Final Project: Scenario #1 Outpatient Surgical Center and Clinics

CIS313: Telecommunications and Computer Networks

Kary Mason

Spring Term 2009

Business Case Scenerio 1: **Outpatient Surgical Center and Clinics**

The following information provides business case information which was basis for analysis and decision making throughout the remainder of this paper:

1. Required LAN w/Bldg A in Skokie, have existing wired LAN only.
2. Expanding to 3 additional buildings. Each building's internal network will be using an Ethernet wired or wireless LANs: one facility in Chicago (Bldg B), the other facility in Lake Forest (Bldg C) and the other facility in Lombard (Bldg D).
3. Approx Users in Bldg A = 39 users + 4 networked printers.
4. 4. Approx Users in Bldg B = 23 users + 3 networked printers.
5. 5. Approx Users in Bldg C = 9 users + 2 networked printers.
6. Approx Users in Bldg D = 15 users + 3 networked printers with the potential to expand 15 additional users + 2 additional networked printers.
7. Bldg A DOES NOT have any Routers and will require WAN access to other new buildings. The other three new facilities will also require access to each other and to Bldg A's via a WAN.
8. Bldg A already has a server and Bldg B will need a new server while Bldg C and D will share Bldg A's server.
9. Approx budget allowed is $130,000; budget is set, no requests can be made.
10. Bldg A will require another additional server for backup purposes.
11. All sites will be connected via WAN of your choice (**FDDI or Leased Lines**).
12. Internet access will be needed for all sites but only Bldg A will have the Firewall installed.

BUDGET CONSIDERATIONS

EQUIPMENT	**GIVEN PRICING**
Small Router	$ 2,500
Midsize Router	$5,000
Enterprise Router	$9,000
Switch (12 port)	$1,000
Switch (24 port)	$1,900
Switch (48 port)	$2,700
Wireless LAN (45 clients only) $1,500	$1,500
Leased line circuits	$1,000
FDDI rings	$14,000
Server	$12,500
Firewall	$5,000
ISP Connection Fee $700	$700

Local Area Network Diagram Justification and Decision Process

Scenario 1 consists of four buildings located in the greater Chicago, Illinois area requiring local area networks (LAN) to provide outpatient surgical services. The buildings are referred to in the diagrams as Buildings A, B, C and D. The LAN diagrams are represented in a logical format to reflect the recommended plans. LAN development is based on the services that are provided at each of these four sites, existing infrastructure, future growth, backup redundancy and reliability needs, and allowed budget of $130,000. Each LAN will be comprised of wired Ethernet and wireless access points (WAP). The WAP will be connected to the Ethernet. Internet access will be provided at all four sites. The PCs, printers, server(s) and router in each building will all be physically connected to the switch by the wired Ethernet. The wiring used will be unshielded twisted pair (UTP), Category 5e. The specific recommendations for each site are as follows:

Building A is an outpatient surgical center located in Skokie, Illinois. It has 5 surgical suites with laboratory and radiology services. There are currently 39 users that will share 25 computers (PCs) and 4 networked printers. The users comprise of physicians, nurses, operating room technicians, laboratory, radiology, scheduling and registration staff. Building A has existing wired Ethernet LAN, including the PCs, networked printers, a 48 port switch, and one server. Two wireless access points will be installed in Building A to accommodate internet access for personal laptop computers and for future growth of the surgical center, since only 45 clients can access one WAP at a time. An additional server will be purchased and used for backup. It will be connected to the Ethernet and run parallel to the other server creating redundancy in order to prevent downtime. Another consideration for this redundancy is because Building C and D will be sharing Building A’s servers. One enterprise router will be chosen to provide internet access for each of the sites and allow Building A to have network access to the other buildings.

