070-221

TEST KING

LEADING THE WAY IN IT
TESTING AND CERTIFICATION TOOLS!

Designing a Microsoft Windows 2000

Network Infrastructure

Version 2.1

Important Note
Please Read Carefully

Study Tips
This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version
We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check for an update 3-4 days before you have scheduled the exam.

Here is the procedure to get the latest version:

1. Go to www.testking.com
2. Click on **Login** (upper right corner)
3. Enter e-mail and password
4. The latest versions of all purchased products are downloadable from here. Just click the links.
   Note: If you have network connectivity problems it could be better to right-click on the link and choose **Save target as**. You would then be able to watch the download progress.

For most updates it enough just to print the new questions at the end of the new version, not the whole document.

Feedback
Feedback on specific questions should be send to feedback@testking.com. You should state

1. Exam number and version.
2. Question number.
3. Order number and login ID.

We will answer your mail promptly.

Copyright
Each pdf file contains a unique serial number associated with your particular name and contact information for security purposes. So if you find out that particular pdf file being distributed by you. Testking will reserve the right to take legal action against you according to the International Copyright Law. So don't distribute this PDF file.

Case Study No: 1

HANSON BROTHERS

Background

Hanson Brothers is an international consulting firm that is based in Portland, Oregon. Hanson Brothers specializes in consulting services for US 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 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.

Organization

Hanson Brothers has 2500 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 American 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 Asian 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 distinct offices.

- Auckland, New Zealand

- Manila, Philippines
- Singapore city, Singapore

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

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

The Latin America 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 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/CSU 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:

- 1000 Pentium III computers that are running Windows NT 4.0
- 1500 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 Windows NT4 DHCP services.

A single Windows NT domain exists for email 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:

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

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

The Portland office will contain an enterprise, a regional and site administrator team. Each regional headquarters office will contain a regional and a site administrator team. Each district office will contain only site administrator.

Although Hanson Brothers has limited Internet presence, Internet resources play an important
Role for the research company performs to its customers. Although our foreign offices have been reporting slow Internet performance, employees at the Portland Office report than 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 sites. All intranet Web servers will be located in Portland Office. One of these Web based applications concern all human resources files in a single location that users can view through their browser. 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 Internet 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 wisely. We want to minimize increase in costs for WAN connectivity wherever possible.

We want to immediately upgrade all Windows NT4 client computers to Windows 2000 professional. We will not 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 network 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 domain will use the following names:

- Asia
- Europe

- LAmerica
- NAmerica
- SPacific

A 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 the 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 have 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 hansbrothers.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 in share printers. All administrator client computers will run Windows 2000. All servers will run Windows 2000

Questions Hanson Brothers

Q. 1
You need to provide Hanson Brothers with a highly available DNS design. What should you do?

A. Create primary DNS zones for the Asia, Europe, LAmerica and SPacific zones on the DNS servers in the Corp domain
B. Create a primary DNS zone in each domain. Configure the DNS servers in the Asia, Europe, LAmerica, NAmerica, and SPacific domains as forwarded to each other.
C. Create a primary DNS zone in each domain as forwarders to the Asia, Europe, LAmerica, North America and SPacific domains.
D. 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, NAmerica and SPacific domains.

Answer: D.
Explanation: In this scenario a primary DNS zone for Corp is created at the DNS server in the Corp domain, and a secondary DNS zone is created for the Corp zone at DNS servers in each of the Asia, Europe, LAmerica, NAmerica and SPacific domains. This will allow all clients in the domains to resolve names in the Corp zone. Name resolution will be localized within the regional domains. As the primary DNS zone has been created in every regional domain, name resolution within a domain will be localized within that domain. The WAN links would therefore not be used for name resolution since all DNS queries will be resolved within each domain.

Incorrect answers:
A: If all primary DNS zones for all domains were created on the DNS server at the central Corp domain, then all name resolution would have to cross WAN links as each regional domain would need to access the central DNS server for name resolution. This would require a lot of bandwidth.
B: All domains must be able to use resources in the central Corp domain. A secondary zone for the Corp domain must be created on the DNS servers at Asia, Europe, LAmerica, NAmerica, and SPacific domains. If not they would not be able to resolve names of Corp domain.
C: There must be a DNS zone for the central Corp domain.

Q. 2
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)

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.)
Domains
Namespace
Collapse
Corp
NAmerica
LAmerica
corp.hansonbrothers.com
hansonbrothers.com
lamerica.corp.hansonbrothers.com
lamerica.hansonbrothers.com
lamerica. namerica.hansonbrothers.com
lamerica.namerica.corp.hansonbrothers.com
namerica.corp.hansonbrothers.com
namerica.hansonbrothers.com
<<Move
Remove>>

Answer:

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.)
Domains
Namespace
Collapse
Corp
corp.hansonbrothers.com
NAmerica
namerica.corp.hansonbrothers.com
LAmerica
lamerica.corp.hansonbrothers.com
corp.hansonbrothers.com
hansonbrothers.com
lamerica.corp.hansonbrothers.com
lamerica.hansonbrothers.com
lamerica. namerica.hansonbrothers.com
lamerica.namerica.corp.hansonbrothers.com
namerica.corp.hansonbrothers.com
namerica.hansonbrothers.com
<<Move
Remove>>

Explanation:
From the scenario we know:

- Hanson Brothers has a registered DNS namespace of hansbrothers.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.
- A new parent domain named Corp will be created.
- Hanson brother will use Active Directory namespaces that are contiguous with the existing registered domain name.

These restrictions force us to use the corp.hansbrothers.com DNS namespace at the Corp domain.

The DNS name space is contiguous so the domain names of the child domains of Corp domain must be added the corp.hansbrothers.com domain name.
The namerica.corp.hansbrothers.com namespace must be used in the NAmerica domain.
The lamerica.corp.hansbrothers.com namespace must be used in the LAmerica domain.

Incorrect answers:
hansbrother.com:
It cannot be used since the new parent Corp domain has been created.
Use Corp.hansonbrothers.com domain at the Corp domain.

lamerica.hansonbrothers.com, namerica.hansonbrothers.com:
These cannot be used since the root domain Corp must use the domain name space corp.hansbrothers.com and LAmerica and Namerica are child domains of this domain in a contiguous DNS name space.

Q. 3
What should you do to improve Internet connectivity for Hanson Brothers?

A. Configure all client computers to use existing proxy server in the Portland Office.
B. Configure an Internet connection in each regional headquarters.
C. Place a proxy server in each regional headquarter outside the United States.
D. Increase the bandwidth between the Portland office and each regional headquarters. Increase the bandwidth to the Internet service provider (ISP)

Answer: C.
Explanation: Bandwidth must be used wisely to save money. That is why a centralized Internet connection is preferred at Hanson Brothers. By placing proxy servers locally in the regional headquarters outside the United States, bandwidth would be saved through caching. It would also provide Internet access, security, and monitoring capabilities.

Incorrect answers:

A: A centralized proxy server solution would create too much WAN traffic.

B: Hanson Brothers wants a centralized Internet connection solution because the links to the regional headquarters outside the United States are very expensive.

D: Hanson Brothers wants to minimize increase in costs for WAN connectivity wherever possible, therefore increasing bandwidth is not a preferred solution.

Q. 4

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

A. Configure all servers to register with WINS and DNS.
B. Configure all client computers to register directly with DNS.
C. Configure DHCP servers to register the A (host) records for Windows 2000 client computers with DNS.
D. Configure all servers to register only with DNS.
E. Configure DHCP servers to register the A (host) records for non Windows 2000 client computers with DNS.
F. Configure all client computers to register with WINS.
G. Configure only non Windows 2000 client computers to register with WINS.

Answer: A, E, F.

Explanation:

A: The down-level clients, Windows 95 and Windows NT 4.0 computers, require a WINS server for name resolution while the Windows 2000 computers require DNS for name resolution. All servers should register themselves with both the WINS server and DNS server so that the clients are able to access them by name.

E: The DHCP servers must be configured to register the A (host) records for non Windows 2000 client computers with DNS, since they are unable to do it themselves, contrary to the Windows 2000 clients.

Incorrect answers:

B: The down-level Windows 95 and Windows NT 4.0 computers are not able to register themselves directly in DNS. The DHCP servers must be configured to register the A (host) records for them with DNS.

C: It is not necessary for the DHCP server to register A (host) records for the Windows 2000 clients as they are able to do it themselves

D: We need to register the servers in WINS as well as we have down-level clients (Windows 95/Windows NT 4.0), cannot use DNS for name to IP resolution and therefore require a WINS server for this purpose.

G: If only non-Windows 2000 client computers register with WINS, the downlevel clients would only be able to access other downlevel clients, not any Windows 2000 computers, since downlevel clients use WINS for name resolution.

Q. 5
Which change should you make to the existing WAN for the North America region before implementing the new network?

A. Install fully meshed site-to-site leased lines between all North America offices.
B. Increase the circuit bandwidth at the Los Angeles, Montreal, New York city and Washington DC, district offices.
C. Create a permanent virtual circuit (PVC) from each office to all other offices.
D. Increase the circuit bandwidth at the Portland Office.

Answer: D.
Explanation: Hanson Brothers have to increase the bandwidth, since they are going to implement a new domain structure and Active Directory. Active Directory in particular would increase network bandwidth usage.

It would be less expensive to increase the bandwidth on only one location, and the logical choice would be the central Office in Portland.

Incorrect answers:
A: A fully meshed site-to-site leased line between all North American offices would provide excellent network bandwidth, but the cost would be tremendous. One requirement is that the increased cost for WAN connectivity would be minimized whenever possible.
B: Increasing the circuit bandwidth at the Los Angeles, Montreal, New York city and Washington DC, district offices would not be the most cost effective solution. It is better to increase the bandwidth only at the central Portland Office.
C: A permanent virtual circuit (PVC) exists from each North America district office to the Portland Office already exists. Adding PVCs between all offices would be a small improvement with a high cost.

Q. 6
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 addresses excluded.
In the regional headquarters, deploy a DHCP server that has one scope for each district office with 80 percent of the address excluded.
B. In the regional headquarters, deploy a DHCP server that has one scope for each district office
C. In each office in the region, deploy a DHCP server that has one scope for the local subnet.
D. In each district office, deploy a DHCP server that has one scope for the local subnet with 20 percent of the address excluded.
In the Corporate headquarters, deploy a DHCP server that has one scope for each district office with 80 percent of the addresses excluded.

