.

Unlike Ethernet, ATM is really a layer-3 technology that also includes specific layer-2 and layer-1 technologies as part of its specification. ATM is compatible with TCP/IP and Ethernet and will carry TCP/IP-Ethernet traffic as though ATM was a layer-2 technology. For this reason, most backbone network designers think of ATM as a layer-2 technology. If this sounds complicated, that's because it is, which is one reason why ATM is not very popular. We will discuss how this works in the section on ATM and traditional

LANs (the two approaches are LANE and MPOA). For the moment, you can think like a backbone designer and consider ATM to be a layer-2 technology, with the usual requirements about having the proper physical hardware at layer 1.

ATM backbone switches typically provide point-to-point full-duplex circuits at 155 Mbps (for a total of 310 Mbps) or 622 Mbps (1.24 Gbps total) from switch to switch. Although originally designed to run on fiber-optic cable, some versions of ATM can run on category 5e twisted-pair cables (although the cables cannot be run as far as they would be for 100Base-T).

ATM is a switched network but differs from switched Ethernet in three important ways. First, ATM uses fixed-length packets (or "cells") of 53 bytes (a 5-byte header containing addressing and QoS information, plus 48 bytes of user data). The small fixed-length packets make switching much faster because it is so simple it can be done in hardware—and hardware switching is substantially faster than software switching.

Second, ATM uses a very different type of addressing from traditional data link layer protocols (e.g., Ethernet) or network layer protocols (e.g., IP). Ethernet and IP assign permanent addresses to each computer so that all messages sent to the same computer use the same address. ATM does not assign addresses to devices; instead it assigns addresses to circuits between devices. ATM defines a *virtual channel (VC)* (sometimes called a *virtual circuit*, although this is not the preferred name) between each sender and receiver, and all packets use the virtual circuit identifier as the address. Each VC identifier has two parts, a path number and a circuit number within that path. Each ATM switch contains a VC table that lists all VCs known to that switch (analogous to a routing table in IP). Because there are potentially thousands of VCs and because each switch knows only those VCs in its VC table, a given VC identifier is used only between one switch and the next.

When an ATM packet arrives at a switch, the switch looks up the packet's VC identifier in its VC table to determine where to send it and what VC identifier should be used when the packet is transmitted on the outgoing circuit. Figure 8.15, for example, shows two switches, each with four ports (or physical circuits). When an incoming packet arrives, the switch looks up the packet's VC identifier in the circuit table, switches the packet to the outgoing port, and changes the VC identifier the packet had when it arrived to a new VC identifier used by the switch at its destination. For example, a packet arriving at switch A via port 1 with a VC identifier of 1,10 would be transmitted out on port 4 to switch B and would be given a new VC identifier of 3,15.

ATM is connection oriented, so all packets travel in order through the VC. A VC can be either a *permanent virtual circuit (PVC)* (i.e., defined when the network is established or modified) or a *switched virtual circuit (SVC)* (i.e., defined temporarily for one transmission and deleted when the transmission is completed).² ATM provides a separate control circuit that is used for nondata communication between devices, such as the setup and takedown of an SVC.

286

²You will notice a slight change in terminology: *VC* is *virtual channel*, whereas *PVC* is *permanent virtual circuit*. The reasons are arbitrary and historical. As you will see in the next chapter, the term *PVC* has the same meaning in X.25 WANs, and because X.25 was developed before ATM, ATM has simply adopted the same terminology.

287 **BACKBONE TECHNOLOGIES**

Outgoing

Circuit

3,15

2,10

2,11

3,26

1.18

4,21

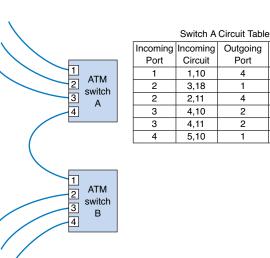


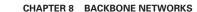
FIGURE 8.15 Addressing and forwarding with asynchronous transfer mode virtual circuits.

The third major difference between ATM and other backbone technologies such as switched Ethernet is that ATM prioritizes transmissions on the basis of QoS. You may recall that Chapter 5 briefly discussed QoS routing. With QoS routing or QoS switching, different *classes of service* are defined, each with different priorities. Each virtual circuit is assigned a specific class of service when it is first established. ATM defines five service classes (see ATM Classes of Service, page 289) that enable the network to prioritize transmissions. For example, circuits containing voice transmissions receive higher priority than circuits containing e-mail transmissions because delays in voice transmissions can seriously affect transmission quality whereas delays in e-mail transmission are less important. If an ATM switch becomes overloaded and it receives traffic on a low-priority circuit, it will store the packet for later transmission or simply refuse the request until it has sufficient capacity.