Building B is an outpatient surgical clinic located in Chicago, Illinois. There are 23 users that will share a total of 20 PCs and 3 networked printers. Each of the 10 exam rooms will have a PC to access the electronic medical records (EMR) and for clinical documentation. An additional 10 PCs will be used for scheduling, registration, and a work area for clinical staff to access information outside of the exam rooms. Building B will need Ethernet and one WAP installed. It will have a 48 port switch to accommodate all of the devices connected to the network. It will need to have a new server. A backup server will also be purchased and connected to the Ethernet to create redundancy and prevent complications from downtime. One midsize router will be needed to provide network access to the other sites. A midsize router will be purchased instead of a small router to accommodate future growth.

Building C is the billing office for Buildings A, B and D. It is located in Lake Forest, Illinois. There are 9 users each requiring a PC and they share 2 networked printers. Building C will also need wired Ethernet and one WAP installed. It will have a 24 port switch to accommodate all of the devices connected to the network. Building C will share Building A's server. Due to the small number of initial users, one small router will be needed to provide network access and still accommodate for future growth.

Building D is an outpatient surgical clinic located in Lombard, Illinois. It has a similar layout to Building B, the outpatient surgical clinic. The main difference between the two locations is the number of users. Currently there are 15 users and 3 networked printers. The plan is to expand to a size similar to the clinic located in Chicago and will include an additional 15 users and 2 networked printers. Since there will be a total of 30 users using 5 printers, a 48 port switch will be required for expected growth. Building D will also share Building A's server. One midsize router will be needed to provide network access to the other sites and accommodate for future growth.

LAN Redundancy and Reliability Recommendations

As described above, each LAN network for the four buildings will include accommodations for redundancy and reliability based on the allowed budget $130,000. Redundancy is crucial since this is a healthcare organization. Downtime needs to be prevented to provide maximum efficiency and effectiveness of patient care. To accommodate the need for reliability, Building A will have a redundant server running parallel to the other since this supports two additional buildings, C and D. Building B will also have a parallel server running. By running the backup servers parallel, it will eliminate the downtime for configuration and placement while maintaining patient care.

In addition to server redundancy, reliability will also be planned for through the purchase of backup switches and routers based on the budget. At this point, it is recommended that purchasing one enterprise router and three midsize routers would be beneficial. The enterprise router can be used for backup of Building A, since it will provide internet connection for all other buildings. The three other midsize routers can be used for backup or future growth for the other buildings.

Wide Area Network Diagram Justification and Decision Process

In Scenario 1, four buildings will require a wide area network (WAN) established to allow access of information between each of the sites. All four buildings provide outpatient surgical services and are located within the greater Chicago area. The WAN diagram is represented in logical format to reflect the recommended plans. WAN development is based on the services that are provided at each of these four sites, existing infrastructure, future growth, backup redundancy and reliability needs, and allowed budget of $130,000.

The WAN will be established using T1 leased lines made of copper. The T1 leased lines will provide the minimum bandwidth required for all communications between each site. The leased lines will be set up based on a full mesh topology. Each building will have a router installed based on the size and needs of each location with lease lines connecting to the other locations allowing communications from all buildings as needed. Recommendations for each building are as follows:

Building A is an outpatient surgical center located in Skokie, Illinois considered to be the headquarters for this organization. This building will require an enterprise router to accommodate communications between Building A and all other sites. Specifically, Building C and D will need to access Building A's server through the WAN. An internet service provider (ISP) will provide internet access to Building C and D through Building A. A firewall will be installed to provide security for incoming communications. A backup enterprise router will be purchased.

Building B is an outpatient surgical clinic located in Chicago, Illinois. A midsize router will be installed instead of a small router due to expected growth with an additional midsize router purchased as backup to ensure minimal downtime. An ISP will also provide internet access at Building B to provide redundancy and ensure minimal downtime if Building A's ISP fails. A firewall will be installed as an added layer of security and to accommodate potential growth of the clinic.

Building C, located in Lake Forest, Illinois, is the billing office for all services provided in Buildings A, B and D. A small router will be installed. A backup midsize router will be purchased instead of a small router to accommodate future growth.

Building D is an outpatient clinic located in Lombard, Illinois. Due to the planned growth of this building, a midsize router will be installed with a backup server (midsize) purchased, however, will not run parallel as in the building A.

