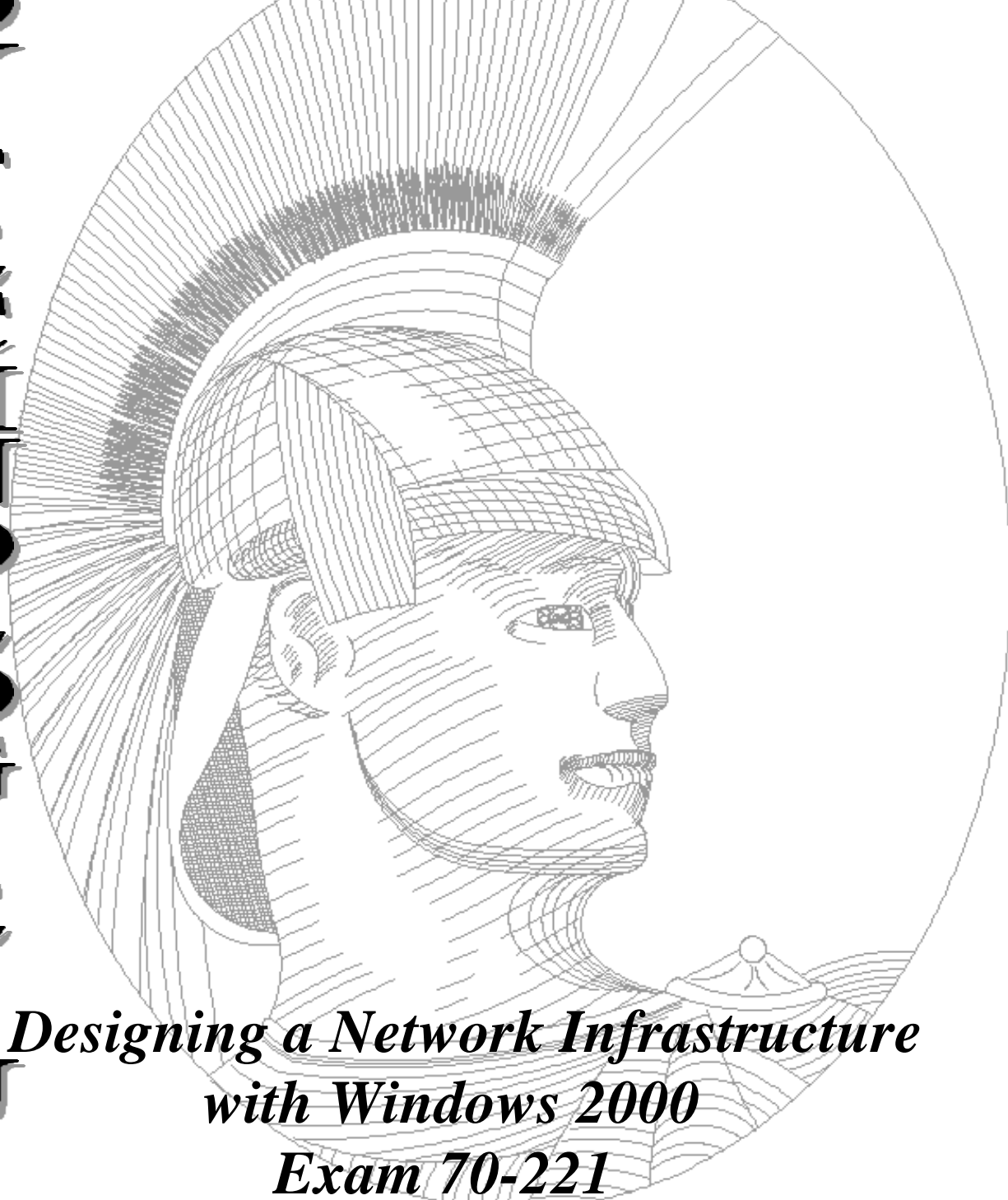


FOR
TECHNICAL
SUSAN

MCSE STUDY GUIDE



*Designing a Network Infrastructure
with Windows 2000
Exam 70-221*

Edition 1

Congratulations!!

You have purchased a *Troy Technologies USA* Study Guide.

This study guide is a selection of questions and answers similar to the ones you will find on the official Designing a Network Infrastructure with Windows 2000 MCSE exam. Study and memorize the following concepts, questions and answers for approximately 10 to 12 hours and you will be prepared to take the exams. We guarantee it!

Remember, average study time is 10 to 12 hours and then you are ready!!!

GOOD LUCK!

Guarantee

If you use this study guide correctly and still fail the exam, send your official score notice and mailing address to:

Troy Technologies USA
8200 Pat Booker Rd. #368
San Antonio, TX 78233

We will gladly refund the cost of this study guide. However, you will not need this guarantee if you follow the above instructions.

*This material is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this material, or any portion thereof,
may result in severe civil and criminal penalties, and will be prosecuted to the
maximum extent possible under law.*

© Copyright 2000 Troy Technologies USA. All Rights Reserved.
<http://www.troytec.com>

Table of Contents

ANALYZING BUSINESS REQUIREMENTS	1
Analyzing Business Models.....	1
Analyzing Organizational Structures.....	2
Analyzing Company Business Strategies	2
Analyzing IT Management	3
ANALYZING TECHNICAL REQUIREMENTS.....	4
Evaluating Technical Environment.....	4
Analyzing the Impact of Infrastructure Design.....	5
Analyzing Client Computer Access Requirements.....	6
Analyzing Disaster Recovery Strategies.....	6
DESIGNING A WINDOWS 2000 NETWORK INFRASTRUCTURE	7
Network Topologies.....	7
Planning TCP/IP Networking Strategies	7
Developing DHCP Strategies	8
Planning Name Services	9
Designing Multiprotocol Networks	9
Distributed File System (Dfs).....	10
DESIGNING FOR INTERNET CONNECTIVITY.....	10
Designing an Internet and Extranet Access Solution.....	10
Designing a Load-Balancing Strategy	11
DESIGNING A WIDE AREA NETWORK INFRASTRUCTURE	12
Designing an Implementation Strategy for Dialup Remote Access	12
Designing a Virtual Private Network (VPN) Strategy.....	13
Using a Routing and Remote Access Service (RRAS) Routing Solution to Connect.....	13
DESIGNING MANAGEMENT AND IMPLEMENTATION.....	13
Designing a Strategy for Monitoring and Managing Windows 2000 Network Services	14
Analyzing the Information.....	16
Responding to Issues.....	17
Designing Network Services for Application Architecture	17
Combining Networking Services.....	17
Designing a Plan for the Interaction of Different Network Services.....	18
Designing a Resource Strategy.....	19

Key Concepts

ANALYZING BUSINESS REQUIREMENTS

The technical aspects of network infrastructure design requires detailed planning. Without thoroughly considering the business requirements for the network infrastructure, the design project is likely to result in a network that is too simple to support the demands placed upon it or too complex to deliver results efficiently and cost effectively.

Analyzing Business Models

There are 5 basic types of business models:

International - In the International model you are likely to see all issues that could possibly be considered. This model increases the complexity of the issues in the National model by including the requirement that all national sites must inter-operate. New issues that arise in this model include cultural and language barriers and international politics.

National - A National business model is applied to a business whose scope spans an entire country. This business model involves all the types of concerns that are included in the Regional model, but includes multiple regions. This increases the importance of each region's concerns, because all regions must interoperate.

Regional - This business model is applied if your design comprises network locations in a particular regional area of a single country. Regional networks often span multiple counties, or states. This model includes considerations that are specific to the region, such as the relationship between communications providers, environmental concerns, and landscape concerns.

Subsidiary - This model is a smaller scale than the models discussed so far. In a Subsidiary model, concerns such as internal company politics increase in importance as you shape your design to allow the subsidiary network to interoperate with the infrastructure owned by the parent company.

Branch Office - In a branch office, you see the smallest business model. In this model, you focus on the specific function of the branch office and what services it must offer to or receive from the company headquarters and other branch offices.

You should also know and understand the following terms:

- **Information flow.** Information flow processes have to do with the way information is distributed throughout the company. It describes what information is available, who needs it, and in what order they receive it. Another term that describes this is "logical data flow." The way information flows logically from one part of the organization to the other happens without regard to physical structures to support it.
- **Communication flow.** Communication flow tracks the path that data follows through the

network infrastructure during the course of day-to-day operations of the business. This is also referred to as "physical data flow."

- **Service and product life cycles.** The entire period from the initial concept of the product or service to the complete removal of the product or service from the market, and all the events that transpire between, is called the *life cycle* of the product or service.
- **Decision-making.** In some organizations, decisions are made quickly and changes can occur rapidly. In others, there is a complicated process that must be executed before the slightest thing can be done.

Analyzing Organizational Structures

The important considerations when designing a network infrastructure are the organization structures within the company. The various organizational structures in place will usually determine the distribution of network resources and the type of network management strategy that will be implemented. Below is a list of organizational structures for you to consider when creating your design:

- **Management model.** The management philosophy prevalent in the organization has a direct impact on how the network is designed. Companies are broadly categorized as having a centralized or decentralized management structure. If management wants to centralize control, this impacts how the network is configured.
- **Company organization.** The organization of the company will prove to be a major consideration for your network infrastructure design. The distribution of resources will follow the company organization closely.
- **Vendor, partner, and customer relationships.** The relationships that a company maintains with its vendors, partners, and customers has an impact on the types of services that the company wants to provide on its network.
- **Acquisitions plans.** Awareness of intended acquisitions or mergers enables you to research the specific issues that will be faced in integrating the networks and to design solutions to those problems from the beginning.

Analyzing Company Business Strategies

The purpose of any network infrastructure is to enable the business to perform its day-to-day activities and meet its objectives with the greatest efficiency. You should know the following factors:

- **company priorities.** Document all the goals of the business and assign a priority number to each one. Goals with higher priority levels get built into the design first, and goals with lower priority values are included in the design only if they can be delivered after satisfying the goals at the higher priority levels.

- **projected growth strategy.** Company growth affects the demands placed on a network infrastructure. It is crucial that you develop an understanding of the company's projected growth as well as its growth strategy to ensure that the network infrastructure design meets the demands placed upon it.
- **laws and regulations.** Sometimes the operation of a particular business is governed by only a few relevant laws or regulations. Other businesses, however, must adhere to a very complex and strict set of laws and regulations. Partnering with the company's legal team can help make you aware of any legal issues that may apply to your project, and enables you to take advantage of its expertise in dealing with these issues.
- **tolerance for risk.** Any time that you design something as mission-critical as a network infrastructure, you must be acutely aware of the risks that are involved in implementing your design. Knowing up front the company's position and tolerance for risk can help you avoid serious problems later. Companies that are very risk-averse may implement more fault-tolerant features to minimize the risk of a network failure; those less worried about network failure will not require the same level of fault tolerance.
- **total cost of ownership.** The aggregation of all costs associated with purchasing, implementing, supporting, and operating a network infrastructure is referred to as the *Total Cost of Ownership* (TCO) of the network infrastructure.

Analyzing IT Management

Your network infrastructure design should include an analysis of the current and proposed IT management structure within the organization. You should be aware of the following areas:

- **Type of administration.** There are basically 2 types, centralized or decentralized. Your network infrastructure design must accommodate the IT administration model, whether handled centrally in one location or distributed across the organization in a decentralized approach.
- **Funding model.** The company's approach to funding the design and implementation projects directly impacts what you can and cannot accomplish with your design.
- **Outsourcing.** If the company for which you are designing a network infrastructure is currently outsourcing any part of the responsibility for installing, administering, and maintaining its network, you need to contact the company representatives who have been charged with the responsibility. These representatives can help you prioritize any issues in the existing infrastructure so that you can design your new infrastructure to resolve these issues, or at least to accommodate them.
- **Decision-making process.** Being familiar with the IT decision-making process and planning ahead can help make the design process flow more smoothly and bring you to the approval stage more quickly and less stressfully.

- **Change-management process.** The main purpose of a change-management process is to eliminate downtime resulting from changes made to the production network environment.

ANALYZING TECHNICAL REQUIREMENTS

The most obvious planning step when creating a network infrastructure design is the analysis of technical requirements. There are several steps to follow in order to perform a thorough and effective analysis of the technical requirements for a network infrastructure design.

Evaluating Technical Environment

Before you can begin your network infrastructure design you must be able to determine three things:

1. What does the customer want to do with the network infrastructure?
2. What does the customer do with its existing network infrastructure?
3. What is the gap between the current infrastructure and the desired infrastructure?

Answering these questions is called *performing a gap analysis*. After performing a gap analysis, consider the following items:

- **Analyze company size and user and resource distribution.** Determine the total size of the user population and any plans for future growth. In addition to the user population total, you should look closely at the distribution of these users.
- **Assess the available connectivity between the geographic location of work sites and remote sites.** Examine each of the work locations in the existing and the planned network infrastructure. For each location, you need to investigate the connectivity options available in that area.
- **Assess net available bandwidth and latency issues.** *Bandwidth* is the measure of the amount of data that a network link may carry at any given time. *Latency* refers to the amount of time between the moment when a network station is ready to transmit data and the moment when the transmission is completed successfully. Latency is sometimes also called "delay".
- **Analyze performance, availability, and scalability requirements of services.** Performance, scalability, and availability are three terms you will hear over and over again. You should know the definition of these three terms:
 1. *Performance* - The capability of the network infrastructure of meeting the demands for network services effectively and efficiently.
 2. *Scalability* - The capability of the network infrastructure of expanding or contracting in accordance with the demand for network services.

3. *Availability* - The percentage of time that the network infrastructure is up and running and available for use.
- **Analyze data and system access patterns.** Assess the peaks and valleys that exist in users connecting to different systems in the organization. Knowing when servers are going to be busy and which machines are affected has an impact on network design.
 - **Analyze network roles and responsibilities.** Determine the types of services that parts of the network will be used for. The role of the server in the organization could provide a clue to its usage and can be helpful in design.
 - **Analyze security considerations.** Security can be physical security at the network level or logical security at the file system level. In Windows 2000, secure communication can also be specified between servers or between clients and servers. The type of security requirements defined by the business practices of the organization can impact the network design.

