1
CHAPTER

NETWORK INFRASTRUCTURE DESIGN

Chapter Outline

Objectives

- Understand the purpose of the three layers of a campus network design
- Understand the issue of data flow and selecting the network media
- Develop techniques for IP allocation and subnet design
- Understand the process of configuring a VLAN
- Understand the issues of configuring the Layer 3 routed network

Key Terms

core
distribution layer
access layer
CIDR
ISP
intranets
NAT
PAT
Overloading
supernet
gateway
broadcast domain
flat network
VLAN (virtual LAN)
port-based VLAN
tag-based VLAN
protocol-based VLAN
VLAN ID
802.1Q
static VLAN
dynamic VLAN
show vlan
vlan database
vlan *vlan_id*
show vlan name *vlan-name*
interface vlan 1
show interface status
trunk port
Inter-Switch Link (ISL)
Switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk encapsulation isl
switchport trunk allowed vlan *vlan_id*
show interfaces trunk
network address
logical address
router interface
routing table
subnet, NET
multilayer switch (MLS)
wire speed routing
routed network
Layer 3 network
SONET
WAN
terminal monitor (**term mon**)
terminal no monitor (**term no mon**)
show ip interface brief (**sh ip int br**)
no switchport
secondary IP address
InterVLAN routing
router on a stick
SVI
DS
CSU/DSU
AMI
B8ZS
Minimum Ones Density
HDLC
PPP
WIC
VWIC
service-module t1
show controller t1 *slot/port*
ATM
Virtual Path Connection (VPC)
Virtual Channel Connection (VCC)
SVC
VPI
VCI

INTRODUCTION

The objective of this chapter is to examine the computer networking issues that arise when planning a campus network. The term *campus network* applies to any network that has multiple LANs interconnected. The LANs are typically in multiple buildings that are close to each other and interconnected with switches and routers. This chapter looks at the planning and designs of a simple campus network, including network design, IP subnet assignment, VLAN configuration, and routed network configuration.

The basics of configuring the three layers of a campus LAN (core, distribution, and access) are first examined in Section 1-1. This section also addresses the important issues of data flow and selecting the proper network media. Section 1-2 examines IP allocation and subnet design. Section 1-3 discusses the VLAN network, including a step-by-step process of how to configure a VLAN, which provides an introduction to the basic switch commands and the steps for configuring a static VLAN. Section 1-4 examines the Layer 3 routed network. This section explores the functions of the router and includes configuration examples in different scenarios.

1-1 PHYSICAL NETWORK DESIGN

Most campus networks follow a design that has core, distribution, and access layers. These layers, shown in Figure 1-1, can be spread out into more layers or compacted into fewer, depending on the size of these networks. This three-layer network structure is incorporated in campus networks to improve data handling and routing within the network. The issues of data flow and network media are also examined in this section.

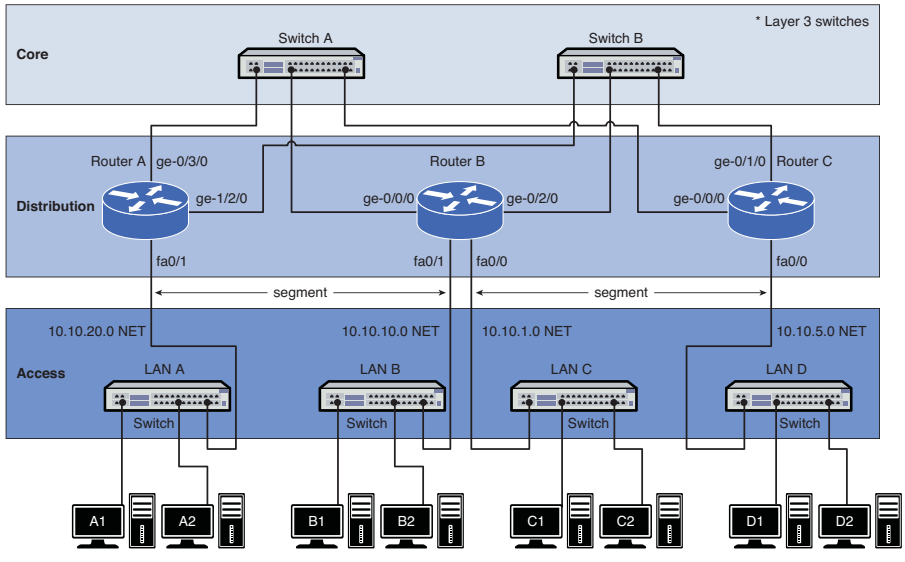


FIGURE 1-1 The core, distribution, and access layers of a campus network

Core

Core
The Backbone of the Network

The network core usually contains high-end Layer 3 switches or routers. The **core** is the heart, or backbone, of the network. The major portion of a network's data traffic passes through the core. The core must be able to quickly forward data to other parts of the network. Data congestion should be avoided at the core, if possible. This means that unnecessary route policies should be avoided. An example of a route policy is *traffic filtering,* which limits what traffic can pass from one part of a network to another. Keep in mind that it takes time for a router to examine each data packet, and unnecessary route policies can slow down the network's data traffic.

High-end routers and Layer 3 switches are typically selected for use in the core. Of the two, the Layer 3 switch is the best choice. A Layer 3 switch is essentially a router that uses electronic hardware instead of software to make routing decisions. The advantage of the Layer 3 switch is the speed at which it can make a routing decision and establish a network connection.

Another alternative for networking hardware in the core is a Layer 2 switch. The Layer 2 switch does not make any routing decisions and can quickly make network connection decisions based on the network hardware connected to its ports. The advantage of using the Layer 2 switch in the core is cost. The disadvantage is that the Layer 2 switch does not route data packets; however, high-speed Layer 2 switches are more affordable than high-speed routers and Layer 3 switches.

An important design issue in a campus network and the core is redundancy. *Redundancy* provides for a backup route or network connection in case of a link failure. The core hardware is typically interconnected to all distribution network hardware, as shown in Figure 1-1. The objective is to ensure that data traffic continues for the entire network, even if a core networking device or link fails.

Each layer beyond the core breaks the network into smaller networks with the final result being a group of networks that are capable of handling the amount of traffic generated. The design should thus incorporate some level of redundancy.

Distribution Layer

Distribution Layer
Point where the individual LANs connect together.

The **distribution layer** in the network is the point where the individual LANs connect to the campus network routers or Layer 3 switches. Routing and filtering policies are more easily implemented at the distribution layer without having a negative impact on the performance of the network data traffic. Also, the speed of the network data connections at the distribution layer is typically slower than at the core. For example, connection speeds at the core should be the highest possible, such as 1 or 10 gigabits, where the data speed connections at the distribution layer could be 100 Mbps or 1 gigabit. Figure 1-1 shows the connections to the access and core layers via the router's Ethernet interfaces.

Access Layer

Access Layer
Where the networking devices in a LAN connect together.

The **access layer** is where the networking devices in a LAN connect together. The network hardware used here is typically a Layer 2 switch. Remember, a switch is a better choice because it forwards data packets directly to destination hosts connected to its ports, and network data traffic is not forwarded to all hosts in the network. The exception to this is a broadcast where data packets are sent to all hosts connected to the switch.

NOTE

Hubs are not recommended at all in modern computer networks.

Data Flow

An important networking issue is how data traffic flows in the core, distribution, and access layers of a campus LAN. In reference to Figure 1-1, if computer A1 in LAN A sends data to computer D1 in LAN D, the data is first sent through the switch in LAN A and then to Router A in the distribution layer. Router A then forwards the data to the core switches, Switch A or Switch B. Switch A or Switch B then forwards the data to Router C. The data packet is then sent to the destination host in LAN D.

The following are some questions often asked when setting up a network that implements the core, distribution, and access layers:

- **In what layer are the campus network servers (web, email, DHCP, DNS, and so on) located?** This varies for all campus networks, and there is not a definitive answer. However, most campus network servers are located in the access layer.
- **Why not connect directly from Router A to Router C at the distribution layer?** There are network stability issues when routing large amounts of network data traffic if the networks are fully or even partially meshed together. This means that connecting routers together in the distribution layer should be avoided.
- **Where is the campus backbone located in the layers of a campus network?** The backbone of a campus network carries the bulk of the routed data traffic. Based on this, the backbone of the campus network connects the distribution and the core layer networking devices.

Selecting the Media

The choices for the media used to interconnect networks in a campus network are based on several criteria. The following is a partial list of things to consider:

- Desired data speed
- Distance for connections
- Budget

The desired data speed for the network connection is probably the first consideration given when selecting the network media. Twisted-pair cable works well at 100 Mbps and 1 Gbps and is specified to support data speeds of 10-gigabit data traffic. Fiber-optic cable supports LAN data rates up to 10 Gbps or higher. Wireless networks support data rates up to 200+ Mbps.

The distance consideration limits the choice of media. CAT 6/5e or better have a distance limitation of 100 meters. Fiber-optic cable can be run for many kilometers, depending on the electronics and optical devices used. Wireless LAN connections can also be used to interconnect networks a few kilometers apart.

The available budget is always the final deciding factor when planning the design for a campus LAN. If the budget allows, fiber-optic cable is probably the best overall choice, especially in the high-speed backbone of the campus network. The cost of fiber is continually dropping, making it more competitive with lower-cost network media, such as twisted-pair cable. Also, fiber cable will always be able to carry a greater amount of data traffic and can easily grow with the bandwidth requirements of a network.

Twisted-pair cable is a popular choice for connecting computers in a wired LAN. The twisted-pair technologies support bandwidths suitable for most LANs, and the performance capabilities of twisted-pair cable is always improving.

Wireless LANs are being used to connect networking devices together in LANs where a wired connection is not feasible or mobility is the major concern. For example, a wireless LAN could be used to connect two LANs in a building together. This is a cost-effective choice if there is not a cable duct to run the cable to interconnect the LANs or if the cost of running the cable is too high. Also, wireless connections are playing an important role with mobile users within a LAN. The mobile user can make a network connection without having to use a physical connection or jack. For example, a wireless LAN could be used to enable network users to connect their mobile computers to the campus network.

1-2 IP SUBNET DESIGN

Once the physical infrastructure for a network is in place, the next big step is to plan and allocate IP space for the network. Take time to plan the IP subnet design, because it is not easy to change the IP subnet assignments once they are in place. It is crucial for a network engineer to consider three factors before coming up with the final IP subnet design. These three factors are

1. The assigned IP address range
2. The number of subnetworks needed for the network
3. The size or the number of IP host addresses needed for the network

The final steps in designing the IP subnet is to assign an IP address to the interface that will serve as the gateway out of each subnet.

IP Address Range

CIDR
Classless Interdomain Routing

ISP
Internet service provider: An organization that provides Internet access for the public.

The IP address range defines the size of the IP network you can work with. In some cases, a classless interdomain routing (**CIDR**) block of public IP addresses might be allocated to the network by an ISP. For example, the block of IP address 206.206.156.0/24 could be assigned to the network. This case allocates 256 IP addresses to the 206.206.156.0 network. In another case, a CIDR block of private IP addresses, like 10.10.10.0/24, could be used. In this case, 256 IP addresses are assigned to the 10.10.10.0 network. For established networks with an IP address range already in use, the network engineer generally has to work within the existing IP address assignments. With a brand new network, the engineer has the luxury of creating a network from scratch.

In most network situations, an IP address block will have been previously assigned to the network for Internet use. The public IP addresses are typically obtained from the **ISP** (Internet service provider). This IP block of addresses could be from Class A, B, or C networks, as shown in Table 1-1.

TABLE 1-1 **Address Range for Each Class of Network**

Class	Address Range
Class A	0.0.0.0 to 127.255.255.255
Class B	128.0.0.0 to 191.255.255.255
Class C	192.0.0.0 to 223.255.255.255

Intranets
Internetwork that provides file and resource sharing.

NAT
Network Address Translation. A technique used to translate an internal private IP address to a public IP address.

PAT
Port Address Translation. A port number is tracked with the client computer's private address when translating to a public address.

Overloading
Where NAT translates the home network's private IP addresses to a single public IP address.

Today, only public Class C addresses are assigned by ISPs, and most of them are not even a full set of Class C addresses (256 IP addresses). A lot of ISPs partition their allotted IP space into smaller subnets and then, in turn, provide those smaller portions to the customers. The bottom line is the limited number of public IP addresses are now a commodity on the Internet, and it is important to note that there are fees associated with acquiring an IP range from an ISP.

Not many institutions or businesses have the luxury of using public IP addresses inside their network anymore. This is because the growing number of devices being used in a network exceeds the number of public IP addresses assigned to them. The solution is that most networks are using private IP addresses in their internal network. Private addresses are IP addresses set aside for use in private **intranets**. An intranet is an internal internetwork that provides file and resource sharing. Private addresses are not valid addresses for Internet use, because they have been reserved for internal use and are not routable on the Internet. However, these addresses can be used within a private LAN (intranet) to create the internal IP network.

The private IP addresses must be translated to public IP addresses using techniques like **NAT** (Network Address Translation) or **PAT** (Port Address Translation) before being routed over the Internet. For example, computer 1 in the home network (see Figure 1-2) might be trying to establish a connection to an Internet website. The wireless router uses NAT to translate computer 1's private IP address to the public IP address assigned to the router. The router uses a technique called **overloading**, where NAT translates the home network's private IP addresses to the single public

IP address assigned by the ISP. In addition, the NAT process tracks a port number for the connection. This technique is called Port Address Translation (PAT). The router stores the home network's IP address and port number in a NAT lookup table. The port number differentiates the computer that is establishing a connection to the Internet because the router uses the same public address for all computers. This port number is used when a data packet is returned to the home network. This port number identifies the computer that established the Internet connection, and the router can deliver the data packet back to the correct computer. An example of this conversion is provided in Figure 1-3. This example shows three data connections originating from the home network of 192.168.0.0/24. A single 128.123.246.55 IP address is used for the Internet connection. Port address translation is being used to map the data packet back to the origination source. In this case, the port numbers are 1962, 1970, and 1973.