ATM and Traditional LANs ATM uses a very different type of protocol than do traditional LANs. It has a small 53-byte fixed-length packet and is connection oriented (meaning that devices establish a virtual channel before transmitting). Ethernet uses larger variable-length packets and is typically connectionless. To use ATM in a BN that connects traditional Ethernet LANs, some translation must be done to enable the LAN packets to flow over the ATM backbone. There are two approaches to this: LANE and MPOA.

With LAN Emulation (LANE), the data link layer packets from the LAN are left intact; they are broken into 48-byte blocks and surrounded by ATM packets. This process is called *encapsulation* and is done by an *edge switch*. The packets flow through the ATM network and are reassembled at an edge switch at the other end before being transmitted into the destination LAN (Figure 8.16). The use of ATM is transparent to users because LANE leaves the original data link layer packets intact and uses the packet's data link layer address to forward the message through the ATM network.

288



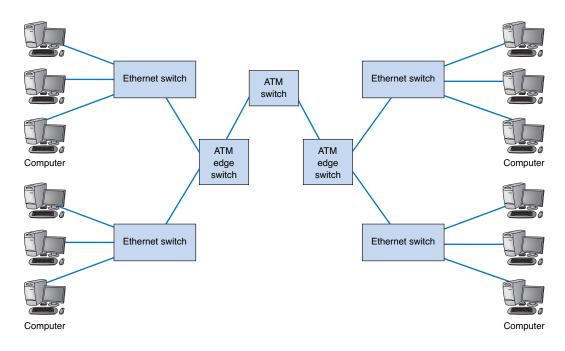


FIGURE 8.16 ATM encapsulation.

Translating from Ethernet into ATM (and vice versa) is not simple. First, the Ethernet address must be translated into an ATM VC identifier for the PVC or SVC that leads from the edge switch to the edge switch nearest the destination. This is done through a process similar to that of using a broadcast message on a subnet to locate a data link layer address (see Chapter 5). ATM is a switched point-to-point network, so it lacks a simple built-in ability to issue broadcast messages. LANE enables the transmission of broadcast messages, but to date, it has been problematic.

Once the VC address for the destination data link layer address has been found, it can be used to transmit the packet through the ATM backbone. However, if no PVC is currently defined from the edge switch to the destination edge switch, then the edge switch must establish a new SVC.

Once the VC is ready, the LAN packet is broken into the series of ATM cells and transmitted over the ATM backbone using the ATM VC identifier. The destination edge switch then reassembles the ATM cells into the LAN packet and forwards it to the appropriate device.

This process is not without cost. The resolution of the Ethernet address into an ATM VC identifier, the setup of the SVC (if necessary), and the packetization and reassembly of the LAN packets to and from ATM cells can impose quite a delay. Recent tests of ATM edge switches suggest that even though they are capable of transmitting at 155 Mbps, the encapsulation delays can reduce performance significantly.

Multiprotocol over ATM (MPOA) is an extension to LANE. MPOA uses the network layer address (e.g., IP address) in addition to the data link layer address. If the packet destination is in the same subnet, MPOA will use data link layer addresses in the

TECHNICAL

FOCUS

8-1 ATM CLASSES OF SERVICE

Asynchronous transfer mode (ATM) provides five classes of service that each receive different priorities in traveling through the network:

- Constant bit rate (CBR) means that the circuit must provide a constant, predefined data rate at all times, much like having a point-to-point physical circuit between the devices. Whenever a CBR circuit is established, ATM guarantees that the switch can provide the circuit; the sum of all CBR circuits at one switch cannot exceed its capacity, even if they are all not active simultaneously. In some ways, CBR is like time division multiplexing, discussed in Chapter 3. CBR was originally designed to support voice transmissions.
- Variable bit rate-real time (VBR-RT) means that the data transmission rate in the circuit will vary but that all cells received must be switched immediately on arrival because the devices (or people) on the opposite ends of the circuit are waiting for the transmission and expect to receive it in a timely

fashion. Each VBR-RT circuit is assigned a standard transmission rate but can exceed it. If the cells in a VBR-RT circuit arrive too fast to transmit, they are lost. Most voice traffic today uses VBR-RT rather than CBR.