Analyzing the Impact of Infrastructure Design

A good infrastructure design includes an analysis of the potential impact of the implementation so that an effective implementation plan can be developed to minimize the costs associated with rolling out of the new design. Consider the following factors when determining the impact of implementing your network infrastructure design:

- **Assess current applications.** Examine each of the applications to determine its requirements in terms of the network infrastructure. Some applications will be very demanding of the network infrastructure, generating heavy traffic and requiring high throughput, and others will not.
- **Analyze network infrastructure, protocols, and hosts.** A computer network is comprised of many parts. Connected to this basic infrastructure are the many individual computer systems that must use the network. These systems are called *hosts*. For hosts to make use of the network infrastructure for communications, they must first agree to a set of rules for doing so. These sets of rules are called *protocols*.
- **Evaluate network services.** List all the network services that are currently in use by the organization. Include in your list the specific network requirements for each service.
- **Analyze TCP/IP infrastructure.** A network that is based on the TCP/IP protocol has certain elements that must be considered carefully at the design stage in order for the network to operate effectively and efficiently. Some of these elements are:
 - The IP addressing scheme
 - The IP address assignment process
 - The hostname registration process
 - The hostname resolution process

- **Assess current hardware.** It is important to note that no matter what you include in your network infrastructure design, it is completely useless if the hardware in place cannot support it. You need to take an inventory of the hardware in the existing network infrastructure and determine which devices need to be upgraded to ensure that each device can support the demand that will be placed upon it.
- **Identify existing and planned upgrades and rollouts.** You need to become aware of any company plans to upgrade its existing applications. If there is an upgrade to an existing application available, the company may want to consider implementing the upgrade at the same time as it implements the new network infrastructure. Upgrading legacy applications may allow you to discontinue the use of older, less efficient protocols.
- **Analyze technical support structure.** A major component of the total cost of ownership for the network infrastructure is the ongoing cost to support that infrastructure. It is important to take the time to examine the organization's technical support structure to determine whether it can effectively support the new network infrastructure.
- **Analyze existing and planned network and systems management.** There are numerous tools available for performing network and systems management. You may find one or more tools currently in use. Tools for monitoring the health of the network infrastructure components are essential for minimizing downtime and troubleshooting costs.

Analyzing Client Computer Access Requirements

The work performed by end users needs to be as effective, efficient, and inexpensive as possible. Enabling this is the ultimate goal of any network infrastructure design. Make sure you do the following:

- **Analyze end-user work needs.** It is imperative that the network infrastructure supports the work needs of the end users. Analyzing end-user work needs involves determining who needs access to which data, when they need it, and where it should be delivered.
- **Analyze end-user usage patterns.** By examining end-user work needs, you know what data is needed, and by whom. You should also know where the data and its users are located. Knowing this information can help you predict the load on the network. Knowing the load at different points on the network can help determine how the network should be segmented, thereby impacting the network design.

Analyzing Disaster Recovery Strategies

The company's existing disaster recovery strategy for client computers, servers, and the network will become an essential tool for protecting the company's systems and data as you implement your new design. You need to know all the details regarding the processes involved in each of the company's disaster recovery strategies in order to determine the impact of your new network infrastructure design on them, and to ensure that these processes remain functional during the implementation of your network infrastructure design.

Disaster recovery mainly deals for backups, but also deals with fault tolerance of the network design. Issues include the loss of a critical network component, such as a backbone switch. What will the business impact be of network failure and how can this be minimized?

These elements need to be considered in designing a network structure. However, the need to provide proper recovery in the case of a disaster (that is, fault tolerance) should be balanced between the associated costs and then finally compared with the specific requirements of the organization.

DESIGNING A WINDOWS 2000 NETWORK INFRASTRUCTURE

A network infrastructure is the collection of technical network components and services that provide the framework for data communications and other network operations. The network infrastructure includes:

- Network hardware, such as cabling, routers, switches, and host computers
- Hardware and software protocols
- Network services that facilitate host communications, such as DHCP, DNS, and WINS
- Data storage and access configuration

Network Topologies

There are two components to network topologies: the physical network structure and the hardware protocol. Physical structure and protocol are closely related, because hardware protocols are designed to work with specific kinds of physical networks. The three most commonly used network topologies are:

1. **Backbone-based networks.** Backbone-based networks consist of multiple segments connected to a central segment, a backbone, through which traffic between segments flows. An example could be a thicknet (10Base5) Ethernet backbone network with multiple thinnet (10Base2) segments connected to the backbone via a router.
2. **Ring networks.** Token-ring and Fiber Distributed Data Interface (FDDI) are two examples of ring networks where the logical implementation of the network topology emulates a ring.
3. **Switched networks.** Switched networks consist of a smart hub that "switches" traffic between different segments. Switches can be layer 2, where the switch port is set to receive packets based on the MAC address, or layer 3, where the destination is determined by the IP address.

Planning TCP/IP Networking Strategies

The TCP/IP protocol suite is the global standard for networking. Windows 2000 Server supports the full implementation of the TCP/IP protocol suite and connectivity and management services for TCP/IP based networks. It is important to know which core protocols, services, and

application-layer protocols will be used on the network and how they will be used in terms of broadcast traffic, retransmission, and session connections required for applications.

A routed network is two or more physical network segments that are linked by one or more routers. You should have a good understanding of the following:

- **Types of routed networks.** Routed networks divide a large network into two or more subnets by using a router. The router forwards packets between the two segments to ensure all traffic reaches the proper host.
- **Routing tables.** Entries within the router that specify to which segments a particular packet is to be forwarded based upon the IP address. Routing tables can be configured manually using static routes or automatically by one of the two routing protocols: Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).
- **Default gateways.** A default gateway is a TCP/IP configuration entry on each host specifying to which router to forward packets not destined for the local network. Hosts also have a routing table and may have multiple default gateways specified to allow for redundancy.
- **Routing protocols.** Routing protocols are protocols used by a router to keep its routing tables updated automatically. The two most common protocols are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).
- **Windows 2000 Server routing configuration.** The configuration of a Windows 2000 machine tells IP to which router to forward packets not for the local segment. This information can be retrieved by using the Ipconfig utility or the Netstat utility.

Developing DHCP Strategies

Dynamic Host Configuration Protocol (DHCP) was originally designed to dynamically assign IP addresses to IP network hosts. Currently, DHCP is also capable of assigning other configuration parameters to an IP host, such as default gateways, name server addresses, multicast addresses, and node type. Some of the other important features of DHCP include the following:

- DHCP client computers must be guaranteed a unique IP address.
- DHCP client computers must be unaffected by a DHCP server reboot. The client computer must receive consistent configuration information regardless of DHCP server reboots.
- A DHCP client computer must be equipped to deal with multiple DHCP responses, because more than one DHCP server may be available to a given segment.
- DHCP servers must support automated assignment of configuration information to client computers.
- Any implementation of DHCP must not require a DHCP server on each segment. DHCP must work across routers or BOOTP relay hosts.
- DHCP must work in a multiprotocol environment.
- DHCP must coexist on a network with statically assigned IP addresses.

- DHCP must interoperate with BOOTP relay agents and must support legacy BOOTP clients.

Planning Name Services

Windows 2000 Server supports two name services: Domain Name System (DNS) and Windows Internet Name Service (WINS). DNS is the Internet name resolution service standard. The physical implementation of a DNS namespace is supported by a distributed database. TCP/IP hosts are identified by a Fully Qualified Domain Name (FQDN). The smallest manageable part of the DNS namespace is known as a *zone*. Zones may be either primary or secondary. A zone contains the DNS information, known as resource records, for a contiguous portion of the DNS namespace. There are several types of resource records in a DNS database. The mechanism for keeping DNS server databases synchronized is called *zone transfer*. DNS servers that are the source for zone transfers are known as *master servers*.

Requests for information are called *queries*. Query types sent to the server from a resolver are called *QTYPE codes*. A DNS server can services two kinds of queries: recursive and iterative. The most common query issued by a resolver is a recursive query. *Recursive queries* place the responsibility for resolving the query on the DNS server. *Iterative queries* are typically used for name-server-to-name-server queries.

The protocol for dynamic update of DNS records is called Dynamic DNS (DDNS). UPDATE records can add or delete DNS resource records. A feature of dynamic DNS updates is that both the DHCP server and Windows 2000 client computer support re-registration, or refreshes. Windows 2000 client computers re-register with the DNS server every 24 hours. Windows 2000 DHCP server re-registers downlevel client computers when their lease is renewed.

Windows 2000 computers use DNS for name resolution. In a mixed environment where WINS is used, Windows 2000 DNS can be configured to perform WINS lookups. When a lookup query fails, the DNS server queries WINS to resolve the name. When integrated into Active Directory, DNS does not use conventional zone files to store records. Instead, DNS records are stored in the Active Directory. To use Active Directory zone information directly, a DNS server must be running on a domain controller. Servers not running on DCs are configured as secondary servers and update using standard DNS protocols. Though Microsoft is moving to DNS as its default name service, many existing networks still use WINS.

Designing Multiprotocol Networks

Although TCP/IP is the network protocol of choice for Windows 2000, other protocols are supported. Windows 2000 includes support for these additional network protocols:

NWLink - is an IPX/SPX compatible protocol used to provide a transport for NetWare connectivity tools and IPX/SPX client computers. Integration of NetWare servers in a Windows 2000 network is provided by Client and Gateway Services for NetWare on a Windows 2000 Server or Advanced Server computer. Individual Windows 2000 Professional clients can configure connectivity to a NetWare server by installing Client Services for NetWare.

NetBEUI - is a nonroutable fast and efficient protocol ideal for small networks. NetBEUI cannot be used alone if support for Windows 2000 Active Directory is required.

DLC - is an IBM-specific protocol used for gateway connectivity and terminal emulator access to IBM midframe and mainframe systems using SNA. Connectivity between SNA and Windows 2000 networks is provided in Microsoft's SNA Server. DLC can also be used to connect to network-attached printers.

AppleTalk - is used in conjunction with File Services for Macintosh and Print Services for Macintosh to allow Macintosh clients to use Windows 2000 Server computers for file and printer sharing.

Windows 2000 supports all NDIS-compliant protocols with drivers for the Windows 2000 operating system, including Banyan Vines IP, DECNet, and others.

Distributed File System (Dfs)

Distributed file system (Dfs) is a management service for file shares and directories. Dfs enables the administrator to combine network resource shares into a single namespace called a Dfs volume. Access to Dfs volumes requires Dfs client computer software. Dfs client computer software is included with Windows NT 4 Workstation, Windows 2000 Professional, and is available for Windows 95 and Windows 98.

A Dfs **Error! Bookmark not defined.** root is the starting point for the hierarchical structure of one or more Dfs volumes. When a Dfs client computer browses or otherwise attempts to access a particular directory in a Dfs tree, the process is handled with referrals. A *referral* routes client computer requests for access to logical Dfs locations to a physical location. A Windows NT Server computer or a Windows 2000 Server computer running the Dfs host service can host one Dfs root.

DESIGNING FOR INTERNET CONNECTIVITY

Obtaining the benefits of the Internet requires that you have a thorough understanding of the technologies and services commonly used. When implemented, these services need to be connected to the Internet in a secure manner.

Designing an Internet and Extranet Access Solution

Components of an Internet and extranet access solution include:

- **Proxy servers.** A Proxy Server provides a number of services that can be used to assist in the management of your connection to the Internet. The Proxy Server acts as a control point between your private network and the public network. This control point enables you to isolate the private network from the public. Proxy Server is used to block incoming traffic from accessing resources on your internal network. Rules can be defined that allow or deny access to specific URLs or protocols. Proxy Server enables these rules to be applied to users

and groups so administrators can create specialized rules that apply to groups of users in their environments. Proxy Server also enables you to optimize your connection to the Internet by caching frequently accessed pages on a local hard drive that can be accessed internally.

- **Firewalls.** A *firewall* is a combination of hardware and software that can be used to reduce the risk of unauthorized access to your network. A firewall can be a packet filtering router, a packet filtering router combined with a circuit-level gateway, or the combination of a packet filtering router, circuit-level gateway, and application gateway. Most often, an effective firewall solution includes a combination of the three technologies.
- **Routing and Remote Access Service (RRAS).** The Routing and Remote Access Service provides multiprotocol routing support for Windows 2000. Through RRAS you can configure LAN-to-LAN, LAN-to-WAN, virtual private network (VPN), Network Address Translation (NAT) routing services, and dialup/virtual private network services.
- **Network Address Translation (NAT).** NAT is implemented through the Routing and Remote Access Service (RRAS). Before you can enable NAT, you must install RRAS. When the NAT server forwards packets, it translates the IP address and port values in the request. The translation data is stored in a database, so return packets can be mapped back to the original host that made the request.
- **Connection Sharing.** The connection sharing service allows a company to set up a single machine to act as a shared access point to the Internet. Private clients route requests to the Connection Sharing server, and the server takes care of translating the private request into a request that can be passed onto the Internet.
- **Web servers and mail servers.** Web servers and mail servers offer data access services to clients that reside inside the corporate network and externally. Web servers offer data through the Hypertext Transfer Protocol (HTTP). Client software called a *browser* is used to access data on Web servers using the HTTP protocol. Web servers that offer data to internal clients form the basis of an intranet. Internet Information Server (IIS) included with Windows 2000 Server, includes an HTTP and SMTP server component, as well as a File Transfer Protocol (FTP) server and Network News Transfer Protocol (NNTP) server.
- **Mail servers.** Mail servers facilitate the transfer of electronic mail to clients internal and external to the corporate network using the Simple Mail Transport Protocol (SMTP) or the Post Office Protocol version 3 (POP3). A POP3 and SMTP server is included with Microsoft Exchange server.

Designing a Load-Balancing Strategy

Network Load Balancing (NLB) is a clustering technology included with the Microsoft Windows 2000 Advanced Server and Datacenter Server products. The technology enables a cluster of systems (between 2 and 32) to be created. To scale performance, NLB distributes IP traffic across multiple cluster hosts. It also ensures high availability by detecting host failures and automatically redistributes traffic to the remaining hosts in the cluster.

With multiple-host load balancing, incoming client requests are distributed among all cluster hosts, and a load percentage can be specified for each host. Load percentages allow hosts with higher capacity to receive a large fraction of the total client load. Single-host load balancing directs all client requests to the host with the highest handling priority. When a port rule uses multiple-host load balancing, one of three client affinity modes must be selected. When no affinity mode is selected, NLB balances the client traffic load from one IP address and different source ports on multiple-cluster hosts. To assist in managing client sessions, the default single-client affinity mode balances all network traffic load from a given client's IP address and a single-cluster host. By default, NLB is configured with a single port rule that covers all ports (0-65,535) with multiple-host load balancing and single-client affinity.

DESIGNING A WIDE AREA NETWORK INFRASTRUCTURE

Beyond the considerations of the LAN network infrastructure, you must also consider connecting the individual LANs to form a WAN. WAN technologies and strategies differ from those of LANs. In configuring and designing a WAN, you need to develop a routing strategy to ensure access to all the sites that make up the WAN.

Though not directly part of designing a WAN, connections for dial-in users and virtual private networks (VPNs) also need to be designed to satisfy requirements for users who work away from the office, as well as branch office connections.

Designing an Implementation Strategy for Dialup Remote Access

In order for users to access the corporate network from remote locations, one connectivity option is a dialup connection to a Remote Access Server (RAS). This enables a remote user to connect to the network using a modem and ordinary telephone line. Here are some issues that you must resolve if you incorporate this type of dialup strategy into your network infrastructure design:

- **Client IP address assignment.** Clients are assigned an IP address when they connect to the RRAS server, via DHCP or from a static pool of addresses.
- **Client name registration.** Name registration is the method used by clients to register their computer names on the network, automatically via DHCP or manually using DDNS or WINS.
- **Name resolution.** Name resolution is the method used by clients to resolve the names of hosts they want to connect to, either by DNS or WINS.
- **User authentication.** Will users be authenticated by a domain controller, the local server, or by a RADIUS server?
- **Cost of long distance calls.** Should you configure callback to reduce the cost of long distance calls to the RRAS server, or a VPN connection through the Internet.