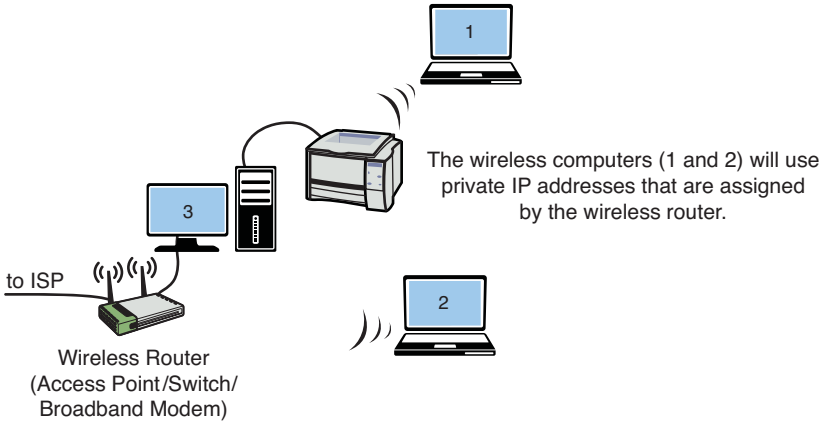


FIGURE 1-2 An example of a home computer connecting to the ISP

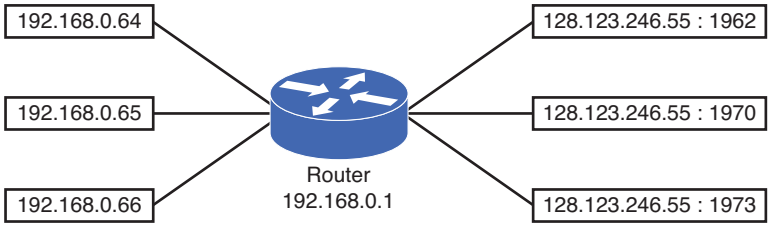


FIGURE 1-3 This example shows the three data connections originating from the home network of 192.168.0.0/24

Determining the Number of Subnetworks Needed for the Network

The use of private IP addresses is a viable technique for creating a large amount of IP addresses for intranet use. Obviously, there is a big difference when designing an IP network for a single network than there is when designing an IP network for multiple networks. When designing an IP network for one single network, things

are quite simple. This type of configuration is typically found in the home, small office, or a small business environment where one IP subnet is allocated and only one small router is involved.

For situations requiring multiple networks, each network must be sized accordingly. Therefore, the subnet must be carefully designed. In addition, networks with multiple subnets require a router or multiple routers with multiple routed network interfaces to interconnect the networks. For example, if the network engineer is using private addresses and needs to design for three different networks, one possibility is to assign 10.10.10.0/24 for the first network, 172.16.0.0/24 for the second network, and 192.168.1.0/24 for the third network. Is this a good approach? Technically, this can be done, but it is probably not logically sound. It makes more sense to group these networks within the same big CIDR block. This will make it easier for a network engineer to remember the IP assignments and to manage the subnets. A better design is to assign 10.10.10.0/24 to the first network, 10.10.20.0/24 to the second network, and 10.10.30.0/24 to the third network. All three networks are all in the same "10" network, which makes it easier for the network engineer to track the IP assignments. The term *subnet* and *network* are used interchangeably in multiple network environments. The term subnet usually indicates a bigger network address is partitioned and is assigned to smaller networks or subnets.

Another design factor that the network engineer must address is the network size. Two questions that a good network engineer must ask are

- How many network devices must be accommodated in the network? (Current demand)
- How many network devices must be accommodated in the future? (Future growth)

Simply put, the IP network must be designed to accommodate the current demand, and it must be designed to accommodate future growth. Once the size of a network is determined, a subnet can be assigned. In the case of a single network, the design is not too complicated. For example, if the network needs to be able to accommodate 150 network devices, an entire Class C address, like 192.168.1.0/24, can be assigned to the network. This will handle the current 150 network devices and leave enough room for growth. In this example, 104 additional IP address will be available for future growth.

When allocating IP address blocks, a table like Table 1-2 can be used to provide the CIDR for the most common subnet masks and their corresponding number of available IP addresses.

TABLE 1-2 **CIDR—Subnet Mask-IPs Conversion**

CIDR	Subnet Mask	IPs
/16	255.255.0.0	65534
/17	255.255.128.0	32768
/18	255.255.192.0	16384

CIDR	Subnet Mask	IPs
/19	255.255.224.0	8192
/20	255.255.240.0	4096
/21	255.255.248.0	2048
/22	255.255.252.0	1024
/23	255.255.254.0	512
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32
/28	255.255.255.240	16
/29	255.255.255.248	8
/30	255.255.255.252	4
/31	255.255.255.254	2
/32	255.255.255.255	1

Even with a much smaller network, like the home network, where only a handful of network computers and peripherals are present, an entire Class C private address is generally allocated to the home network. In fact, most home routers are preconfigured with a private Class C address within the 192.168.0.0–192.168.0.255 range. This technique is user friendly and easy to use and sets aside private IP addresses for internal network use. This technique virtually guarantees that users will never have to worry about subnetting the CIDR block.

For a bigger network that must handle more than 254 network devices, a supernet can be deployed. A supernet is when two or more classful contiguous networks are grouped together. The technique of supernetting was proposed in 1992 to eliminate the class boundaries and make available the unused IP address space. **Supernet**ting allows multiple networks to be specified by one subnet mask. In other words, the class boundary could be overcome. For example, if the network needs to be able to accommodate 300 network devices, two Class C networks, like 192.168.0.0/24 and 192.168.1.0/24, can be grouped together to form a supernet of 192.168.0.0/23, which can accommodate up to 510 network devices. As shown in Table 1-2, a /23 CIDR provides 512 available IP addresses. However, one IP is reserved for the network address and another one is reserved for the network broadcast address. Therefore, a /23 CIDR yields 512 – 2 = 510 usable host IP addresses.

Supernet
Two or more classful contiguous networks are grouped together.

Determining the Size or the Number of IP Host Addresses Needed for the Network

The problem with randomly applying CIDR blocks to Class A, B, and C addresses is that there are boundaries in each class, and these boundaries can't be crossed. If a boundary is crossed, the IP address maps to another subnet. For example, if a CIDR

block is expanded to include four Class C networks, all four Class C networks need to be specified by the same CIDR subnet mask to avoid crossing boundaries. The following example illustrates this.

Example 1-1

Figure 1-4 shows three different networks with different size requirements. The needed capacity (number of devices) for each network is specified in the figure. Your task is to determine the CIDR block required for each network that will satisfy the number of expected users. You are to use Class C private IP addresses when configuring the CIDR blocks.

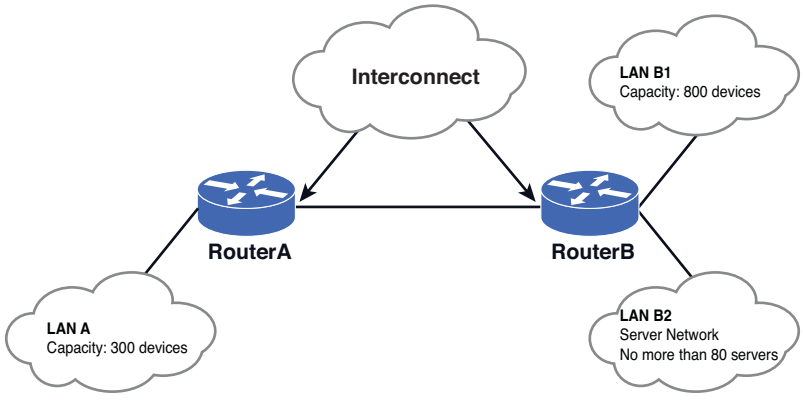


FIGURE 1-4 Three different networks

Solution:

For LAN A, a CIDR block that can handle at least 300 networking devices must be provided. In this case, two contiguous Class C networks of 192.168.0.0/24 and 192.168.1.0/24 can be grouped together to form a 192.168.0.0/23 network. Referring to Table 1-2, a /23 CIDR with a subnet mask of 255.255.254.0 provides 512 IP addresses which more than satisfies the required 300 networking devices.

The next question is to determine what the network address is for LAN A. This can be determined by ANDing the 255.255.254.0 subnet mask with 192.168.0.0 and 192.168.1.0.

192. 168. 0. 0	192. 168. 1. 0
255. 255. 254. 0 (/23)	255. 255. 254. 0 (/23)
192. 168. 0. 0	**192. 168. 0. 0**

This shows that applying the /23 [255.255.254.0] subnet mask to the specified IP address places both in the same 192.168.0.0 network. This also means that this CIDR block does not cross boundaries, because applying the subnet mask to each network address places both in the same 192.168.0.0 network.

For LAN B1, the requirement is that a CIDR block that can handle 800 network devices must be provided. According to Table 1-2, a /22 CIDR yields 1,022 usable host IP addresses and is equivalent to grouping four Class C networks together. Therefore, a /22 CIDR can be used.

The next decision is selecting the group of IP addresses to create the CIDR block and decide where the IP addresses should start. Recall that the 192.168.0.0 and 192.168.1.0 networks are being used to create the LAN A CIDR block. Should LAN B1 start from 192.168.2.0/22, which is the next contiguous space? The answer is no. The 192.168.2.0/22 is still within the boundary of the 192.168.0.0/23 network. Remember, the requirement is that a CIDR block that can handle 800 network devices must be provided and that boundaries cannot be crossed, and the designer must be careful not to overlap the networks when assigning subnets to more than one network. In this case, when the /22 subnet mask (255.255.252.0) is applied to 192.168.2.0, this yields the network 192.168.0.0. The AND operation is shown:

192. 168. 2. 0
255. 255.252. 0 (/22)
192. 168. 0. 0

This happens to be the same network address as when the /23 CIDR subnet mask (255.255.254.0) is applied to any IP within the range of 192.168.0.0-192.168.1.255, as shown:

192. 168. 0. 0	192. 168. 1. 255
255. 255. 254. 0 (/23)	255. 255. 254. 0 (/23)
192. 168. 0. 0	192. 168. 0. 0

There is an overlap between 192.168.0.0/23 and 192.168.2.0/22. Moving to the next contiguous Class C of 192.168.3.0/22, we still find that it's still in the 192.168.0.0:

192.168.3.0
255.255.252.0 (/22)
192.168.0.0 is still in the same subnet.

Based on this information, the next Class C range 192.168.4.0/22 is selected. This yields a nonoverlapping network of 192.168.4.0, so the subnet 192.168.4.0/22 is a valid for this network:

192.168.4.0
255.255.252.0 (/22)
192.168.4.0 is **not** the same subnet; therefore, this is an acceptable CIDR block.

Recall that the CIDR for LANB1 is a /22 and is equivalent to grouping four Class C networks. This means that LANB1 uses the following Class C networks:

192.168.4.0
192.168.5.0
192.168.6.0
192.168.7.0

The IP subnet design gets more complicated when designing multiple networks with different size subnets. This generally means that the subnet mask or the CIDR will not be uniformly assigned to every network. For example, one network might be a /25 network or /22, while another is a /30 network.

The next requirement is that a CIDR block that can handle 800 network devices must be tasked to assign a CIDR block to LAN B2. This LAN is a server network that houses a fixed number of servers. The number is not expected to grow beyond 80 servers. One easy approach is to assign a /24 CIDR to this network.

This means that the next network is 192.168.8.0/24, which is the next nonoverlapping CIDR block after 192.168.4.0/22. The /24 CIDR gives 254 host IP addresses, but only 80 IP addresses are required. Another approach is to size it appropriately. According to Table 1-2, a good CIDR to use is a /25, which allows for 126 host IP addresses. Therefore, a network 192.168.8.0/25 can be used for this network.

Assigning a 192.168.8.0/24 CIDR, which can accommodate 254 hosts, seems like a waste, because the network is expected to be a fixed size, and it will house no more than 80 servers. By assigning a 192.168.8.0/25 CIDR, enough room is left for another contiguous CIDR, 192.168.8.128/25. Obviously, this is a more efficient way of managing the available IP space.

Last but not least is the interconnection shown in Figure 1-4. This is the router-to-router link between Router A and Router B. The interconnection usually gets the least attention, but it exists everywhere in the multiple networks environment. Nonetheless, a CIDR block has to be assigned to it. Because there are always only two interface IP addresses involved plus the network and broadcast address, giving an entire Class C address would definitely be a waste. Typically, a /30 CIDR is used for this type of connection. Therefore, a CIDR block for the interconnection between Router A and Router B can be 192.168.9.0/30. This yields two IP host addresses: one for Router A and one for Router B.

The complete subnet assignment for Example 1-1 and Figure 1-4 is provided in Table 1-3.

TABLE 1-3 **Completed Design of Subnets for Figure 1-4**

Network	Subnet	CIDR	Subnet Mask
LAN A	192.168.0.0	/23	255.255.254.0
LAN B1	192.168.4.0	/22	255.255.252.0
LAN B2	192.168.8.0	/24 or /25	255.255.255.0 or 255.255.255.128
Interconnect	192.168.9.0	/30	255.255.255.252

IP Assignment

The next task requirement is that a CIDR block that can handle 800 network devices must be required to assign an IP address to each routed interface. This address will become the **gateway** IP address of the subnet. The gateway describes the networking device that enables hosts in a LAN to connect to networks (and hosts) outside the LAN. Figure 1-5 provides an example of the gateway. Every network device within its subnet (LAN) will use this IP address as its gateway to communicate from its local subnet to devices on other subnets. The gateway IP address is preselected and is distributed to a network device by way of manual configuration or dynamic assignment.