Answer: A.
Explanation: The 80/20 rule is used to split the scope to provide redundancy. The DHCP servers placed locally at the district offices should have a local scope with 20 percent of the addresses excluded. The DHCP servers placed more centrally at the regional headquarters have one scope for each district office, and 80 percent of the addresses excluded.

Redundancy refers to ensuring that the network still operates properly even if a server becomes unavailable.

Most of the clients would receive IP configuration from the local DHCP server and thus saving network bandwidth.

Incorrect answers:
B: A single DHCP server at the regional office configured with scopes for each district office, would neither provide redundancy in case of failure, nor would it minimize network bandwidth; IP configuration traffic would cross the WAN links between the district and regional offices.
C: By deploying a DHCP server locally in each region, DHCP traffic would be minimized but there would not be any redundancy in case of failure of a DHCP server.
D: This solution is opposite. Most clients would get their IP configuration from the central DHCP server at the regional office. It is better exclude few (20%) IP addresses from the scopes of the local DHCP servers, and to exclude many (80%) from the scopes of the central DHCP server at the regional office.

Q. 7
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)

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.)
Locations
Tasks
Collapse
Australia
Singapore
Philippines
New Zealand
<<Move
Remove>>
Configure a DNS server as a forwarder to the corp domain server
Configure a DNS server as a forwarder to the Australia DNS server
Configure a DNS server as a forwarder to the New Zealand DNS server
Configure a DNS server as a forwarder to the Philippine DNS server
Configure a DNS server as a forwarder to the Singapore DNS server
Configure a DNS server so that it has root hints to Internic name servers
Create a DNS server that hosts a standard secondary zone.
Create a primary Active Directory integrated zone
Create a secondary zone of the Corp zone.
Create a DNS sever that hosts a standard primary zones
Install DNS services on a domain controller

Answer:

Explanation:
Australia
Create a primary Active Directory integrated zone:
Hanson brothers has a requirement that DNS zones should be configured to run in a multi-master mode. Multi-master mode requires an Active Directory integrated zone.

Create a secondary zone of the Corp zone:
A secondary zone of the Corp zone would provide redundancy and it would also improve performance by decreasing name resolution traffic on the WAN links.

Install DNS services on a domain controller:
Since an Active Directory integrated zone should be used, DNS has to be installed on a Domain controller.

Singapore, Philippines, New Zealand:
Configure a DNS server as a forwarder to the Australia DNS server
No DNS server is installed at the local office. Instead the regional Australia DNS server is used for name resolutions. The Australia DNS server is authoritative for the zone.

Q. 8
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.
B. Move the DHCP service from member servers to domain controllers.
C. Place a DHCP relay agent on each DHCP server to propagate DHCPINFORM messages.
D. Replace all Windows NT4 DHCP servers with Windows 2000 DHCP servers.
E. Place all users into the DHCP Users group.

Answer: A, D.
Explanation: A: It is a requirement from the Active Directory Design Team leader that each regional administrator team will manage all DHCP servers in its region regardless of the server's physical location. By placing all members of the Regional Administrator team into the DHCP Administrators group this will be achieved.

Note: The DHCP Administrators group provides a way to grant limited administrative access to the DHCP server only, while not providing full access to the server computer. Other users or groups added as members of this group are granted the right to fully administer the applicable server in the DHCP console, but are not able to perform other administrative actions on the server computer.

D: Windows 2000 DHCP servers are safer then Windows NT 4.0 DHCP servers. Windows 2000 provides unauthorized DHCP server detection. This prevents unauthorized DHCP servers from joining an existing DHCP network in which Windows 2000 Server and Active Directory are deployed.

Incorrect answers:
B: This would decrease security. It is more secure to run the DHCP server on a member server compared to running it on a Windows 2000 Domain Controller. It is also a requirement from Hanson Brothers that all DHCP servers should reside on member servers.
C: All routers are already BOOTP enabled. That is they will allow all DHCP traffic to pass. DHCP Relay agents are therefore unnecessary
E: Placing all users in DHCP users group would provide all users with read access of the DHCP database. This would neither be good for security nor would it provide the regional administrator team ability to administer the DHCP servers.

Note: DHCP Setup automatically adds a special-purpose local users group, called the DHCP Users group, when DHCP is installed. Users belonging to this local group have read-only access to the local DHCP database and information via the DHCP console.

Q. 9

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 tasks, use tasks only once)
Teams
Tasks
Collapse
Enterprise administrator team
Regional administrator team
Site administrator team
<<Move
Remove>>
Authorize DHCP servers
Change user passwords
Configure DNS server settings
Configure password policy
Manage Active Directory replication schedule
Manage WINS replication
Modify schema
Monitor event logs on individual servers
Provide end-user support

Answer:

Explanation:

Enterprise:

Authorize DHCP servers:
Only Enterprise Adminstrators would be able to Authorize the DHCP servers in the domain.
Configure password policy:
Password policies should be configured at the Domain level so a consistent policy would be applied throughout the domain..
Modify schema:
Modify schema should be done at the most central point.

Regional administrator teams:

Manage WINS replication, Manage Active Directory replication scheduling
WINS and Active Directory replication is distributed throughout the network and should be delegated to reduce the work load on the Enterprise administrator team.
Configure DNS server settings:
Will have primary DNS servers for each domain at regional level so DNS must be managed regionally.

Site:

Monitor event logs on individual servers

Monitoring of individual servers is done locally at the site level.
Change user password:
Password changes should be done by personal close to user at the site level.
Provide end user support
End user support is provided at the site level.

Q. 10
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
B. In each regional headquarters, deploy a distributed file system (Dfs) root server that has a human Resources child node. In the Portland Office, deploy a Dfs replica server.
C. In the Portland Office, deploy a distributed file system (Dfs) root server. In each regional headquarters, deploy a child node.
D. In each regional headquarters, deploy a distributed file system (Dfs) root server. In the Portland office, deploy a child node.

Answer: A.
Explanation: The DFS root server should be deployed centrally at the Portland Office. Deploy the child nodes for each region centrally as well. In each region a DFS replica server, corresponding to the child node for that region, is deployed.

This DFS hierarchy will be consistent across the entire company, and the web servers located at Portland will be able to access the local Human Resource files from each region.

Incorrect answers:
B: The structure must be top-down, not bottom up. There is consistent DFS hierarchy.
C: The child nodes must be set up on the root server, not only in the regions. DFS replica servers are needed as well.
D: There should be only one DFS root server, not one in each regional headquarters, to provide for a consistent hierarchy across the company.

Case Study 2

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, DC.

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

Employees in the Boston headquarters are using 486 or Pentium class client computers that are connected to a single Windows NT 4 domain; Company 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

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 airport in Atlanta, Boston, Chicago and Washington DC will contain a passenger lounge. A maximum of 10 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 want 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 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.

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 cards 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

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 1: 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 2000 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 DC airport.

1. Provide WAN connectivity to Washington, DC.
2. Test the old reservation application and the new reservation application.
3. Test the new Windows 2000 infrastructure from the Washington DC 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 DC 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 BLUE SKY AIRLINES

Q. 1
Which client hardware should you use for the gate machines in the airports?

A. Windows Terminal.
B. New Pentium III client computers.
C. Existing 486 client computers from corporate headquarters.
D. Existing 3270 terminals.

Answer: A.
Explanation: The gate machines at the airports will be used as a front end to the SQL Server database. Windows Terminal computers which are computers running Windows Terminal Emulation software will be used for this purpose since their hardware requirement and cost is kept low.

Incorrect answers:
B: It is not necessary to use new and expensive Pentium III computers.
C: The scenario states that the 486 client computers will be upgraded.
D: 3270 terminals cannot be used to connect the SQL Server. They are used to connect to IBM main frames.

Q. 2
Which component or components must you place locally on the passenger lounge network? (Choose all that apply)

A. Kiosk computer
B. Hub
C. Domain controller
D. DNS server
E. Routing and Remote access
F. Microsoft Proxy Server
G. DHCP Server

Answer: A, B.
Explanation: The passenger lounge will provide internet access to passengers. The passenger will either use their own laptops or the kiosk computer.

A: A kiosk computer in each passenger lounge to provide Internet access to customers without laptops. The kiosk computer is a requirement of this scenario.

B: The passenger lounge will provide Internet access to the kiosk computers and a maximum of 10 laptops. To share the WAN connection a hub is needed.

Incorrect answers:
C: Lounge clients will authenticate through RRAS. The domain controllers are placed in Boston.
D: Name resolution will provide through Routing and Remote Access Server using DNS server placed at Boston Headquarters.
E: The Routing and Remote Access will be placed centrally at Headquarters at Boston, not locally at passenger lounge network.
F: Internet Access will be provided from the Boston Headquarters. A Proxy Server placed locally is not called for.
G: The DHCP server will be centrally at the Boston Headquarters.

Q. 3
Which component or components will you need in Washington DC to complete Phase III? (Choose all that apply)

A. DHCP Server
B. WINS Server
C. Hub
D. DNS server
E. Client hardware
F. Domain controller
G. Router

Answer: C, E, and G.
Explanation: Phase III is to implement a test deployment in the Washington DC airport.
C: The physical WAN connection to the Boston Headquarters will be used by several computers. This can be accomplished by simply sharing it through a HUB.
E: Some client hardware is needed: the kiosk computer at the passenger lounge and the Windows Terminal computers which will be running the new ticketing and reservation application.
G: The Washington DC airport and all the other airports as well, will have two subnets: one LAN for employees, and one LAN for the passengers. To provide for this a router is needed.

Note: *Phase III includes the following steps:*

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

Incorrect answers:

B: Name resolution is provided through the DNS servers located at the Boston Headquarters. WINS is not needed at the airport.
D: Name resolution is provided through the DNS servers located at the Boston Headquarters. DNS is not needed at the airport.
F: There is no need of a domain controller at the airport. Authentication will be provided through the Routing and Remote Access server located at the Boston Headquarters, where the Domain Controllers are located.