Designing a Virtual Private Network (VPN) Strategy

Another alternative that provides remote users connectivity to the corporate network is a virtual private network (VPN), which provides secure access to remote users across the Internet. Security is provided by encapsulating all transmissions across the Internet link within an encrypted data stream. Windows 2000 supports the Point-to-Point Tunneling Protocol (PPTP) and the Layer-2 Tunneling Protocol (L2TP). Internet Protocol Security (IPSec) can be used in conjunction with L2TP to provide an encrypted, secure tunnel across the Internet.

Using a Routing and Remote Access Service (RRAS) Routing Solution to Connect

The Routing and Remote Access Service (RRAS) provides multiprotocol routing support for Windows 2000. You can configure LAN-to-LAN, LAN-to-WAN, virtual private network (VPN), Network Address Translation (NAT) routing services, and dialup/virtual private network services.

When using RRAS to provide LAN-to-LAN or LAN-to-WAN routing services using the TCP/IP protocol, two dynamic routing protocols are supported: Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). On a RIP enabled network, routers keep their respective routing tables updated by communicating with neighbor routers. Approximately every 30 seconds, RIP routers broadcast their list of reachable networks. The primary drawback to RIP networks is bandwidth consumption due to the RIP announcements. The OSPF routing protocol works best with large networks. The two main features of OSPF are that routing table updates occur only when one or more routers on the network recognizes a change and that OSPF calculates routes using a shortest-path tree.

DESIGNING MANAGEMENT AND IMPLEMENTATION

The last step in your network infrastructure design project is to create a strategy for implementing and managing your design recommendations. A fully detailed implementation plan is probably the responsibility of the deployment team, but a well-developed deployment strategy can give the team some direction from the start.

After the design has been implemented, it needs to be managed and supported. Because the network infrastructure is new, the team needs to become acquainted with the design before being able to do its job effectively. There are essentially four main steps to managing a network:

1. **Identify what to manage.** In general terms, this means that you must first decide what you need to manage and what you do not need to manage.
2. **Monitor the network.** This involves using the Performance tool and the Network Monitor, among others, to gather information about the status of the systems that make up the network and about the physical network.

3. **Analyze the information.** You will gather a significant amount of data as you monitor an entire network. It is important that you analyze the data in real time. You should be able to recognize a problem before it becomes critical.
4. **Respond to issues.** The point of monitoring is to detect problems and to be able to respond to them. This means you should know what you need to do to resolve each crisis that could arise.

Designing a Strategy for Monitoring and Managing Windows 2000 Network Services

You need to devise a strategy for monitoring the key Windows 2000 services that are offered on the network infrastructure. The services need to be monitored for both availability and performance. Each service on the network needs to be managed to ensure that it is operating at peak efficiency. Some of the Windows 2000 network services that you want to monitor and manage include:

- **Global Catalog servers.** The central repository containing a subset of attributes of all objects in Active Directory, the Global Catalog is populated by Active Directory replication using Remote Procedure Calls (RPC) over either TCP/IP or SMTP.
- **Lightweight Directory Access Protocol (LDAP).** LDAP is the protocol used to search the Global Catalog and Active Directory.
- **Certificate Services.** Certificate Services is a component of Windows 2000 enabling you to issue X. 509 certificates that can be used by the Encrypting File System (EFS), IIS, and other Windows 2000 services.
- **Proxy Server.** Microsoft Proxy Server is a separate Microsoft product providing caching, filtering, and other services to optimize Internet access.
- **Domain Name System (DNS) Servers.** DNS is used by Active Directory to provide information on which services can be found on which machine. It is also used by clients to resolve hostnames to IP addresses, and is used by DHCP to update a hostname and IP address when a DHCP lease is issued or expired.
- **Dynamic Host Configuration Protocol (DHCP).** DHCP provides for the automatic assignment of IP addresses and other settings to computers on the network. It is also used by Remote Installation Services (RIS) to provide the IP address of a RIS server during client boot.
- **Routing and Remote Access Service (RRAS).** RRAS provides dialup remote access services, virtual private network (VPN) services, and Network Address Translation (NAT) services. This enables clients to access the network using the Public Switched Telephone Network (PSTN) and analog modems, ISDN, or the Internet. It also provides Internet connection sharing capabilities by masking internal IP addresses to a single external address through NAT.

- **Windows Internet Naming System (WINS).** WINS resolves NetBIOS computer names to IP addresses. This enables clients requiring NetBIOS naming to be able to connect to the right computer.
- **Distributed File System (Dfs).** Dfs enables clients to find network shares more easily by providing a central access point with information on the physical location of many shares. Clients connect to the Dfs root and then are redirected to the appropriate host instead of remembering the names of all hosts and which shares exist on them. With Windows 2000 Active Directory, Dfs can also provide for fault tolerance and replication of data in shares.

There are many tools available for monitoring and managing network services. Many of them come in the form of a Microsoft Management Console (MMC) snap-in. The available tools include the following:

- **Performance logs and alerts.** These are a subset of the System Monitor MMC snap-in in which you can configure alerts that can be fired whenever a specific performance threshold is surpassed. Alerts enable you to configure an action that should be taken or a notification that should be sent on the network or both.
- **Service Monitor events.** The Service Monitor is built into Windows 2000, and it monitors certain services that are designed to use it. It can restart a service, restart the server, or run a program to send a notification of the failure.
- **Simple Network Management Protocol (SNMP).** The SNMP agent service on Windows 2000 can use various Management Information Bases (MIBs) to access and report the status of various parts of the operating system. The agent can then respond to a query from a third-party management station or send traps to the management station. A *trap* is an occurrence of a significant event.
- **Event logs.** The Event Log Service can provide you with a great deal of information for troubleshooting a problem. The logs can also be used to calculate uptime for various services and to capture problems that happened. They report five types of events: Information, Warning, Error, Success Audit, and Failure Audit. In Windows 2000 there are six main event logs, each of which provides different information:
 - Applications log - Any application that is written to Microsoft standards has the capability of recording information in the Applications log.
 - Security log - Events that deal with the security of the system are tracked in this log.
 - System log - All the device drivers, services, and other system-related components record their errors in the system log.
 - Directory service - This log tracks events that relate to the Active Directory database and its replication.
 - DNS server - This log tracks events that affect the DNS server.
 - File replication service - This manages the replication of the files in the SYSVOL.

- **Network Monitor.** The Network Monitor is used to capture the traffic that is received or sent from a single computer. This enables you to actually see what packets are being generated from the services on a system and to monitor or troubleshoot problems on the network.
- **Command-line utilities.** Windows 2000 provides a number of command-line utilities that can be integrated into a script or called using the Task Scheduler to verify network performance. Some of the most commonly used utilities are
 - Netdiag - This utility performs a series of tests to isolate networking and connectivity problems. It can also determine the functional state of your network client.
 - Ping - This utility troubleshoots IP connectivity.
 - Tracert - This utility displays a list of routers along the path between a source host and a destination.
 - Pathping - This utility is a combination of Ping and Tracert. Over a period of time, Pathping sends packets to each router on the path to a final destination, and then computes results based on the packets returned from each hop. Pathping shows the degree of packet loss at any given router or link, so you can pinpoint which routers or links might be causing network problems.
 - Nslookup - This utility troubleshoots DNS problems.
 - Netstat - This utility displays protocol statistics and current TCP/IP connections for each network interface in a computer.
 - Nbtstat - This utility displays protocol statistics and current TCP/IP connections that use NetBIOS over TCP/IP (NetBT). It can also be used to verify the NetBIOS name cache.
- **Scripting and programming solutions.** The Windows Scripting Host is a utility available for Windows 2000 that dramatically increases the ability of an administrator to create scripts that can be used to perform monitoring or other administrative tasks. The scripting host enables you to create scripts that are written in Visual Basic Scripting edition or JScript as well as other languages, such as Perl.
- **Windows Management Instrumentation (WMI).** The WMI provides a single point of integration through which you can access status information from many sources within a computer. The WMI is a service that is started by default on Windows 2000-based computers and is also available on Windows 95-and Windows 98-based computers.

Analyzing the Information

In most cases, after you collect the data that you want to use to manage your network, the next item on the agenda is to analyze the data. This can be done in a number of ways depending on the type of data that you are looking at and what you are trying to find in the data. The following are some of the common methods:

- **Manual inspection.** In cases where you manually inspect data, there should be little data and the source of the data and response to conditions should be documented.
- **Spreadsheets.** These can be used when you are looking for fluctuations or for trends.

- **Databases.** As with using spreadsheets, this method is useful if you are looking for trends or if you are seeking an anomaly in a large data sample.
- **Programmed solutions.** In cases where you are looking for a specific type of change in service or you need to ensure that there will be a response regardless of the time that the change in service took place, you can use a programmatic solution. This includes third-party software.

Responding to Issues

After you have analyzed the information, you need to establish a plan to respond to any issues that arise. You can respond in one of two ways:

1. **Reactive response.** When responding reactively to information that you have obtained, you are essentially trying to fix a situation that has already taken place, such as a critical network component
2. **Proactive response.** Proactive response is the correction of a potential problem before it takes place. With proper analysis of logs, you can track the use of network components and determine when a problem might occur.

Designing Network Services for Application Architecture

When you deploy network services across an enterprise, you need to ensure that each service performs a function that supports the application software in use by the enterprise. The application software that an organization chooses to use serves the purpose of enabling the company employees to perform their day-to-day tasks. The network services deployed by the enterprise should serve to support the requirements of each of the applications that are used. This is the main function of the network infrastructure.

Combining Networking Services

By combining multiple networking services on a single computer you simplify the network and use hardware resources more efficiently. You can combine services onto a single system as long as you bear the following points in mind:

- Combining the services must meet the design criteria for security, availability, and performance on the network.
- The computer hardware resources such as RAM, CPU, disk, and network can support the combined services.
- The goal is to reduce the number of computers that must be managed.

There are times when you may combine services for other reasons, such as redundancy or perhaps security or performance. There are several cases where this could be the case, including the following:

- **Security.** When using remote access or a screened subnet, you can isolate the networking services that manage confidential data on a single server.
- **Availability.** By combining services on multiple servers, you can reduce the probability of a failure that results in the loss of the service overall.
- **Performance.** Where two services work closely together, such as the Global Catalog and a Domain Dfs root, you can reduce the network traffic or optimize the computer resources that are underused by combining the services on a single system.

Another method to ensure proper use of resources is to make use of Windows 2000 Clustering services to combine services on a cluster. When installing SQL Server or Exchange, or even for DNS and WINS, you can configure these services to run on a Windows 2000 cluster that will provide load balancing and automatic fail-over.

Designing a Plan for the Interaction of Different Network Services

Windows 2000 network services offer the essential services that provide the basic foundation of the Windows 2000 network infrastructure, but these services do not function completely independently. Several of the basic services found in a Windows 2000 network infrastructure rely on the presence and performance of other services. Planning the implementation of a particular service often involves planning the configuration and implementation of a number of other services.

The resource requirements of the various key Windows 2000 services are outlined in the table below. You should not combine services with high-resource requirements on the same server, but many services with low-resource requirements may be combined, providing memory, processor, network, and disk resources are available.

<i>Networking Service</i>	<i>Processor</i>	<i>Memory</i>	<i>Disk</i>	<i>Network</i>
DHCP	High	Low	High	Low
DHCP Relay Agent	Medium	Low	None	Medium
DNS	Medium	Low	High	Low
WINS	Low	Low	High	Medium
WINS Proxy	Low	Low	None	Low
RRAS as a NAT server	High	High	None	High
Microsoft Proxy Server	High	High	High	High
RRAS as a router	Medium	High	None	High
IAS as a RADIUS server	Medium	High	None	Low
IPSec	High	Low	None	Low
VPN tunneling with encryption	High	Low	None	Low

Designing a Resource Strategy

When developing your implementation and management strategies, you want to examine the resources that will reside in the network infrastructure you have created. After you have enumerated them and have an understanding of the requirements for implementing and managing them, you want to do the following:

Plan for the placement and management of resources. Care should be taken when deciding where to place each of the resources on the network. Network design requires that location consider the bandwidth requirements for each resource and which users will be making use of the resource in question. Then, you need to ensure that the resource is not going to use bandwidth in other parts of the network in order to satisfy user requests. Properly placing the resource in the correct physical location that allows minimal use of bandwidth is the goal.

Plan for growth. One of the most important aspects of an effective network design is scalability. Make sure that your plan takes into account the company's anticipated growth and growth strategy so that your design can scale accordingly.

Plan for decentralized or centralized resources. When you understand the geographical and political organization of a company, you can determine whether network resources will be centralized or. However, placing resources in a physically different location from the centralized management team may be the right choice to minimize network bandwidth utilization, while still allowing a centralized management model. It is not necessary to adopt a decentralized management model when resources are in many locations, nor is it necessary to have a centralized model when resources are in a single location. The physical placement of computers will not change the management style of the organization.

Parnell Aerospace

Parnell Aerospace is a design and manufacturing company that creates guidance systems for aircraft and rockets. The company's manufacturing capability is limited to building and testing prototype components. Parnell Aerospace contracts with other companies to mass produce its products.

Parnell Aerospace is located in two buildings in a large industrial park. The buildings are next door to one other. Building 1 houses offices for the accounting, finance, human resources, research, and sales departments. Building 2 houses the prototype manufacturing floor and offices for the production department and the IT department. The main corporate data center is also located in Building 2, and a small server room is located in Building 1.

Parnell Aerospace employs 275 people. Of these employees, 200 work in Building 1 and 75 work in Building 2.

IT Environment:

Overview:

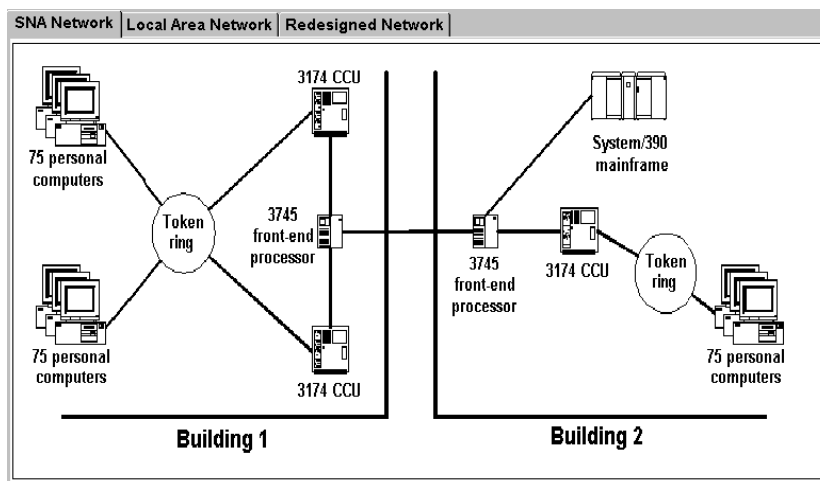
Parnell Aerospace contains mostly IBM mainframe computers. Recently, Parnell Aerospace has started to add Windows based servers and client computers to the IT environment.