Gateway
Describes the networking device that enables hosts in a LAN to connect to networks (and hosts) outside the LAN.

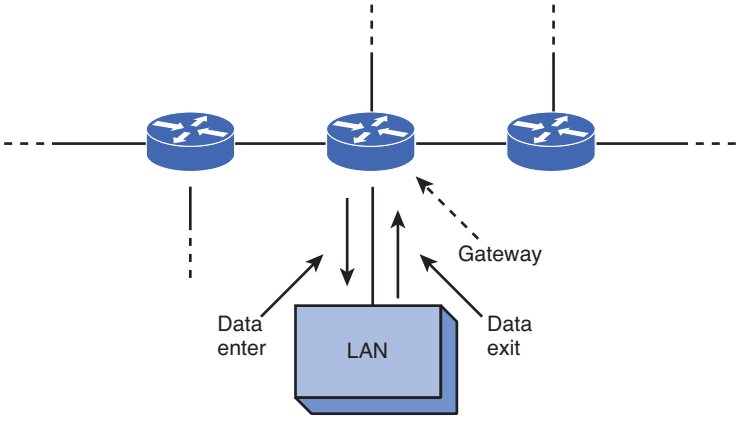


FIGURE 1-5 The gateway for a network

For LAN A in Example 1-1, the IP address 192.168.0.0 is already reserved as the network address, and the IP address 192.168.0.255 is reserved as the broadcast address. This leaves any IP address within the range 192.168.0.1–192.168.0.254 available for use for the gateway address. Choosing the gateway IP address is not an exact science. Generally, the first IP address or the last IP address of the available range is chosen. Whatever convention is chosen, it should apply to the rest of the subnets for the ease of management. Once the gateway IP address is chosen, this IP address is reserved and is not to be used by any other devices in the subnet. Otherwise, an IP conflict will be introduced. The following is an example of how the gateway IP addresses could be assigned to the LANs in Example 1-1.

Network	Gateway
LAN A	192.168.0.1
LAN B1	192.168.4.1
LAN B2	192.168.8.1

1-3 VLAN NETWORK

This section examines the function of using a switch in a VLAN within the campus network. The terminology and steps for implementing VLANs will be presented first. The second part examines basic Cisco switch configuration and provides an introduction to the commands needed for configuring the VLAN. The third part of Section 1-3 demonstrates the commands needed to set up a static VLAN. Next is a discussion on VLAN tagging using 802.1Q. The section concludes with a look at configuring an HP Procurve switch.

LANs are not necessarily restricted in size. A LAN can have 20 computers, 200 computers, or even more. Multiple LANs also can be interconnected to essentially create one large LAN. For example, the first floor of a building could be set up as one LAN, the second floor as another LAN, and the third floor another. The three LANs in the building can be interconnected into essentially one large LAN using switches, with the switches interconnected, as shown in Figure 1-6.

Broadcast Domain
Any broadcast sent out on the network is seen by all hosts in this domain.

Is it bad to interconnect LANs this way? As long as switches are being used to interconnect the computers, the interconnected LANs have minimal impact on network performance. This is true as long as there are not too many computers in the LAN. The number of computers in the LAN is an issue, because Layer 2 switches do not separate **broadcast domains**. This means that any broadcast sent out on the network (for example, the broadcast associated with an ARP request) will be sent to all computers in the LAN. Excessive broadcasts are a problem, because each computer must process the broadcast to determine whether it needs to respond; this essentially slows down the computer and the network.

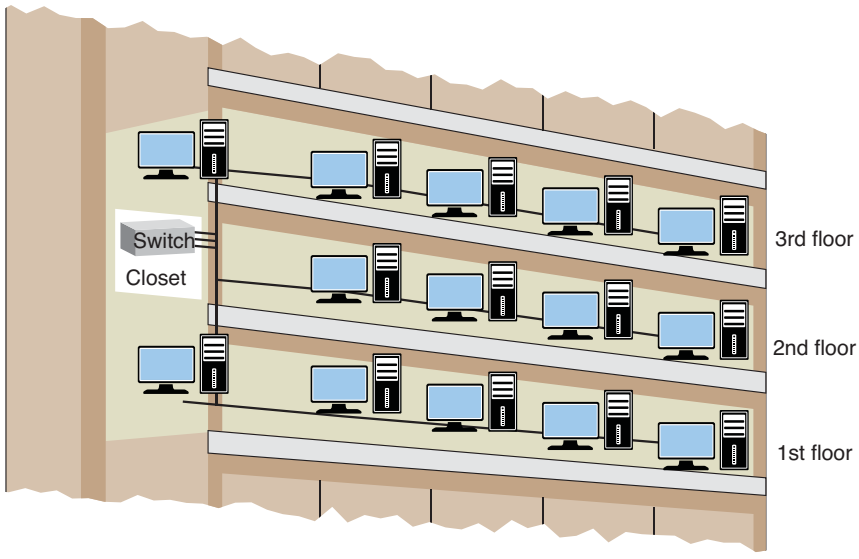


FIGURE 1-6 Three floors of a building interconnected using switches to form one large LAN

A network with multiple LANs interconnected at the Layer 2 level is called a **flat network**. A flat network is where the LANs share the same broadcast domain. The use of a flat network should be avoided if possible for the simple reason that the network response time is greatly affected. Flat networks can be avoided by the use of virtual LANs (VLAN) or routers. Although both options can be used to separate broadcast domains, they differ in that the VLAN operates at the OSI Layer 2, while routers use Layer 3 networking to accomplish the task. The topic of a virtual VLAN is discussed next.

Flat Network
A network where the LANs share the same broadcast domain.

Virtual LAN (VLAN)

Obviously, if the LANs are not connected, then each LAN is segregated only to a switch. The broadcast domain is contained to that switch; however, this does not scale in a practical network, and it is not cost effective because each LAN requires its own Layer 2 switches. This is where the concept of virtual LAN (VLAN) can help out. A VLAN is a way to have multiple LANs co-exist in the same Layer 2 switch, but their traffic is segregated from each other. Even though they reside on the same physical switch, they behave as if they are on different switches (hence, the term virtual). VLAN compatible switches can communicate to each other and extend the segregation of multiple LANs throughout the entire switched network. A switch can be configured with a VLAN where a group of host computers and servers are configured as if they are in the same LAN, even if they reside across routers in separate LANs. Each VLAN has its own broadcast domain. Hence, traffic from one VLAN cannot pass to another VLAN. The advantage of using VLANs is the network administrator can group computers and servers in the same VLAN based on the organizational group (such as Sales, Engineering) even if they are not on the same physical segment—or even the same building.

VLAN (Virtual LAN)
A group of host computers and servers that are configured as if they are in the same LAN, even if they reside across routers in separate LANs.

There are three types of VLANs: **port-based VLANs**, **tag-based VLANs**, and **protocol-based VLANs**. The port-based VLAN is one where the host computers connected to specific ports on a switch are assigned to a specific VLAN. For example, assume the computers connected to switch ports 2, 3, and 4 are assigned to the Sales VLAN 2, while the computers connected to switch ports 6, 7, and 8 are assigned to the Engineering VLAN 3, as shown in Figure 1-7. The switch will be configured as a port-based VLAN so that the groups of ports [2,3,4] are assigned to the sales VLAN while ports [6,7,8] belong to the Engineering VLAN. The devices assigned to the same VLAN will share broadcasts for that LAN; however, computers that are connected to ports not assigned to the VLAN will not share the broadcasts. For example, the computers in VLAN 2 (Sales) share the same broadcast domain and computers in VLAN 3 (Engineering) share a different broadcast domain.

Port-Based VLAN
Host computers connected to specific ports on a switch are assigned to a specific VLAN.

Tagged-Based VLAN
Used VLAN ID based on 802.1Q.

Protocol-Based VLAN
Connection to ports is based on the protocol being used.

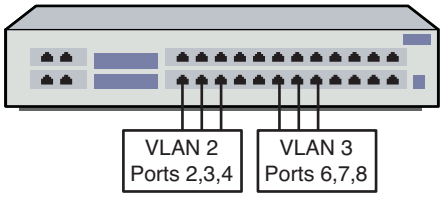


FIGURE 1-7 An example of the grouping for port-based VLANs

VLAN ID
Used to identify that a frame belongs to a specific VLAN.

802.1Q
This standard defines a system of **VLAN tagging** for Ethernet frames.

In tag-based VLANs, a tag is added to the Ethernet frames. This tag contains the **VLAN ID** that is used to identify that a frame belongs to a specific VLAN. The addition of the VLAN ID is based on the **802.1Q** specification. The 802.1Q standard defines a system of VLAN tagging for Ethernet frames. An advantage of an 802.1Q VLAN is that it helps contain broadcast and multicast data traffic, which helps minimize data congestion and improve throughput. This specification also provides guidelines for a switch port to belong to more than one VLAN. Additionally, the tag-based VLANs can help provide better security by logically isolating and grouping users.

In protocol-based VLANs, the data traffic is connected to specific ports based on the type of protocol being used. The packet is dropped when it enters the switch if the protocol doesn't match any of the VLANs. For example, an IP network could be set up for the Engineering VLAN on ports 6,7,8 and an IPX network for the Sales VLAN on ports 2,3, and 4. The advantage of this is the data traffic for the two networks is separated.

Static VLAN
Basically, a port-based VLAN.

Dynamic VLAN
Ports are assigned to a VLAN based on either the computer's MAC address or the username of the client logged onto the computer.

There are two approaches for assigning VLAN membership:

- **Static VLAN:** Basically a port-based VLAN. The assignments are created when ports are assigned to a specific VLAN.
- **Dynamic VLAN:** Ports are assigned to a VLAN based on either the computer's MAC address or the username of the client logged onto the computer. This means that the system has been previously configured with the VLAN assignments for the computer or the username. The advantage of this is the username and/or the computer can move to a different location, but VLAN membership will be retained.

VLAN Configuration

This section demonstrates the steps for configuring a static VLAN. In this example, the ports for VLAN 2 (Sales) and VLAN 3 (Engineering) will be defined. This requires that VLAN memberships be defined for the required ports. The steps and the commands will be demonstrated.

show vlan
Used to verify what ports have been defined for the switch.

The **show vlan** command can be used to verify what ports have been defined for the switch. By default, all ports are assigned to VLAN 1. An example using the **show vlan** command is provided next.

```
SwitchA# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
--
1    default                          active    Fa0/1, Fa0/2,
Fa0/3, Fa0/4
                                                Fa0/5,
Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9,
Fa0/10
```

This shows that all the FastEthernet interfaces on the switch are currently assigned to VLAN 1, which is a default VLAN. In the next step, two additional VLANs will be created for both Sales and Engineering. The two new VLANs will have the VLAN ID of 2 and 3 respectively, and each VLAN will be assigned a name associated to it. This is accomplished by modifying the VLAN database using the **vlan database** command, as shown in the next steps.

vlan database
The command used on older Cisco switches to enter the VLAN database.

```
SwitchA#vlan database

SwitchA(vlan)#vlan 2 name Sales
VLAN 2 modified:
    Name: Sales
SwitchA(vlan)#vlan 3 name Engineering
VLAN 3 modified:
    Name: Engineering
```

On newer Cisco switches, users will get the following message that the command **vlan database** is being deprecated:

```
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.
```

Cisco has moved away from the VLAN database-style command to an IOS global command. Similarly to other IOS global commands, the switch must be in the configuration mode (config)#. However, the concept remains the same that a VLAN must be created for it to be activated and ready for use. The steps for creating the VLAN on newer Cisco switches are as follows:

```
SwitchA# conf t
SwitchA(config)#vlan 2
SwitchA(config-vlan)#name Sales
SwitchA(config-vlan)#vlan 3
SwitchA(config-vlan)#name Engineering
SwitchA(config-vlan)#exit
SwitchA(config)#exit
```

To start configuring a VLAN, one must specify which VLAN needs to be configured using the **vlan** [*vlan_id*] command. If the specific VLAN does not exist, this command will create the VLAN as well. As shown in the preceding example, the command **vlan 2** is entered to configure vlan 2 and then the command name **Sales** is entered to configure the name associated to the VLAN. The similar steps are done for VLAN 3 with the name Engineering.

vlan [*vlan_id*]
The IOS global command used to create VLAN ID.