Q. 4
How should you design the Microsoft SQL Server environment?

A. Use one SQL Server computer
B. Use two SQL Server computers without database replication
C. Use two SQL Server computer with database replication
D. Use two clustered SQL Server computers.

Answer: D.
Explanation: Two clustered SQL Servers would provide improved performance and redundancy in case of failures.

Incorrect answers:
A: Using only one SQL Server would provide no redundancy in case of failure. This would not be acceptable.
B: Two separate SQL Servers without clustering and without replication would not share any data. This would complicate the database model, and it would not provide for redundancy in case of failure of one of SQL Server computers.
C: Database replication between two SQL server computers would be a good idea if they were located at different physical locations. In this scenario both would be placed at the central Headquarter in Boston. Replication is unnecessary and clustering should be used instead. Replication and clustering both provide redundancy both clustering improves performance while replication increases network bandwidth usage.

Q. 5
You need to assign the correct address range for each location. Move appropriate IP address ranges to the appropriate location or locations Use only address ranges that apply.

(You might need to reuse address ranges)

You need to assign the correct address range for each location. Move the appropriate IP address ranges to the appropriate location or locations. (Use only address ranges that apply. You might need to reuse address ranges.)
Locations
Collapse
Washington,DC, corporate LAN
Washington,DC, passenger lounge LAN
Atlanta corporate LAN
Atlanta passenger lounge LAN
<<Move
Remove>>
IP Addresses
10.0.1.0/24
10.0.2.0/24
10.1.2.0/24
10.1.3.0/24
192.168.1.0/24
192.168.2.0/24
192.168.3.0/24

Answer:

You need to assign the correct address range for each location. Move the appropriate IP address ranges to the appropriate location or locations. (Use only address ranges that apply. You might need to reuse address ranges.)
Locations
Collapse
Washington,DC, corporate LAN
10.1.2.0/24
Washington,DC, passenger lounge LAN
192.168.1.0/24
Atlanta corporate LAN
10.1.3.0/24
Atlanta passenger lounge LAN
192.168.1.0/24
<<Move
Remove>>
IP Addresses
10.0.1.0/24
10.0.2.0/24
10.1.2.0/24
10.1.3.0/24
192.168.1.0/24
192.168.2.0/24
192.168.3.0/24

Explanation:
Washington DC corporate LAN: 10.1.2.0 with a subnet mask of 255.255.255.0
The Corporate LAN uses the network address of 10.1.0.0.
The first airport with WAN connectivity is Washington DC – this is during Phase III of the deployment. At Phase IV WAN connectivity is provided to all airports.

The only two correct subnets to 10.1.0.0 are 10.1.2.0 and 10.1.3.0. The Washington DC corporate LAN should have the first available subnet 10.1.2.0 since it is deployed earlier than Atlanta.

Washington D.C. passenger lounge LAN: 192.168.1.0 with a subnet mask of 255.255.255.0
All passenger lounges will be connected to the 192.168.1.0 VLAN Red network. The VLAN Red network will not be subnetted.

Atlanta Corporate LAN: 10.1.3.0 with a subnet mask of 255.255.255.0
Atlanta Corporate LAN is a subnet to the Boston Headquarter LAN 10.1.0.0. Atlanta Corporate LAN gets the 2nd available subnet 10.1.3.0

Atlanta passenger lounge LAN: 192.168.1.0 with a subnet mask of 255.255.255.0
All passenger lounges will be connected to the 192.168.1.0 VLAN Red network. The VLAN Red network will not be subnetted.

Incorrect answers:
10.1.2.0 with a subnet mask of 255.255.255.0 should be used at Washington not Atlanta since Washington is deployed before Atlanta. With the same line of thought 10.1.3.0 must be used at Atlanta and not at Washington.

10.0.1.0 with a subnet mask of 255.255.255.0:
The Corporate LAN has an IP address of 10.1.0.0/16. 10.0.1.0/24 is not a subnet of 10.1.0.0/16.

10.0.2.0 with a subnet mask of 255.255.255.0
The Corporate LAN has an IP address of 10.1.0.0/16. 10.0.2.0/24 is not a subnet of 10.1.0.0/16.

192.168.2.0 with a subnet mask of 255.255.255.0.
The VLAN Red network has an IP address of 192.168.1.0/24. 192.168.2.0/24 is a separate network compared to 192.168.1.0/24.

192.168.2.0 with a subnet mask of 255.255.255.0.
The VLAN Red network has an IP address of 192.168.1.0/24. 192.168.2.0/24 is a separate network compared to 192.168.1.0/24.

Q. 6
You need to allow the pilots access to the intranet Web server, what should you do? (Choose all that apply)

A. Deploy proxy services
B. Deploy Active Directory
C. Use remote access policies
D. Use the access by user administrative model to control remote access
E. Deploy certificate services

Answer: B, C, E.
Explanation:
B: The existing Windows NT 4.0 domain will be upgraded to a Windows 2000 domain that will be used to build a Windows 2000 infrastructure. This would require Active Directory services.
C: Remote access policies are needed to decide which users get access or not. Only the pilots should get access to a confidential section of the intranet Web server.
E: The pilots will need strong encryption to access a confidential section of the intranet Web server. All pilots will be issued portable computers running Windows 2000 and configured with smart cards readers. The smart card readers require the use of the Extensible Authentication Protocol (EAP), which provides secure authentication and strong encryption. To be able to use EAP with the smart card readers, computers certificates have to be issued and this requires certificate services.

Incorrect answers:
A: The user administrative model is used to configure user accounts on an individual basis. Configuring remote access for every user account would require a lot of administration and is not the best solution.
D: Proxy services are used to configure which type of information is allowed to flow in and out of the network. Proxy services aren't used to administer remote access.

Q. 7
Which five components should be deployed or installed during Phase 1?
(There are 10 answer choices. Choose five)

A. DNS Server
B. Domain Controller
C. Active Directory
D. Terminal Services
E. Routing and Remote Access
F. Microsoft SQL Server
G. TCP/IP
H. 3270 emulation software
I. DHCP server
J. Microsoft SNA Server

Answer: D, F, G, H, J.
Explanation:

D: The new two-tier application must be able to access the SQL database from a terminal session. The terminal session uses Windows 2000 Terminal services.
F: SQL Server is required. A copy of the existing mainframe database should be imported into a SQL Server database.
G: Terminal Services is a Windows 2000 service that requires the TCP/IP protocol.
H: The emulation software application must be installed. This is the IBM 3270 emulation software.
J: Users must be able to use the existing mainframe database from a Windows 2000 Terminal session. MICROSOFT SNA Server must be used to access the IBM mainframe database from a Windows environment.

Note: *This is Phase 1*
Phase 1: 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.

Incorrect answers:
A: Name resolution, DNS, isn't required until Phase II.
B: Active Directory is deployed during Phase II. This would require Domain controllers. There is no need for any Domain controllers during Phase I.
C: Active Directory is deployed during Phase II.
I: DHCP isn't required until Phase II when Washington DC gets WAN connectivity.

Q. 8
Which strategy or strategies should you use for the DHCP design at the airports? (Choose all that apply)

A. In each passenger lounge, deploy one DHCP server that has one scope
B. In the 10.1.0.0 network in Boston, deploy two DHCP servers
Configure each server so that it has 12 scopes
Configure an exclusion for 50 percent of the addresses in each scope
C. In the 192.168.1.0 network in Boston, deploy one DHCP server that has four scopes
D. In the 192.168.1.0 network in Boston, deploy one DHCP server that has one Scope.
E. In each airport, deploy one DHCP server that has scope with 25 percent of the address space excluded.
In the Boston headquarters, deploy one DHCP server that has 12 scopes
Configure an exclusion for 75 percent of the addresses in each scope
F. 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

Answer: D, F.
Explanation:
D: The 192.168.1.0 network in Boston is the subnet at Boston HQ that belongs to VLAN red. VLAN red is not subnetted and consists of a single subnet. There is no need for more than one scope.
Two DHCP servers for VLAN Red would provide redundancy but it is not listed here.
F: The 10.1.0.0 network will be subnetted so that each airport gets one subnet.
Blue Sky Airlines is currently serving four airports: Boston, Massachusetts, Chicago, Illinois, and New York city. Blue Sky Airlines will expand to four more airports: Atlanta, Georgia, Cincinnati, Ohio, Dallas, Texas and Washington, DC.
Subnetting would require a total of eight subnets. A scope would be required for each subnet. For redundancy two DHCP servers should be deployed. Each DHCP server should have eight scopes, one for each subnet. By configuring an exclusion for 50 percent of the addresses in each scope both DHCP servers would be able to service all eight airports.

Incorrect answers:
A: The passenger lounge computers at the airports belong to the VLAN Red network. This network is not subnetted. If a DHCP server with the scope of the VLAN Red network were deployed at each network they would cause DHCP lease collisions. Instead put one DHCP server for VLAN Red at the central Headquarters in Boston.
B: Blue Sky Airlines will service eight airports. Only eight scopes are needed, not twelve.
C: The 192.168.1.0 network in Boston is not subnetted and the DHCP server for this network only needs one scope, not four.
E: Eight, not twelve scopes are needed.

Q. 9
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 on VLAN Red and an Internet Information Services (IIS) server on the Corporate LAN in headquarters
B. Deploy a VPN server on VLAN Red and an Internet Information Services (IIS) server on the DMZ
C. Deploy a VPN server in the DMZ and an Internet information Services (IIS) server on the Corporate LAN in headquarters
D. Deploy a VPN server on the Corporate LAN in headquarters and an Internet Information Services server on the DMZ

Answer: C.
Explanation: The scheduling application runs on an IIS server. The flight personnel will use Internet to get remote access. A VPN server will give the personnel access the network and the IIS server.

The passengers use the lounge to get Internet access through the VLAN Red network. No passenger is able to use the corporate LAN network. The web server should therefore be placed on the Corporate LAN of security reasons.
A demilitarized zone (DMZ) is a zone protected with two firewalls. A DMZ usually has one secure LAN interface and a public less secure Internet interface. The firewalls should be configured so that Internet users only get access to the DMZ and not to the local LAN.
The IIS server must be protected and put on the Corporate LAN in headquarters. The VPN server must be connected to Internet and should be put in the DMZ.