SNA Network:

The current SNA environment consists of an IBM System/390 mainframe computer. Several years ago, 3270 terminals were replaced by personal computers running emulation hardware and software. The Parnell Aerospace LAN consists of a token ring network. Each building contains one ring. The two rings are connected a token ring bridge.

The company uses the mainframe for design work and to run simulations to test new designs. The accounting, human resources, and payroll databases are also stored on the mainframe.

Parnell Aerospace SNA network diagram is displayed in the exhibit.



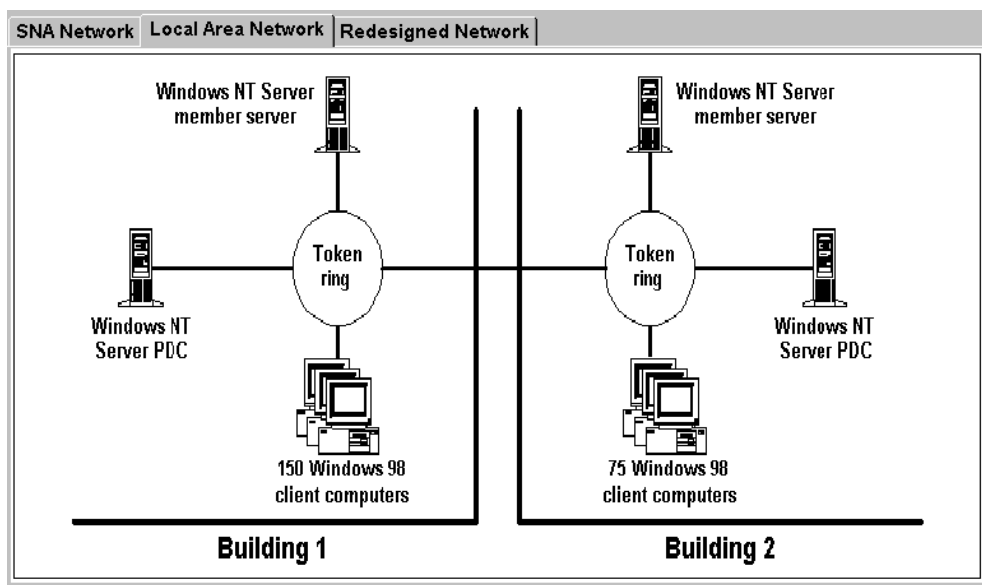
Client/Server LAN Environment:

The LAN environment shares the bridged token rings used by the SNA network. The LAN environment consists a Windows NT 4.0 domain named PARNELLDOM. The primary domain controller (PDC) is located in the Building 2 data center. A backup domain controller (BDC) is located in the Building 1 server room. Two Windows NT Server 4.0 computers function as member servers in the domain. These member servers provide file and print services to client computers, as well as corporate e-mail and database applications. One member server is located in each building. One of these member servers also functions as an internal Web server that hosts product information pages.

All server computers are running NetBEUI as their transport protocol. All client computers are running Microsoft 98. All client computers have NetBEUI and a third-party SNA protocol stack installed.

The Windows NT Server computers each have Pentium II 450-MHz processors, 256 MB of RAM, and 10 GB of hard disk space. The Windows 98 client computers each have Pentium II 266-MHz processors, 64 MB of RAM, and 2 GB of hard disk space.

The Parnell Aerospace LAN diagram is displayed in the exhibit.



Applications:

Four mission-critical design and simulation applications are hosted on the mainframe. These applications be changed, and there are no suitable non-mainframe-based alternatives.

Exchange Server 5.5 is installed on the member server in Building 2 and is used for corporate e-mail. The customer and supplier databases are hosted on Microsoft SQL Server 6.5, which is installed on the member server in Building 1.

Client computers use a third-party terminal emulation application to communicate with the mainframe. Client computers use Microsoft Access 97 to connect to the SQL Server computer through a named pipes connection.

Interviews:

Chief Information Officer (CIO):

This network is very expensive to own and to operate. The vendor service contracts for our mainframe cost us several hundreds of thousands of dollars each year. Although we do not want to lose our investment in our current hardware and software, I want to move to a network environment that reduces our costs significantly but does not impact our business operations.

I want a network that reduces our cost of ownership and improves productivity for our users. Also, I want our partners to be able to access our network for joint projects.

IT Manager:

Even though client/server PC-based networks are gaining in usability and power, some of our tasks require the power that only a mainframe can give us. I want to improve the interoperability between our mainframe and Windows based networks and to minimize cost and the need for additional hardware.

I want a network environment that is completely interoperable between our two different networking topologies. The new environment should be stable, robust, and more efficient to manage.

We want to allow our partner companies to remotely access our network by means of dial-up connections. The partners need tightly controlled access to the mainframe. However, the partners do not need access to the client/server network.

System Administrator:

The network functions well as it is, but we want to improve the manageability and availability of our client/server network.

We also want to reduce the amount of administrative work we have on the IBM hardware, especially the cluster control units (CCUs). In our network, they are prone to failure, which results in expensive downtime.

We want to cut our maintenance overhead, especially for the client/server network. Most of our time is spent managing users, computers, and resources in the Windows NT domain. Client computer configuration should be automatic and fault tolerant.

We also want a more stable and manageable client computer environment. Microsoft Windows 98 is not robust enough for our demands, especially when we have to run two different network protocol stacks on it. We want to reduce the network overhead on the client computers by removing many of the SNA protocol functions from the client computers.

User:

The network seems very slow at times. Sometimes, it takes several minutes to find a resource, such as a file or a printer. Locating servers on the network is also a very slow process, especially during the morning hours.

Envisioned IT Environment:**General Requirements:**

All network services must provide redundancy for fault tolerance. A single protocol must be used in the client/server network. This protocol must be scalable enough to meet any anticipated future growth.

For performance reasons, network traffic must be minimized, especially between Building 1 and Building 2.

The new design must provide the partners with remote access to the network. All partners have client computers that are running either Microsoft Windows 98 or Windows 2000. External partners want to use a Web browser to browse, search, and download product documents that are stored on the mainframe. Because this data is confidential, any remote access traffic must be secure, and only authorized users must be allowed to dial in. The strongest possible encryption must be used for all connections.

No Internet connectivity is required or desired at this time. However, the company management wants to explore this issue later.

Restrictions:

The existing network topology is fixed and cannot be redesigned or replaced. If necessary, however, some SNA network components can be decommissioned if suitable alternative solutions are implemented.

Client Computer access to the mainframe applications and resources must be fault tolerant.

A small budget has been allocated for new equipment. At most, two new servers can be purchased. A small Budget has also been allocated for new software. Enough money has been allocated to upgrade existing operating systems on all computers. Parnell Aerospace owns several server licenses for the entire Microsoft BackOffice suite. The company also owns enough client access licenses so that all client computers can run 311 BackOffice server-based applications simultaneously.

Anticipated Growth:

The company expects its business to grow by as much as 50 percent per year over the next five years. However, the company projects minimal growth in its personnel and no growth in its physical location.

Project Plan:

You propose a phased migration of the existing client/server network to Windows 2000.

Phase I: Upgrade the Windows NT Server domain controller computers to Windows 2000 Advanced Server. The new domain name will be parnellaerospace.com.

Phase II: Upgrade the Windows NT Server member server computers to Windows 2000 Advanced Server. The upgraded computers should function as member servers in the parnellaerospace.com domain.

Phase III: Upgrade the Microsoft Windows 98 client computers to Windows 2000 Professional.

Phase IV: Install Microsoft SNA Server 4.0 on a new member server in each building.

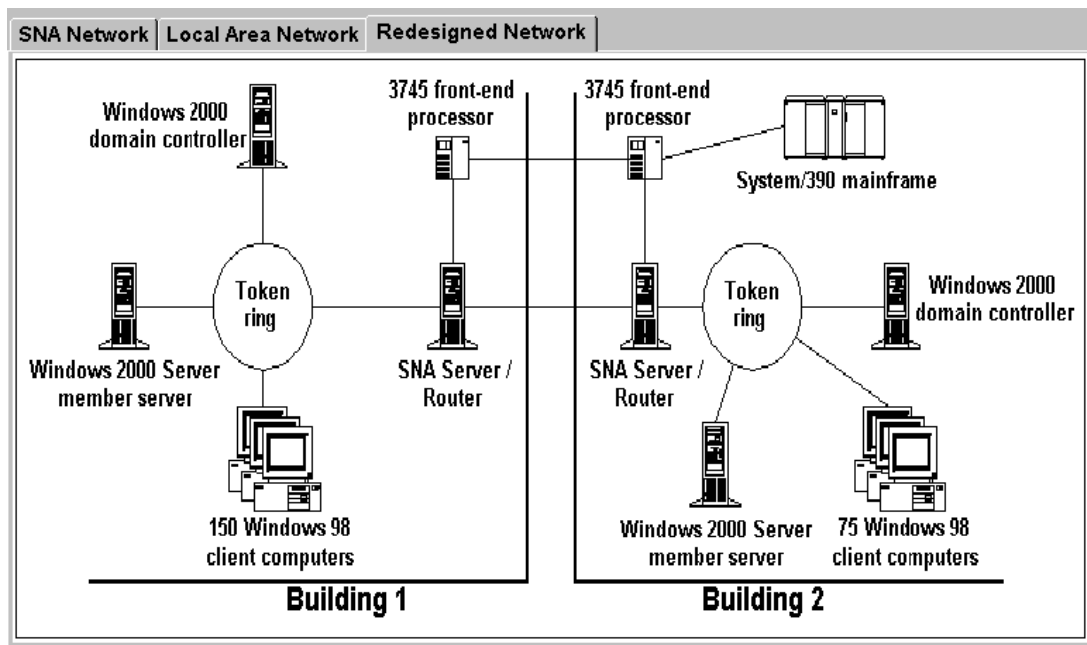
Phase V: Install SNA Client software on the client computers.

Phase VI: Install Routing and Remote Access on the member servers running SNA Server and enable routing between the two buildings.

Phase VII: Implement a parallel test of the existing SNA network infrastructure and the new SNA network infrastructure.

Phase VIII: Decommission the 3174 cluster control units and the token-ring bridge.

The Parnell Aerospace redesigned network diagram is displayed in the exhibit.



Questions

1. You need to design an initial test model for Internet access. No external traffic can be allowed into the network, and administrators need to control which Web sites internal users can gain access to. Which technology should you use?

A: Proxy Server

2. What is the minimum number of IP subnets you will require in your new network design?

A: 3

3. You need to design the DHCP strategy for Parnell Aerospace. What should you do?

A: On each subnet, place a DHCP server that has a scope configured for each subnet in the network.

4. You need to implement a network routing strategy for Parnell Aerospace. What should you do?

A: Implement static routes on all router interfaces.

5. Which factor poses the greatest risk to your Windows 2000 deployment plan?

A: disruption of SNA application access

6. You need to allow external partners dial-in access to resources on the network. What should you do? (Choose all that apply.)

*A: Allow direct dial-in connections that use MS-CHAP for authentication.
Allow direct dial-in connections that use MS-CHAP version 2 for authentication.
Require strong encryption on all connections.*

7. What is the minimum number of DNS servers you should use in the new network?

A: 2

8. Which two factors should you consider in your new network design? (Choose two.)

*A: remote connectivity
interoperability with the existing environment*

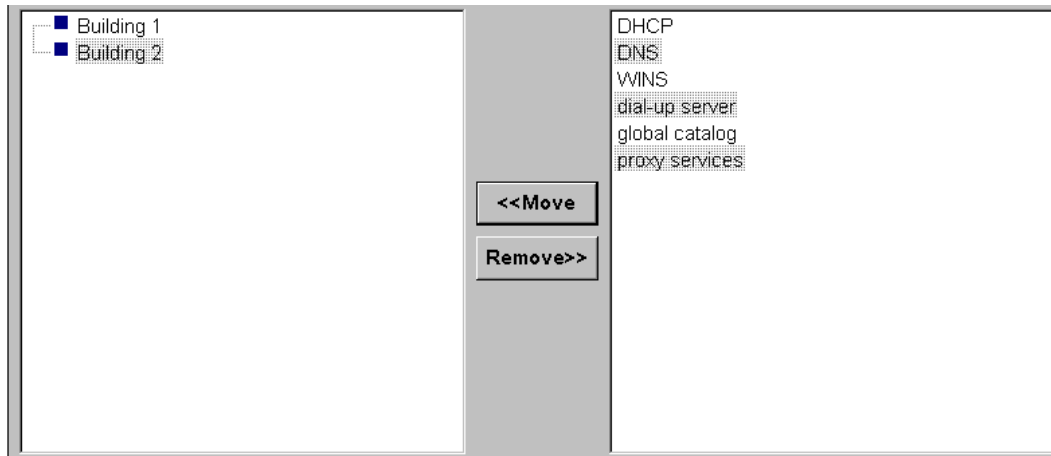
9. What are the two most critical problems in the current network? (Choose two.)

*A: The network is difficult to manage and monitor.
The network is slow.*

10. What is the minimum number of WINS servers you should use in the new network?

A: 1

11. You are designing the initial placement of network services at Parnell Aerospace. Move the appropriate services to the appropriate building location or locations.



A:

<i>Building 1</i>	<i>Building 2</i>
DHCP	DHCP
DNS	DNS
Global Catalog	WINS
	Dial-up Server
	Global Catalog

Blue Sky Airlines

Background:

Blue Sky Airlines serves destinations to four airports: Boston, Massachusetts', Chicago, Illinois; New York City, New York; and Philadelphia, Pennsylvania. The company headquarters is located in Boston three miles from the airport.

Blue Sky Airlines has announced an expansion of its services to four more airports: Atlanta, Georgia; Cincinnati, Ohio; Dallas, Texas; and Washington, D.C.

Organization:

Blue Sky Airlines employs more than 400 personnel. Approximately 220 of these employees work at the Boston headquarters.

Employees in the Boston headquarters are using 486 or Pentium-class client computers that are connected to a single Windows NT 4.0 domain. Company headquarters contains a data center and an IT department.

Blue Sky Airlines currently serves four airports and has approximately 20 employees who work on-site at each airport. At each airport, one of these employees functions as a liaison to the IT department and can perform minor tasks at the direction of the corporate IT personnel. Blue Sky Airlines also employs more than 100 flight personnel.

Existing IT Environment:

Blue Sky Airlines uses a ticketing and reservation application on a mainframe computer that is located in the Boston data center. The airports contain terminals that connect to cluster controllers. Each cluster controller is connected to a front-end processor at the Boston headquarters by means of a 56-Kbps point-to-point circuit that is running SNA protocol.