WAN Redundancy and Reliability and Recommendations

As described above, a full mesh topology of leased lines will be used to provide redundancy between sites accounting for possibility of problematic leased lines maintaining communications and minimizing downtime of the WAN since the other buildings are reliant on Building A or Building B due to server location.

Additional redundancies addressed to ensure minimal downtime and reliability include the purchase of backup routers for each building and two different ISP providers. The additional routers will play a dual role addressing the concern of potential growth.

Since these four buildings represent outpatient surgical services, the medical providers will have the expectation of obtaining large amounts of clinical information, such as lab and imaging results in a timely manner. This information will be shared from building to building via the leased lines.

The files produced by imaging studies are high resolution with a significant impact on bandwidth requirements. Therefore, the speed of receiving this information will decrease.

Although the T1 leased lines will provide sufficient bandwidth to handle incoming communications, such as the imaging files, maximum speed is up to 1.544 Mbps. Recommendation is to upgrade the leased lines to Synchronous Optical NETwork (SONET). The disadvantage to the organization is the added cost, however, the advantage of rapid and efficient access of imaging studies and other clinical information should be considered.

The speeds of the SONET service are provided in tiers, so they can be upgraded as needed. Tier one provides a speed of 51.84 Mbps. The range can be increased to estimated speeds of 9,953.28 Mbps. The network will be monitored for actual usage of the T1 leased lines to see if the correct speed is being provided for maximum efficiency. This will provide the information required to review when an upgrade would be needed.

The leased lines will have a three year service line agreement as well as the ISPs. The connections fees with be a recurring cost every three years. The current budget proposal for this network is located in the attached spreadsheet.

Network Security

Security is a critical issue for the Illinois Surgical Services company due to the healthcare services it provides. Numerous laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), require that patient data be protected and secured. The U.S. Department of Health and Human Services enforces HIPAA laws through heavy fines and penalties for noncompliance. Recently, the U.S. government has proposed The Cyber Security Act of 2009, requiring more security standards of critical infrastructure for companies; therefore, these networks will have a combination of many security components to meet these complex requirements. The use of multiple layers of security will decrease the risk of unauthorized access to the network and further to patient information. Specific security policies and recommendations will address security threats.

In order to determine the specific security needs of a network, it would be critical to complete a risk analysis which provide understanding of areas of low risk (printers, internet) and higher risk (LAN, Servers). The information gathered from the analysis will guide the strategic strategy of the organization related to security needs.

Access Control Plan

Access control includes authentication, authorization and auditing. In order to control and ensure authentication, firewall have placed at the connection of the leased line access points protecting the network from outside intrusions from outside the network. Stateful Firewall Filtering will ensure that packets not initiated from an established connection are blocked and logged. In addition, the filtering will inspect packets to prior to be processed, permit connections from internal to external hosts and stop attempted connections from external sources.

Through the use of Access Control Lists by the IT network analyst any attempt to access the network from external sources will be monitored and logged. This is done through the use of an Intrusion Detection Systems (IDS) which is a monitoring system that looks at the network activity and access looking for suspicious packets. In addition, an Intrusion Prevention System (IPS) would be implemented for deep packet inspection. Use of these systems will require defined rules indicating external sites that are blocked from access as well as rules for external connections.

Server and Router Protection

The servers located in Buildings A and B are components of the network at high risk due to the confidential information it contains making at risk for viruses, worms and Trojan horse downloads as well as hacking. The back- up server is also at high risk since it is running parallel on the network . Protection will be provided by firewalls coupled with firewall software. Firewall hardware will be specifically located at Buildings A and B because they will provide internet access to Buildings C and D and patient information will travel from building to building via the WAN utilizing leased lines. Firewall hardware and software updates will be maintained per recommended guidelines by the network analyst. Firewalls will protect all the buildings from external threats by stateful firewall filtering, intrusion prevention system filtering, other filtering methodologies that stop complex attacks, such as denial-of-service (DoS). DoS attacks make the computer unavailable to its users by giving the computer multiple irrelevant attack packets, so the legitimate packets cannot be processed.   The firewall hardware will use application-specific integrated circuits (ASICs) that allow the processing speed needed for the IPS filtering.