Illustration:
LAN (IIS, secure)---Firewall----DMZ (VPN)----Firewall---Internet (public)

Incorrect answers:
A: VLAN Red and the corporate LAN are separate LANS. By putting the VPN server on VLAN Red and the IIS server on the corporate LAN, no one would be able to access the IIS server through the VPN server.
B: Deploying the VPN server and the IIS server on VLAN Red would be bad for security reasons, since passengers have access to VLAN Red through the lounges at the airports.
D: The IIS would be more secure if it was placed on the Corporate LAN, and it should not be placed in the DMZ. If the VPN server is placed on corporate LAN the firewalls would have to be configured to give internet access to the corporate LAN, which would reduce security.

Q. 10
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
Load balance the Microsoft SQL Server computers
Load balance the Terminal Server
B Load balance the Internet information services servers
Cluster the Microsoft SQL server computers
Load balance the Terminal Servers
C Load balance the Internet Information Services servers
Cluster the Microsoft SQL Server computers
Deploy stand alone Terminal Servers
D Cluster the Internet Information Services servers
Cluster the Microsoft SQL Server computers
Cluster the Terminal Servers

Answer: B.
Explanation: The Internet Information Servers (IIS) should be load balanced for performance.
The SQL Servers should be clustered for performance and redundancy.
The Terminal servers are load balanced for performance.

Incorrect answers:

A: It is important that the SQL Server computers should be clustered for redundancy. Load balancing them would provide better performance but no redundancy.

C: The terminal servers should not be stand-alone. They must be integrated into the domain. They should also be load balanced for performance.

D: The Terminal servers should be optimized for performance by load balancing. Clustering the Terminal Servers would decrease the available connections.

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

A. 255.255.255.0
B. 255.255.255.224
C. 255.255.255.248
D. 255.255.255.252

Answer: A.

Explanation: Dallas Airport is connected to the Airport Lan (see WAN connectivity exhibit). The Airport LAN is connected to the corporate network which uses 10.1.0.0 with a subnet mask of 255.255.0.0. The corporate network should be subnetted for the Airport LAN at the four Airports connected to this LAN (Cincinatti, Dallas, New York, Philadelphia). We decide the appropriate subnet mask by counting the IP devices at Dallas..

At Dallas (and Cincinatti, , New York, Philadelphia) you have the following IP devices:

10 ticket machines
10 ticket printers
10 passenger laptops per lounge

This sum up to 30 IP devices. However, all locations must have the same subnet mask, and the airport in Atlanta, Boston, Chicago and Washington DC will contain a passenger lounge. So additional IP addresses must be used for the kiosk computer and 10 passenger computers. In total 41 devices must be supported.

The subnet mask of 255.255.255.0 is adequate as it allows for 254 hosts.

Note: The lowest and the highest address in the range are always reserved and cannot be used for hosts.

Incorrect answers:

B: A subnet mask of 255.255.224.0 would provide for 30 hosts, but 41 are needed since all subnet must have the same subnet mask.
Another argument against using this subnet mask is that neither VLAN Red nor the corporate LAN, which use the subnet mask 255.255.255.0 at the airports are subnetted to 255.255.224.0.

C: The subnet mask 255.255.255.248 would only provide for 14 hosts.

D: The subnet mask 255.255.255.252 would only provide for 2 hosts.

CASE STUDY NO: 3

PARNELL AEROSPACE

Background:
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 contacts with other companies to mass production of its products.

Parnell Aerospace is located in two buildings in a large industrial park. The buildings are next door to one another. 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.

Existing 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 by a token ring bridge.

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

The 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 of a Windows NT 4.0 domain named PARNELDOM. 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 Windows 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 cannot be changed, and there are no suitable non-mainframe-based alternatives.

Microsoft 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):
The 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 news servers can be purchased. A small budget has also been allocated for new software. Enough money has been allocated to upgrade existing operation systems on all computers. Parnell Aerospace owns several server licenses for the entire Microsoft Back Office suite. The company also owns enough client access licenses so that all client computers can run all Back Office 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:

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 VII: Decommission the 3174 cluster control units and the token ring bridge

(See pictures for redesigned network design)

3745
Front-End
Processor
3745
Front-End
Processor
Windows 2000
Domain Controller
System 390 Mainframe
Token-ring
Token-ring
Windows 2000
Member Server
SNA Server /
Router
SNA Server /
Router
Windows 2000
Domain Controller
150 Windows 2000
Professional PC's
Windows 2000
Member Server
75 Windows 2000
Professional PC's
Building 1
Building 2

QUESTIONS PARNELL AEROSPACE

Q. 1
What are the two most critical problems in the current network (choose two)

A. The network is slow.
B. The network requires updating.
C. The network is difficult to manage and monitor.
D. The network suffers from too much downtime.
E. The network is not scalable enough to meet projected growth.

Answer: C, D.
Explanation:
Parnell Aerospace wants to improve manageability and availability of their network

C: the CIO says: "This network is very expensive to own and operate".
D: The CIO says: "The network suffers from too much downtime". The system administrator agrees.

Incorrect answers:
A: System Administrator: "The network functions well as it is but we want to improve the manageability and availability of our client server network".
B: The network does not need updating, since Parnell Aerospace says that the network topology is fixed and cannot be redesigned or replace.
E: Parnell Aerospace estimates a minimal growth in users and no growth in location. It seems the network is scalable enough for the requirements.

Q. 2
Which two factors should you consider in your new network design? (Choose two)

A. Cost of implementation
B. Replacement of the existing topology
C. Remote connectivity
D. Interoperability with the existing environment
E. Internet connectivity

Answer: C, D.
Explanation:
C: The new design must provide partners with Remote Access to the network.
D: Parnell Aerospace wants a network environment that is completely interoperable between their two different networking topologies.

Incorrect answers:

A: Parnell Aerospace has allocated enough money has been allocated to upgrade existing operating systems on all computers

B: The existing network topology is fixed and cannot be redesigned or replaced.

E: Parnell Aerospace does not require or desire any Internet connectivity at this time.

Q. 3

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

A. On one subnet, place a DHCP server that has a scope configured for each subnet in the network.
B. On one subnet, place a DHCP cluster that has a scope configured for each subnet in the network.
C. On each subnet, place a DHCP server that has a scope configured for each subnet in the network.
D. On each subnet, place a DHCP server that has a scope configured for that subnet only.
E. On each subnet, place a DHCP cluster that has a scope configured for that subnet only.

Answer: C.

Explanation: Install one DHCP server in each subnet. Configure each DHCP with two scopes: one for the local subnet and one for the remote subnet. Make proper exclusion of IP addresses. The 80/20 rule might be used for example.

This would provide redundancy. In case of router failure all clients would still receive IP configurations from the local DHCP server.

Incorrect answers:

A: Only a single DHCP server would not provide any fault tolerance. If the DHCP server fails no clients would receive IP configuration, and if the router fails the remote clients wouldn't receive IP configuration.

B: If all DHCP servers were placed on the same subnet the remote clients would be unable to receive IP configuration in case of router failure.

D: Placing one DHCP server in every subnet is a good strategy, but they must be configured with two scopes each; one for the local subnet and one for the remote subnet.

E: Scopes must be configured for both subnets.

Q. 4

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

A. Allow dial-in connections that use PAP for authentication
B. Allow direct dial-in connections that use MS-CHAP for authentication
C. Allow direct dial-in connections that use MS CHAP version 2 for authentication
D. Allow VPN connections that use PPTP to secure communications

E. Allow VPN connections that use L2TP to secure communications
F. Require basic encryption on all connections
G. Require strong encryption on all connections
H. Enable IPSEC on all connections

Answer: B, C, G.
Explanation:
B: A computer installed with the Windows 98 operating system, which has not been upgraded to support MS CHAP V2, will be able to use MS-CHAP, but not MS-CHAP v2. Some dial-in users have Windows 98 computers so MS-CHAP must be allowed.
C: MS-CHAP V2 is a more secure than MS-CHAP. Windows 2000 supports MS-CHAP V2 so it is a good idea to allow this protocol for authentication.
G: Remote users will download confidential product documents. Parnell Aerospace requires the strongest possible encryption for all remote connections.

Incorrect answers:
A: The PAP authentication protocol does not use any encryption and the login name and password are sent in plain text. This does not satisfy the requirement from Parnell Aerospace that all remote access traffic is secure.
D: VPN connections cannot be used for dial-in access.
VPN enables users working at home or on the road to connect securely to a remote corporate server by using the routing infrastructure provided by a public internetwork such as the Internet. A VPN connection also allows a corporation to connect with its branch offices or with other companies over a public internetwork while maintaining secure communications.
E: VPN connections cannot be used for dial-in access.
F: Basic Encryption cannot be used since Parnell Aerospace requires that the strongest possible encryption must be used for all connections.
H: IPSec can be used for VPNs or for local network traffic, but it cannot be used on dial-in connections.

Q. 5
You need to design an initial test mode for Internet access. Administrators need to control which Web sites internal users can gain access to. Which technology should you use?

A. NAT
B. Proxy server
C. Firewall
D. Connection sharing
E. Routing and Remote access

Answer: B.
Explanation:
A: Proxy server would provide administrators the possibility to control which Web sites the local users can gain access to.

Incorrect answers:

A: NAT, Network Address Translation, would provide the Internet access to local users, but it would not provide the administrators with control on which Web sites internal users can gain access to.

C: A firewall would enable the administrators to decide which kind of traffic would be allowed to flow between the local network and Internet. This control would be at protocol and port level. It would not allow administrators to control which Web sites internal users can gain access to.

D: Internet connection sharing would provide the Internet access to local users, but it would not provide the administrators with control on which Web sites internal users can gain access to.

E: Routing and Remote Access is not used for Internet access. It is used for routing, dial-in access and dial out access.

Q. 6

Answer:

Explanation:

DHCP

One DHCP server should be placed in each building (subnet) to provide redundancy and improve performance. Each DHCP server should be have two scopes: one for the local subnet and one for the remote subnet, for example by using the 80/20 rule.

DNS

DNS is needed to provide name resolution. By putting one DNS server in each building we get redundancy, which meets the requirement of Parnell Aerospace that all network services must provide redundancy for fault tolerance.