Envisioned IT Environment:

Airports:

All airports will have a ticket counter and five gates. The following equipment will be dynamically assigned a TCP/IP address and will be located in each airport:

- 10 ticket counter machines
- 10 gate counter machines
- 10 ticket printers

At any given time, no more than five users at each airport will be using the ticketing and reservation application.

The airports in Atlanta, Boston, Chicago, and Washington, D.C., will contain a passenger

lounge. A maximum of 113 ticketed passengers can connect their portable computers to the passenger lounge LAN and gain access to the Internet through the Boston headquarters. All passenger lounges will be part of a single, bridged VLAN named Red.

Passengers will be able to use all TCP/IP protocols without having to make any changes to their portable computers as long as the computers are using DHCP. Additionally, each passenger lounge will contain one kiosk computer so that passengers without portable computers can access the same Web-based flight information and reservation application that Internet users can access.

WAN Connectivity:

Blue Sky Airlines wants to migrate from the existing 56-Kbps point-to-point SNA circuits to a frame relay network that will connect all airports to the Boston headquarters.

At each airport containing a passenger lounge, Blue Sky Airlines will install a BOOTP-capable router that is configured with four interfaces: two Ethernet interfaces, one ISDN interface, and one interface that connects to the frame relay network. Company employees will connect to the corporate WAN by means of Ethernet interface 1. Customers in the passenger lounges will connect to the Internet by means of Ethernet interface 2. All devices on the network that are connected to Ethernet interface 2 will be assigned to VLAN Red.

Blue Sky Airlines will install a BOOTP-capable router that is configured with five interfaces in the Boston headquarters. This router will have three Ethernet interfaces, one Primary Rate Interface (PRI), and one interface that connects to the frame relay network. Ethernet interface 1 will connect to the corporate LAN and will have a network address of 10.1.0.0/16. Ethernet interface 2 will connect to a hub and all devices on this LAN will be assigned to VLAN Red. This network will have a network address of 192.168.1.0/24. Ethernet interface 3 will be connected to a firewall for access to the Internet. All private corporate resources will be assigned addresses in the 10.0.0.0 address space. Routers will not allow any traffic to pass between the two LANs at corporate headquarters.

A diagram of the envisioned company network is displayed below.

Applications and Services:

Blue Sky Airlines wants to migrate from the existing mainframe ticketing and reservation application to a new two-tier application. The user interface will only run on Windows 2000 and will connect to a SQL database. This SQL database must provide high availability and performance. The company also wants to develop two Web applications that will use the information in this SQL database. The first Web application will enable the public to make reservations, purchase tickets, and confirm flight information. The second Web application will enable only flight personnel to check and exchange their scheduled flights.

To support these new applications, two servers running Microsoft SQL Server, two servers running Terminal Services, and two servers running Internet Information Services (IIS) will be deployed in Boston. All pilots will be issued portable computers running Windows 2000 and configured with smart card readers. Pilots will need access to a confidential section of the

intranet Web server. Only the pilots will need strong encryption to access this section of the Web server.

Bandwidth Requirements:

Blue Sky Airlines has done some testing of the new ticketing and reservation application and estimates the following bandwidth requirements:

- Client application to Microsoft SQL Server: 30 Kbps
- Terminal session running the client application: 10 Kbps
- Client application to a ticket printer: 15 Kbps

Blue Sky Airlines wants to provide enough bandwidth in the passenger lounges so that while one user is using 128.Kbps streaming video, all other users still have 56 Kbps of shared bandwidth to browse the Internet. The connection from the Boston headquarters to the frame relay network should be 75 percent of the total minimum required bandwidth for all other company locations.

Interviews:**Chief Information Officer (CIO):**

The existing mainframe-based ticketing and reservation application makes the IT environment in the airports simple and easy to maintain. The complexity of the airport environments must remain as low as possible.

I want to keep our existing centralized IT model in place. For this reason, as many services as possible should be located in the Boston headquarters. If possible, we need to standardize the equipment in each airport so that even an untrained IT liaison will be able to replace the client devices with minimal configuration.

We also need to give our flight personnel the ability to view and modify their flight schedules from their homes or from portable computers in their hotel rooms.

Network Administrator:

Users at the Boston headquarters have multiple drives mapped to several shared folders. Because drives are mapped inconsistently, it is extremely difficult for users to find and browse information. We want to restructure how users find information and prevent them from being able to view the existing shared folders in Network Neighborhood. We want all users to be able to connect to a single shared folder by means of the path `\\domain\public`.

Project Manager:

I have created the following project plan for the testing of and migration to the new ticketing and reservation application.

Phase I: Complete proof of concept for reservation application migration.

1. Deploy Windows 2000 on client computers in the Boston headquarters.
2. Deploy Terminal Services.

3. Install the emulator application.
4. Make a copy of the existing mainframe database and import the copy into the new SQL database.
5. Test applications.

Acceptance criteria: From a Terminal session, users will be able to use the existing mainframe application and will be able to run the new two-tier application client and access the SQL database.

Phase II: Implement Windows 2880 infrastructure for the Boston headquarters.

- Upgrade the servers in the existing Windows NT 4.0 domain to Windows 2000.

Acceptance criteria: Existing and enhanced functionality will be demonstrated by using Windows 2000 on the client computers and servers in the Boston headquarters.

Phase III: Implement a test deployment in the Washington, D.C., airport.

1. Provide WAN connectivity to Washington, D.C.
2. Test the old reservation application and the new reservation application.
3. Test the new Windows 2000 infrastructure from the Washington, D.C., location.
4. Collect benchmark data.
5. Install and test passenger lounge functionality.
6. Test the kiosk computer.

Acceptance criteria: All aspects of the new reservation application and the new airport infrastructure will be installed and tested in the company's new Washington, D.C., location.

Phase IV: Deploy new equipment to all airports.

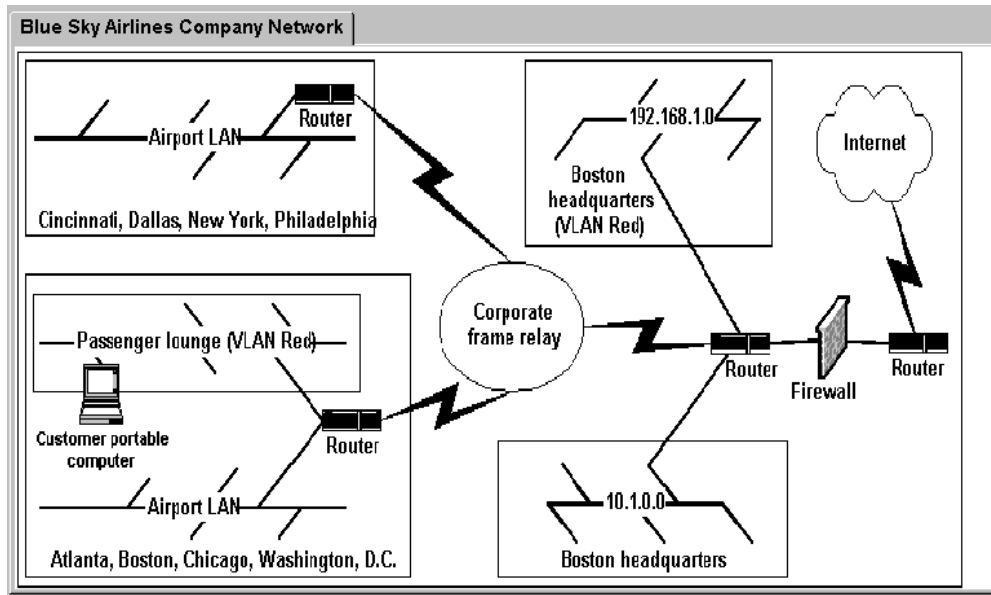
1. Provide WAN connectivity to all airports.
2. Install LAN infrastructure.
3. Train users.
4. Replace existing equipment in all airports.

Acceptance criteria: All airports will be running the old mainframe reservation application on the new equipment.

Phase V: Migrate to the new reservation application.

1. Migrate data from the mainframe to Microsoft SQL Server.
2. Convert all airports.
3. Open new airports.

Acceptance criteria: Reservation data will be migrated from the mainframe and put into production with the new reservation application.



Questions

1. You need to meet the technical requirements for the new ticketing and reservation application. What should you do?

A: Load balance the Internet Information Services (IIS) servers. Cluster the Microsoft SQL Server computers. Load balance the Terminal servers.

2. You need to allow the pilots access to the intranet Web server. What should you do? (Choose all that apply.)

*A: Deploy Certificate Services.
Use remote access policies.
Deploy Active Directory.*

3. Which five components should be deployed or installed during Phase I? (There are 10 answer choices. Choose 5)

*A: Terminal Services
Microsoft SNA Server
TCP/IP
3270 emulation software
Microsoft SQL Server*

4. Which component or components must you place locally on the passenger lounge network? (Choose all that apply.)

A: *kiosk computer*
hub

5. Which component or components will you need in Washington, D.C., to complete Phase III? (Choose all that apply.)

A: *hub*
client hardware
router

6. Which strategy or strategies should you use for the DHCP design at the airports? (Choose all that apply.)

A: *In the 192.168.1.0 network in Boston, deploy one DHCP server that has one scope.*
In the 10.1.0.0 network in Boston, deploy two DHCP servers.
Configure each server so that it has eight scopes.
Configure an exclusion for 50 percent of the addresses in each scope.

7. Which client hardware should you use for the gate machines in the airports?

A: *Windows Terminal*

8. You need to design a strategy so that flight personnel can connect to the scheduling application. What should you do?

A: *Deploy a VPN server in the DMZ and an Internet Information Services (IIS) server on the corporate LAN in headquarters.*

9. How should you design the Microsoft SQL Server environment?

A: *Use two clustered SQL Server computers*

10. Which subnet mask should you assign to the Dallas airport?

A: *255.255.255.0*

Hanson Brothers

Background:

Hanson Brothers is an international consulting firm that is based in Portland, Oregon. Hanson Brothers specializes in consulting services for U.S. companies that want to establish business operations in foreign countries.

Hanson Brothers assists companies by analyzing the factors that influence their expansion into new geographical regions. Hanson Brothers also arranges for these companies to meet with the government agencies that control the establishment of manufacturing facilities in their countries. In recent years, Hanson Brothers has expanded its business by offering its customers additional services such as housing procurement, recruiting, and legal services.

Organization:

Hanson Brothers has 2,500 employees in 20 countries. The Hanson Brothers corporate headquarters is located in Portland, Oregon. Five regional headquarters oversee district offices.

The Portland office operates as the Hanson Brothers corporate headquarters and as the North America regional headquarters. The North America region includes eight district offices:

- Atlanta, Georgia
- Chicago, Illinois
- Cincinnati, Ohio
- Denver, Colorado
- Los Angeles, California
- Montreal, Canada
- New York City, New York
- Washington, D.C.

The Asia regional headquarters is located in Victoria, Hong Kong. The Asia region includes four district offices:

- Bangkok, Thailand
- Calcutta, India
- Hanoi, Vietnam
- Shanghai, China

The South Pacific regional headquarters is located in Sydney, Australia. The South Pacific region includes three district offices:

- Auckland, New Zealand
- Manila, Philippines
- Singapore City, Singapore

The Europe regional headquarters is located in London, England. The Europe region includes three district offices:

- Brussels, Belgium
- Geneva, Switzerland
- Madrid, Spain

The Latin America regional headquarters is located in Buenos Aires, Argentina. The Latin America region includes four district offices:

- Bogota, Colombia
- Caracas, Venezuela
- Mexico City, Mexico
- Sao Paulo, Brazil

Existing IT Environment:

Each North America office is connected to a frame relay network by means of a 56-Kbps circuit. A permanent virtual circuit (PVC) exists from each North America district office to the Portland office. A 128-Kbps leased line connects the Portland office to each regional headquarters. Each regional headquarters outside the United States connects to its district offices by means of a 256-Kbps leased line. The Portland office is connected to the Internet by means of a T1 line to an Internet service provider (ISP).

Routers and DSU/CSUs are installed at all company locations. Routers contain hardware from a variety of manufacturers. All routers are BOOTP enabled.

Hanson Brothers has the following client computers evenly distributed throughout its organization:

- 1,000 Pentium II computers that are running Windows NT 4.0
- 1,500 Pentium I computers that are running Microsoft Windows 95

One primary domain controller, one backup domain controller, and five file and print servers are located in the Portland office. The Portland office also contains two proxy servers, configured as an array, that provide Web-cache services and Internet access control. A few locations throughout the company contain servers that provide NT 4.0 DHCP services.

A single Windows NT domain exists for e-mail authentication and for Internet access control on the proxy array. Client computers throughout the company log on to the domain only when they need to access these services.

Interviews:

Chief Executive Officer (CEO):

In the past four years, we have undergone rapid growth. For example, we have opened many new offices in n locations, and the number of employees in our company has tripled.

Chief Information Officer (CIO):

Our corporate philosophy favors the centralized control of most business processes. However, this philosophy is being strained by the company's rapid growth and expansion. We want to decentralize the administration of the network by creating three categories of administrator teams: Enterprise, Regional, and Site.

The Portland office will contain an Enterprise, a Regional, and a Site administrator team. Each regional headquarters office will contain both a Regional and a Site administrator team. Each district office will contain only a Site administrator team.

Hanson Brothers has a limited Internet presence, Internet resources play an important role in the research our company performs for its customers. Although our foreign offices have been reporting slow Internet performance, employees at the Portland office report that Internet performance is more than acceptable.

In our company, we want to deploy several important Web-based applications. This deployment requires the creation of internal Web services. All intranet Web servers will be located at the Portland office. One of these Web-based applications consolidates all human resources files into a single location that users can view through browsers. These files are created and updated regularly by the human resources directors in each regional headquarters. These directors will need local access to their files, and the intranet server will need local access to the human resources files created and updated in these locations.

Because the links to the regional headquarters outside the United States are very expensive, the bandwidth must be used very wisely. We want to minimize increases in costs for WAN connectivity wherever possible.

We want to immediately upgrade all Windows NT 4.0 client computers to Windows 2000 Professional. We will want to immediately upgrade all Windows NT 4.0 client computers to Windows 2000 Professional. We will upgrade the existing Microsoft Windows 95 client computers. We will replace them over the next two years with new computers running Windows 2000 Professional.

Security Manager:

Currently, the Portland office has an Internet connection that is secured with a firewall. The firewall is running address translation (NAT). My security team is located in the Portland office, and all extranet connections will be located in this office.

Active Directory Design Team Leader:

For our Active Directory design, we will use a model containing a single forest with a single tree

that has multiple domains. Each domain will contain one regional headquarters and all of its district offices. The domains will use the following names:

- Asia
- Europe
- LAmerica
- NAmerica
- SPacific

The new parent domain named Corp will also be created to hold the Enterprise administrator team accounts and the forest-level accounts.

We will use Active Directory namespaces that are contiguous with the existing registered domain name. All DHCP servers will reside on member servers, and the DNS zones should be configured to run in a multi-master mode. The security team will configure the firewall so that no Active Directory DNS server will have access to the Internet. Each regional headquarters will contain a domain controller that is configured as a replication bridgehead server. Each Regional administrator team will manage all DHCP servers in its region regardless of servers' physical location.