Firewall filtering has rules for evaluating packets that attempt to open a connection. These rules are automatically applied unless specifically overruled by the access control lists. Each router will have an access control list specified by the security analyst.   Access control lists (ACLs) are sets of rules that modify the default behavior of firewalls. ACLs allow connections to some internal servers and prevent connections to some external servers. The security analyst will modify how the filtering mechanisms work depending on the needs of the organization.

In addition to firewalls, servers need to be set up to protect themselves through other hardening measures. These measures include frequently backing up data and implementing software updates called patches to prevent vulnerabilities. Timely patch installation will prevent hackers from exploiting the servers. Servers need to have anti-virus software installed with regular performance updates.

Each of the servers and routers will also have a digital certificate only allowing access to authorized personnel. Each user will be given a public key that everyone knows and a private key that only the user will know. Although digital certificates are costly, they provide strong security for the health information because the private keys are long and random.

The server and router rooms will be protected physically by code-compliant electronic locking devices. It is recommended that these locks are provided by a company that backs their products by customer support and a lifetime warranty. Each building will be physically secured after the hours of operation with a security alarm system.

Additional Protection Measures

An antivirus policy will be established for this organization. Since firewalls rarely do antivirus filtering, all e-mail messages with attachments, webpage downloads, and other traffic will be filtered to an anti virus filtering server. In addition to the servers, each PC and laptop will contain antivirus software. These programs scan arriving e-mail messages or other information for signatures or patterns that identify viruses, worms or other malware. The security analyst will ensure that recommended anti-virus software updates are being installed.

The PCs will also have other hardening measures. The security analyst will patch vulnerabilities and implement data backup. It will be important for the security analyst to teach client PC users to prevent errors and establish a policy that regularly discourages sabotage of hardening measures. The security policy will specifically warn users about phishing, a social engineering attack that entices users to enter user names and passwords or other information into authentic looking email or websites. Employees will be discouraged to open spam, unfamiliar email, and email attachments that may allow the installation of spyware or keystroke loggers, providing password or other personal information. Spyware and other threats can be installed without user knowledge to collect user information and other habits, such as data mining searches. As new employees are hired, they will need to be informed of security policies and procedures and be required comply with these measures.

Virtual Private Network

A virtual private network (VPN) will be established. The VPN will allow medical providers and other personnel remote access of patient information via a secured network over the Internet. The VPN will have Secure Sockets Layer/Transport Layer Security (SSL/TLS). SSL/TLS has gateways to allow an authenticated user reach any internal web server. This can provide access to any web-based application securely.

Authentication

Authentication will be used to prove an applicant's identity to a verifier. Dual layer authentication will be required for access through individual user names and passwords. The organization will enforce strict policy regarding password utilization establishing the use of strong passwords (8 character string of upper-case or lower-case letter, the digits from 0 to 9) for network access. The physicians and other medical providers will have electronic signatures for their documents that are authorized by a pin number. The organization will utilize an authentication tool (Digital Certificate) due to the sensitivity of information as user authentication.

Authorized Devices

Access to any network devices and/or applications with be defined based on the an employee's title which will define the job description and responsibilities. User profiles will be established based on this specific information will include what user access will be provided by the IT security. These profiles will define application as well as limits on functionality of an application and read versus write capability.

Mobile Device Security

Mobile devices such as laptops and smart phones can put healthcare data at risk, since these devices are easily lost or stolen. It will be mandated that all clinical information be accessed through a central server. Per policy, no saved clinical information will be allowed on any mobile devices.

Major Security Incident Response

Major incidents in breaches of private health information will be responded to by the computer security incident response team (CSIRT). This team will require members of senior management, security staff, IT managers, department managers, public relations and legal departments to review these incidents, establish plans to secure the network, punish the attackers, and ensure follow-up recommendations are being implemented.