The rest of the VLAN commands are almost identical in the older switches and newer switches. The next step is used to verify that the new VLANs have been created using the **show vlan** command:

```
Switch#show vlan

VLAN Name                         Status          Ports
---- ------------------------- --------- ---------------------------
--
1    default                      active        Fa0/1, Fa0/2, Fa0/3,
Fa0/4
                                                     Fa0/5, Fa0/6,
Fa0/7, Fa0/8
                                                     Fa0/9, Fa0/10
2    Sales                        active
3    Engineering           active
```

This shows that both the Sales and Engineering VLANs have been created. In the next steps, ports will be assigned to the newly created VLANs. This requires that the configuration mode be entered and each FastEthernet interface (port) must be assigned to the proper VLAN using the two commands **switchport mode access** and **switchport access vlan** *vlan-id*. An example is presented for FastEthernet interface 0/2 being assigned to VLAN 2 on a Cisco switch:

```
SwitchA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)#int fa 0/2
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vlan 2
SwitchA(config-if)#end
```

The next step is used to verify that FastEthernet 0/2 has been assigned to the Sales VLAN (VLAN2). This can be verified using the **show vlan brief** command, as shown. This command only displays the interfaces assigned to each VLAN:

```
SwitchA#sh vlan brief

VLAN Name                   Status      Ports
---- ---------------------------- --------- ------------------------
---
1    default                        active     Fa0/1, Fa0/3, Fa0/4,
Fa0/5
                                                Fa0/6, Fa0/7,
Fa0/8, Fa0/9
                                                Fa0/10
2    Sales                          active     Fa0/2
```

The next steps are to assign ports 3 and 4 to the Sales VLAN (VLAN 2) and ports 6,7,8 to Engineering (VLAN 3). Once this is completed, the port assignments can be verified using the **show vlan** command, as shown:

```
SwitchA#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
---
1    default                          active    Fa0/1, Fa0/5,
Fa0/9, Fa0/10

2    Sales                            active    Fa0/2, Fa0/3,
Fa0/4

3    Engineering                      active    Fa0/6, Fa0/7, Fa0/8
```

You can look specifically at the assignments for only one of the VLANs by entering the command **show vlan name** *vlan-name*, where *vlan-name* is the name assigned to the VLAN. Note that the name is case-sensitive. You can also use the number of the VLAN instead of using the command **show vlan id** *vlan-id*. Examples of both are presented:

show vlan name *vlan-name*
The command to look specifically at only one of the VLANs.

```
SwitchA#show vlan name Engineering

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
---
3    Engineering                      active    Fa0/6, Fa0/7,
Fa0/8


Switch#show vlan id 3

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
---
3    Engineering                      active    Fa0/6, Fa0/7,
Fa0/8
```

On Layer 2 switches, an IP address can be assigned to a VLAN interface. This merely assigns an IP address to a switch, so that a switch can communicate with other network devices on the same VLAN and vice-versa. The IP VLAN interface does not perform any routing functions when running as a layer 2 switch. As a matter of fact, the IP VLAN interface is not required in order for a switch to start forwarding packets and perform its other Layer 2 functions. By default, the **interface VLAN 1** is automatically created. The following command sequence demonstrates how to assign the IP address to the VLAN interface:

interface VLAN 1
The default vlan for the switch.

```
SwitchA(config)# interface VLAN 1
SwitchA(config-if)# ip address 192.168.1.1 255.255.255.0
SwitchA(config-if)# no shutdown
```

Note that the IP address is being set for VLAN 1. The interface for the switch is also enabled at this same point using the **no shutdown** command, as shown. In order for the interface VLAN to be up, at least one switch port in the VLAN must

show interface status
Used to verify the status of a switchport.

be up or have a physical link. The status of a switch port can be verified with the command **show interface** or, better yet, with the command **show interface status**. Although the command **show interface** shows detailed information of individual interface one at a time, the command **show interface status** displays the status of all the switch ports including their speed, duplex, and VLAN, as shown. This gives a quick and precise look of the port status of a switch where port density is high.

```
SwitchA#show interface status

Port    Name    Status       Vlan       Duplex  Speed Type
Fa0/1           connected    1          a-full    a-100
10/100BaseTX
Fa0/2           connected    2          a-full    a-100
10/100BaseTX
Fa0/3           connected    2          a-full    a-100
10/100BaseTX
Fa0/4           connected    2          a-full    a-100
10/100BaseTX
Fa0/5           connected    1          a-full    a-100
10/100BaseTX
Fa0/6           connected    3          a-full    a-100
10/100BaseTX
Fa0/7           connected    3          a-full    a-100
10/100BaseTX
Fa0/8           connected    3          a-full    a-100
10/100BaseTX
Fa0/9           connected    1          a-full    a-100
10/100BaseTX
Fa0/10          connected    1          a-full    a-100
10/100BaseTX
```

The overall configuration of the switch can be viewed using the **show running-config** (**sh run**) command, as shown. (Only a part of the configuration is displayed.)

```
Switch#sh run      -    -
Building configuration...

Current configuration : 1411 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
ip subnet-zero
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
```

```
!
interface FastEthernet0/1
!-
 interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
    .      .
    .    .
    .      .
    .    .
interface FastEthernet0/5
!
interface FastEthernet0/6
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
 no ip route-cache
!
ip http server
!
line con 0
line vty 0 15
 login
end
```

The running-configuration for the switch shows that the FastEthernet interfaces have been assigned to the proper VLANs. Additionally, this shows that an IP address has been assigned to the default interface VLAN1.

This portion of the text has demonstrated the steps for creating a static VLAN. Both Sales and Engineering VLANs were created, and specific ports on the switch were assigned to the respective VLANs. Unassigned ports remained as part of the default VLAN 1.

VLAN Tagging

This section explores the concept of VLAN tagging (802.1Q) and demonstrates the steps required for this configuration. The concept of VLAN tagging can be explained using the example network shown in Figure 1-8. In this network, the Sales team is spread out in two different buildings. Therefore, the Sales VLAN network must be available in both buildings. Each building has its own network switch, and both switches are connected via one physical link.

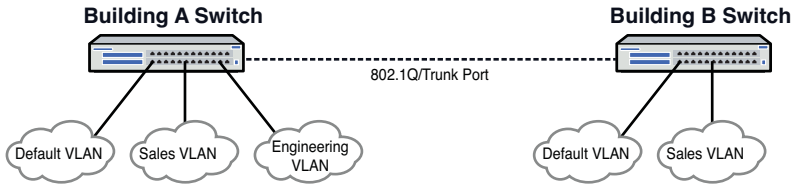


FIGURE 1-8 An example of a scenario with two VLANS spread across two buildings

Trunk Port
A switch interface or port configured to carry multiple VLANs.

Inter-Switch Link (ISL)
The Cisco proprietary VLAN tagging protocol.

In a scenario like this, not only is it necessary to have the same Sales VLAN running on both building switches, it is also important to have members of the same VLAN being able to communicate with each other across buildings and to adhere to the same VLAN restrictions. To accomplish this, a technique called VLAN tagging is used. VLAN tagging is a technique deployed on a switch interface to carry Ethernet frames of multiple VLANs. The interface must connect to another switch port, router port, or network device that understands VLAN tagging, and both sides must agree on the VLAN tagging protocol.

The standard protocol for VLAN tagging is IEEE 802.1Q. This standard protocol is widely supported by every switch manufacturer, as well as Cisco. A switch interface or port configured to carry traffic for multiple VLANs is often referred to as a **trunk port**. The term was made famous by Cisco, and it is used explicitly as the VLAN tagging command in Cisco switches. Note that Cisco has its own proprietary VLAN tagging protocol called **Inter-Switch Link (ISL)**. The big difference between ISL and 802.1Q is how the frame is treated. In ISL, every Ethernet frame is encapsulated within a 26-Byte header containing the VLAN ID and a 4 Byte CRC at the end. This makes the size of an ISL frame bigger than an 802.1Q frame, as discussed next.

To accomplish the VLAN tagging of the Ethernet frames, IEEE 802.1Q simply inserts additional data to the Ethernet frame header, as shown in Figure 1-9. An 802.1Q tag is a 4-Byte tag field that is inserted between the Source Address field and the Ethernet Type/Length field. By inserting an additional 4-Byte field, the Ethernet frame size is increased. Its minimum frame size is now increased from 64 Bytes to 68 Bytes, and its maximum frame size is now increased from 1,518 Bytes to 1,522 Bytes. Figure 1-9 also provides a detailed calculation of the Ethernet frame size. Because of the additional tag field and the increased frame size, it is important that both sides of the link be compatible. Otherwise, the tagged Ethernet frames will not be understood and, therefore, the frames will be dropped by a non-802.1Q-compliant interface.

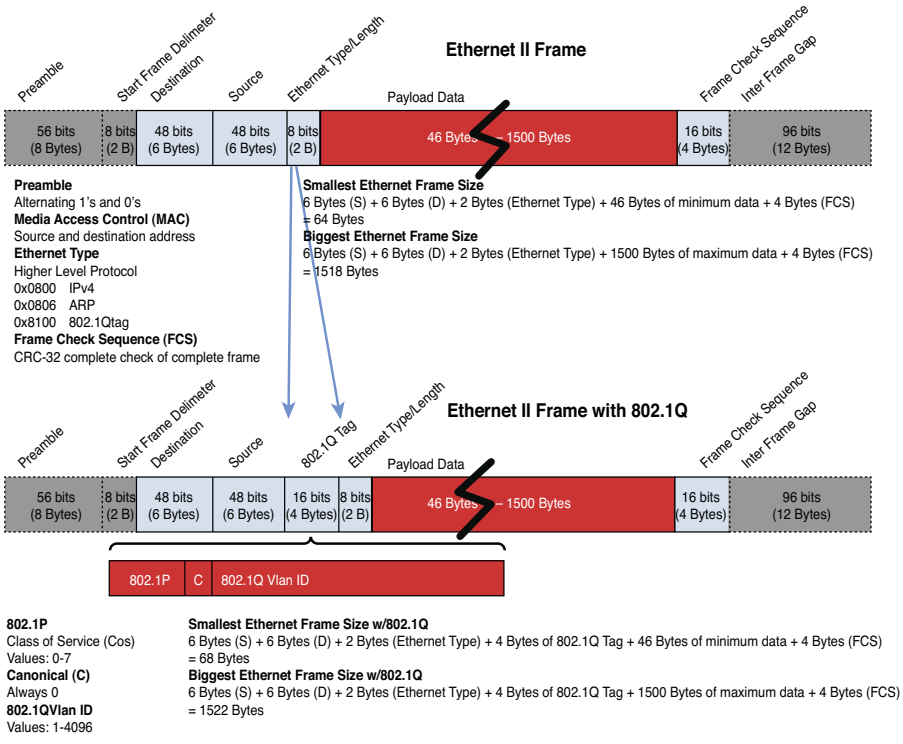


FIGURE 1-9 Typical Ethernet frame versus Ethernet frame with 802.1Q tag

802.1Q Configuration

This section demonstrates the steps for configuring 802.1Q VLAN tagging. The 802.1Q VLAN tagging is configured at the switch interface that interconnects to another network switch. In this case, interface FastEthernet 0/1 of Switch A is selected as a 802.1Q VLAN tagging port or a trunk port. The following demonstrates how to configure an interface as a trunk port on a Cisco switch.

First, the interface is assigned as a trunk port by the command **switchport mode trunk**. This essentially turns on trunking. The next step is to define the tagging protocol, which is 802.1Q, in this case. The command **switchport trunk encapsulation dot1q** is used. If ISL is used, the command would be **switchport trunk encapsulation isl**. The next command, **switchport trunk allowed vlan *vlan-id***, is optional, but it is useful in limiting VLANs that can be carried across the link.

```
SwitchA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)#int fa 0/1
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#switchport trunk encapsulation dot1q
SwitchA(config-if)#switchport trunk allowed vlan 1,2
SwitchA(config-if)#end
```

switchport mode trunk

Turns on trunking.

switchport trunk encapsulation dot1q

This command defines that 802.1Q tagging protocol is being used.

switchport trunk encapsulation isl

This command defines that the tagging protocol is ISL.

switchport trunk allowed vlan *vlan-id*

This command is used to limit the VLANs that can be carried across the link.

show interfaces trunk
This command is used to verify the 802.1Q configuration.

By default, all configured VLANs are allowed across the trunk port. In order for VLAN tagging to work properly, it is important to configure the same commands on SwitchB's trunk port. To verify the 802.1Q configuration, the command **show interfaces trunk** can be used:

```
SwitchA#sh interfaces trunk
Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on                 802.1q             trunking      1

Port        Vlans allowed on trunk
Fa0/1       1,2

Port        Vlans allowed and active in management domain
Fa0/1       1,2

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,2
```

Networking Challenge: Static VLAN Configuration

Use the Net-Challenge Simulator Software included with the text's companion CD-ROM to demonstrate that you can perform basic switch and static VLAN configuration and set up a trunk connection. Place the CD-ROM in your computer's drive. Open the *Net-Challenge* folder, and click **NetChallengeV3-2.exe**. After the software is running, click the **Select Challenge** button. This opens a Select Challenge drop-down menu. Select the **Chapter 1 - Static VLAN Configuration** challenge to open a checkbox that can be used to verify that you have completed all the tasks. Do the following:

1. Enter the privileged EXEC mode on the switch (password: **Chile**).
2. Enter the switch's configuration mode: **Router(config)**.
3. Set the hostname of the switch to switch-A.
4. Configure the IP address for VLAN 1 interface with the following:

   IP address: 10.10.20.250

   Subnet mask: 255.255.255.0
5. Enable the VLAN 1 interface.
6. Use the command to display the current VLAN settings for the switch.
7. Issue the command that lets you modify the VLAN database.
8. Create a VLAN 2 named Sales.
9. Verify that a new Sales VLAN has been created.
10. Issue the command to enter the fa0/2 interface configuration mode.
11. Enter the sequence of commands that are used to assign interface fa0/2 to the Sales VLAN.
12. Enter the command that enables you to display the interface assigned to each VLAN.

13. Enter the command that enables you to view specifically the assignments for the Sales VLAN.
14. Issue the command that allows you to view the switch's running-configuration.
15. Issue the command to turn on trunking for SwitchA.
16. Issue the command to set trunk encapsulation to 802.1Q.
17. Issue the command that enables VLAN 1 and VLAN 2 to be carried across the link.

