Project Scenario 1

Final Project

Network Plan and Documentation

Developed in partial fulfillment

of the requirements of CIS 313

Masters in Medical Informatics Program

Northwestern University

November 30, 2008

Gordon Bleil & David Burgess

This network plan was developed based on the initial information available from Scenario 1, basic Ethernet structures were set up in and between each of four buildings. The following is a synopsis of the expectation.

Current Status and Expectations

This company is currently located in 4 buildings. The building in Skokie (Building A) has an existing wired LAN but no router. The company would like to arrange for this to be the primary network management site and sole path for Internet access. The other buildings have no established networks. Overall company has the following equipment needs:

Building - Location	Users	Networked Printers	Servers	Firewall	Routers
A – Skokie	39	4	1 (existing) & 1 backup (new)	1 (new)	1(new)
B – Chicago	23	3	1 (new)		1(new)
C – Lake Forest	9	2			1(new)
D – Lombard	15	3			1(new)
D – (Expansion)	(15)	(2)			

The company has planned to spend about $130,000 on this project. They are not capable of getting more money than this at this time. The current plan is to develop the current equipment into the network, but would like to assure the plan will allow for extra development in building D. The Server in Building A will support the LAN's in Building C & D, but Building B will need it's own server. The company was advised that an FDDI is the desired method for communicating between buildings.

Network Plan and Recommendations

Diagram Description:

This diagram shows each of the 4 individual Ethernets, with connections between buildings primarily accomplished by Leased Lines. In the background, the FDDI is available as a backup network connection. The darker blue bars identify the Ethernets to be implemented, and the lighter blue bar attached to Building D is the expected expansion. The diagram is intended to show the overall characteristics and connections for the system. Detailed schematics will be required for final installation. Details of these connections are listed below.

Notes:

The legend included in the LAN diagram does not include the back up server and is not enumerated consistently with the number of users/printers as it represents the number of symbols on the diagram. Please refer to the symbol descriptions for details.

Decision making: In order to more effectively make decisions on this network, it was decided to develop an fictitious company structure.

Intended Usage: This plan was established for a data services company that provides database management for many small local businesses. They access data on remote servers through VPN's set up on their clients' computers. There is no import or processing of data from client computers onto their own computers. They have opted to utilize a single access point for the company to the Internet for security reasons. They have offices in several locations within the Chicago area in order to be closer to the businesses they work with. Since their clients are all small local businesses, they find it helpful to assist their clients personally. Their clients don't have a lot of depth in their own businesses. The buildings' different capacities are commensurate with the penetration of the market in that vicinity. The area around Building D has been growing rapidly and it is expected that new clients will be added soon.

User types: No high security users are anticipated beyond the CEO, CFO, CIO, and COO. Super users will include department heads.

Message types: General business messages are expected - email, sharing spreadsheets, text documents and databases. Routine security with these messages would be appropriate.

LAN:

User Computers: Not included in the network setup bid. Decisions on LAN structure are based on all computers being Desktops, hardwired.

Server Computers: Each of the 3 servers will have similar capacity with RAID 5 arrays allowing for limited risk of data loss. Capacities will allow for redundancy between sites and with the back up server in Building A.

Switches: The number of computers in each building is easily covered by one large switch. No workgroups were defined, but if any workgroup (e.g. administration, finance, specific department) identifies security concerns this can be divided accordingly. The number of ports needed for building C is less due to the small size of this office. Due to this small size it was decided to use only the router, which can provide the switching services without the addition of other equipment.

Access Lines: Category 5 UTP should be sufficient for transmission using the 100Base-TX standard since large volumes of data transmission are not anticipated.

Wireless Access: Considered not to be useful based on the intended usage and facility structure. Service providers in the field are able to access the company computers via VPN to the main office when needed.

WAN: Summary - Leased T1 lines will service the wide area network for the company. Building A will provide access to the Internet through an Internet service provider. Building B will access building A through a leased T1 line. This is necessitated by the need to utilize building B's server if the server in A fails. Building C and D will communicate to building A as the primary server through

T1 lines. Buildings C and D will have secure access to building B's backup server through building A. An FDDI system will provide backup if the current T1 lines fail.

Routers: The number of ports on each router was not defined, but presumed to be at least 8 ports (more likely 16).

Routers were set up for separate connection to building B due to the presence of its server.

C&D buildings will be under the management of the primary server in A, and routing is likely to be easier using this structure.

Trunk Lines: WAN access and trunk lines will be fiber optic. The nature of these connections (i.e. direct T1 type vs. secure Internet) is not defined but anticipated to be as diagrammed. The plan is to assure high speed, broadband access to the Internet, as this is a key component of the business.