- Variable bit rate-nonreal time (VBR-NRT) means that the data transmission rate in the circuit will vary and that the application is tolerant of delays.
- Available bit rate (ABR) means that the circuit can tolerate wide variation in transmission speeds and many delays. ABR circuits have lower priority than VBR-NRT circuits. They receive the lowest amount of guaranteed capacity but can use whatever capacity is available (i.e., not in use by CBR, VBR-RT, and VBR-NRT circuits).
- Unspecified bit rate (UBR) means that the circuit has no guaranteed data rate but that data are transported when capacity is available. When the network is busy, UBR packets are the first to be discarded. Using UBR is a bit like flying standby on an airline.

same manner as LANE. If the packet is addressed to a different subnet, MPOA will use the network layer address to forward the packet. In an ATM MPOA network, a series of *route servers* (also called MPOA servers or MPSs) are provided that perform somewhat the same function as DNS servers in TCP/IP networks (see Chapter 5): route servers translate network layer addresses (e.g., IP addresses) into ATM virtual circuit identifiers.

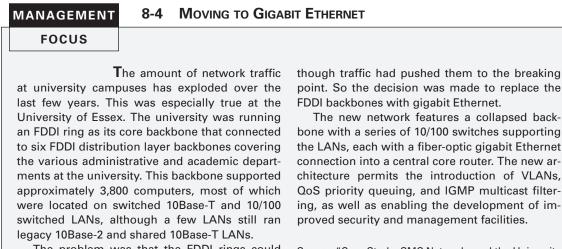
THE BEST PRACTICE BACKBONE DESIGN

The past few years have seen radical changes in the backbone, both in terms of new technologies (e.g., gigabit Ethernet) and in architectures (e.g., collapsed backbones, VLANs). Ten years ago, the most common backbone architecture was the routed backbone, connected to a series of shared 10Base-T hubs in the LAN. For many years, experts predicted that ATM would be the preferred backbone technology and that there was a good chance that ATM would gradually move into the LAN. Today, however, with the arrival of gigabit Ethernet, things are different.

Our recommendations for the best practice backbone design depend heavily on data rates and cost, as they did for LANs in the previous chapters. The design of backbone net-

290

CHAPTER 8 BACKBONE NETWORKS



The problem was that the FDDI rings could not be increased from the standard 100 Mbps alpoint. So the decision was made to replace the FDDI backbones with gigabit Ethernet.

The new network features a collapsed backbone with a series of 10/100 switches supporting the LANs, each with a fiber-optic gigabit Ethernet connection into a central core router. The new architecture permits the introduction of VLANs, QoS priority queuing, and IGMP multicast filtering, as well as enabling the development of improved security and management facilities.

SOURCE: "Case Study: SMC Networks and the University of Essex," www.ComputerWeekly.com, 2004.

works raises two new factors: backbone architecture and the need to translate between protocols. We begin with architectures and then turn our attention to effective data rates, translation, and costs.

Architectures

The most effective architecture in terms of cost and performance is a collapsed backbone (either rack-mounted or using a chassis switch) because it provides best performance at the least cost. VLANs come a close second, but as they are less mature at this point, many organizations prefer to stay with tried-and-true technologies. As VLANs mature, more organizations will begin to gain experience with them.

Effective Data Rates

As you will recall, the effective data rate of the hardware layers is the maximum practical speed in bits that the hardware layers can be expected to provide and depends on four basic factors: nominal data rates, error rates, efficiency of the data link layer protocols used, and efficiency of the media access control protocols. We will assume that error rates are similar between different technologies. Our analyses therefore focus on nominal data rates, data link protocol efficiency, media access control protocol efficiency, and the impact of translations. Gigabit Ethernet was examined in the previous chapter, so we focus on ATM.

Data Link Protocol Efficiency ATM adds 5 bytes of overhead to every 53-byte cell. On top of this, we must also include the overhead bits added by the physical layer protocols such as SONET. Without showing all calculations, this gives an efficiency of approximately 87 percent.

Media Access Control Protocol Efficiency Because ATM uses full-duplex transmission, its media access control protocol efficiency is almost 100 percent. This

THE BEST PRACTICE BACKBONE DESIGN 291

means, for example, that an ATM network providing 155-Mbps circuits is capable of providing a total network capacity of about 135 Mbps simultaneously in both directions, or a total of about 270 Mbps (87% efficiency $\times 100\%$ capacity $\times 155$ Mbps = 135 Mbps). An ATM network providing 622-Mbps circuits is capable of providing a total network capacity of about 540 Mbps simultaneously in both directions, or a total of about 1080 Mbps.

Conversion between Protocols

ATM requires Ethernet packets to be converted into ATM protocols before they can be sent across backbones using these technologies.