Network Administrator:

Currently, all routers are configured by using static routes. However, as our company expands, static routing is becoming increasingly inefficient.

We had a lot of downtime with the old system, and redundancy is extremely important to us.

We have several applications that all offices within a region use. We want to give the regional administrators the ability to manage these installation packages. An administrator also needs the ability to publish these applications so that they can be installed the first time they are used. Although some of the installation packages are large, we want the quickest installation possible. Almost all users will require access to the Internet so that they can browse the Web. However, only a few users will need access to FTP. The users in a region visit many of the same company and government Web sites as other users in their region.

Hanson Brothers has a registered DNS namespace of hansonbrothers.com. This namespace is held by a UNIX server in the corporate office that is running BIND version 4.8.3. This server will not be upgraded.

All client computers in the company must register with DNS. Client computers will access other client computers to share printers. All administrator client computers will run Windows 2000. All servers will run Windows 2000.

Questions

1. Which change should you make to the existing WAN for the North America region before implementing the new network?

A: Increase the circuit bandwidth at the Portland office.

2. What should you do to improve Internet connectivity for Hanson Brothers?

A: Place a proxy server in each regional headquarters outside the United States.

3. Hanson Brothers needs to accommodate the Human Resources intranet application in the new network. What should you do?

*A: In the Portland office, deploy a Distributed file system (Dfs) root server that has a child node for each region.
In each regional headquarters, deploy a Dfs replica server that corresponds to the child node for that region.*

4. You need to provide Hanson Brothers with a highly available DNS design. What should you do?

*A: Create a primary DNS zone in each domain.
Create secondary DNS zones for the Corp zone on the DNS servers in the Asia, Europe, LAmerica, NAmERIC and SPacific domains.*

5. You need to provide a secure DHCP design that will minimize the risk of unauthorized DHCP servers appearing on the network. What should you do? (Choose all that apply.)

*A: Place all members of the Regional administrator team into the DHCP Administrators group.
Replace all Windows NT 4.0 DHCP servers with Windows 2000 DHCP servers.*

6. How should you design the name registration strategy for Hanson Brothers? (Choose all that apply.)

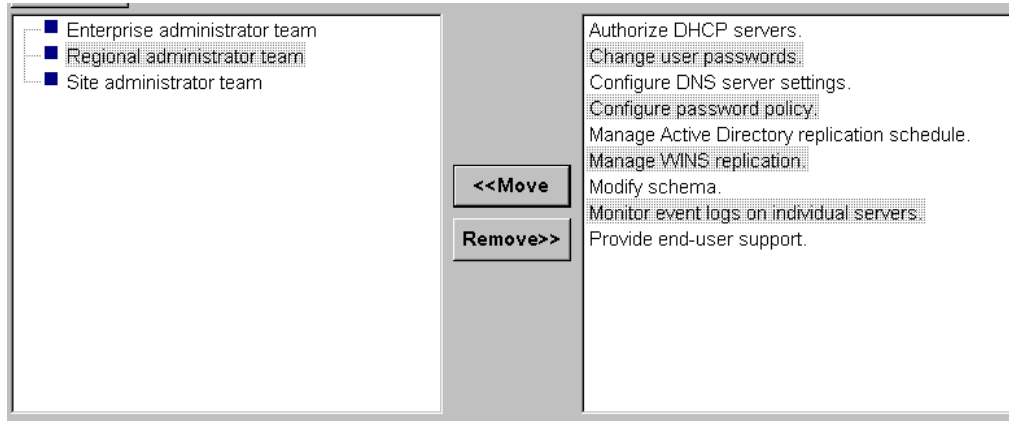
*A: Configure all servers to register with DNS and WINS.
Configure DHCP servers to register the A (host) records for non-Windows 2000 client computers with DNS.
Configure all client computers to register with WINS.*

7. How should you implement DHCP for the district offices in the Europe region?

*A: In each district office, deploy a DHCP server that has one scope for the local subnet with 20 percent of the addresses excluded.
In the regional headquarters, deploy a DHCP server that has one scope for each district office with 80 percent of the addresses excluded.*

8. You need to assign management and monitoring tasks to the administrator teams. Move each task to the administrator team that should perform it. (Use all task. Use tasks

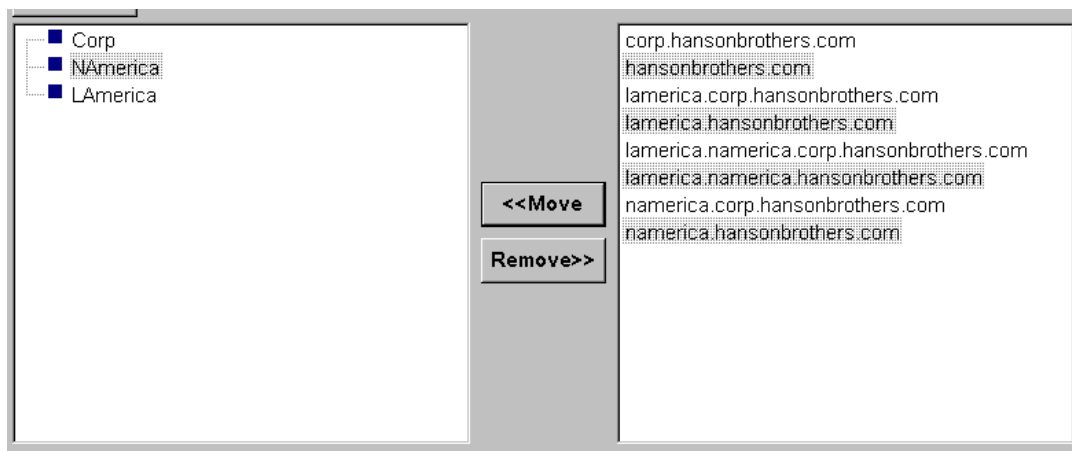
only once.)



A:

Enterprise Team	Regional Team	Site Team
Configure password policy	Configure DNS server settings	Authorize DHCP servers
Manage AD replication sched.	Manage WINS replication	Change User Passwords
Modify schema	Monitor event logs on servers	Provide end-user support

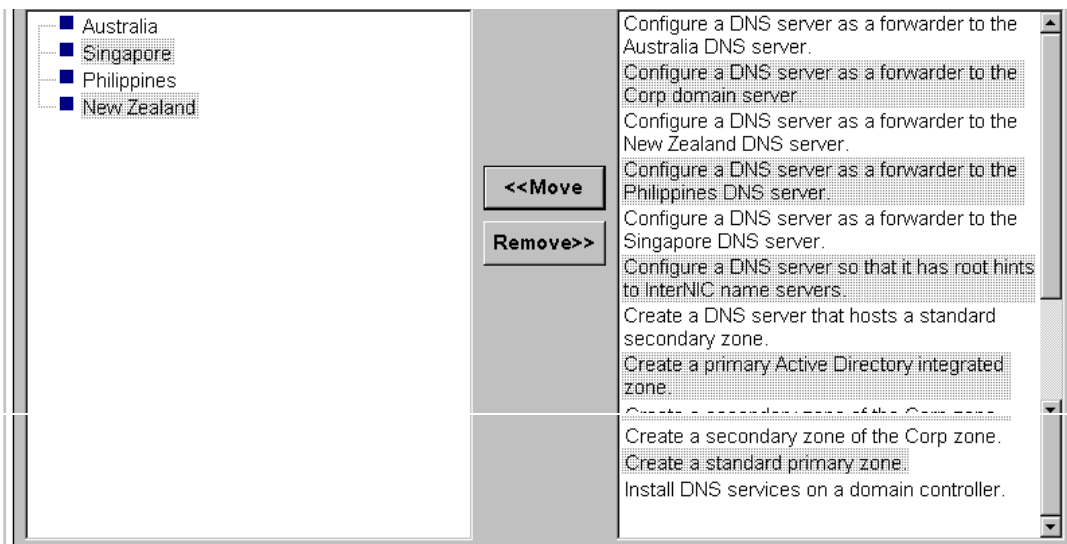
9. You need to create the DNS namespace design. Move the appropriate DNS namespaces to the appropriate company domains (Use only namespaces that apply. Use namespaces only once.)



A:

Corp	NAmerica	LAmerica
corp.hansonrothers.com	Namerica.corp.hansonbrothers.com	Lamerica.corp.hansonbrothers.com

10. You need to create the DNS deployment strategy for the SPacific domain. Move the appropriate deployment tasks to the location or locations where the tasks will be performed. (Use only deployment tasks that apply. You might need to reuse deployment tasks.)



A:

Australia	Singapore	Philippines	New Zealand
Create a standard primary zone	Configure a DNS server as a forwarder to the Australia DNS server	Configure a DNS server as a forwarder to the Australia DNS server	Configure a DNS server as a forwarder to the Australia DNS server
Create a DNS server that hosts a standard secondary zone			
Create a secondary zone of the Corp zone			

Municipal Hospital

Background:

Municipal Hospital provides medical services for the community. Its facilities include the central hospital building, an outpatient clinic, and two satellite medical centers. The central hospital building contains 300 patient rooms, 60 offices, 45 examination rooms, and 10 operating theaters. The central hospital building contains 3,500 employees. Of these employees, 2,000 require access to resources located on hospital computers. The outpatient clinic is located approximately 50 meters away from the central hospital building. The outpatient clinic contains 250 employees. The two satellite medical centers are located in outlying suburban areas. Each satellite medical center employs 350 people.

Municipal Hospital is also associated with a medical office building. The office building is located approximately one mile away from the central hospital building. The office building houses 300 additional people.

IT Environment:

Central Hospital Building:

The central hospital building contains a 4-Mbps token ring network. The network contains a single ring that consists of multiple interconnected hubs. Servers and token ring hubs are contained in a server room in the basement of the central hospital building. The network uses IBM LAN Server as its network operating system and OS/2 Warp as its client operating system. The network contains 100 client computers that provide user access to network resources. Approximately 20 people share each client computer.

Outpatient Clinic:

The outpatient clinic has a small 10-Mbps Ethernet LAN that is not connected to the hospital network. The LAN Windows NT Server 3.51 as its network operating system and Windows NT Workstation 3.51 as its client operating system. The LAN contains 100 client computers that provide user access to resources. Approximately 150 of the employees at the facility share these client computers.

Medical Office Building:

Because it consists of many affiliated but independent physicians' offices, the medical office building does not have a single network infrastructure. Several offices have small networks, but these networks do not connect each other or with the central hospital network. Other offices have one or more stand-alone computers. The computers in the office building are running either Windows NT Workstation 4.0 or Microsoft Windows 98.

Satellite Medical Centers:

Each satellite medical center has a 10-Mbps Ethernet LAN that is not connected to the hospital network. These LANs use Windows NT Server 3.51 as the network operating system and Windows NT Workstation 3.51 as the client operating system. Each medical center contains 75 client computers. Approximately 200 of the employees at each medical center share the client

computers.

Interviews:

Chief Information Officer (CIO):

Our IT environment is unmanageable. We are using outdated technology in the central hospital, and we have no communication between facilities. Our existing equipment and software cannot provide the services that our patients and vendors want. We spend too much money maintaining our network, especially in training our IT personnel to service these outdated systems.

I want a network that reduces our cost of ownership, while improving productivity for all users. Municipal Hospital wants to ensure that patient information, such as scanned x-rays, can be easily shared between our facilities and by our affiliated physicians in real time. We want to explore technologies that would allow patients to access their medical records over the Web. I also want to provide facilities where our patients could access medical libraries and communicate with their physicians over the Internet.

We have allocated funding to completely replace the network infrastructure and to provide links between all hospital buildings. Our budget also includes enough funds to replace all servers and client computers.

Municipal Hospital wants to place a computer terminal in each patient room, examination room, and operating theater, so patient information will always be available and can be updated immediately by hospital staff.

IT Manager:

Our network is hopelessly obsolete and is operating very close to capacity. My department personnel spend so much time implementing fixes and patches on our operating systems, they cannot respond to the needs of our users and patients. We need a flexible, scalable physical network infrastructure that has enough bandwidth to handle expected growth and traffic in our network. We also need complete reliability in our network operating system.

I want a single network for all of our facilities: the central hospital building, the outpatient clinic, and the satellite medical centers. We need a single network topology that can grow with our company, and a single operating system platform that will provide easy access to resources for all users.

We want to establish an Internet presence so we can serve our patients and staff more effectively, but we need control who has access to the network and to secure patient records and other sensitive information from unauthorized access.

We want to allow affiliated physicians at the medical office building to access our network resources. Because do not control the office building or its network infrastructure, we need to design an access solution that will function regardless of the operating systems the physicians have in their offices. However, we will not provide for or allow access to our network by means of direct dial-up connections.

Network Administrator:

We need a network that serves the needs of our entire user community. The network needs to be reliable, interoperable, and manageable. Client computer configuration on the network should be automatic and fault tolerant. All network services must be completely fault tolerant and available at all times.

For performance reasons, we need to limit the number of computers on any single subnet to 200.

We also want to provide Internet connectivity for our user community, so that physicians and staff can access medical databases and other resources. We need to be able to control this access to ensure proper usage, to maintain security on our internal network, and to minimize the amount of outbound Internet traffic on the WAN links.

Envisioned IT Environment:**General Requirements:**

The new network design must consider all aspects of client/server networking, including name resolution, resource sharing, and application support.

A single protocol should be used in the client/server network. This protocol must be scalable enough to meet anticipated growth.

In the future, the IT staff will need to connect to the network from external locations for remote administration purposes. These IT personnel will be using Windows 2000 exclusively.

The new network design must provide for secure outbound Internet connectivity for internal users.

Anticipated Growth:

Within a year, hospital management expects to begin construction on a new wing of the central hospital building. This addition will contain 100 additional patient rooms, 20 additional offices, 15 additional examination rooms, and a new emergency room with a trauma center. The construction will take approximately one year.

Proposed Design:

Your proposed design for the new Municipal Hospital network includes the following components:

- LAN environment: The existing LAN topologies in all facilities will be upgraded to 100-Mbps Ethernet.
- WAN environment: The central hospital and the satellite offices will be connected by means of dedicated and private T1 lines.
- Internet connectivity: The central hospital will connect to the Internet by means of a T1 line. All Internet traffic will be routed through the central hospital.
- Operating system: All server operating systems will be upgraded to Windows 2000 Advanced Server, and all client operating systems will be upgraded to Windows 2000

Professional.

- Logical network: A single Windows 2000 domain will be used.
- Applications: Microsoft Systems Management Server (SMS) :2.0 will be used for all network management and desktop support. Microsoft SQL Server 7.0 will be used for all company databases, such as patient information and human resources.