WINS

There are downlevel clients, Windows 98 clients, which use WINS and not DNS for name resolution. To provide redundancy one WINS server is used in each building.

Dial-up Server

The dial-in users want to access resources on the mainframe. The mainframe is located in building 2. It is therefore best to put the dial-up server in building 2. There is no need for a separate dial-up server in building 1.

Incorrect Answers

Global catalog
Since there is only one well-connected domain Global Catalog Servers would not increase performance.

Proxy Services
A proxy server would provide Internet access, but Parnell Aerospace does not require or desire any Internet connectivity at this time.

Q. 7
You need to implement a network routing strategy for Parnell Aerospace. What should you do?

A. Implement Internet group management protocol (IGMP) on all router interfaces
B. Implement static routes on all router interfaces.
C. Implement Open Shortest Path Forest (OSPF) on all router interfaces
D. Implement Routing Information Protocol (RIP) version 1 on all router interfaces
E. Implement routing Information Protocol (RIP) version 2 on all router interfaces

Answer: B.
Explanation: There are only two subnets and two routers. The simple and best solution is to use static routes on all router interfaces. It is the fastest and most secure solution.

There is no need of a dynamic router interface in this static LAN. And therefore there is no need for Routing Protocols (RIP V1, RIP V2, IGMP, OSPF).

Incorrect answers:
A: There is no need for a routing protocol in a static LAN. IGMP would provide multicasting, which is a limited form of broadcasting, to communicate and manage information between all member devices in a multicast group
C: There is no need for a routing protocol in a static LAN. RIP is a distance-vector routing protocol that broadcasts the information to neighboring routers. These broadcasts keep all internetwork routers synchronized.
D: There is no need for a routing protocol in a static LAN. RIP V2 is an improvement of RIP V1 that, for example, support password authentication and variable length subnet masks.
E: There is no need for a routing protocol in a static LAN. OSPF is best suited to a large-to-very-large, multipath, dynamic IP internetwork such as a corporate or institutional campus, or worldwide corporate or institutional internetwork.

Q. 8
What is the minimum number of DNS servers you should use in the new network?

A. 0
B. 1

C. 2
D. 3
E. 4
F. 5

Answer: C.
Explanation: DNS must be used to provide name resolution for the Windows 2000 clients. Two is needed for fault tolerance. Parnell Aerospace requires that every network service provide redundancy.

Incorrect answers:
A: Windows 2000 clients requires DNS for name resolution.
B: Two DNS servers are needed for redundancy.
D: Two DNS servers would be able to support thousands of clients and offers redundancy, three DNS servers would support more clients than are required on this network.
E: Two DNS servers would be able to support thousands of clients and offers redundancy, four DNS servers would support more clients than are required on this network.
F: Two DNS servers would be able to support thousands of clients and offers redundancy, five DNS servers would support more clients than are required on this network.

Q. 9
What is the minimum number of WINS server you should use in the new network?

A. 0
B. 1
C. 2
D. 3
E. 4
F. 5

Answer: C.
Explanation: There are Windows 98 clients. These clients must use WINS for name resolution.

Incorrect answers:
A: Windows 2000 clients are able to use DNS for name resolution. But there Windows 98 clients on the network and they must use WINS for name resolution.
B: One WINS server would provide name resolution for the downlevel Windows 98 clients. But Parnell Aerospace requires that all network services must provide redundancy for fault tolerance.
D, E, F: Two WINS servers would be able to support thousands of clients and would meet the required redundancy for in this network. We therefore do not need more than two WINS servers.

Q. 10
What is the minimum number of IP subnets you will require in your new network design?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: C.
Explanation: One subnet is needed for each building. A third subnet is needed for the connecting segment between the buildings.

Incorrect answers:
A: Using only one subnet would increase network traffic, and would make the routers obsolete.
B: A third subnet is required to link the routing interface between the two buildings.
C, D: There is no need for more subnets than three.

Q. 11
Which factor poses the greatest risk to your Windows 2000 deployment plan?

A. Disruption of SNA application access
B. Disruption of file and print access
C. Disruption of domain authentication
D. Disruption of client and server application access
E. Disruption of remote connectivity

Answer: A.
Explanation: The mainframe applications are mission critical. The SNA application provides connectivity to the mainframe.

Note: A System Network Architecture (SNA) Server acts as a gateway for transaction and queuing to IBM mainframes running S/390 and AS/400 for example.

Incorrect answers:
B: Disruption of file and print access is not mission critical.
C: Disruption of domain authentication is not mission critical.
D: Disruption of client and server application access is not mission critical.
E: Remote access for partners is not mission critical.

CASE STUDY NO: 4

STATE UNIVERSITY

Background:
State university offers undergraduate, graduate and professional degrees in Arts, Business, Engineering, Humanities, Law, and Sciences. The study body contains 10000 students, 6000 students are enrolled in undergraduate programs, and 4000 students are enrolled in graduate and professional programs. State university has 2000 faculty members, 2000 administrative staff members, offices, classrooms and dorms are located in 30 campus buildings

Organization:
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 administrates 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 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 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 department in the same school.

Some other 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 in the same building. However, in large schools, such as Arts, Engineering and Sciences, some departments occupy different buildings

Student Housing:

State University contains 25 dorms. Approximately 5000 undergraduate students and 500 graduate and professional students live in on-campus dorms. The rest of the students live off campus.

Existing 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.

Inside each building, network cables connect the wrong 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 email and Usenet news services.

WAN Connectivity:
State University provides dial up services to its faculty students, and staff and allows them Internet access through dial up connections.

State university has a bank of 512 modems that are all operating 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.

Dial Up services are supported for client computers running Windows 95 or Windows 98, NT and MacOS 7.5 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.

Network Services:
The computing services department hosts the main public Web site for State University and public Web sites for many of the administrative departments and schools. The schools of Engineering Law and Business host their public Web sites on their own Web servers. The computing services department provides Internet email and Usenet News services for state University.

State University contains the following DNS domains.

- stateuniversity.edu (for the entire University)
- engineering.stateuniversity.edu (for the school of Engineering)
- law.stateuniversity.edu (for the school law)
- mba.stateuniversity.edu (for the school of business)

Services department delegates the other three zones to DNS servers that are maintained by network support personnel in their respective schools. The DNS servers do not support SRV records

State University has the Internet domain name stateuniversity.edu and uses an internal network address of 172.10.0.0. Most of the computers on the network use statically IP addresses.

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 an 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)
- Floor 2 and 3: Department of chemistry (school of sciences)
- Floor 4, 7 and 8: Department of physics (school of sciences)
- Floor 5, 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
- Floor 2 and 3: Department of biology (School of sciences) containing = 400 computers
- Floors 4, 7 and 8: department of Mathematics (School of sciences) containing 350 computers

- Floor 5, 6, 9 and 10: department of computer science and Engineering (school of Engineering) containing 1200 computers

Building 34 houses the Registrar's offices and 350 computers. Building 56 has 200 computers on a single IP subnet that has a network address of 172.19.23.0. Building 67 has 400 computers on two IP subnets that have network addresses of 172.19.42.0 and 172.19.43.0. All the computers in Building 67 are in the same physical subnet. Dorm A has 175 single occupancy rooms. Dorm B has 200 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 10 Base T 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.

The computing services department wants to implement a policy that will limit all VPN sessions to two hours for all VPN connections.

The computing services department has decided to use Windows 2000 Routing and Remote Access to provide dialup 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 STATE UNIVERSITY

Q. 1
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 subnet masks to the appropriate subnet masks to the appropriate building or buildings.
(Use only subnet masks that apply. You might need to reuse subnet masks)

Answer:

-

Explanation: For every building we must decide the appropriate network mask. The network mask will be based on the number of computers (hosts) in each building. The subnet mask must support the correct number of hosts. Some buildings might have several subnets.

Dorm A
Dorm A has 175 single occupancy rooms; 175 students that would need internet access.
Eight bits would provide for the 175 hosts; 2**7=128 < 175 < 256=2**8.
The network mask would be 24 (32-8) bits,
Network mask, binary: 11111111.11111111.11111111.00000000
Network mask, decimal: 255.255.255.0.

Dorm B
Dorm B has 200 double occupancy rooms: 400 students that would need Internet access.
Nine bits would provide for the 400 hosts; 2**8=256 < 400 < 512=2**9.
The network mask would be 23 (32-9) bits.
Network mask, binary: 11111111.11111111.11111110.00000000
Network mask, decimal: 255.255.254.0.

Building 25
We have the following setup:
Floor 1 (Administrative offices): 40 computers
Floor 2, 3 (Department of biology): 400 computers
Floor 4, 7, 8 (Department of Mathematics): 650 computers
Floor 5, 6, 9, 10 (Department of computer science and Engineering): 1200 computers

This adds up to 2290 DHCP clients.

Twelve bits would provide for the 2290 hosts; 2**11=2048 < 2290 < 4096=2**12.
The network mask would be 20 (32-12) bits.
Network mask, binary: 11111111.11111111.11110000.00000000
Network mask, decimal: 255.255.240.0

Building 34
Building 34 houses 350 computers
Nine bits would provide for the 350 hosts; 2**8=256 < 350 < 512=2**9.
The network mask would be 23 (32-9) bits.
Network mask, binary: 11111111.11111111.11111110.00000000
Network mask, decimal: 255.255.254.0.

Q. 2
Which protocols or protocols should you support in the new network?
(Choose all that apply)

A. NetBT
B. NetBeui
C. TCP/IP
D. IPX/SPX
E. NBIPX
F. AppleTalk

Answer: A, C, F.
Explanation:
A: The network contains clients that require WINS. WINS require the NetBT protocol, NetBIOS over TCP/IP.
C: The TCP/IP must be supported since the University both needs Internet access and a scalable and routable protocol.
F: There are MacOS 7.5 clients on the network. These clients need the Appletalk protocol to be able to use the shared printers, which is a requirement from the University.

Incorrect answers:
B: NetBEUI is an old nonroutable protocol used in workgroups. It should not be supported in this network, which is a domain that includes several subnets and routers.
D: IPX/SPX, the protocol from Novell, should not be supported since there are no NetWare computers on the network.
E: NetBIOS over IPX should not be support, since there are no Novell resources on the network.