ATM uses *encapsulation* to convert packets, which means that the Ethernet packet is simply surrounded by an ATM cell—or more properly by a series of ATM cells—which are removed when the packet reaches the last ATM switch in the backbone. In general, encapsulation is a fast process. However, ATM must generate new routing information using its virtual channels. Performing this new routing is very time consuming. Tests suggest this address translation process decreases efficiency anywhere from 30 to 40 percent depending on the specific brand of ATM equipment in use. Thus, the actual effective data rate of 155-Mbps ATM when used to connect Ethernet LANs is approximately 80 Mbps in either direction, for a total of 160 Mbps. The actual effective data rate of 622 Mbps is probably closer to 380 Mbps each way or 760 Mbps in total because it suffers from a low percentage of efficiency loss.

As we discussed in the last chapter, the effective data rate of full-duplex gigabit Ethernet is approximately 1.8 Gbps. The results are summarized in Figure 8.17.

Recommendations

Given these trade-offs in costs and effective data rates, there are several best practice recommendations. First, the best practice architecture is a collapsed backbone or VLAN. Second, the best practice recommendation for backbone technology is gigabit Ethernet, which is why shipments of ATM have dropped significantly over the past year.

Considering the LAN and backbone environments together, the ideal network design is likely to be a mix of layer-2 and layer-3 Ethernet switches. Figure 8.18 shows one likely design. The access layer (i.e., the LANs) uses 100Base-T layer-2 Ethernet switches running on cat 5e or cat 6 twisted-pair cables to provide flexibility for 100Base-T or

Technology	Effective Data Rate			
Full Duplex 1 GbE	1.8 Gbps			
Full Duplex 10 GbE	18 Gbps			
155 Mbps ATM (Full Duplex)	160 Mbps			
622 Mbps ATM (Full Duplex)	760 Mbps			
Assumptions: collapsed backbone connecting Ethernet LANs that transmit mostly large frames.				

FIGURE 8.17 Effective data rate estimates for backbone technologies.



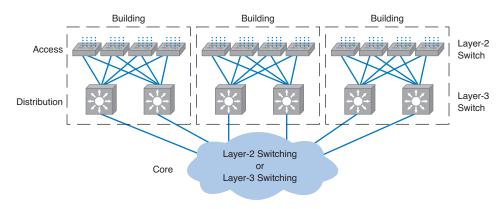


FIGURE 8.18 The best practice network design.

1000Base-T. The distribution layer uses layer-3 Ethernet switches that use 100Base-T or more likely 1000Base-T/F (over fiber or cat 6 or 7) to connect to the access layer. To provide good reliability, some organizations may provide redundant switches, so if one fails, the backbone continues to operate. The core layer uses layer-3 Ethernet switches running 10 GbE or 40 GbE over fiber.

TECHNICAL 8-2 MULTIPROTOCOL LABEL SWITCHING

FOCUS

Multiprotocol Label Switching (MPLS) is a new approach to improving QoS and the movement of packets with different layer-2 protocols through TCP/IP networks. MPLS uses a PVC approach to routing similar to that used by ATM LANE or MPOA.

With MPLS, routers called *Label Switched Routers* (LSRs) are used. The network manager defines a series of PVCs (which MPLS calls *Forwarding Equivalence Classes [FEC]*) through the network of LSRs. Each FEC has a reserved data rate and a QoS in the same way that ATM PVCs have them.

When a packet arrives at the edge of the MPLS network, an edge LSR reads the destination address on the incoming packet. The edge LSR can be configured to use the IP address, the IP address and the source or destination port, the ATM address, or the address in any protocol understood by the LSR. The edge LSR accepts the incoming packet and attaches an MPLS *label* (a packet that contains the FEC address). The edge LSR then forwards the packet to the next LSR as defined in the FEC.

This LSR reads the MPLS label and removes it from the incoming packet, consults its MPLS address table to find the packet's next destination, attaches a new MPLS label with the new FEC address, and forwards the packet to the next LSR in the FEC.

This process continues until the packet reaches the edge LSR closest to its final destination. This edge LSR strips off the MPLS label and forwards the packet outside of the MPLS network in exactly the same format in which it entered the MPLS network.

The advantage of MPLS is that it can easily integrate different layer-2 protocols and also provide QoS in an IP environment. It also enables traffic management the same as applicationbased VLANs by enabling the network manager to specify FEC based on both the IP address and the source or destination port.

IMPROVING BACKBONE PERFORMANCE

The method for improving the performance of BNs is similar to that for improving LAN performance. First, find the bottleneck, then solve it (or, more accurately, move the bottleneck somewhere else). You can improve the performance of the network by improving the performance of the computers and other devices in the network, by upgrading the circuits between computers, and by changing the demand placed on the network (Figure 8.19).