Configuring the HP Procurve Switch

This should not come as a surprise to learn that many switch manufacturers follow a similar configuration path as the Cisco switches. A similar Cisco-styled command-line interface (CLI) is deployed by those manufacturers as well. The following is an example of how to configure an HP Procurve switch. The first step is to enter the configuration mode using the command **configure**. Next, the VLAN # is entered using the **vlan 2** command. Finally, the VLAN is assigned a name from the (vlan-2) prompt using the command **name-Sales**:

```
SwitchHP# configure
SwitchHP(config)#vlan 2
SwitchHP(vlan-2)#name Sales
```

The command **show vlan** also exists on the HP switches, but the output result is different than the one produced from Cisco switches. The HP's **show vlan** command does not provide ports with VLAN membership, while the Cisco command does:

```
  SwitchHP# show vlan
 Status and Counters - VLAN Information

  Maximum VLANs to support : 8
  Primary VLAN : DEFAULT_VLAN
  Management VLAN :

  802.1Q VLAN ID Name                 Status       Voice Jumbo
  -------------- ------------ ------------ ----- -----
  1              DEFAULT_VLAN           Port-based   No    No
  2              Sales                  Port-based   No    No
```

On a Cisco switch, the VLAN membership is configured at the interface level. On an HP switch, it is configured at the VLAN level, where each VLAN contains its port members. This example shows how a VLAN membership is assigned on an HP switch:

```
SwitchHP# configure
SwitchHP(config)#vlan 2
SwitchHP(vlan-2)#untagged 48
```

In VLAN 2, port 48 is configured as an untagged member. This means that the port is not a tagged VLAN port. It is essentially just a port-based VLAN. It was mentioned earlier that the HP's command **show vlan** does not give much detail. To get more VLAN details, one must specify the VLAN ID. The **show vlan 2** command can be used to verify that port 48 has been assigned to the Sales VLAN (VLAN2):

```
SwitchHP# show vlan  2
  Status and Counters - VLAN Information - Ports - VLAN 2

  802.1Q VLAN ID : 2
  Name : Sales
  Status : Port-based  Voice : No
  Jumbo : No

  Port Information    Mode Unknown    VLAN     Status
  ------------------    -------------------- ----------  ---------
  48                        Untagged               Learn        Up
```

On HP switches and other switch manufacturers, the command syntax for enabling a port to carry 802.1Q tagged frames is basically the same. On HP switches, there is not a trunk command. The step is to simply assign tagging ability to the switch port by issuing the command **tagged** *port_number*. Because this is a non-Cisco switch, 802.1Q is the only VLAN tagging protocol that can be used. The following command sequence demonstrates how to configure an interface port 24 on an HP switch as a 802.1Q VLAN tagging port:

```
SwitchHP# conf
SwitchHP(config)# vlan  1
SwitchHP(vlan-1)# tagged 24
SwitchHP(vlan-1)# exit
SwitchHP(config)# vlan 2
SwitchHP(vlan-2)# tagged 24
SwitchHP(vlan-2)# exit
```

Unlike Cisco switches where an 802.1Q is configured at the interface level, the tagging configuration is done at the VLAN level on HP switches. Port 24 is designated as tagged port for both VLAN 1 and VLAN 2, which enables it to carry VLAN 1 and VLAN 2 frames. Generally, untagged ports belong to one specific VLAN, while tagged ports can belong to one or more VLANs.

1-4 ROUTED NETWORK

This section examines the Layer 3 network and how data is routed in the network. This section also introduces another Layer 3 device, the multilayer switch. You need to understand the advantages and disadvantages of this device. This section also introduces interVLAN configuration, which enables VLANs to communicate

across networks. The section concludes with a look at both serial and ATM configurations. Some network engineers will argue that the serial and ATM technologies are a dying technology and are now considered obsolete. However, being obsolete does not mean they are nonexistent. These technologies are still being used throughout the world, and it is still an important topic.

Router

The router is a powerful networking device used to interconnect LANs. The router is a Layer 3 device in the OSI model, which means the router uses the **network address** (Layer 3 addressing) to make routing decisions regarding forwarding data packets. In the OSI model, the Layer 3, or network, layer responsibilities include handling of the network address. The network address is also called a *logical address,* rather than being a physical address (such as the MAC address, which is embedded into the network interface card [NIC]). The **logical address** describes the IP address location of the network and the address location of the host in the network.

Network Address
Another name for the Layer 3 address.

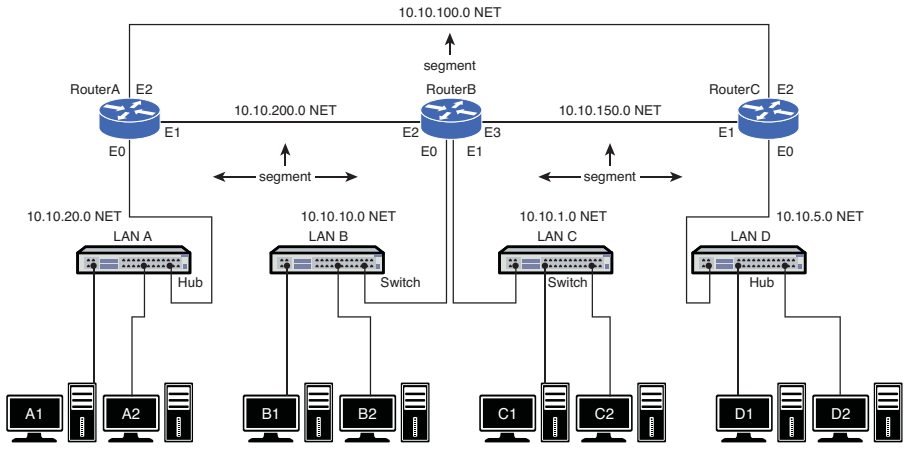
Logical Address
This describes the IP address location of the network and the address location of the host in the network.

Essentially, the router is configured to know how to route data packets entering or exiting the LAN. This differs from the bridge and the Layer 2 switch, which use the Ethernet address for making decisions regarding forwarding data packets and only know how to forward data to hosts physically connected to their ports.

Routers are used to interconnect LANs in a campus network. Routers can be used to interconnect networks that use the same protocol (for example, Ethernet), or they can be used to interconnect LANs that are using different Layer 2 technologies, such as an Ethernet, ATM, T1, and so on. Routers also make it possible to interconnect to LANs around the country and the world and interconnect to many different networking protocols. The router ports are *bidirectional,* meaning that data can enter and exit the same router port. Often, the router ports are called the **router interface**, which is the physical connection where the router connects to the network.

Router Interface
The physical connection where the router connects to the network.

The network provided in Figure 1-10 is an example of a simple three-router campus network. This configuration enables data packets to be sent and received from any host on the network after the routers in the network have been properly configured. For example, computer A1 in LAN A could be sending data to computer D1 in LAN D. This requires that the IP address for computer D1 is known by the user sending the data from computer A1. The data from computer A1 will first travel to the switch where the data is passed to Router A via the FA0/0 FastEthernet data port. Router A will examine the network address of the data packet and use configured routing instructions stored in the router's routing tables to decide where to forward the data. Router A determines that an available path to Router C is via the FA0/2 FastEthernet port connection. The data is then sent directly to Router C. Router C determines that the data packet should be forwarded to its FA0/0 port to reach computer D1 in LAN D. The data is then sent to D1. Alternatively, Router A could have sent the data to Router C through Router B via Router A's FA0/1 FastEthernet port.



RouterA Port Addresses (LAN A)		RouterB Port Addresses (LAN B)		RouterB Port Addresses (LAN C)		RouterC Port Addresses (LAN D)	
Ethernet 0 (Gateway Address)	10.10.20.250	Ethernet 0 (Gateway Address)	10.10.10.250	Ethernet 1 (Gateway Address)	10.10.1.250	Ethernet 0 (Gateway Address)	10.10.5.250
Ethernet 1	10.10.200.1	Ethernet 2	10.10.200.2	Ethernet 2	10.10.200.2	Ethernet 1	10.10.150.2
Ethernet 2	10.10.100.1	Ethernet 3	10.10.150.1	Ethernet 3	10.10.150.1	Ethernet 2	10.10.100.2
LAN A Computers		**LAN B Computers**		**LAN C Computers**		**LAN D Computers**	
Computer A1	10.10.20.1	Computer B1	10.10.10.1	Computer C1	10.10.1.1	Computer D1	10.10.5.1
Computer A2	10.10.20.2	Computer B2	10.10.10.2	Computer C2	10.10.1.2	Computer D2	10.10.5.2
Subnet Mask	***255.255.255.0***	***Subnet Mask***	***255.255.255.0***	***Subnet Mask***	***255.255.255.0***	***Subnet Mask***	***255.255.255.0***

FIGURE 1-10 The three-router campus LAN

Routing Table
Keeps track of the routes to use for forwarding data to its destination.

Delivery of the information over the network was made possible by the use of an IP address and **routing table**. Routing tables keep track of the routes used for forwarding data to its destination. RouterA used its routing table to determine a network data path so computer A1's data could reach computer D1 in LAN D. After the data packet arrived on Router C, an ARP request is issued by Router C to determine the MAC address of computer D1. The MAC address is then used for final delivery of the data to computer D1.

If Router A determines that the network path to Router C is down, Router A can route the data packet to Router C through Router B. After Router B receives the data packet from Router A, it uses its routing tables to determine where to forward the data packet. Router B determines that the data needs to be sent to Router C. Router B will then use its FA0/3 FastEthernet port to forward the data to Router C.

Gateway Address

As previously discussed, the term *gateway* is used to describe the address of the networking device that enables the hosts in a LAN to connect to networks and hosts outside the LAN. For example, the gateway address for all hosts in LAN A will be 10.10.20.250. This address is configured on the host computer, as shown in Figure 1-11. Any IP packets with a destination outside the LAN A network will be sent to this gateway address. Note that the destination network is determined by the subnet mask. In this case, the subnet mask is 255.255.255.0.

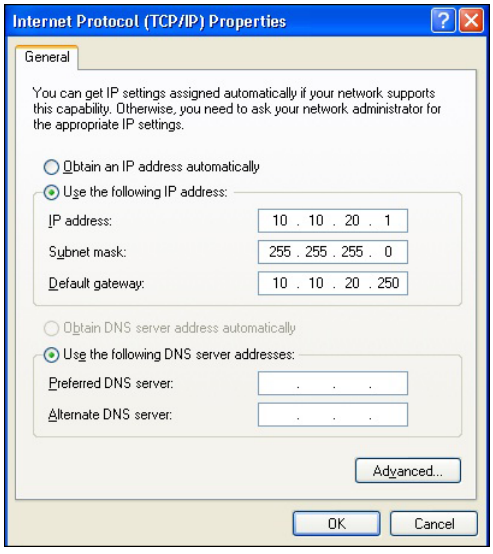


FIGURE 1-11 Network settings configuration for the default gateway

Network Segments

The *network segment* defines the networking link between two LANs. There is a segment associated with each connection of an internetworking device (for example, router-hub, router-switch, router-router). For example, the IP address for the network segment connecting LAN A to the router is 10.10.20.0. All hosts connected to this segment must contain a 10.10.20.x, because a subnet mask of 255.255.255.0 is being used. Subnet masking is fully explained in *Network Essentials* Chapter 6, "TCP/IP."

Routers use the information about the network segments to determine where to forward data packets. For example, referring to Figure 1-10, the network segments that connect to Router A include

10.10.20.0
10.10.200.0
10.10.100.0

The segment is sometimes called the **subnet** or **NET**. These terms are associated with a network segment address, such as 10.10.20.0. In this case, the network is called the 10.10.20.0 NET. All hosts in the 10.10.20.0 NET will have a 10.10.20.x IP address. The network addresses are used when configuring the routers and defining which networks are connected to the router.

Subnet, NET
Other terms for the segment.

According to Figure 1-11, all the computers in LAN A must have a 10.10.20.x address. This is defined by the 255.255.255.0 subnet mask. For example, computer A1 in LAN A will have the assigned IP address of 10.10.20.1 and a gateway address of 10.10.20.250. The computers in LAN B (see Figure 1-10) are located in the

10.10.10.0 network. This means that all the computers in this network must contain a 10.10.10.x IP address. In this case, the *x* part of the IP address is assigned for each host. The gateway address for the hosts in LAN B is 10.10.10.250. Notice that the routers are all using the same .250 gateway address. Remember, any valid IP address can be used for the gateway address, but it is a good design procedure to use the same number for number for all routers. In this case, .250 is being used. In other cases, it could be .1 or .254.

The subnet mask is used to determine whether the data is to stay in the LAN or is to be forwarded to the default gateway provided by the router. The router uses its subnet mask to determine the destination network address. The destination network address is checked with the router's routing table to select the best route to the destination. The data is then forwarded to the next router, which is the next hop address. The next router examines the data packet, determines the destination network address, checks its routing table, and then forwards the data to the next hop. If the destination network is directly connected to the router, it issues an ARP request to determine the MAC address of the destination host. Final delivery is then accomplished by forwarding the data using the destination host computer's MAC address. Routing of the data through the networks is at Layer 3, and the final delivery of data in the network is at Layer 2.

Multilayer Switch

Multilayer Switch (MLS)
Operates at Layer 2, but functions at the higher layers.

Wire Speed Routing
Data packets are processed as fast as they arrive.

So far, the topic of network switches revolves around their Layer 2 functionalities. Today, the scope of operations has changed for switches. Newer switch technologies are available to help further improve the performance of computer networks. This new development started with Layer 3 switches and now there are multilayer switches. The term used to describe these switches that can operate above the OSI Layer 2 is **multilayer switches (MLS)**. An example is a Layer 3 switch. Layer 3 switches still work at Layer 2, but additionally work at the network layer (Layer 3) of the OSI model and use IP addressing for making decisions to route a data packet in the best direction. The major difference is that the packet switching in basic routers is handled by a programmed microprocessor. The multilayer switch uses application specific integrated circuits (ASIC) hardware to handle the packet switching. The advantage of using hardware to handle the packet switching is a significant reduction in processing time (software versus hardware). In fact, the processing time of multilayer switches can be as fast as the input data rate. This is called **wire speed routing**, where the data packets are processed as fast as they are arriving. Multilayer switches can also work at the upper layers of the OSI model. An example is a Layer 4 switch that processes data packets at the transport layer of the OSI model.