Q. 3

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 technical requirements only once.)
Design Component
Techical Requirement
Collapse
DNS strategy
DHCP strategy
WINS strategy
Router placement and configuration
Domain controller placement and configuration
Dial-up and VPN strategy
Firewall strategy
<<Move
Remove>>
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

Answer:

Explanation:

Design of active directory

The design of Active Directory would impact the Domain controllers; their placement and configuration..

Internal and external web sites

The decisions on which web sites should be internal and on which web sites should be external would impact the DNS strategy.

Some web sites might be internal and only accessible by students and staff who physically access the network at the university. Other web sites would be public and accessible to the whole Internet community.

Management of IP address allocation

Management of IP address allocation how IP configuration is automated would impact the DHCP strategy.

Access for research sponsors and partners

Remote access is accomplished either by Dial-up connection or by VPN.

Remote access restrictions for faculty and staff

Remote access restrictions would impact the design of Dial-up and VPN strategy.

Off campus users access the internal network

To limit and control the off campus users access to the internal network we must restrict the remote access, either dial-up or VPN access.

Access for research sponsors and partners
Research sponsors and partners should have limited access. They will only be allowed to use certain protocols and certain servers. This is achieved with an appropriate firewall strategy.

Note: A firewall can enhance security using various methods, including packet filtering, circuit-level gateways, and application gateways. Advanced enterprise firewalls, such as ISA Server, combine several methods to provide protection at multiple network layers.
Key ISA Server firewall features and technologies include:

- Multilayer Firewall
- Stateful Inspection
- Broad Application Support
- Integrated Virtual Private Networking (VPN)

Q. 4
What is the minimum number of primary Windows 2000 WINS Servers you will need in the new network?

A. 1
B. 2
C. 10
D. 25
E. 90

Answer: B.
Explanation: WINS is required for name resolution since there are down-level clients like Windows 98 on the University network. A minimum of two WINS servers should be used for redundancy purposes. Two WINS servers are also sufficient to serve all the computers on the University.

Note: Clients can, by definition, only be configured with one primary WINS Server. But we are talking but WINS servers on the network.

Incorrect answers:
A: We require a second WINS server to provide for redundancy.
C, D: Two WINS servers would easily be able to serve all the clients of network and would meet our requirements for redundancy. There is thus no need for any more than two WINS servers.

Q. 5

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
B. Use a single, static IP address that use network address translation (NAT)
C. Use a static pool of addresses
D. Use private addressing

Answer: A.
Explanation: DHCP is the preferred method to handle automatic IP configuration both locally and on dial-in connections.

Incorrect answers:
B: NAT is used to share an Internet connection to a local LAN. It has a DHCP allocator, which can provide the local clients with IP configuration. NAT cannot be with dial-in connections.
C: A static pool of IP addresses would be a less flexible and elegant solution compared to using a DHCP server.
D: Private addressing cannot be used to allocate IP addresses for clients dialing into the LAN.

Q. 6
Your design will include internal and external DNS servers that are configured as authoritative for the stateuniversity.edu zone. You need to specify how you should configure these DNS servers (Move the appropriate configuration tasks to the DNS server or servers where the tasks should be performed (Use only configuration tasks…)

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.)
DNS Servers
Configuration Tasks
Collapse
Internal DNS Server
External DNS Server
Add records for the university email 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 look-up
Manually add records for all computers in the university
<<Move
Remove>>

Answer:

Explanation:

Internal DNS servers

By allowing dynamic updates on the internal DNS Servers the administrators will avoid the labor of manually adding DNS records for the local clients.

The administrative effort of handling the Internal DNS servers should be delegated. This is done by delegating the engineering.stateuniversity.edu, law.stateuniversity.edu and mba.stateuniversity.edu zones.

The down-level clients, the Windows 98 clients, require WINS for name resolution.

Incorrect answers:

Manually adding records for all computers in the university would be a daunting administrative task. It would be better to use Dynamic DNS (DDNS) and allow dynamic updates on the internal DNS servers.

External DNS Servers

Records for all servers that should be available for the public external users should be added to the external DNS Servers. These records would include records for the university email servers, VPN servers and public web servers.

External public users should not be allowed to dynamically update and, register themselves, on the external DNS servers. That would be a security risk.

The engineering.stateuniversity.edu, law.stateuniversity.edu and mba.stateuniversity.edu zones are internal and should not be available to external users. Therefore they should not be delegated on the external DNS servers.

DNS, not WINS, is used for name resolution on the Internet.

Q. 7
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.)

Answer:

Explanation:
Currently a modem pool is used for remote dial-in access.
The computing services department wants to implement a policy that will limit all VPN sessions to two hours for all VPN connections.

Students
To meet the requirement of the two hour limit of all VPN sessions for all VPN connections the Set maximum session time condition must be used on the Remote Access Policy for the students.

Incorrect answers Students:
There is no requirement to set maximum idle time. Instead maximum session time is used to restrict the length of a remote access session, which is a requirement from the University.
There is no requirement to restrict the traffic with IP filters.

Faculty and staff
To meet the requirement of the two hour limit of all VPN sessions for all VPN connections the Set maximum session time condition must be used on the Remote Access Policy for Faculty and staff.

Incorrect answers Faculty and staff:

There is no requirement to set maximum idle time. Instead maximum session time is used to restrict the length of a remote access session, which is a requirement from the University.
There is no requirement to restrict the traffic with IP filters.

Research sponsors and partners
To meet the requirement of the two hour limit of all VPN sessions for all VPN connections the Set maximum session time condition must be used on the Remote Access Policy for the Research sponsors and partners.

By applying the Day and time restrictions on the Research sponsors and partners remote access policy, the security would be increased.

By using the IP filter restriction, security could be increased by restricting incoming and outgoing traffic on port level.

We should also specify the IP address of the Network Access Server..

Incorrect answers Research sponsors and partners:
There is no requirement to set maximum idle time. Instead maximum session time is used to restrict the length of a remote access session, which is a requirement from the University.

Incorrect answers:
Multilink isn't used at the University.
There is no security requirement to use strong encryption on the remote sessions.
This is dial-in access, so no telephone number has to be specified.

Q. 8
Your 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 building 58 and 67?

Your 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 building 56 and 67 by using 70/30 address split between the

DHCP Servers

Collapse

- DHCP Server A
- DHCP Server B

<<Move

Remove>>

Scopes

Scope 172.19.23.10 to 172.19.23.254 (excluded: 172.19.23.179 to 172.19.23.254)

Scope 172.19.23.10 to 172.19.23.254 (excluded: 172.19.23.10 to 172.19.23.178)

Scope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.23.179 to 172.19.42.254)

Scope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.42.10 to 172.19.42.178)

Scope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.42.179 to 172.19.43.254)

Scope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.43.10 to 172.19.43.178)

Superscope with:Scope 172.19.23.10 to 172.19.23.254 (excluded: 172.19.23.179 to 172.19.23.254) andScope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.42.10 to 172.19.42.178)

Superscope with:Scope 172.19.23.10 to 172.19.23.254 (excluded: 172.19.23.179 to 172.19.23.254) andScope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.43.10 to 172.19.43.178)

Superscope with:Scope 172.19.23.10 to 172.19.23.254 (excluded: 172.19.23.179 to 172.19.23.254) andScope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.42.10 to 172.19.42.178) and Scope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.43.10 to 172.19.43.178)

Superscope with:Scope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.42.179 to 172.19.42.254) andScope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.43.179 to 172.19.43.254)

Superscope with:Scope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.42.10 to 172.19.42.178) andScope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.43.10 to 172.19.43.178)

Superscope with:Scope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.42.179 to 172.19.42.254) andScope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.43.10 to 172.19.43.178)

Answer:

Your 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 building 56 and 67 by using 70/30 address split between the

DHCP Servers

Collapse

- DHCP Server A
  - Scope 172.19.23.10 to 172.19.23.254 (excluded: 172.19.23.179 to 172.19.23.254)
  - Superscope with:Scope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.42.10 to 172.19.42.178) andScope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.43.10 to 172.19.43.178)
- DHCP Server B
  - Scope 172.19.23.10 to 172.19.23.254 (excluded: 172.19.23.10 to 172.19.23.178)
  - SuperScope with 172.19.42.10 to 172.19.42.254 (exclude 172.19.42.179 to 172.19.42.254), Scope 172.19.43.10 to 172.19.43.254 (exclude 172.19.43.179 to 172.19.43.254)

<<Move

Remove>>

Scopes

Scope 172.19.23.10 to 172.19.23.254 (excluded: 172.19.23.179 to 172.19.23.254)
Scope 172.19.23.10 to 172.19.23.254 (excluded: 172.19.23.10 to 172.19.23.178)
Scope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.23.179 to 172.19.42.254)
Scope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.42.10 to 172.19.42.178)
Scope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.42.179 to 172.19.43.254)
Scope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.43.10 to 172.19.43.178)
Superscope with:Scope 172.19.23.10 to 172.19.23.254 (excluded: 172.19.23.179 to 172.19.23.254) andScope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.42.10 to 172.19.42.178)
Superscope with:Scope 172.19.23.10 to 172.19.23.254 (excluded: 172.19.23.179 to 172.19.23.254) andScope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.43.10 to 172.19.43.178)
Superscope with:Scope 172.19.23.10 to 172.19.23.254 (excluded: 172.19.23.179 to 172.19.23.254) andScope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.42.10 to 172.19.42.178) and Scope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.43.10 to 172.19.43.178)
Superscope with:Scope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.42.179 to 172.19.42.254) andScope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.43.179 to 172.19.43.254)
Superscope with:Scope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.42.10 to 172.19.42.178) andScope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.43.10 to 172.19.43.178)
Superscope with:Scope 172.19.42.10 to 172.19.42.254 (excluded: 172.19.42.179 to 172.19.42.254) andScope 172.19.43.10 to 172.19.43.254 (excluded: 172.19.43.10 to 172.19.43.178)

Explanation:

Background

On the 70/30 address split: Use the 70/30 design rule for balancing scope distribution of addresses where multiple DHCP servers are deployed to service the same scope. Using more than one DHCP server on the same subnet provides increased fault tolerance for servicing DHCP clients located on it. With two DHCP servers, if one server is unavailable, the other server can take its place and continue to lease new addresses or renew existing clients.