Improving Computer and Device Performance

The primary functions of computers and devices in BNs are routing and protocol translations. If the devices and computers are the bottleneck, routing can be improved with faster devices or a faster routing protocol. Static routing is accomplished faster than dynamic routing (see Chapter 5) but obviously can impair circuit performance in high-traffic situations. Dynamic routing is usually used in WANs and MANs because there are many possible routes through the network. BNs often have only a few routes through the network, so dynamic routing may not be too helpful since it will delay processing and increase the network traffic because of the status reports sent through the network. Static routing will often simplify processing and improve performance.

ATM requires the encapsulation of Ethernet packets before they can flow through the backbone. This additional processing slows the devices connecting the BN to the attached LANs. One obvious solution is to use the same protocols in the backbone and the LANs. If you have Ethernet LANs, gigabit Ethernet backbones can reduce processing at the connecting devices.

Most backbone devices are store-and-forward devices. One simple way to improve performance is to ensure that they have sufficient memory. If they don't, the devices will lose packets, requiring them to be retransmitted.

Performance Checklist

Increase Computer and Device Performance

- Change to a more appropriate routing protocol (either static or dynamic)
- Buy devices and software from one vendor
- Reduce translation between different protocols
- · Increase the devices' memory

Increase Circuit Capacity

- · Upgrade to a faster circuit
- Add circuits

Reduce Network Demand

- Change user behavior
- Reduce broadcast messages



Improving Circuit Capacity

If network circuits are the bottlenecks, there are several options. One is to increase overall circuit capacity (e.g., by going from 100Base-T Ethernet to gigabit Ethernet). Another option is to add additional circuits alongside heavily used ones so that there are several circuits between some devices (as in Figure 8.11). Circuit capacity can also be improved by replacing a shared-circuit backbone with a switched-circuit backbone (e.g., by replacing Ethernet with switched Ethernet).

In many cases, the bottleneck on the circuit is only in one place—the circuit to the server. A switched network that provides 100 Mbps to the client computers but a faster circuit to the server (e.g., 1000Base-T) can improve performance at very little cost.

Reducing Network Demand

One way to reduce network demand is to restrict applications that use a lot of network capacity, such as desktop videoconferencing, medical imaging, or multimedia. In practice, it is often difficult to restrict users. Nonetheless, finding one application that places a large demand on the network and moving it can have a significant impact.

Much network demand is caused by broadcast messages, such as those used to find data link layer addresses (see Chapter 5). Some application software packages and NOS modules written for use on LANs also use broadcast messages to send status information to all computers on the LAN. For example, broadcast messages inform users when printers are out of paper, or when the server is running low on disk space. When used in a LAN, such messages place little extra demand on the network because every computer on the LAN gets every message.

This is not the case for switched LANs or LANs connected to BNs because messages do not normally flow to all computers. Broadcast messages can consume a fair amount of network capacity. In many cases, broadcast messages have little value outside their individual LAN. Therefore, some switches, and routers can be set to filter broadcast messages so that they do not go to other networks. This reduces network traffic and improves performance.

IMPLICATIONS FOR MANAGEMENT

As the technologies used in LANS and WLANs become faster and better, the amount of traffic the backbone network needs to support is increasing at an even faster rate. Coupled with the significant changes in the best practice recommendations for the design of backbone networks, this means that many organizations have had to replace their backbones completely. We would like to think that these have been one-time expenditures, but, as traffic grows, demand placed on the backbone will continue to increase; meaning the amount spent on switches and routers for use in the backbone will increase. Designing backbone networks to be easily upgradable is now an important management goal.

As recently as five years ago, ATM was seen as a viable technology for use in backbone networks. Today, however, most organizations view ATM as a legacy backbone technology: no new backbone networks will be installed using it, but existing backbones will still be supported and upgraded. Therefore, most vendors have stopped the development of ATM technologies intended for use in backbone networks. As vendors stop development of tech-

294

SUMMARY 295

nologies, they more quickly become legacy technologies. The implication is that organizations that still use ATM in their backbone will be faced with a need to invest more funds to replace these outgoing technologies.

On the other hand, as Ethernet moves more extensively into the backbone and pushes out ATM, the costs associated with buying and maintaining backbone devices and training networking staff will continue to decrease, since now there will be one standard technology in use throughout the LAN, WLAN, and backbone. The new focus is on faster and faster versions of Ethernet. While we will spend more on new equipment, performance will increase much more quickly, and the cost to operate the equipment will decrease.