Through this evolution, the line between routers and multilayer switches is getting more and more blurry. Routers were once considered the more intelligent device, but this is no longer true. With new developments, the multilayer switches can do almost everything the routers can. More importantly, most of the Layer 3 switch configuration commands are almost identical to the ones used on the routers. Routers tend to be more expensive when it comes to cost per port. Therefore, most of the traditional designs have a router connecting to a switch or switches to provide more port density. This can be expensive depending on the size of the network. So, there has been a shift toward deploying multilayer switches in the network LAN environment in place of routers. In this case, the routers and switches in Figure 1-10 then

could all be replaced with multilayer switches. This also means there will be less network equipment to maintain, which reduces the maintenance cost and makes this a more cost-effective solution. With its greater port density, a multilayer switch can serve more clients than a router could. However, there is a common drawback for most multilayer switches: These devices only support Ethernet. Other Layer 2 technologies, such as ATM, DSL,T1, still depend on routers for making this connection.

Layer 3 Routed Networks

As discussed previously, the hosts are interconnected with a switch or hub. This allows data to be exchanged within the LAN; however, data cannot be routed to other networks. Also, the broadcast domain of one LAN is not isolated from another LAN's broadcast domain. The solution for breaking up the broadcast domains and providing network routing is to incorporate routing hardware into the network design to create a **routed network**. A routed network uses Layer 3 addressing for selecting routes to forward data packets, so a better name for this network is a **Layer 3 network**.

Routed Network
Uses Layer 3 addressing for selecting routes to forward data packets.

Layer 3 Network
Another name for a routed network.

In Layer 3 networks, routers and multilayer switches are used to interconnect the networks and LANs, isolating broadcast domains and enabling hosts from different LANs and networks to exchange data. Data packet delivery is achieved by handing off data to adjacent routers until the packet reaches its final destination. This typically involves passing data packets through many routers and many networks. An example of a Layer 3 network is shown in Figure 1-10. This example has four LANs interconnected using three routers. The IP address for each networking device is listed.

The physical layer interface on the router provides a way to connect the router to other networking devices on the network. For example, the FastEthernet ports on the router are used to connect to other FastEthernet ports on other routers or switches. Gigabit and 10-gigabit Ethernet ports are also available on routers to connect to other high-speed Ethernet ports (the sample network shown in Figure 1-10 includes only FastEthernet ports). Routers also contain other types of interfaces, such as serial interfaces and Synchronous Optical Network (**SONET**) interfaces. These interfaces were widely used to interconnect the router and the network to other wide-area networks (**WAN**). For example, connection to WANs requires the use of a serial interface or SONET interface to connect to a communications carrier, such as Sprint, AT&T, Century Link, and so on. The data speeds for the serial communication ports on routers can vary from slow (56 kbps) up to high-speed DS3 data rates (47+ Mbps), and the SONET could range from OC3 (155 Mbps), OC12 (622 Mbps), or even OC192 (9953 Mbps).

Synchronous Optical Network (SONET)
Used to interconnect the router and the network to other WANs.

WAN
Wide-area network.

Routed Port Configuration

Routers can have Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1,000 Mbps), and 10 gigabit (10 GB), Serial, and ATM interfaces. These routers

can have multiple interfaces, and the steps for configuring each interface are basically the same. Each interface is assigned a number. For example, a router could have three FastEthernet interfaces identified as

FastEthernet 0/0
FastEthernet 0/1
FastEthernet 0/2

The notation 0/0 indicates the [*interface-card-slot/port*].

On Cisco's routers, a routed port can be configured simply by assigning an IP address to the interface. Once an IP address and its subnet mask are assigned to the interface and the interface is enabled, a Layer 3 network is created. The interface IP address becomes the gateway for that network. To program the interface, the router must be in the configuration mode. The following demonstrates how to configure a router's FastEthernet 0/0 port (FastEthernet 0/0, also listed as fa0/0 and FA0/0) as a routed interface.

```
Router(config)# int fa0/0
Router(config-if)# ip address 10.10.20.250 255.255.255.0
Router(config-if)#no shut
2w0d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
```

terminal monitor (term mon)
Displays log messages on the remote terminal.

Notice that the router prompts you that the line protocol on interface FastEthernet 0/0 changed state to up. These log messages are always displayed when connecting via the console port. However, they are suppressed when it is a remote terminal session, like Telnet or SSH. To display log messages on the remote terminal, issue the command **terminal monitor** or **term mon** at the router prompt:

```
Router# term mon
```

terminal no monitor (term no mon)
Disables the logging to the terminal.

The log messages can be useful when bringing up a new connection. Sometimes, they can be annoying if the router is logging too many events. To disable the logging to the terminal, the command is **terminal no monitor** or **term no mon**. One would think the command syntax would start with **no**, like typical Cisco command, but it is not so in this case:

```
Router# term no mon
```

show ip interface brief (sh ip int brief)
Verifies the status of the router interfaces.

The command **show ip interface brief (sh ip int brief)** entered at the enable prompt (**Router#**) can be used to verify the status of the router interfaces. The following is an example:

```
Router# sh ip int brief
Interface        IP-Address     OK?  Method  Status  Protocol
FastEthernet0/0  10.10.20.250   YES  manual  up      up
FastEthernet0/1  unassigned     YES  manual  administratively down
down
FastEthernet0/2  unassigned     YES  manual  administratively down
down
```

The output shows that the interface FastEthernet0/0 was configured with the IP address and its status is up. Because the FastEthernet0/1 and FastEthernet0/2 were not

yet configured, their IP addresses are shown as unassigned and their interfaces are still administratively shut down.

Also, a routed port can be assigned to a multilayer switch. This configuration is simple and the same as configuring a router port. The first step is to convert the native switch port to a router port. This is accomplished by issuing the command **no switchport** on the desired switch interface. Then, the IP address and other configuration can be applied to the interface just like a typical router port:

no switchport
Converts the native switch port to a router port.

```
SwitchA(config)# interface FastEthernet0/1
SwitchA(config-if)# no switchport
SwitchA(config-if)# ip address 192.168.1.1 255.255.255.0
SwitchA(config-if)# no shutdown
```

One concept that is worth exploring is **secondary IP address**. The primary address is the IP address that is assigned to the interface. The secondary IP address is a way to support multiple IP addresses per router interface. Hence, it allows multiple Layer 3 networks to reside on the same physical link. Secondary IP addresses can be useful when you want to add more networks without having to disturb the existing network or to use it as a transitional network for network migration. Some people might just want to run multiple logical subnets on one physical subnet. To add a secondary IP address to the interface, the command is **ip address** [*ip_address*] [*subnet_mask*] **secondary**. The keyword **secondary** is used to specify the secondary IP address. The secondary IP address configuration is as follows:

Secondary IP Address
Allows multiple Layer 3 networks to reside on the same physical link.

```
Router(config)# interface FastEthernet0/0
Router(config-if)# ip address 10.10.20.250 255.255.255.0
Router(config-if)# ip address 172.16.1.1 255.255.255.0 secondary
```

In order to configure the secondary IP address, the primary IP address must exist first. There can be as many secondary IP addresses as needed. The secondary IP address cannot be verified with the **show int** or **show ip int brief** command. The results will only display the primary IP address information.

InterVLAN Routing Configuration

As previously discussed in Section 1-3, "VLAN Network," each VLAN is its own broadcast domain. It cannot forward traffic across its VLAN boundaries. However, it is almost impractical in today's applications for a VLAN not to be able to communicate beyond itself. To enable communications among VLANs, **InterVLAN routing** is required.

InterVLAN routing
Enables communications among VLANs.

router on a stick
Eliminates connecting a link from each VLAN to a router port by utilizing a trunk or 802.1Q port.

The most logical solution to route traffic between different VLANs is to introduce or create a Layer 3 routed network between them. One traditional way is to connect each VLAN to a router interface. Then, each router interface is configured as a different Layer 3 network. This enables VLANs to communicate and pass traffic via the Layer 3 IP network. For a few VLANs, this does not present an issue, but for a large number of VLANs, this could create some issues. This means that every VLAN will require a physical connection to a router port. Router ports are expensive, and this design can be costly as the number of VLANs increases and more physical links are required. A more common and popular design is to implement a **router on a stick**. The router on a stick design eliminates connecting a link from

each VLAN to a router port by utilizing a trunk or 802.1Q port. A single trunk port is connected to a router, and it passes the tagged VLAN traffic to the router, as depicted in Figure 1-12.

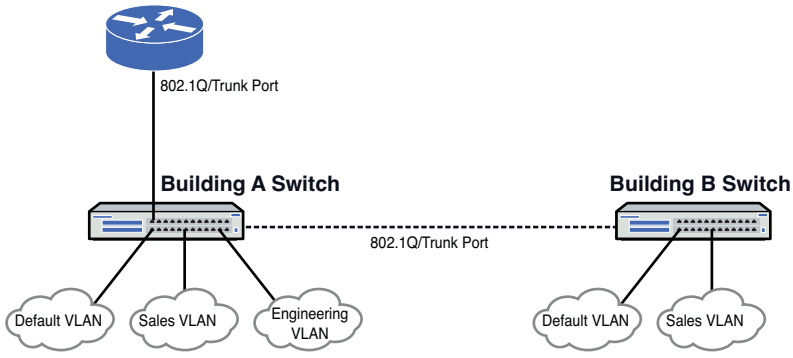


FIGURE 1-12 Router on a stick topology

This design requires that the router must be configured to accept the tagged VLANs. A Layer 3 network is then assigned to each VLAN coming to the router. To accomplish this, subinterfaces are created under the router interface at which the switch trunk port is terminated. The subinterface is a virtual interface, and its notation is a dot followed by the subinterface number. In the example provided, the subinterfaces are listed as FastEthernet0/0.1, 0.2, and 0.3. For the ease of programming, it is recommended to keep the subinterface number the same as the VLAN ID. Recall that the default VLAN is 1, the Sales VLAN is 2, and the Engineering VLAN is 3. The next step is to define the VLAN tagging encapsulation. In this case, it is dot1q, which essentially is 802.1Q. With the encapsulation, the appropriate VLAN ID is specified. Next, the IP address is assigned creating a routed Layer 3 network for a VLAN. The following example demonstrates how to configure a Cisco router for a 802.1Q interVLAN routing:

```
Router(config)#interface FastEthernet0/0
Router(config-if)#no ip address
Router(config-if)#interface FastEthernet0/0.1
Router(config-if)#description Default VLAN
Router(config-subif)#encapsulation dot1Q 1
Router(config-subif)#ip address 172.16.10.1 255.255.255.0

Router(config-subif)#interface FastEthernet0/0.2
Router(config-subif)#description Sales VLAN
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 172.16.20.1 255.255.255.0

Router(config-subif)#interface FastEthernet0/0.3
Router(config-subif)#description Engineering VLAN
Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 172.16.30.1 255.255.255.0
```

As mentioned in Section 1-3, an IP address can be assigned to a VLAN interface for management purposes. The IP VLAN interface does not perform any routing functions when running as a Layer 2 switch. However, this concept is changed in multilayer switching. Different virtual interfaces can be created on each of the VLANs. These interfaces are called **SVIs** (switched virtual interfaces). When an SVI is created and the IP address is assigned, the multilayer switch that has routing enabled can start routing VLANs. Thus, an SVI acts like a virtual router interface. The SVI is another way to route VLANs. SVI's deployment is common in multilayer switches. The following example demonstrates how to configure an SVI:

SVI
Switched virtual interfaces.

```
SwitchA(config)# ip routing
SwitchA(config)# interface VLAN 1
SwitchA(config-if)# ip address 192.168.1.1 255.255.255.0
SwitchA(config-if)# no shutdown

SwitchA(config)# interface VLAN 2
SwitchA(config-if)# ip address 192.168.2.1 255.255.255.0
SwitchA(config-if)# no shutdown
```

The command **ip routing** is entered to ensure the routing is enabled on a multilayer switch. After that, the switched virtual interfaces are created for every VLAN that we want to route. Then, the IP address is assigned to each SVI interface. By default the SVI interface is not enabled, hence the command no shutdown needs to be issued. The preceding example shows the steps on how to enable configuring an SVI for VLAN 1 and VLAN2.

Serial and ATM Port Configuration

As mentioned in the previous section, routers can have different types of interfaces, such as a serial and Asynchronous Transfer Mode (ATM) interfaces. At one time, these interfaces were the standard of WAN connection technologies. Now, they are being replaced by Ethernet WAN based technology. Some network engineers will argue that the serial and ATM technologies are a dying technology and are now considered to be obsolete. However, being obsolete does not mean they are nonexistent. Many of the rural networks in America and around the world still use these technologies for their WAN connection and rely on these technologies to deliver services to people's homes and businesses. Therefore, it is still beneficial to have a basic understanding of these legacy technologies and how they operate. After all, knowledge is always a commodity.

Serial technology provides communications data rates for end users in the form of **DS**-0 to DS-3 and T1 to T3. The T1/DS-1 and T3/DS-3 designations are actually the same data rates and the terms are used interchangeably. The Bell system *T* carriers were established in the 1960s primarily for transporting digitized telephone conversations. In the early 1980s, the digital signal (DS) subscriber lines became available. Table 1-4 lists the data rates for the T/DS carriers. The DS0 designation is for the base rate of the digital signal lines, basically the data rate of a digitized telephone call. The DS0 channels can be multiplexed together to provide more transmission bandwidth. For example, the T1 line is capable of carrying 24 DS-0 transmissions, which provide the data rate of 1.544 Mbps.

DS
Digital signal.

TABLE 1-4 **Data Rates for the T and DS Carriers**

Designation	Data Rate
DS-0	64 kbps
T1 (DS-1)	1.544 Mbps
T2 (DS-2)	6.312 Mbps
T3 (DS-3)	44.736 Mbps

CSU/DSU
Channel service unit/data service unit.