On superscopes: Use superscopes for multiple DHCP servers on each subnet in a LAN environment. A superscope allows a DHCP server to provide leases from more than one scope to clients on a single physical network.

Building 56 has 200 computers on a single IP subnet that has a network address of 172.19.23.0.

Building 67 has 400 computers on two IP subnets that have network addresses of 172.19.42.0 and 172.19.43.0. All the computers in Building 67 are in the same physical subnet.

Solution:
In this scenario we must use two different DHCP techniques to find the correct solution.
To provide redundancy we must use the 70/30 address split technique.
To support the two subnets in building 67 we must combine two scopes into a superscope.
We must combine these techniques.
The solution will consist of two scopes and two superscopes.

DHCP A
The DHCP A server is located in building 56.

Scope for building 56
The subnet of building 56 is 172.19.23.0, and there are 200 computers in this building
A scope including 70% of the IP addresses must be created for subnet 172.19.23.0. We do this by creating a scope for the subnet that has 30% of the IP addresses excluded.

The correct scope for building 56 on DHCP A is:
172.19.23.10 to 172.19.23.254 (excluded: 172.19.23.179 to 172.19.23.254)

Superscope for building 67
We must also create a scope for the subnet in building 67. We only want to include 30% of the IP address so 70% of the IP addresses must be excluded.

Building 67 has two IP subnets that have network addresses of 172.19.42.0 and 172.19.43.0.
We must use a superscope, combining two scopes. First we look at the two scopes for the two subnets.

First scope: 172.19.42.10 to 172.19.42.254 (exclude 172.19.42.10 to 172.19.42.178)
Second scope: 172.19.43.10 to 172.19.43.254 (exclude 172.19.43.10 to 172.19.43.178)
Then we combine them into a superscope and get the correct scope for building 67 on DHCP

A:
Superscope with Scope 172.19.42.10 to 172.19.42.254 (exclude 172.19.42.10 to 172.19.42.178) And Scope 172.19.43.10 to 172.19.43.254 (exclude 172.19.43.10 to 172.19.43.178)

DHCP B
The DHCP is located in building 67.

Scope for building 56
The subnet of building 56 is 172.19.23.0, and there are 200 computers in this building

A scope including 30% of the IP addresses must be created for subnet 172.19.23.0. We do this by creating a scope for the subnet that has 70% of the IP addresses excluded.

The correct scope for building 56 on DHCP B is:
172.19.23.10 to 172.19.23.254 (excluded: 172.19.23.10 to 172.19.23.178)

Superscope for building 67
We must also create a scope for the subnet in building 67. We want to include 70% of the IP address so 30% of the IP addresses must be excluded.

Building 67 has two IP subnets that have network addresses of 172.19.42.0 and 172.19.43.0.
We must use a superscope, combining two scopes. First we look at the two scopes for the two subnets.

First scope: 172.19.42.10 to 172.19.42.254 (exclude 172.19.42.179 to 172.19.42.254)
Second scope: 172.19.43.10 to 172.19.43.254 (exclude 172.19.43.179 to 172.19.43.254)
Then we combine them into a superscope and get the correct scope for building 67 on DHCP

B:
Superscope with Scope 172.19.42.10 to 172.19.42.254 (exclude 172.19.42.179 to 172.19.42.254) And Scope 172.19.43.10 to 172.19.43.254 (exclude 172.19.43.179 to 172.19.43.254)

Q. 9
How should you implement DNS to provide support Active Directory?

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

B. Install standard DNS servers in the Active Directory domains.
Configure them as primary servers for the corresponding zones
Configure the existing primary DNS servers as secondary servers

C. Configure the existing DNS zones and servers to host Active Directory domains

D. Install Active Directory integrated DNS servers in each Active Directory domains.
Configure them as authoritative for the _mscds state university.edu zone within the corresponding domain

E. Install DNS servers in the active directory domains
Configure them as secondary servers to existing primary DNS servers for the corresponding zones.

Answer: A.
Explanation: State University will implement a Windows 2000 Active Directory based enterprise network. This allows them to use Active Directory DNS. Some of the benefits:

- Support for the service (SRV) resource records. For example, this allows the netlogon service to find a domain controller for domain user authentication.
- Secure zone replication
- and generally less administrative effort

The namespace is not contiguous:

- stateuniversity.edu (for the entire University)
- engineering.stateuniversity.edu (for the school of Engineering)
- law.stateuniversity.edu (for the school law)
- mba.stateuniversity.edu (for the school of business)

Therefore we must configure the Active Directory integrated DNS servers as authoritative for the corresponding zones.

Incorrect answers:

B: Active Directory Integrated DNS servers are preferred. The existing DNS servers should be upgraded or replaced with Active Integrated DNS servers.

C: The Active Directory integrated DNS zones must be authoritative for their respective zones, since the namespace isn't contiguous.

D: It is not necessary to configure the DNS zones as authoritative for the _mscds state university.edu zone within the corresponding domain. This implies a new naming scheme.

E: Active Directory Integrated DNS servers are preferred.

CASE STUDY NO: 5

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 theatres. The central hospital building contains 3,500 employees. Of these employees 2000 require access to resources located on hospital computers. The outpatient clinic is located approximately 50 meters away from the 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 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 central hospital building. The network uses IBM LAN servers as its network operating system and OS/2 Warp as its client operating system. The network contains 100 client computers and provides 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 uses 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 with each other or with central hospital network. Other offices have the computers in the office are running either Windows NT Workstation 4.0 or 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 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 computer.

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. We want the hospitals to easily share the information such as scanned x-rays. That would allow patients to access their medical records on our web.

We have allocated funding to completely replace the network infrastructure and to provide links between all hospital buildings. Municipal hospital wants a terminal in each patients room, examination room and operation theatre.

IT MANAGER
Our network engineers spend too much time implementing fixes and patches on our operating systems. They spend so much time implementing fixes on our operating system, 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 our facilities: the central hospital building, the outpatient clinic, and the satellite medical center. We need a single network topology that can grow with our company.

We want to establish an Internet presence so we can serve our patients and staff more efficiently but we need control who has access to the network and to secure the patient records from un-authorized access.

We want to allow affiliated physicians at the medical office building to access our network resources. Because we do not control the office building or its network infrastructure, we need to design an access solution that will function regardless of the operating system the physicians have in their offices.

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.

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 the medical database and other resources. We need to be able to control this access to ensure proper usage, to maintain security and to minimize the amount of outbound Internet traffic on 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 environment. The protocol must be scalable enough to meet anticipated growth.
In the future the IT staff will need to connect to the Internet from external locations for remote access purposes. These IT personnel will be using Windows 2000 exclusively.

ANTICIPATED GROWTH
Within a year, the hospital management expects to begin construction on a new wing of central hospital building. The addition will contain 100 additional patient rooms, 20 additional offices, 15 additional examination offices and a new emergency room with trauma center. The construction will approximately take 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 building and satellite offices will be connected by means of dedicated and private T1 lines.
- *Internet Connectivity:* The central hospital building 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 computers will be upgraded to Windows 2000 Professional.
- *Logical Network:* A single Windows 2000 domain will be used.
- *Application Microsoft System Management Server (SMS):* 2.0 will be used for all network management and desktop support. Microsoft SQL Server will be used for all company databases, such as patient information and human resources.

QUESTIONS MUNICIPAL HOSPITAL

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

A. The network is difficult to manage and monitor.
B. The network is not usable.
C. The network suffers from poor performance.
D. The network requires upgrading.
E. The network suffers from too much down time.

Answer: A, D.
Explanation:
A: The main problem is that the patches and fixes of network require a lot of manpower. The CIO says, "Our IT environment is unmanageable." This means that the network is difficult to manage and monitor.
D: The CIO says “We are using outdated technology in the central hospital". Thus means that the network requires upgrading

Incorrect answers:
B: The network is usable, but it takes a lot of manpower to keep it usable.
C: The network is close to its capacity, but it does not suffer from poor performance yet. The main problem is that the management of the network takes a lot of manpower.
E: The network does not suffer from too much down time, but it difficult to manage.

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

A. New network topology.
B. Remote connectivity.
C. Inter-operability with the existing environment.
D. Internet connectivity
E. The cost of implementation.

Answer: A, B, D.
Explanation:
A: A new network topology is specifically required in this scenario. Funding has been allocated to completely replace the network infrastructure.

B: The hospital wants to share patient information. They want this information to be easily accessed remotely. Patients should be allowed to access their medical records over the web. They also want to allow affiliated physicians at the medical office building to access our network resources.
D: The new network design must provide for secure outbound Internet connectivity for internal users

Incorrect answers:
C: Essentially the old equipment will be replaced by new equipment so inter-operability with the existing environment is not of major concern.
E: This cost of the implementation is not a major concern since the budget includes enough funds to replace server and client computers.

Q. 3
You are designing an Internet access solution for the internal users. Which technology should you use?

A. Routing and remote access
B. Proxy server array
C. Proxy server
D. Down stream proxy server
E. Firewall

Answer: B.
Explanation: A proxy server would meet the requirements of the internet access.

- They are able to control the internet access and ensure proper usage.
- A proxy server can be configured only to allow certain ports. It can also be used to prevent access to certain web sites.
- They can maintain security on the internal network.
- Inbound ports can also be closed by a proxy server.
- They can minimize the amount of outbound traffic on the WAN links.
- The proxy server caches downloaded pages, and use the cache instead of the internet when it is appropriate. This saves network bandwidth.

A Proxy Server Array is preferred to a single Proxy Server because of load balancing and redundancy.

Note: An array of Proxy Servers is a group of Proxy Servers that are treated as if they were one server. You can even administer an array of Proxy Servers like a single server. Setting up an array is also the method used to enable distributed caching.

When accessing an array, a client determines which Proxy Server will service its request by sending a mathematical hash. This hash is a number derived from a formula that takes into account items such as the number of Proxy Servers, the URL requested, and the anticipated workload. By using this hash, the Proxy Server array will know which Proxy Server is best suited to handle the job.

Incorrect answers:

A: Routing and remote access isn't used for Internet access.