SUMMARY

Network Components There are two basic components to a BN: the network cable and the hardware devices that connect other networks to the backbone. The cable is essentially the same as those used in LANs, except that it is usually fiber optic to provide higher data rates. The hardware devices include routers, gateways, and switches. Switches connect two LAN segments that use the same data link and network protocol and forward only those messages that need to go to other network segments. Routers connect two or more LANs that use the same or different data link protocols but employ the same network protocol. Gateways connect two or more LANs that use the same or different data link and network protocols (usually different). Layer-2 switches are similar to bridges, whereas layer-3 switches are similar to routers.

Backbone Architectures Network designers often think about three distinct technology layers when designing backbones. The access layer is the LAN, the distribution layer connects the LANs together, and the core layer connects the distribution-layer BNs together. The distribution layer is usually a backbone within a building whereas the core layer often connects buildings and is sometimes called the campus network. A routed backbone uses a set of routers or layer-3 switches to connect LANs together and moves messages using layer-3 addresses. A collapsed backbone uses one device, usually a layer-2 switch, to connect the LANs. A VLAN uses layer-2 or layer-3 switches to build logical or virtual LANs that enable the network manager to assign capacity separate from physical location.

ATM ATM is a packet-switched technology originally designed for use in WANs. ATM uses 53-byte fixed-length packets with no error control of full-duplex 155 Mbps or 622 Mbps point-to-point circuits. ATM enables QoS and uses virtual circuits rather than permanently assigning addresses to devices. To use ATM in a BN that connects LANs, some conversion must be done on the LAN packets to enable them to flow over the ATM backbone. With LANE, an ATM edge switch encapsulates the Ethernet packet, leaving the existing data link layer packet intact, and transmits it on the basis of data link layer addresses. MPOA is an alternative that can use network-layer addresses for transmission.

Best Practice Backbone Design The best practice backbone design depends on cost, effective data rates, and the need to convert protocols. While ATM provides reasonably fast transmission, the need to convert from the Ethernet packets used in the LAN to ATM packets in the backbone imposes significant time delays. Given the trade-offs in costs and effective data rates, the best backbone architecture for most organizations is a collapsed backbone (using a rack or a chassis switch). The recommended technology is gigabit Ethernet.

Improving Backbone Performance Backbone performance can be improved by converting all devices to use the same data link layer and network layer routing protocols to provide consistency throughout the network. Upgrading to faster circuits and adding additional circuits on very busy backbones can also improve performance. Finally, one could move servers closer to the end users or reduce broadcast traffic to reduce backbone traffic.

296

CHAPTER 8 BACKBONE NETWORKS

KEY TERMS

access layer application-based VLAN asynchronous transfer mode (ATM) backbone network (BN) campus network chassis switch classes of service collapsed backbone core layer distribution layer edge switch encapsulation enterprise network forwarding equivalence class (FEC) gateways IEEE 802.1q IP-based VLAN label switched router (LSR) LAN Emulation (LANE) layer-1 VLAN layer-2 switch layer-2 VLAN layer-3 switch layer-3 VLAN layer-4 VLAN MAC-based VLAN main distribution facility (MDF) module multiprotocol label switching (MPLS) multiprotocol over ATM (MPOA) multiprotocol router multiprotocol switch multiswitch VLAN patch cables permanent virtual circuit (PVC) policy-based VLAN port-based VLAN rack routed backbone router single-switch VLAN switched virtual circuit (SVC) virtual channel (VC) virtual circuit virtual LAN (VLAN)

QUESTIONS

- 1. Compare and contrast switches, routers, and gateways.
- **2.** How does a layer-2 switch differ from a layer-3 switch?
- 3. How does a router differ from a layer-3 switch?
- **4.** Under what circumstances would you want to use a router?
- **5.** Under what circumstances would you want to use a multiprotocol router?
- **6.** What is an enterprise network?
- **7.** What are the three technology layers important in backbone design?
- 8. Explain how routed backbones work.
- 9. Where are routed backbones most commonly used?
- **10.** Explain how collapsed backbones work.
- **11.** What are the key advantages and disadvantages of routed and collapsed backbones?
- Compare and contrast rack-based and chassis switchbased collapsed backbones.
- 13. What is a module and why are modules important?
- 14. Explain how single-switch VLANs work.
- 15. Explain how multiswitch VLANs work.
- **16.** Explain the differences among layer-1, -2, -3, and -4 VLANs.
- **17.** What is IEEE 802.1q?
- **18.** Which backbone architecture is the most flexible? Why?