It is also recommended that laptops use computer on a card technology for additional security. These cards can be inserted into the laptop and have their own battery, memory, processor, operating system, and software. The laptops will not work without the card, so a thief cannot simply remove the card to obtain access. IT can also remotely lock stolen and lost laptops. The cards can receive information from IT staff even when the laptop is switched off by working off their own battery power. IT staff can then see whether security features are properly configured remotely. The cards automatically encrypt all the data on the laptop. IT can remotely disable the encryption/decryption keys to further secure the information. The card also includes a Global Positioning System (GPS), which allows for device tracking. There will need to be dedicated server for this card technology used on these laptops. IT staff can troubleshoot laptops problems remotely through VPN connection and applications from a central interface. The cards have the 3G wireless data connectivity, so there can be an automatic VPN login when the laptop boots. The laptops can synchronize data with a database of medical information located at the company. The constant connection provides easier patch management.

As the surgical center, clinics and billing office expand, it will be important for the analyst to determine if more staff is needed to implement a secure network. If other buildings get their own ISP and establish connections to other buildings, then additional firewalls will need to be installed. As this organization grows, another security analyst may need to be hired to carry out the security needs of the organization.

Auditing

Through the use of log files maintained providing information on system access and network activity and utilization, analysis will be performed for any rogue activity. If suspicious behavior are identified in depth user audits will be conducted.

Capacity and Future Growth Analysis

In order to effectively meet the requirements of the Illinois Surgical Services organization, the network will be analyzed to determine if the current capacity meets the demands of its users. It is anticipated that this organization will expand to include other surgical centers and clinics and another billing office site. Network analysts will provide valuable insights on how to plan for future capacity and growth and manage the current network effectively, including improving throughput and increasing efficiency.

Traffic Management

Traffic management is needed to ensure that this organization has adequate capacity on its networks. This is accomplished through several ways. First, over-provisioning of devices increases network traffic further than what is currently needed. Second, it is vital to set priorities allowing latency-sensitive traffic to go first during congestion times. Third, quality of service guarantees reserving capacity for certain applications. Fourth, traffic shaping examines traffic at access switches to filter out unwanted traffic and ensure that applications do not take up their assigned percentage of the capacity.

Local Area Network Capacity

Software tools will be purchased to determine whether the Ethernet is fully saturated at its present capacity. Ethernet networks are considered fully saturated at 33 percent. This data will be reviewed and updates will be made accordingly. With the expansion of these services, medical providers will also have more need for remote connectivity. Wireless proliferation will be accommodated by adding more wireless access points (WAP), since only 45 clients can access one WAP at a time. Building A has two WAP in order to accommodate the 39 known users and the additional future users. Buildings B, C, and D will have one WAP installed due to its current capacity.

Wide Area Network Capacity

Building A and Building B will have an ISP installed to accommodate the present number of internet users and for future growth of the organization. In addition, Building B's ISP will act as a backup in case Building A's service fails. Buildings C and D may also need ISPs installed in the future if additional clinics and surgical centers are added to the wide area network. Additional users and more patient data will increase the demand on the bandwidth of the leased lines necessary for network communication. The bandwidth usage will be monitored through network software tools. Traffic data logs will be collected throughout the day to determine the usage peak times and other fluctuations. Special attention will be given to bottlenecks. If the T1 leased lines do not have sufficient bandwidth due to the usage needs, especially for imaging results, they can be upgraded to the SONET technology as discussed in the recommendation section.

Switch Utilization

Building A's switch has 48 ports. It has 39 users currently. The switch will accommodate the 35 devices known devices, including 25 PCs, 4 printers, 2 servers, one firewall, one router and the two WAPs. This leaves additional ports to be used as needed. An extra 48 port switch has been purchased to be used for future capacity or backup. Building B will also have a 48 port switch. This will accommodate the 23 users utilizing the 20 PCs, 3 printers, one WAP and two servers connected to the Ethernet. Building C will have a 24 port switch. There are 9 users each requiring a PC and 2 networked printers and one WAP. It will have a 24 port switch to accommodate all of the devices connected to the network.