C: A proxy server array is preferred to a proxy server because of load balancing and redundancy is case of failure.

D: A downstream proxy server is a proxy server that is used inside the corporate network. It is used in conjunction with another proxy server, which gives Internet access.

E: A firewall is use to protect resources. It is not used to provide Internet access.

Q. 4

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

A. Allow direct dial-in connections that use MS-CHAP for authentication.
B. Allow direct dial-in connections that use EAP-TLS and smart card for authentication.
C. Allow direct dial-in connections that use PAP for authentication.
D. Allow VPN connections that use PPTP to secure communications.
E. Allow VPN connections that use L2TP to secure communications.
F. Enable IPSEC on all connections.
G. Require basic encryption on all connections.
H. Require strong encryption on all connections.

Answer: E, F, H.
Explanation:

E: VPN connections with L2TP with IPSec provide better security, than PPTP. VPN requires Windows 2000, but all IT personnel use Windows 2000 computers.

F: VPN with L2TP does not provide any security without IPSec. IPSec must be enabled on all connections.

H: Strong encryption would provide the best possible encryption.

Incorrect answers:

A, B, C: Municipal Hospital states that they will not provide for or allow access to the network by means of direct dial-up connections.

D: PPTP is an extension of PPP. PPP was designed for dial-up or dedicated point-to-point connections. PPTP would require one the following authentication protocols: PAP, MS-CHAP, CHAP, and EAP.
L2TP with IPSec would provide stronger data encryption than PPTP.

G: Strong encryption is more secure than basic encryption.

Q. 5

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. 255.255.240.0
B. 255.255.248.0
C. 255.255.252.0
D. 255.255.254.0
E. 255.255.255.0

Answer: E.
Explanation: For performance reasons Municipal Hospital need to limit the number of computers on any single subnet to 200. This would require eight bits for hosts (2**7=128 < 200 < 256=2**8).

And the network mask would be 24 (32-8) bits.
Network mask, binary: 11111111. 11111111. 11111111.00000000
Network mask, decimal: 255.255.255.0

Incorrect answers:
A: A network mask of 255.255.240.0 would provide for 4096 hosts, but Municipal hospital only want a maximum of 200 hosts on each network. This would not be the best network mask.
B: A network mask of 255.255.248.0 would provide for 2048 hosts, but Municipal hospital only wants a maximum of 200 hosts on each network.
C: A network mask of 255.255.252.0 would provide for 1024 hosts, but Municipal hospital only wants a maximum of 200 hosts on each network.
D: A network mask of 255.255.254.0 would provide for 512 hosts, but Municipal hospital only want a maximum of 200 hosts on each network.

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

A. 5
B. 6
C. 7
D. 8
E. 9

Answer: D.
Explanation:
Background
To determine the number we need to take the following facts in considerations:

- there is a requirement of a maximum of 200 computers on each subnet
- we need to determine the number of physical locations in this scenario

- we need to carefully calculate the amount of computers at each physical location. This must also include future growth.
- we need to take into account the router-to-router subnets that are required to connect the physical locations

Determining the physical locations
The central building and the Outpatient clinic is only 50 m. apart so they belong to the same physical location.
Satellite 1 is a physical location.
Satellite 2 is a physical location

Calculate the number of computers at each physical location
Central Building including Outpatient clinic

Central Building:
100 existing computers.
300 patients rooms.
60 offices.
45 examination rooms
10 operating theaters.
Outpatient clinic:
100 existing computers.
New Wing:
100 Patient rooms.
20 Offices.
15 Examination rooms.
1 Emergency room.

This sums up to 761 IP devices, which requires 4 subnets since there is a maximum of 200 computers on each subnet.

Satellite 1
75 computers. 1 single subnet.

Satellite 2
75 computers. 1 single subnet.

Router-to-router subnets
1 is needed to connect the Central location with Satellite 1.
1 is needed to connect the Central location with Satellite 1.
A total of 2 router-to-router subnets are needed.

If we sum up all the subnets we see that eight subnets are required.

Q. 7
How many WINS servers should you use in your design?

A. 0
B. 1
C. 2
D. 3
E. 4
F. 5

Answer: C.
Explanation: There are downlevel clients, Windows 98 and Windows NT, which cannot use DNS for name resolution, and must use WINS instead. Two WINS servers are used for redundancy in case of failure.

Note: Even though the Hospital eventually will replace the downlevel clients with Windows 2000 computers that does not need WINS, the downlevel clients must be supported during this phase.

Incorrect answers:
A: We need WINS for the downlevel clients.
B: One WINS server would not provide any fault tolerance.
D, E, F: There are less than 1000 clients in total, including future growth. Two WINS servers are able to supporter several thousands of clients.

Q. 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 network services.)

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 network services.)
Locations
Collapse
Central Hospital Building
Outpatient Clinic
Satellite Medical Center 1
Satellite Medical Center 2
Medical Office Building
<<Move
Remove>>
Services
DHCP
DNS
WINS
Domain Controller

Answer:

Explanation:

Central hospital building:

All the listed network services are need at the central location.
DCHP: provides the clients with automated IP configuration.
DNS: name resolution and a requirement for a Windows 2000 Domain.
WINS: there are downlevel clients, Windows 98 and NT 4.0 computers, which need WINS for name resolution. These computers will be used until the upgrade phase is completed.
Domain Controller: they are needed for the Windows 2000 Domain.

Outpatient clinic:

The Outpatient clinic is located very close to the central hospital building and is included in the same network. There is no need of any separate network services.

Satellite medical center 1 and 2:

For redundancy and network performance use Domain controller, DNS and DHCP.
WINS is not needed since two WINS servers at the central hospital building would service the whole network.

Medical office building:

The Medical Center does not need anything since it is not part of the Hospital network.
The Medical Center will be provided remote access to the Hospital network

Q. 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 configuration tasks to the appropriate component or components.

(Use only tasks that apply. You might need to reuse tasks.)

Answer:

Explanation:

Domain controller in the hospital

The Hospital network will be upgraded to a Windows 2000 Domain. The Dial-in permissions are part of the Active Directory and must be configured on a Domain Controller.

Remote access servers

We must configure the PPTP VPN Ports.

Configure remote access policies,

The remote access polices must be used to configure authentication and data encryption.

Require PAP for authentication

The remote access solution that must function regardless of the operating systems the physicians have in their offices. This forces us to use the PAP authentication protocol, since not all operating systems support MS-CHAPv1 and MS-CHAPV2.

Windows 2000 Application and file Servers

Application and file servers on not used to configure remote access.

Remote access client computers

The PPTP VPN Connections of the remote access clients must be configured to match the configuration on the remote access servers.

External firewall

We should configure protocol filters to tighten security.

Incorrect answers:

Configure L2TP VPN Ports
PPTP is used not L2TP.

Configure L2TP connections
PPTP is used not L2TP.

Configure and assign IPSec rules
IPSec only works with L2TP and PPTP is used in the solution.

Require MS-CHAP V1 for authentication
We do not know which operating system the RAS clients will use. We cannot require MS-CHAP V1.

Require MS-CHAP V2 for authentication
We do not know which operating system the RAS clients will use and therefore we cannot require that they use MS-CHAP v2. MS-CHAP v2 can only be used on computers using Microsoft operating systems.

Require basic or strong encryption.
With the PAP authentication protocol we cannot use basic or strong encryption.

Q. 10
You are designing the LAN and WAN topology for Municipal Hospital. You need to identify which components are represented in the following graph. 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.)

D
A
B
C
Internet
Outpatient Clinic
Central Hospital Building
E
F
G
H
I
J
Satelitte Medical Center 1
Satelitte Medical Center 2

You are designing the LAN and WAN topology for Municipal Hospital. You need to identify which components are represented. Move an appropriate network component to each letter in the network topology list. (Use only network components that apply. You
Topology List
Collapse
Central Hospital Building
A
B
C
Outpatient Clinic
D
Satellite Medical Center 1
E
F
G
Satellite Medical Center 2
H
I
J
<<Move
Remove>>
Components
CSU/DSU
Bridge
Brouter
Hub or Switch
Repeater
Router

Answer:

Explanation:
Central Hospital Building

A: Router
The router connects the Outpatient clinic and the Central Hospital Building.
The router also connects to a CSU/DSU.

B: CSU/DSU
The CSU/DSU works like an interface between the local network routers and the Internet.
This CSU/DSU connects to the router in the Central Hospital building and to a CSU/DSU on each Satellite Medical Centers.

Note: CSU/DSU [Channel Service Unit / Data Service Unit] is a piece of equipment that connects a leased line from the telephone company to the customer's equipment (such as a router). It performs line encoding and conditioning functions and often has a loopback function for testing.

Although CSU/DSU's look similar to modems, they are not modems, and they do not modulate or demodulate between analog and digital. All they really do is interface between a 56K, T1, or T3 line and serial interface (typically a V.35 connector) that connects to the router. Many newer routers have 56K or T1 CSU/DSUs build into them.

C: Hub or switch
The hub (or more likely hubs) or switch provides network access to the computers in the Central Hospital building.

Note: A Hub is a repeater and OSI device that transfers input data from one attached device to all other Hub attached devices. The device does not perform any filtering or redirection of data.

Note: A Switch functions in a similar fashion to a Bridge but typically makes use of multiple ports. In networks, a Switch filters and forwards packets between LAN segments and operates at the data link layer (layer 2) of the OSI Reference Model and therefore supports any packet protocol. In a loaded network a Switch is used to isolate data flow and improve performance.

Outpatient Clinic

D: Hub or switch
Provides network access to the computers in the Outpatient Clinic

Satellite Medical Center 1

E: CSU/DSU
This CSU/DSU connects to a router in Satellite Medical Center 1 and to the CSU/DSU that is connected to the Internet.

F: Router
The router connects Satellite Medical center 1 subnet to the rest of network

G: Hub or switch
Provides network access to the computers in Satellite Medical center 1

Satellite Medical Center 2

H: CSU/DSU
This CSU/DSU connects to a router in Satellite Medical Center 2 and to the CSU/DSU that is connected to the Internet.

I: Router
The router connects Satellite Medical center 2 subnet to the rest of network

H: Hub or switch
Provides network access to the computers in Satellite Medical Center 2.