The communications carrier will require the serial data connection be made through a **CSU/DSU** (channel service unit/data service unit). The CSU/DSU provides the hardware data interface to the carrier. This includes adding the framing information for maintaining the data flow, storing performance data, and providing line management. The T1 data stream is broken into frames. Each frame consists of 24 voice channels (8 kbps)—8 bits per channel plus one framing bit, for a total of 193 bits. There are two framing techniques used in T1: D4 and ESF. D4, sometimes known as SF (Super Frame), is the original framing technique. Later on, ESF (Extended Super Frame) was introduced as an improvement in data performance over D4 framing.

AMI
Alternate mark inversion. A fundamental line coding scheme developed for transmission over T1 circuits.

B8ZS
Bipolar 8 zero substitution. A data encoding format developed to improve data transmission over T1 circuits.

Minimum Ones Density
A pulse is intentionally sent in the data stream even if the data being transmitted is a series of all 0s.

HDLC
High-level data link control, a synchronous proprietary protocol.

PPP
Point-to-Point Protocol. A full duplex protocol used for serial interface connections such as that provided by modems.

Along with Framing, T1 requires line coding. The data connection to the communications carrier requires that the proper data encoding format be selected for the CSU/DSU. Data are encoded in such a way that timing information of the binary stream is maintained and the logical 1s and 0s can still be detected. A fundamental coding scheme that was developed for transmission over T1 circuits is alternate mark inversion (**AMI**). The AMI code provides for alternating voltage level pulses V(+) and V(-) to represent the 1s. With AMI, a long string of 0s can produce a loss of timing and synchronization. This deficiency can be overcome by the transmission of the appropriate start, stop, and synchronizing bits, but this comes at the price of adding overhead bits to the data transmission and consuming a portion of the data communication channel's bandwidth. The bipolar 8 zero substitution (**B8ZS**) data encoding format was developed to improve data transmission over T1 circuits. T1 circuits require that a minimum ones density level be met so that the timing and synchronization of the data link is maintained. Maintaining a **minimum ones density** means that a pulse is intentionally sent in the data stream even if the data being transmitted is a series of all 0s. Intentionally inserting the pulses in the data stream helps maintain the timing and synchronization of the data stream. B8ZS is sometimes referred to as clear channel by the Telecommunication engineers. Both framing and line coding are configured at the CSU/DSU. The configuration must match at both ends of the connection. The CSU/DSU could be its own unit or it could be built into the router serial interface. Typically, AMI signaling is paired with D4/SF, while B8ZS signaling uses frames that are grouped into ESF.

Two other serial line protocols commonly used in wide-area networking are high-level data link control (**HDLC**) and Point-to-Point Protocol (**PPP**). Both protocols are used by routers to carry data over a serial line connection, typically over direct connections, such as with T1. PPP is used for serial interface connections, such as that provided by modems. PPP is a full duplex protocol and is a subset of the HDLC data encapsulation.

The routers at each end must be configured with the proper data encapsulation. *Data encapsulation* means the data is properly packaged for transport over a serial communications line. The type of encapsulation depends on the hardware being used to make the connection. The command for setting the data encapsulation is **encapsulation** (**encap**). The options for the data encapsulation on the router can be viewed by entering **encap ?** at the router's (config-if)# prompt, as demonstrated here:

```
Router(config-if)#encap ?
  atm-dxi      ATM-DXI encapsulation
  frame-relay  Frame Relay networks
  hdlc         Serial HDLC synchronous
  lapb         LAPB (X.25 Level 2)
  ppp          Point-to-Point protocol
  smds         Switched Megabit Data Service (SMDS)
  x25          X.25
```

The following configuration example is from an older Cisco router, which has a serial interface connecting to a CSU/DSU. The steps for setting the data encapsulation to HDLC and PPP on the Serial1/0 interface and configuring the serial interface IP address are shown. The T1 encapsulation on Cisco routers is HDLC by default, if the encapsulation is not specified. The encapsulation can be overwritten by issuing the new encapsulation option. Finally, the interface can be enabled via the command **no shut**.

```
Router# conf t
Router(config)# int s1/0
Router(config-if)#encap hdlc
Router(config-if)#ip address 10.10.128.1 255.255.255.0
Router# conf t
Router(config)# int s1/0
Router(config-if)#encap ppp
Router(config-if)# no shut
2w0d: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
2w0d: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to up
```

The status of the serial interfaces can be checked using the **sh ip int brief** command, as demonstrated here:

```
Router# sh ip int brief
Interface       IP-Address       OK?   Method   Status    Protocol
FastEthernet0   10.10.20.250     YES   manual     up      up
FastEthernet0/1  unassigned        YES   manual     administratively
down      down
FastEthernet0/2  unassigned        YES   manual     administratively
down      down
Serial1/0        10.10.128.1      YES   manual     up      up
```

The data encapsulation can be verified by using the **sh int s0/0** command. The last line in this example shows that the encapsulation is PPP:

```
Router#sh int s1/0
Serial0 is up, line protocol is up
Hardware is HD64570
Description: ISP Connection
Internet address is 192.168.1.2/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
```

The type of network being configured and the equipment being used to make the direct connection determines the selection of the format for data encapsulation. For example, Cisco routers automatically configure the serial interfaces to run HDLC, but the Cisco routers support many data encapsulation formats. The HDLC data encapsulation formats are implemented differently by some vendors, and there are times when some equipment is not interoperable with other equipment even though they both have specified the HDLC encapsulation. In that case, another encapsulation format such as PPP can be used to make the direct connection.

WIC
WAN interface cards.

VWIC
Voice/WAN interface cards.

service-module t1
The router command for configuring T1 framing, line coding, and the clock source.

On newer Cisco routers, there is a variety of T1 interface cards available. Most of them fall under these two types. They are either WAN interface cards (**WIC**s) that only provide data support or they are Voice/WAN interface cards (**VWIC**s) that can provide both voice and data support. These types of cards all have an integrated CSU/DSU, which makes it convenient for setup. In this case, a T1 connection with an RJ45 interface can be directly connected to the card. If the names WIC and VWIC are not confusing enough, the configuration steps for these cards will certainly create some confusion. The configuration steps are presented next.

The first example shows the configuration of a router with a T1 WIC card. The T1 configuration, usually programmed on a CSU/DSU, is now done under a serial interface. The T1 framing, line coding, and clock source are configured via command **service-module t1**. In this case, ESF is selected as the framing technique, and B8ZS is used as the line coding. The clock source line means the clock is provided by the carrier through the T1 line. This is critical for synchronizing the T1 transmission. The timeslot defines the speed of the DS0 channel and the number of DS0 channels being used.

```
Router(config)#interface Serial0/1
Router(config-if)#ip address 10.10.128.1 255.255.255.0
Router(config-if)#service-module t1 timeslots 1-24 speed 64
Router(config-if)#service-module t1 framing ESF
Router(config-if)#service-module t1 linecode B8ZS
Router(config-if)#service-module t1 clock source line
Router(config-if)#encapsulation ppp
```

The second example shows the configuration of a router with a T1 VWIC type card. The framing, line coding, and clock source are now defined under a T1 controller. Next, a corresponding serial interface is created with an IP address and the T1 encapsulation:

```
Router(config)#controller T1 1/0
Router(config-controller)#framing esf
Router(config-controller)#clock source line
Router(config-controller)#linecode b8zs
Router(config-controller)#channel-group 0 timeslots 1-24 speed 64

Router(config-if)#interface Serial1/0:0
Router(config-if)#ip address 10.10.128.1 255.255.255.0
Router(config-if)#encapsulation ppp
```

You can verify the T1 status with the command **show controller T1** *slot/port*. This command displays the T1 status with details that one would find in a CSU/DSU. The output result shows the T1 is up in a good clean state. So far, there are no errors for the last 24 hours:

show controller T1 *slot/port*
Verifies the status of the T1 interface.

```
Router#show controller T1 1/0
T1 0/1/0 is up.
  Applique type is Channelized T1
  Cablelength is long 0db
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  Version info Firmware: 20090408, FPGA: 13, spm_count = 0
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
  CRC Threshold is 320. Reported from firmware  is 320.
  Data in current interval (195 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail
Secs
  Total Data (last 24 hours)
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail
Secs
```

Asynchronous Transfer Mode (**ATM**) is a cell relay technique designed for voice, data, and video traffic. It uses fixed length data packets called cells. The size of each cell is 53 bytes with 5 bytes being the ATM header. The ATM protocol was designed for use in high-speed multimedia networking, including operation in high-speed data transmission found in SONET's OC-1, OC-3, OC-12, OC-48, and OC-192.

ATM
Asynchronous transfer mode.

Virtual Path Connection (VPC)
Used to connect the end users.

Virtual Channel Connection (VCC)
Carries the ATM cell from user to user.

Switched Virtual Circuit (SVC)
A dynamic virtual circuit that is established on demand by end devices through the Network-Network Interface signaling method.

ATM is connection oriented, using two different types of connections: a **virtual path connection (VPC)** and a **virtual channel connection (VCC)**. A VCC is used to carry the ATM cell data from user to user. The virtual channels are combined to create a virtual path connection, which is used to connect the end users. Virtual circuits can be configured as permanent virtual connections (PVC) or they can be configured as switched virtual circuits (**SVC**).

Five classes of services are available with ATM, based on the needs of the user. In some applications, users need a constant bit rate for applications such as teleconferencing. In another application, users might need only limited periods of higher bandwidth to handle bursty data traffic. Table 1-5 describes the five ATM service classes.

TABLE 1-5 **Five ATM Service Classes**

ATM Service Class	Acronym	Description	Typical Use
constant bit-rate	CBR	Cell rate is constant.	Telephone, video-conferencing television
Variable bit-rate/ non–real time	VBR-NRT	Cell rate is variable.	Email
Variable bit-rate/ real time	VBR-RT	Cell rate is variable but can be constant on demand.	Voice traffic
Available bit-rate	ABR	Users are allowed to specify a minimum cell rate.	File transfers/email
Unspecified bit-rate	UBR		TCP/IP

VPI
Virtual path identifier.

VCI
Virtual channel identifier.

ATM uses an 8-bit virtual path identifier (**VPI**) to identify the virtual circuits used to deliver cells in the ATM network. A 16-bit virtual channel identifier (**VCI**) is used to identify the connection between the two ATM stations. The VPI and VCI numbers are provided by the telco. Together, the numbers are used to create an ATM PVC (permanent virtual circuit) through the ATM cloud, as demonstrated in Figure 1-13.

The VPI/VCI numbers (1/33) shown in Figure 1-13 are for the ATM PVC interface. Router A connects to the ATM cloud via an ATM physical interface on the router. Router B also connects to the ATM cloud via an ATM physical interface on the router. In this example, the name for the physical interface on Router A is ATM 4/0. This is comparable to the E0 name for the router's Ethernet0 interface.

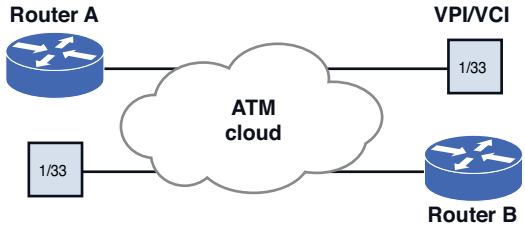


FIGURE 1-13 An example of a connection to an ATM cloud

The following listing is from a router configured to run ATM:

```
Interface ATM 4/0
description net atm (1 2 3 4 5 6 7 8 9)
no ip address
atm scrambling cell-payload atm framing cbitplcp
no atm ilmi-keepalive
```

The first line, **Interface ATM 4/0**, identifies the physical interface being configured (in this case, ATM interface 4). The second line, **description net atm (1 2 3 4 5 6 7 8 9)**, is a description of the ATM connection. The name of the connection is net; it is an ATM connection, and the telco circuit number is 1 2 3 4 5 6 7 8 9. The third line, **no ip address**, indicates that no IP address is specified for the ATM interface. The physical interface on an ATM connection is not assigned an IP address. The two commands **atm scrambling cell-payload** and **atm framing cbitplcp** are entries required to make the connection to the telco interface. Telco specifies the format for these commands. The entry **no atm ilmi-keepalive** is used to disable the generation of keepalive messages.

The next group of commands is used to configure the router's subinterface:

```
interface ATM4/0.33 point-to-point
description PVC to CityB (1 2 3 4 5 4 3 2 1)
ip address 192.168.23.1 255.255.255.0
pvc netB 1/33
vbr-nrt 3000 3000 1 broadcast encapsulation aal5snap
```

The entry interface **ATM 4/0.33 point-to-point** indicates that the VCI number for the subinterface is 33 and it is on the ATM 4 physical interface. It also indicates that this is a point-to-point connection. The second line is for the description of the subinterface. It indicates that this is a PVC for connecting to CityB's network, and the telco circuit number is 1 2 3 4 5 4 3 2 1. The third line specifies the IP address for the subinterface.

The entry **pvc netB 1/33** creates a PVC with a VPI of 1 and a VCI of 33. The entry **vdr-nrt 3000 3000 1** is used to configure the peak, average, and burst options for voice traffic over the PVC. This parameter is typically specified by telco. The output pcr (peak cell rate) is 3,000 kbps and the output scr (sustained cell rate) is 3000 kbps. The **1** indicates an output mbs (maximum burst size) of 1.

The entry **broadcast** enables broadcasts to be forwarded across the ATM PVC. The entry **encapsulation aal5snap** indicates that the ATM adaptation layer 5 is to be used to prepare the data for transmission over ATM. AAL5 encapsulation is typically specified to transport TCP/IP data traffic over ATM.