- **19.** How does gigabit Ethernet differ from ATM?
- **20.** Is ATM a laye-2 or layer-3 technology? Explain.
- **21.** Discuss three important characteristics of ATM.
- 22. How does ATM perform addressing?
- **23.** How can ATM be used to link Ethernet LANs?
- **24.** What is encapsulation and how does it differ from translation?
- 25. How can you improve the performance of a BN?
- **26.** Why are broadcast messages important?
- **27.** Which has greater throughput: ATM or switched 100Base-T Ethernet?
- 28. How does an ATM MPOA carry an Ethernet packet?
- **29.** How does ATM LANE carry an Ethernet packet?
- **30.** What are the preferred technologies used in the three technology layers in backbone design?
- **31.** What are the preferred architectures used in the three technology layers in backbone design?
- 32. What do you think is the future of ATM and Ethernet?
- **33.** Some experts are predicting that Ethernet will move into the WAN. What do you think?
- **34.** Some companies continue to use ATM in their backbones and to install new ATM backbones, even though they are aware of the best practice recommendations now favoring gigabit Ethernet. Why do you think they choose ATM over gigabit Ethernet?

EXERCISES

- **8-1.** Survey the BNs used in your organization. Do they use Ethernet, ATM, or some other technology? Why?
- **8-2.** Document one BN in detail. What devices are attached, what cabling is used, and what is the topology? What networks does the backbone connect?
- **8-3.** You have been hired by a small company to install a backbone to connect four 100base-T Ethernet LANs (each using one 24-port hub) and to provide a connection to the Internet. Develop a simple backbone

and determine the total cost (i.e., select the backbone technology and price it, select the cabling and price it, select the devices and price them, and so on). Prices are available at www.datacommwarehouse .com, but use any source that is convenient. For simplicity, assume that category 5, category 5e, category 6, and fiber-optic cable have a fixed cost per circuit to buy and install, regardless of distance, of \$50, \$60, \$120, and \$300, respectively.

MINI-CASES

I. Pat's Engineering Works

Pat's Engineering Works is a small company that specializes in complex engineering consulting projects. The projects typically involve one or two engineers who do data intensive analyses for companies. Because so much data are needed, the projects are stored on the company's high-capacity server but moved to the engineers' work-stations for analysis. The company is moving into new offices and wants you to design its network. It has a staff of 8 engineers (which is expected to grow to 12 over the next 5 years), plus another 8 management and clerical employees who also need network connections but whose needs are less intense. Design the network. Be sure to include a diagram.

II. Hospitality Hotel

Hospitality Hotel is a luxury hotel whose guests are mostly business travelers. To improve its quality of service. It has decided to install network connections in each of its 600 guest rooms and 12 conference meeting rooms. Last year, the hotel upgraded its own internal networks to switched 10Base-T, but it wants to keep the public network (i.e., the guest and meeting rooms) separate from its private network (i.e., its own computer systems). Your task is to design the public network; do not worry about how to connect the two networks together (that's the job of another consultant). Be sure to include a diagram.

III. Transco

Reread Management Focus 8-1. What other alternatives do you think that Transco considered? Why do you think they did what they did?

IV. Central Parking

Reread Management Focus 8-2. What other alternatives do you think that Indiana University considered? Why do you think they did what they did?

V. IONA

Reread Management Focus 8-3. What other alternatives do you think that IONA considered? Why do you think they did what they did?

VI. University of Essex

Reread Management Focus 8-4. What other alternatives do you think that University of Essex considered? Why do you think they did what they did?

VII. Western Trucking

Western Trucking operates a large fleet of trucks that deliver shipments for commercial shippers such as food stores, retailers, and wholesalers. Their main headquarters building and secondary building are shown in Figure 8.20. They currently have a mix of shared 10Base-T and switched 10Base-T LANs, connected by a series of switches. They want to upgrade to a faster network. Design a new network for them, including the architecture and specific backbone and LAN technologies to be used.

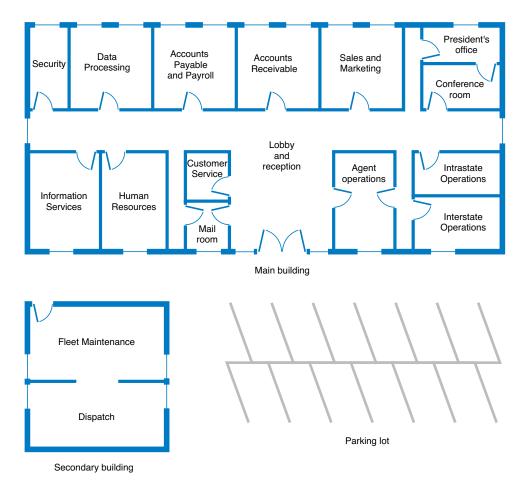


FIGURE 8.20 Facility map of the Western Trucking headquarters.