Questions

1. What are the two most critical problems in the current network? (Choose two.)

*A: The network requires upgrading.
The network is difficult to manage and monitor.*

2. Which factor or factors should you consider in your network design? (Choose all that apply.)

*A: Internet connectivity
new network topology
remote connectivity*

3. You are designing a TCP/IP solution for this network. You are using a private Class B address. Which subnet mask should you use to meet current and projected growth requirements?

A: 255.255.255.0

4. You need to allow the IT personnel to access the network while maintaining the requirements for security and authorization. What should you do? (Choose all that apply.)

*A: Allow VPN connections that use L2TP to secure communications.
Require strong encryption on all connections.*

5. You are designing an Internet access solution for the internal users. Which technology should you use?

A: proxy server array

6. What is the minimum number of internal IP subnets you should use in your design?

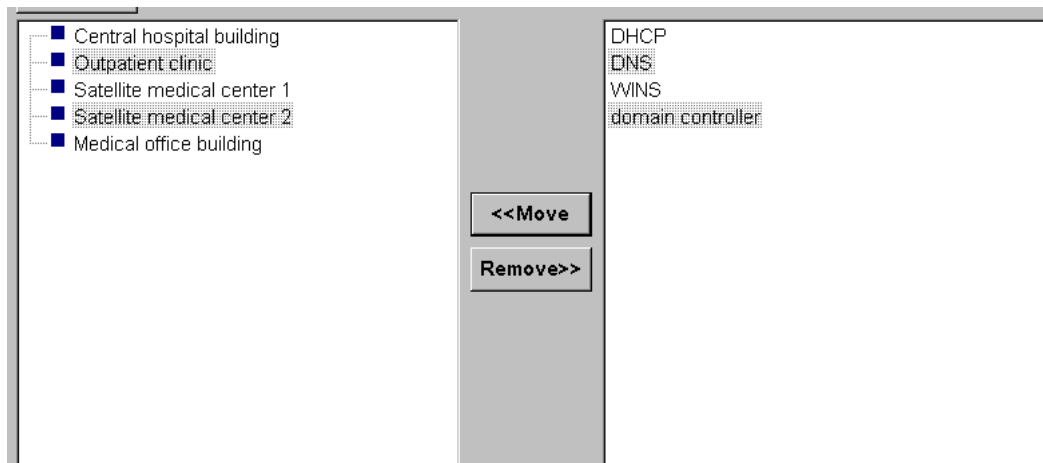
A: 6

7. How many WINS Servers should you use in your sign?

A: 2

8. You are designing the placement of network services. Move each network service to

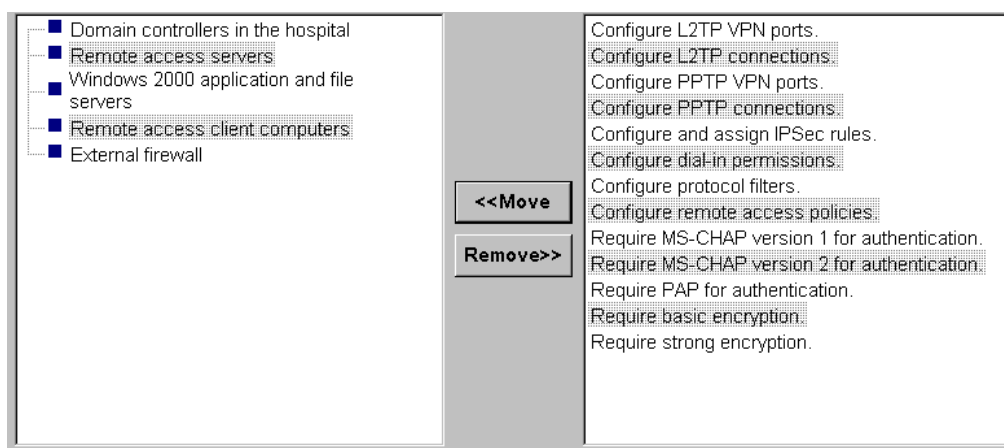
the appropriate location or locations. (Use all network services. You might need to reuse some network services.)



A:

Central hospital	DHCP	DNS	WINS	domain controller
Outpatient clinic	domain controller			
Satellite medical 1	domain controller			
Satellite medical 2	domain controller			
Medical office	domain controller			

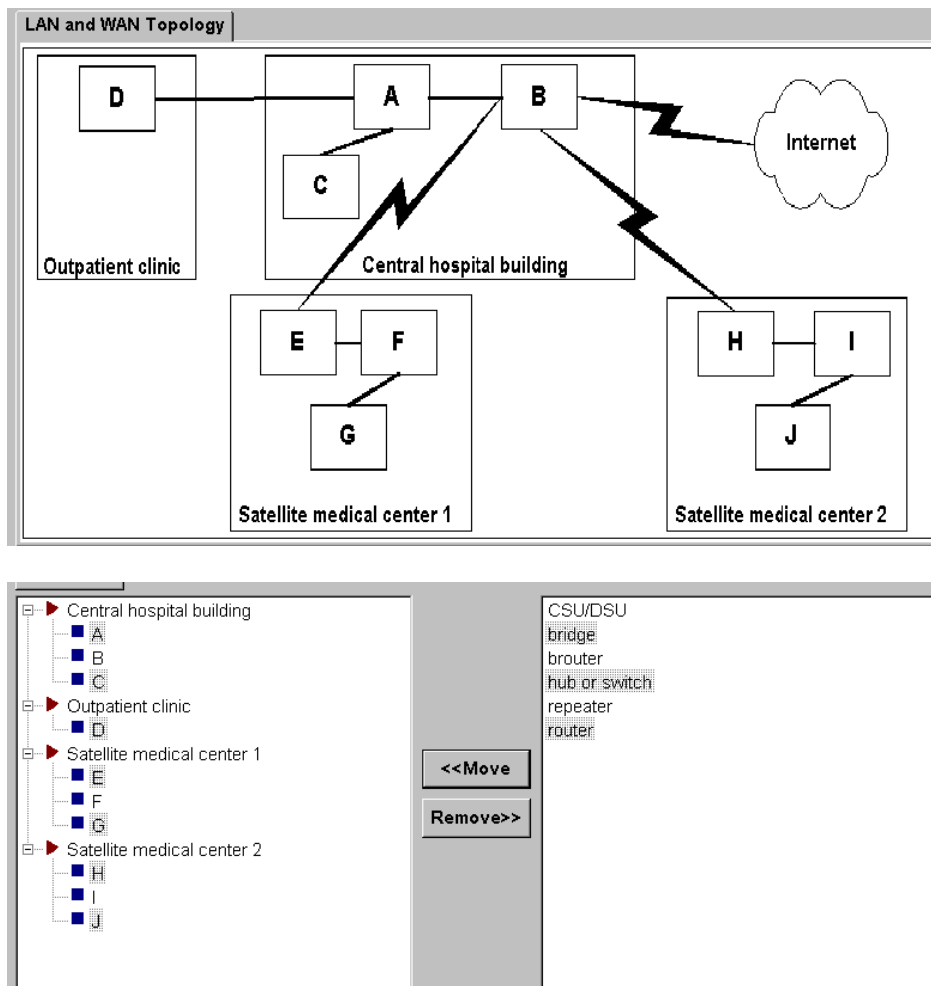
9. You are designing a remote access solution for physicians in the medical office building. You need to decide which remote access technologies should be configured. Move the appropriate remote access tasks to the appropriate component or components. (Use only tasks that apply. You might need to reuse some tasks.)



A:

DCs in hosp.	configure dial-in permissions		
Remote access servers	configure L2TP VPN ports	configure remote access policies	require basic encryption
W2K app & file servers	N/A		
Remote access clients	configure L2TP connections		
External firewall	N/A		

10. You are designing the LAN and WAN topology for Municipal Hospital. You need to identify which components are represented. Check the Exhibit below, and then move an appropriate network component to each letter in the Network Topology list. (Use only network components that apply. You might need to reuse network components.)



A: BEH = router
ACDFGIJ = hub or switch

State University

State University offers undergraduate, graduate, and professional degrees in Arts, Business, Engineering, Humanities, Law, and Sciences. The student body contains 10,000 students; 6,000 students are enrolled in undergraduate programs, and 4,000 students are enrolled in graduate and professional programs. State has 2,0130 faculty members and 12,000 administrative staff members. Its offices, classrooms, and dorms are located in 90 campus buildings.

Organization:

Administration:

State University has many administrative departments. Support personnel in each department and school maintain and support client computers, applications, and department servers. The computing services department administers the network infrastructure and shared applications for State University. The computing services department is located in its own building.

Before the computing services department was created, the schools of Business, Engineering, and Law hired network personnel and implemented their own networks. For political reasons, these schools continue to operate with their own network personnel and implemented their own networks. For political reasons, these schools continue to operate more or less independently, although they must follow the guidelines set by the computing services department. This department has final authority over the network.

Schools:

State University has the following schools:

- School of Arts
- School of Business
- School of Engineering
- School of Humanities
- School of Law
- School of Sciences

Most schools contain more than one department. Each department has its own offices and labs and operates independently from other departments in the same school.

Some departments also have one or more research labs. Research labs consist of faculty members and graduate students. Some research labs form partnerships with research sponsors and with research labs at other colleges and universities.

All the departments within a school are typically housed in the same building. However, in large schools, such as , Engineering, and Sciences, some departments occupy different buildings.

Student Housing:

State University contains 25 dorms. Approximately 5,000 undergraduate students and 500 graduate and professional students live in on-campus dorms. The rest of the students live off campus.

IT Environment:**Physical Network:**

The physical network is maintained by the computing services department. A 100-Mbps fiber-optic backbone runs through the campus. Each building has a wiring closet that contains a single router with multiple interfaces. A fiber-optic cable connects the backbone to one router interface in each building. All the routers in State University support BOOTP.

Dial-up services are supported for client computers running Microsoft Windows 95 or Windows 98, Windows NT, and Mac OS 7.5.5 or later.

Many research labs have FTP sites and Web sites to exchange data with their sponsors and research partners. Some research labs even allow their sponsors and partners to run applications on servers in the research labs by using Telnet sessions.

Computers:

All faculty members and administrative personnel have computers. Most of these client computers are running Microsoft Windows 95, Windows 98, or Windows NT 4.0. However, many client computers on the network are running Mac OS 7.5.5. The School of Engineering and the School of Sciences also have many computers that are running UNIX.

All schools have created student computer labs to provide students with shared computers and printers they can use. The computers in these labs are running Windows 95, Windows 98, Windows NT, or Mac OS 7.5.5.

Students, faculty, and staff within a department usually access computers and printers in the same department. Many departments report unnecessary network traffic from other departments.

Inside each building, network cables connect the wiring closet to individual rooms through a network of hubs, routers, and patch panels. The network supports only Ethernet network adapter cards.

State University uses dual-homed servers to host its main Web site and to provide e-mail and Usenet News services.

WAN Connectivity:

State University provides dial-up services to its faculty, students, and staff and allows them Internet access dial-up connections.

State University has a bank of 512 modems that all operate at 56.6 Kbps. Half of these modems are dedicated to student access. To gain access to these modems, students can dial one of two numbers: 555-0101 or 555-0202. The first number allows students to connect for a maximum of one hour. The second number allows them to connect for maximum of two hours. The remaining modems are shared by students, faculty, and staff. To gain access to these modems, users dial 555-0303. Connections that use this number last a maximum of three hours.

State University has the Internet domain name stateuniversity.edu and uses an internal network address of 172.19.0.0. Most of the computers on the network use statically assigned IP addresses. The DNS servers do not support SRV records.

Security:

The use of Telnet, FTP sites, and Web sites by research groups and their sponsors and partners has exposed the State University network to many security risks. To allow the open exchange of ideas between research labs and their sponsors and partners, the current firewall configuration is very weak.

Campus Buildings:

Building 23 has eight floors. The floors are occupied as follows:

- Floor 1: Administrative offices (School of Engineering)
- Floors 2 and 3: Department of Chemistry (School of Sciences)
- Floors 4, 7, and 8: Department of Physics (School of Sciences)
- Floors 5 and 6: Department of Civil Engineering (School of Engineering)

Building 25 has 10 floors. The floors are occupied as follows:

- Floor 1: Administrative offices (School of Sciences) containing 40 computers
- Floors 2 and 3: Department of Biology (School of Sciences) containing 4813 computers
- Floors 4, 7, and 8: Department of Mathematics (School of Sciences) containing 650 computers
- Floors 5, 6, 9, and 11: Department of Computer Science and Engineering (School of Engineering) containing 1,21313 computers

Building 34 houses the Registrar's offices and 3513 computers. Building 56 has 2130 computers on a single IP subnet that has a network address of 172.19.23.13. Building 67 has 4130 computers on two IP subnets that have network addresses of 172.19.42.13 and 172.19.43.13. All the computers in Building 67 are on the same physical subnet. Dorm A has 175 single-occupancy rooms. Dorm B has 2013 double-occupancy rooms.

Envisioned IT Environment:

Physical Network:

The network topology will be reconfigured as needed to minimize all network traffic. All dorm rooms will be wired to provide a single 10BaseT connection for every student.

WAN Connectivity:

The dial-up service has become overloaded. However, instead of investing in more modems, State University wants to provide VPN services to all students, faculty, and staff. State University will maintain the current set of modems and dial-up services for the near future.

As part of improving security, research sponsors and partners will be allowed to access computers and resources on the intranet by means of VPN connections only.

The computing services department wants to implement a policy that will limit all VPN sessions to two hours for all VPN connections and will allow research sponsors and partners to connect during business hours only. No Internet access will be allowed through VPN connections.

The computing services department has decided to use Windows 2000 Routing and Remote Access to provide dial-up and VPN services.

Computers:

Because the computing services department wants to minimize its administrative and management effort, State University will implement a Windows 2000 Active Directory-based enterprise network. The root domain will be stateuniversity.edu, and it will have the following child domains:

- engineering.stateuniversity.edu
- law.stateuniversity.edu
- mba.stateuniversity.edu

State University will upgrade all of its Windows-based computers to Windows 2000 during a period of two years. All the Mac OS 7.5.5, UNIX, and VMS-based computers will continue to be supported as needed.

In their dorm rooms, students will be allowed to use computers running Microsoft Windows 95, Windows 98, Windows NT, Windows 2000, and Mac OS 7.5.5 or later.

Network Services:

The computing services department wants to require the use of DHCP for all computers that are capable of using DHCP. Additionally, the computing services department will require the use of secure, dynamic DNS updates for DHCP-allocated addresses.

Security:

The firewall must be strengthened to tightly control access to computers on the intranet. Research sponsors and partners will still be allowed to use Web sites and FTP sites that are set up by the research labs. Research partners and sponsors will still be allowed to run programs by establishing Telnet sessions to specific computers. However, this access must be limited only to computers that belong to the respective research labs. Within a research lab, some research partners might want to keep data separate from the data of other research partners.

Questions

1. What is the minimum number of primary Windows 2000 WINS servers you will need in the new network?

A: 2

2. How should you implement DNS to provide support for Active Directory?

A: Install Active Directory integrated DNS servers in the Active Directory domains. Configure them as authoritative for the corresponding zones.