To display the ATM interfaces, enter the **show atm vc** router command, as demonstrated in the following ouput:

```
router#sh atm vc
Interface  VCD/                          Peak  Avg/Min Burst
           Name  VPI  VCI Type Encaps SC  Kbps  Kbps    Cells  Sts
2/0.32     1     1    32  PVC  SNAP   UBR 100000                UP
2/0.33     2     1    33  PVC  SNAP   UBR 3000                  UP
2/0.34     6     1    34  PVC  SNAP   CBR 5000                  DOWN
```

The **1/0.32** indicates this is the 1/0 physical interface and the .32 is the PVC. The type is a **PVC** (permanent virtual circuit), the encapsulation is **SNAP** (the Subnetwork Access Protocol), the service class is **UBR**, which is an unspecified bit rate running TCP/IP. The bit rate is **100000** kbps and the status (**Sts**) is **UP**.

The next command shows how to display only a specific ATM virtual channel (VC); the command is **show atm vc interface atm1/0.33**. This command only displays the atm1/0.33 virtual channel. The types of ATM interfaces typically listed are DS3 (44.736 Mbps), OC-3 (155.52 Mbps), OC-12 (622.08 Mbps), and OC-192 (9953.28 Mbps) .

```
router#sh atm vc interface atm1/0.33
VCD/                                             Peak  Avg/Min Burst
Interface  Name      VPI  VCI  Type Encaps SC    Kbps  Kbps    Cells
Sts
1/0.33     2         1    33   PVC  SNAP   UBR 3000
UP
router#
```

The last command examined is used to display information on the interface. The command used is **show controller atm** *slot/port*. In this case, the information on the atm1/0 interface is displayed. Part of the display for the atm1/0 interface is listed:

```
router#sh controller atm1/0
Interface ATM1/0 is up
Hardware is ENHANCED ATM PA Plus - OC3 (155000Kbps)
Framer is PMC PM5346 S/UNI-155-LITE, SAR is LSI ATMIZER II
Firmware rev: X102, Framer rev: 0, ATMIZER II rev: 4
  idb=0x638A43E0, ds=0x638AC000, vc=0x638F76E0
  slot 1, unit 1, subunit 0, fci_type 0x03A9, ticks 226930
  2400 rx buffers: size=512, encap=64, trailer=28, magic=4
Curr Stats:
  VCC count: current=6, peak=6
  AAL2 VCC count: 0
  AAL2 TX no buffer count: 0
```

SUMMARY

The fundamentals of configuring and managing a campus network have been presented in this chapter. This has been an overview of the campus network infrastructure, and you should understand that each of the topics presented in this chapter could easily be expanded to fill an entire textbook(s). What you should understand from this reading is that configuring and managing a campus network is a major task. You should appreciate the fact that configuring and managing a campus type

network requires the expertise of many people with many different networking capabilities, as well as understand the following:

- The importance and function of the three layers of a campus network
- The issue of data flow in a network
- Have an understanding of IP allocation and subnet design
- Understand the steps and process for configuring a VLAN
- Understand the issues of configuring the Layer 3 routed network

QUESTIONS AND PROBLEMS

Section 1-1

1. What networking equipment is usually found in the core of a campus network?
2. How are route policies applied in the core?
3. What is the advantage of using a Layer 3 switch in the core of the campus network?
4. Can a Layer 2 switch be used in the core of the campus network? Why or why not?
5. What is the function of the distribution layer in a campus network?
6. Can routing policies be implemented in the distribution layer? Why or why not?
7. What is the purpose of the access layer?
8. The campus network servers are typically located in what layer?
9. Why are routers typically not interconnected at the distribution layer?
10. What is the name for the part of the campus network that carries the bulk of the routed data traffic?
11. List three criteria for selecting the network media. Which is the final decision factor?
12. Which media is the best choice in a campus network?
13. Referring to Figure 1-1 from the beginning of the chapter, discuss how data flows from a computer in LAN B to a computer in LAN D. Assume that Switch A has been configured to be the preferred switch.

Section 1-2

14. What are three factors that should be considered before coming up with the final IP subnet design?
15. What are the address ranges for Class A, B, and C IP addressing?
16. Which public IP address space is now being assigned by the ISPs?
17. What is an Intranet?
18. What is the purpose of NAT and PAT?
19. What is overloading?
20. Which of the following are questions that the network engineer should ask when designing addressing for the IP network? (Select two.)
    a. How many network devices must be accommodated in the network?
    b. What is the cost of applying IP addresses to each network?
    c. How many network devices must be accommodated in the future?
    d. What Layer 3 technology should be used for routing?

21. What is the subnet mask for the following CIDRs and the number of available IP addresses?

    /16, /22, /25, /30

22. Most home routers are preconfigured with what private class address, and what is the typical range of IP addresses?

23. What technique is used when a CIDR block greater than 254 IP addresses is required?

24. Is there a problem randomly applying CIDR blocks?

25. A /22 CIDR block is being used for supernetting. What subnet will IP addresses 192.168.80.0 to 192.168.83.0 be in?

26. How is a network address of 192.168.6.0 and a subnet mask of 255.255.254.0 written in CIDR?

27. A CIDR block contains the following subnets with the IP addresses of

    192.168.68.0/22

    192.168.69.0/22

    192.168.70.0/22

    192.168.71.0/22

    Are there any problems with this group of subnets in the CIDR block? Show your work.

28. Are there any problems if the following four Class C networks are used to create a /22 CIDR block?

    192.168.78.0/22

    192.168.79.0/22

    192.168.80.0/22

    192.168.81.0/22

29. Figure 1-14 shows three different networks with different size requirements. The needed capacity (number of devices) for each network is specified in the figure. Your task is to determine the CIDR block required for each network that will satisfy the number of expected users. You are to use Class C private IP addresses when configuring the CIDR blocks. Assign IP addresses and gateway addresses to the networks. The IP addresses should start with 192.168.0.0. Design your network so that the minimum IP address space is consumed.

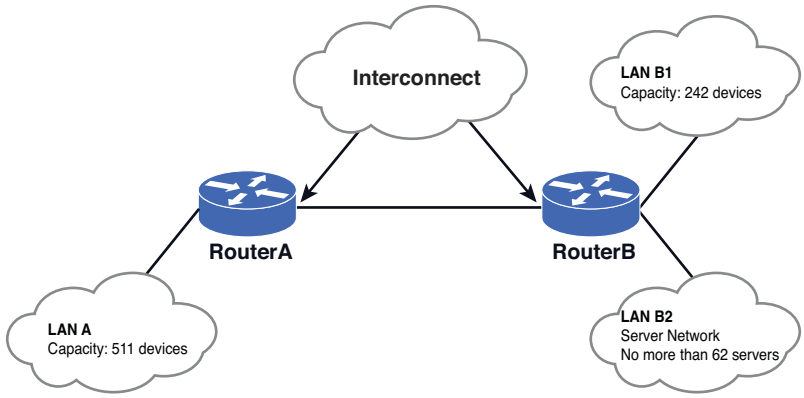


FIGURE 1-14 The networks for problem 29

Section 1-3

30. What is a VLAN?
31. What is a flat network?
32. List the three types of VLANs.
33. What type of VLAN is port-based?
34. Which type of LAN is based on 802.1Q specifications?
35. In what type of VLANs are port assignments created when they are assigned to a specific VLAN?
36. In this VLAN, ports are assigned to a VLAN based on either the computer's MAC address or the username of the client logged onto the computer.
37. The 802.1Q standard defines which of the following?
    a. Defines a system of VLAN tagging for Ethernet frames
    b. Provides specifications for inter router communication
    c. Helps to contain broadcast and multicast data traffic that help to minimize data congestion and improve throughput
    d. Provides guidelines for a switch port to belong to more than one VLAN
    e. All of the above
38. What commands are used to assign the IP address 192.168.20.5 to VLAN1?

```
SwitchA(config-if)#ip address 172.16.32.2 255.255.255.0
```

39. What switch command is used to display the interfaces assigned to a VLAN?
40. List the commands used to create VLAN5 and name this VLAN Marketing group.
41. List the commands used to assign FA0/5 to the Marketing-group VLAN (VLAN5). Show the switch prompts.

42. What Cisco IOS command is used to turn on trunking for a Cisco switch?
43. What is SwitchA(config-if)#**switchport trunk encapsulation dot1q** used for?
44. What command is used to enable ISL for trunking on a Cisco switch?
45. What is the Cisco IOS command that is used to limit the VLANs carried across the trunk if only VLANs 2 and 4 are allowed?
46. On an HP ProCurve Switch, what does it mean for a port to be untagged?
47. On an HP ProCurve Switch, what does it mean for a port to be tagged?
48. The following information is input to an HP ProCurve switch:

```
SwitchHP# conf
SwitchHP(config)# vlan  3
SwitchHP(vlan-1)# tagged 15
SwitchHP(vlan-1)# exit
SwitchHP(config)# vlan 5
SwitchHP(vlan-2)# tagged 15
```

What does inputting these commands on the HP switch indicate?

Section 1-4

49. Define Network address and Logical address.
50. What is the purpose of a routing table?
51. What is the purpose of a gateway address?
52. What is a network segment?
53. Define "wire speed" routing.
54. Switches that can operate above the OSI Layer 2 are called what?
55. What is another name for a routed network?
56. What types of interfaces were widely used to interconnect the router and the network to other wide area networks (WAN)?
57. What is the Cisco IOS command for turning on the **display of log messages for the remote terminal?**
58. What does the following information indicate?

```
Interface        IP-Address   OK?  Method  Status Protocol
FastEthernet0/0  10.10.200.2  YES  manual  up     down
```

59. What does the following command do?

```
SwitchA(config-if)# no switchport
```

60. What is the purpose of the following command sequence, and why is this done?

```
Router(config)# interface FastEthernet0/0
Router(config-if)# ip address 10.10.20.250 255.255.255.0
Router(config-if)# ip address 172.16.1.1 255.255.255.0 secondary
```

61. Define InterVLAN routing.
62. What does the router on a stick design do?

63. What is the purpose of the switched virtual interfaces?
64. What is the purpose of a CSU/DSU?
65. List the sequence of router commands required to set the data encapsulation to hdlc.
66. List the sequence of router commands required to set the data encapsulation to ppp.
67. List the command used on a router to verify the data encapsulation being used on the serial 0/0 interface.
68. List the command used to set the framing to ESF on the router's serial 0/0 interface.
69. List the command that can be used to verify the T1 status on port 0/0.
70. What is ATM?
71. List the command used to enable ATM on serial interface 3/0.
72. Your supervisor asks you if a Layer 2 switch could be used in the core of the campus network. Prepare a response to your supervisor. Be sure to justify your recommendation.
73. How does a Layer 3 switch differ from a Layer 2 switch?

Critical Thinking

74. Figure 1-15 shows three different networks with different size requirements. The needed capacity (number of devices) for each network is specified in the figure. Your task is to determine the CIDR block required for each network that will satisfy the number of expected users. You are to use Class C private IP addresses when configuring the CIDR blocks. Assign IP addresses and gateway addresses to the networks. The IP addresses should start with 192.168.0.0. Design your network so that the minimum IP address space is consumed.

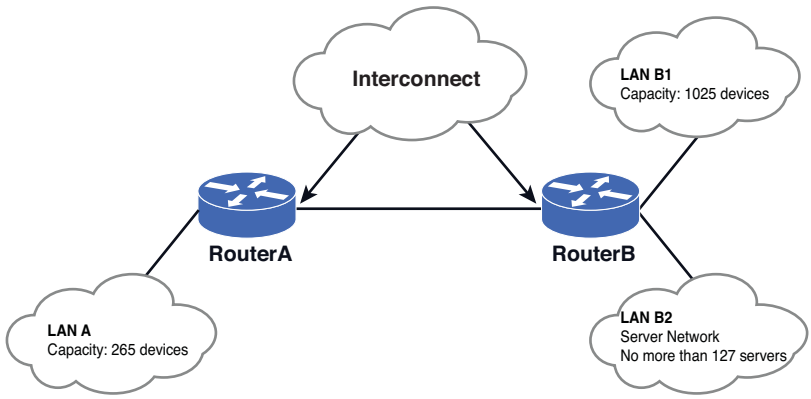


FIGURE 1-15 The networks for problem 74

75. A router has a TI WIC card. Your task is to configure the serial 0/0 interface to satisfy the following requirements. Specify the commands to accomplish this task.

    IP address: 192.168.12.3

    Subnet mask: 255.255.255.0

    Service: DS0 / 24 channels

    Framing: ESF

    Linecode: B8ZS

    Clock source: Line

    Encapsulation: ppp

76. A non-Cisco switch configured with two VLANs: 2 and 100. VLAN 2 is a 192.168.10.0/24 network, and VLAN 100 is a 172.16.20.0/24 network. This switch is not 802.1Q compliant. How can we route between these VLANs given that we have a Cisco router with 3 available interfaces: FastEhternet 0/1, 1/0, and 1/1?

77. The following five computers are connected to a switch. Their information is as follows:

	IP Address	Subnet Mask	Gateway	VLAN
Computer1	192.168.1.5	255.255.254.0	192.168.1.1	1
Computer2	192.168.2.5	255.255.254.0	192.168.2.1	1
Computer3	192.168.3.5	255.255.255.0	192.168.3.1	3
Computer4	192.168.4.5	255.255.255.0	192.168.4.1	3
Computer5	192.168.5.5	255.255.255.0	192.168.5.1	5

    The switch is connected via its 802.1Q port to a router. The router has the following configuration:

```
!
interface FastEthernet0/0

interface FastEthernet0/0.3
 description VLAN 3
 encapsulation dot1Q 3
 ip address 192.168.3.1 255.255.254.0

interface FastEthernet0/0.5
 description VLAN 5
 encapsulation dot1Q 5
 ip address 192.169.5.1 255.255.255.0
```

    Discuss the connectivity among the computers.

78. What is the expected behavior in the following network scenarios?

    a. When connecting SwitchA port 2, which is a member of port-based VLAN 10, to Switch B port 24, which is a member of port-based VLAN 5.

    b. When connecting SwitchA port 3, which is a member of port-based VLAN 3, to Switch B port 1, which is configured as a 802.1Q trunk port.