CASE STUDY

NEXT-DAY AIR SERVICE

See the Web site.

HANDS-ON ACTIVITY

Network Mapping

A backbone network connects one or more LANs to each other and usually to the Internet or to another backbone that eventually leads to the Internet. Each of these backbones usually connects many computers.

Network mapping software enables you to generate a map of the computers on all the LANs connected to a backbone. There are many good network mapping packages. Two of my favorites are LANState and LAN Surveyor. LANState is simpler to use but works best for small networks. LAN Surveyor is more complex, but can map large networks.

Both work in the same way. They use the ping command (see Chapter 5) to send IMCP requests to all possible IP addresses in any range you specify. Any computer that responds is added to the map.

Mapping A Small Network

The first step is to download and install LANState. A demo version of the software is available free of charge from 10-Strike Software (www.10-strike.com/lanstate).

You begin by creating a new network map (choose File Create). Then use the Network Map Creation Wizard and choose to Scan an IP-address range. You will be asked to enter an address range Choose some range, ideally the address range of a small network. I choose to use my home network range (192.168.1.1 through 192.168.1.254). When the scan is complete you will see a list of computers. Click Finish to see a map of these computers.

LANState does not do a good job of drawing a map, but you can rearrange the computers by dragging and dropping them. You can also add lines to make the map look more like a network diagram. Figure 8.21 shows the small network in my house. I have a router (192.168.1.1) that connects a number of computers to the Internet. I also have a wireless access point (192.168.1.100) and a music server (192.168.1.52). When I did this map, three computers were turned on and responded to LANState's pings (192.168.1.102, 192.168.1.103, 192.168.1.111). Computers and devices that are not turned on do not respond to the pings and therefore are not mapped. Since I use dynamic addressing, the addresses of my computers will change every time I turn them on.

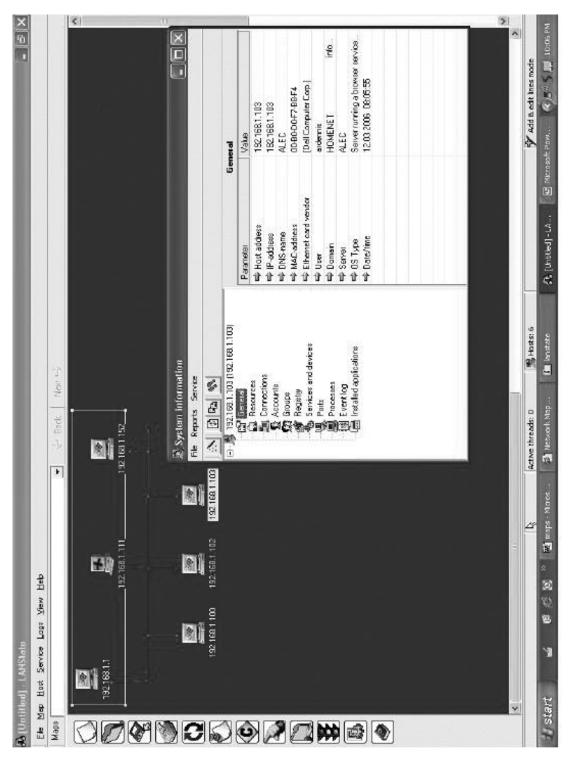
You can also left click on any device and choose System Information and General to learn more about that device. Figure 8.21 also shows the information about my son's computer (192.168.1.103). It shows the MAC address (i.e., the Ethernet address), the card manufacturer, and Windows workgroup peer-to-peer network information (i.e., application layer address) for this computer.

Mapping A Large Network

The first step is to download and install LAN Surveyor. A demo version of the software is available free of charge from Neon Software (www.neon.com/ls1.shtml). Installing the software and setting it up to run is more complex, so be sure to follow the setup and configuration instructions.

You begin by creating a new network map (choose File New). You will be asked to enter an address range. Choose some range, ideally the address range of a large network. I choose to use part of the Indiana University network (129.79.1.1 through 129.79.1.254). There is no rule preventing you from scanning anyone's network, but many companies (and individuals) feel that scanning their networks is an invasion of privacy, so scan carefully. When the scan is complete, you will see a map of computers.

My scan of this one small part of the Indiana University network found 124 computers. Figure 8.22 shows a partial list of the computers and their IP addresses and host names (i.e., application layer addresses).



Œ

ŧ

FIGURE 8.21 Network mapping with LANState.

300

CHAPTER 8 BACKBONE NETWORKS