3. Which method should you use to allocate IP addresses to client computers that connect by using dial-up services?

A: Obtain IP addresses from a DHCP server.

4. Which protocol or protocols should you support in the new network? (Choose all that apply.)

*A: TCP/IP
APPLETALK*

5. You need to specify the remote access policies for all VPN servers. Move the appropriate remote access policy elements to the appropriate user class or classes. (Use only policy elements that apply. You might need to reuse policy elements.)

<ul style="list-style-type: none"> Students Faculty and staff Research sponsors and partners 	<div><<Move</div> <div>Remove>></div>	<ul style="list-style-type: none"> Allow Multilink connections. Apply day and time restrictions. Force strong encryption. Set maximum idle time. Set maximum session time. Specify the IP address of the network access server (NAS). Specify the telephone number of the network access server (NAS). Use IP filters.
---	---	--

A:

Student	Faculty and staff	Research sponsors & partners
Set maximum idle time	Set maximum idle time	Set maximum idle time

6. You need to specify how you should configure the DNS servers. Move the appropriate configuration tasks to the DNS server or servers where the tasks should be performed. (Use only configuration tasks that apply)

<ul style="list-style-type: none"> Internal DNS server External DNS server 	<div><<Move</div> <div>Remove>></div>	<ul style="list-style-type: none"> Add records for the university's e-mail servers, VPN servers, and public Web servers. Allow dynamic updates. Delegate the engineering.stateuniversity.edu, law.stateuniversity.edu, and mba.stateuniversity.edu zones. Enable WINS Lookup. Manually add records for all computers in the university.
--	---	--

A:

Internal DNS Server	External DNS Server
Allow dynamic updates	Add records for the university email servers, VPN servers and public web servers
Delegate the engineering.stateuniversity.edu, law.stateuniversity.edu and mba.stateuniversity.edu zones	
Enable WINS lookup	

7. You need to specify how the technical requirements will impact your design. Move each technical requirement to the design component that it will impact. (Use all technical requirements. Use each only once.)

<ul style="list-style-type: none"> ■ DNS strategy ■ DHCP strategy ■ WINS strategy ■ Router placement and configuration ■ Domain controller placement and configuration ■ Dial-up and VPN strategy ■ Firewall strategy 	<div style="border: 1px solid black; padding: 2px; margin: 2px; width: 60px; float: left;"> <<Move </div> <div style="border: 1px solid black; padding: 2px; margin: 2px; width: 60px; float: left;"> Remove>> </div> <div style="clear: both;"></div>	access for research sponsors and partners design of Active Directory internal and external Web sites management of IP address allocation off-campus users access to internal network remote access restrictions for faculty and staff
--	--	--

A:

DNS strategy	Design of Active Directory
	Internal and external Web sites
DHCP strategy	Management of IP address allocation
WINS strategy	None
Router placement and configuration	Access for research sponsors and partners
Domain controller placement and config.	None
Dial-up and VPN strategy	Remote access restrictions for faculty & staff
Firewall strategy	Off-campus users access the internal network

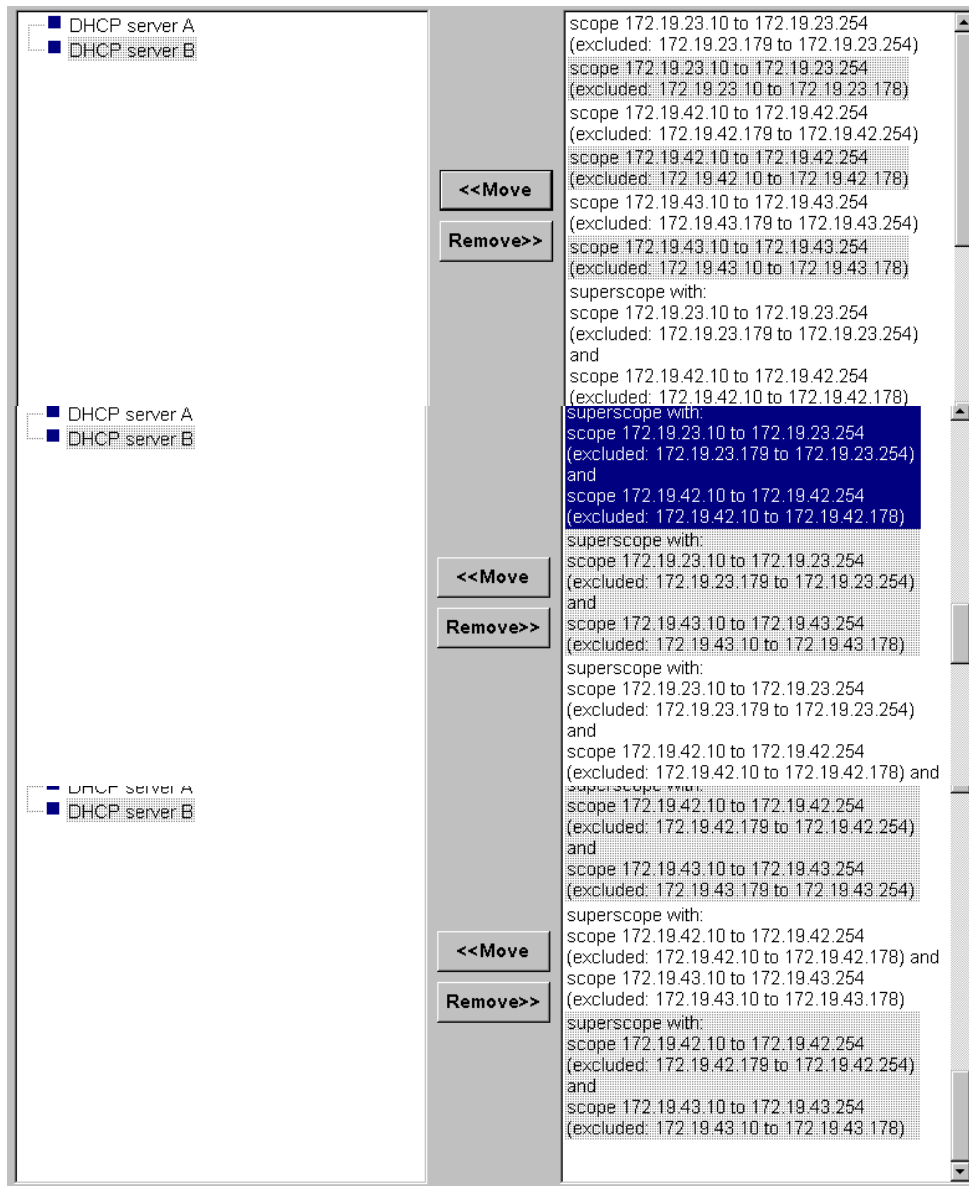
8. You need to specify the minimum IP subnet design for Dorm A, Dorm B, Building 25, and Building 34. Move the appropriate subnet masks to the appropriate building or buildings. (Use only subnet masks that apply. You might need to reuse subnet masks.)

<ul style="list-style-type: none"> ■ Dorm A ■ Dorm B ■ Building 25 ■ Building 34 	<div style="border: 1px solid black; padding: 2px; margin: 2px; width: 60px; float: left;"> <<Move </div> <div style="border: 1px solid black; padding: 2px; margin: 2px; width: 60px; float: left;"> Remove>> </div> <div style="clear: both;"></div>	255.252.0.0 255.255.0.0 255.255.128.0 255.255.240.0 255.255.248.0 255.255.252.0 255.255.254.0 255.255.255.0 255.255.255.192 255.255.255.211
--	--	--

A:

Dorm A	Dorm B	Building 25	Building 34
255.255.255.0	255.255.255.0	255.255.248.0	255.255.254.0

9. You design uses two DHCP servers to support the whole campus. These two servers will be located in the computing services department. You need to specify the scopes and/or superscopes for buildings 56 and 67 by using a 70/30 address split between the servers.



*A: DHCP B = Scope 172.19.23.10 to 172.19.23.254
(Excluded: 172.19.23.179 to 172.19.23.254)*

Index

A

Active Directory ... 9, 10, 14, 15, 32, 36, 37, 50, 51, 53
Active Directory zone 9
affinity mode 12
alerts 15
AppleTalk 10
application gateway 11
Applications log 15
authentication 12, 26, 35
availability 4, 11, 14, 17, 23, 29

B

backbone 7, 48
Backbone-based 7
bandwidth 4, 13, 19, 29, 30, 36, 38, 42
Bandwidth 4, 29
Banyan Vines IP 10
BOOTP relay 8, 9
broadcast 8, 13
browser 11, 23
business models 1

C

cabling 7
caching 11, 14
centralized 2, 3, 19, 30, 36
Certificate Services 14, 32
change-management process 4
circuit-level gateway 11
Client and Gateway Services for NetWare 9
Client Services for NetWare 9
cluster 11, 12, 18, 23, 25, 28
clustering 11
command-line utilities 16
connection sharing 11, 14

D

DDNS 9, 12
decentralized 2, 3, 19
decision-making process 3
DECNet 10
default gateway 8
Dfs 3, 10, 15, 18, 38
Dfs client 10
Dfs host service 10
Dfs root 10, 15
Dfs tree 10
Dfs volume 10
Dfs volumes 10
DHCP3, 7, 8, 9, 12, 14, 18, 25, 27, 28, 33, 35, 37, 38,
39, 45, 50, 51, 53, 54

dialup 11, 12, 13, 14
Directory service 15
disaster recovery 6
disk 17, 18, 21
Distributed file system 10, 38
DLC 10
DNS, 7, 9, 12, 14, 15, 16, 18, 26, 27, 37, 38, 39, 40,
45, 49, 50, 51, 52, 53
domain controller 9, 12, 21, 24, 35, 37, 45
Domain Name System 9, 14
Dynamic DNS 9
Dynamic Host Configuration Protocol 8, 14
dynamic routing 13

E

EFS 14
encrypted 13
Encrypting File System 14
Ethernet 7, 29, 41, 43, 48
Event Log 15

F

fail-over 18
fault tolerance 3, 7, 15, 23
fault-tolerance 3
FDDI 7
Fiber Distributed Data Interface 7
File Services for Macintosh 10
File Transfer Protocol 11
firewall 11, 29, 36, 37, 46, 49, 51
FQDN 9
FTP 11, 37, 48, 49, 51
Fully Qualified Domain Name 9

G

gap analysis 4
Global Catalog 14, 18, 27

H

hardware 6, 7, 11, 17, 20, 22, 23, 33, 35
host computers 7
hostname 5, 14
hosts 5, 8, 9, 11, 12, 15, 21, 40
HTTP 11
hub 7, 29, 33, 46
Hypertext Transfer Protocol 11

I

IIS 11, 14, 29, 32, 33
Information flow 1
Internet Information Server 11

Internet Protocol Security	13
intranet	11, 29, 32, 36, 38, 50, 51
IP address	5, 7, 8, 11, 12, 14, 51, 53
IP addressing	5
Ipconfig	8
IPSec	13, 18, 26
IPX/SPX	9
ISDN	14, 29
<i>Iterative queries</i>	9

J

JScript	16
---------------	----

L

L2TP	13, 26, 44, 46
LAN	11, 12, 13, 20, 21, 28, 29, 31, 33, 41, 43, 46
Latency	4
Layer-2 Tunneling Protocol	13
LDAP	14
lease	9, 14
legacy applications	6
<i>life cycle</i>	2
Lightweight Directory Access Protocol	14
load balancing	12, 18
logical security	5
lookups	9

M

MAC address	7
Macintosh	10
mail servers	11
Management Information Bases	15
<i>master servers</i>	9
memory	18
MIBs	15
Microsoft Management Console	15
MMC	15
multicast	8
multiple-cluster hosts	12

N

name cache	16
name resolution	9, 12, 43
namespace	9, 37, 39
NAT	11, 13, 14, 18, 36, 51
Nbtstat	16
NDIS	10
NetBEUI	10, 21
NetBIOS	15, 16
Netdiag	16
Netstat	8, 16
NetWare	9
Network Address Translation	11, 13, 14
Network Load Balancing	11
Network Monitor	13, 15
Network News Transfer Protocol	11

network services	4, 5, 11, 13, 14, 15, 17, 18, 23, 26, 43, 44
------------------------	--

Network services	7
network topologies	7
NLB	11, 12
NNTP	11
Nslookup	16
NWLink	9

O

Open Shortest Path First	8, 13
OSPF	8, 13
outsourcing	3

P

packet filtering	11
packets	7, 8, 11, 16
Pathping	16
Performance	4, 13, 15, 18
Perl	16
physical security	5
Ping	16
Point-to-Point Tunneling Protocol	13
POP3	11
Post Office Protocol	11
PPTP	13
Print Services for Macintosh	10
priorities	2
Proactive response	17
processor	18, 28
projected growth	3, 44
<i>protocols</i>	5, 6, 7, 8, 9, 10, 13, 28, 51
Proxy Server	10, 14, 18, 25

Q

<i>QTYPE codes</i>	9
--------------------------	---

R

RAS	12
Reactive response	17
recursive query	9
referral routes	10
registration	5, 9, 12, 38
Remote Access Server	12
Remote Installation Services	14
Remote Procedure Calls	14
replication	14, 15, 37, 39
resolver	9
resource records	9
RIP	8, 13
RIS	14
routed network	8
router	8, 11, 16, 18, 26, 29, 33, 46, 48
routers	7, 8, 13, 16, 35, 37, 48
Routing and Remote Access Service	3, 11, 13, 14
Routing Information Protocol	8, 13

Routing protocols	8
routing table	8, 13
routing tables	8, 13
Routing tables	8
RPC	14
RRAS	3, 11, 12, 13, 14, 18
rules	5, 10

S

scalability	4, 19
secondary servers	9
Security log	15
Simple Mail Transport Protocol	11
Simple Network Management Protocol	15
SMTP	11, 14
SNA	10, 20, 21, 23, 24, 26, 28, 29, 32
SNA Server	10
SNMP	15
static routes	8, 26, 37
Switched networks	7
switches	7
system log	15
System Monitor	15
SYSVOL	15

T

Task Scheduler	16
TCP/IP	3, 5, 7, 8, 9, 13, 14, 16, 28, 32, 44, 51
thicknet	7
thinnet	7
Token-ring	7

tolerance for risk	3
total cost of ownership	3, 6
<i>Total Cost of Ownership</i>	3
Tracert	16
trap	15
tunnel	13

V

virtual private network	11, 13, 14
Visual Basic Scripting	16
VPN3, 11, 12, 13, 14, 18, 26, 33, 44, 46, 50, 51, 52, 53	

W

WAN	11, 12, 13, 29, 31, 36, 37, 43, 46, 48, 50
Web servers	11, 36
Windows Internet Name Service	9
Windows Management Instrumentation	16
Windows Scripting Host	16
WINS7, 9, 12, 15, 18, 26, 27, 38, 39, 44, 45, 51, 52, 53	
WMI	16

X

X. 509	14
--------------	----

Z

zone	9, 38, 40
zone transfers	9