Building D will have a 48 port switch. Currently there are 15 users and 3 networked printers. The plan is to expand to a size similar to the clinic located in Chicago and will include an additional 15 users and 2 networked printers. Since there will be a total of 30 users using 5 printers, a 48 port switch will be required for expected growth.

Router Utilization

Building A has an enterprise router and an additional router can be used for future growth. Building B has one midsize router to provide network access to the other sites. A midsize router will be purchased instead of a small router to accommodate future growth. Building C has a small number of initial users, so one small router will be needed to provide network access and still accommodate for future growth. Building D will have one midsize router. Although a small router could have been used, using a midsize router will accommodate for future growth.

Server Utilization

The servers will be monitored to determine if additional server space is needed through the network management tools. Email communication can fill up server space quickly. Each user will be allotted a limited amount of space. Buildings A and B will have two servers configured that run redundantly to the network. If the servers get overloaded with data, then additional servers will need to be purchased and added to the other buildings. Presently, building C will share Building A's server. If more sites are added, then an additional server may be need for that building due to all the billing information. Building D will also share Building A's server. Future growth demands may indicate the need for another server installed at Building D depending on the amount of clinical information.

Data Collection

Network capacity analysis and growth forecasts will be determined through data collection from various devices in the network using traffic management and shaping tools. The Simple Network Management Protocol (SNMP), recommended by the Internet Engineering Task Force (IETF), will be implemented. The network administrator will work at a central computer that runs a network management program, which is responsible for all of the managed devices, such as printers, switches, routers, user PCs, application programs and other hardware and software. The managed devices have software and hardware call agents that the network administrator can communicate with to obtain error information and general traffic statistics.

Specific problems can be identified through a specialized agent called the RMON probe (remote monitoring probe). The RMON probe can obtain information about the distribution of packet sizes, processed number of packets, number of errors and various error types, most active hosts, and other statistical summaries. Another tool called EtherPeek captures all packets arriving and leaving a NIC and provides many summarization tools, showing overall trends and specifics. Broad statistical trends over periods of time can provide key information allowing effective changes to be made to the network. After the data is collected, it needs to be validated to prevent flaws in the analysis, so the best options can be chosen for the network and organizational needs.

Other software, called OPNET, can be used to test network scenarios and perform realistic simulations for each building. Configurations can be altered to verify performance measures. Adjustments to the network elements will be made based on the findings of the simulation.

Financial Considerations

In order to make necessary changes to meet the organization's future requirements and growing network demands, the total cost of ownership (TCO) of the network will need to be considered and evaluated. The TCO is the total of all costs over the life span of the network, including the fully configured cost of hardware and software, initial installation costs, vendor setup costs, IT and end-user labor and ongoing costs such as upgrades and labor costs and fees for the service level agreements. Future LAN and WAN expansion may be a financial consideration for this organization based on the present limited budget availability of $130,000.

Recommendations/Conclusion:

The configuration built utilized $124,500 this fiscal year of the allotted $130,000 which could represent over estimates to ensure all needs were met during the initial LAN and WAN set up. The network and WAN in its current state will support significant growth due to the sizing of routers and switches and redundancies provided described for each building. Based on the business case information, there is minimal growth planned for the immediate future and, therefore, would recommend budgeting for growth in the next budget cycle. Request should include funding for network hardware/switch upgrades, hardware upgrades, upgrade to SONET as mentioned in the WAN recommendations. Depending on the growth of the organization, long term organizational goals and future plans of the IT infrastructure, the organization may want to consider the addition of additional WAP's and moving printer to a dedicated print server allowing additional space on the switches. Again, this is dependent on the organizational goal and if the plan includes the addition of wireless devices to expanded areas. Other considerations should be given to ensure upgrades and renewals of items such as antivirus software and network monitoring tools.