The original plan had been to adapt an existing FDDI backbone for continued connection between sites. This was an inherited element from the company when it was purchased these buildings in the 1990's. Changes in Internet and Ethernet technology have caused replacement equipment for FDDI to be unavailable in the marketplace. Currently the FDDI system does remain functional but will need some restructuring for this network. Based on this, it was decided to move to a T1 line for connections between all buildings and use the FDDI as a backup.

Software: This in not included in the network setup bid.

Security analysis: To implement adequate security for this corporation further knowledge is needed. The corporation will need to prioritize their assets that require protection, e.g. is the company's information very sensitive or very valuable to another firm if stolen?

Risk level Assessment - Users of this system will be accessing the open Internet to a moderate degree, but the primary business is to access other company networks for management of their data. It will be company policy to require that each of these companies maintain appropriate security, and a portion of the service contract will include the right to verify this security effectiveness. The server software is expected to remain Windows' based, resulting in that anticipated moderate level of security risk. There will remain significant risk to the network from user access to the open Internet, email and internal user misuse/abuse.

Protection against theft/loss

Antiviral/Spyware - will be monitored centrally system wide with updates sent to each PC at log on. All elements of system will be scanned daily.

Access Control Plan

Physical Access -Access to the servers will be limited to IT personnel and department heads. A separate room with locking door will be used to house the servers and routers. The room will need to be vented with circulating air to maintain optimal server temperature control.

Servers - will be limited to authorized users - System operators, C-level personnel will have full access, but these devices will be in locked closets due to the risk of direct physical access by non-authorized persons.

PC's - will be limited to use by authorized users, but there is significant risk of PC's being left open. Employee policies to keep desktops locked will be recommended.

Routers/Switches - will be password protected but in relatively open areas. Risk of access is low.

Logical Access -

Firewall - offering ingress and egress filtering of requests to send data. This would protect the system from outside their network and help prevent unexpected data transmission outbound.

Internal management of files and file sharing: a system of authentication would require proof of identity prior to use of a resource.

Authorization of personnel to describe -

Specific actions users could perform to the system or files.

Potential time or location restrictions on access to files

Minimal identification requirements: user name and password for access to the network.

Password length recommended being at least 8 characters long and containing one numerical character. The password will have to be changed every thirty days.

If the company desires further security then biometric authentication will be utilized. This could include and is not limited to fingerprint scanners, facial recognition and iris scanning. These would require further financial funding to be implemented at the company's request.

External management of files and file sharing: not allowed

<u>Identification and Management of losses:</u>

Auditing of meta-data will allow the corporation to view and analyze user's preferences and usage of the system. This meta-data would also be potentially helpful to measure employee performance and points accessed.

Any discrepancies from anticipated usage would be evaluated with the user and appropriate manager. There would be 3 anticipated responses:

Access considered appropriate - no change, activity documented

Policy changes - reasons documented

Changes to user rights - reasons documented

<u>Hardware:</u> The Firewall in Building A will offer good protection for all sites from threats anticipated from planned access to the Internet. With no planned Wireless LAN connections risk of Wireless incursion would be limited to rogue devices.

Software: Security of the WAN will be done by VPN between sites. This will enable secure transfer of all data between sites. Other software (e.g. antiviral and spyware) was not included in the network setup bid. We would recommend using a network solution such as McAfee or Symantec.

Budget/Cost analysis: See attached spreadsheet. Additional items may be needed to assure reasonable redundancy and limited down time. Please see Recommendations below for further details. This proposal is felt to represent a reasonable balance between network needs and costs, keeping within the range established.

Redundancy/reliability: At the present time there is the capacity to set up RSTP (rapid spanning tree protocol) between the routers to Building B and Building C/D using the FDDI. This would provide protection against failure of either router or the leased lines. There is a back up Server in Building A, and the Server in Building B can be set up to accept full network function if needed.

Potential Points of Failure:

Server – limited potential due to routine back up plans, mirrored servers and secondary back up in building B.

Trunk lines – using the FDDI as a back up to Leased lines decreases this risk significantly

Internet access – will be through a single router (the one used for Building a-C/D) and single firewall

Routers – limited risk due to the ability to use the FDDI to bypass most routers, albeit with lower throughput. The Building A router to the firewall is the greatest single point of failure risk. Router failure in Building C is also a particular risk as it is being used for local LAN management as a well as Leased Line access. Recommendations include early purchase of a backup router and firewall.

Switches – if any uplink port fails, the users attached to this subnet will be able to use the back up FDDI to access the Internet. Total switch failure is less likely than port failures. There is excess port capacity to manage this. Total switch failure would be a significant risk for most of the LAN's, but critical PC's could be connected via router ports until this could be corrected.

Access lines and PC's – will fail only the local user and that person can move to another PC if needed, or perform other work until their device is repaired.

Capacity/Future Growth Analysis:

The current network design meets the needs of the business with minimal reserve. This initial reserve level was established based on current staffing and business activity levels. Each Ethernet was set up with the 10 percent reserve capacity regarding port connections. Traffic is not being monitored significantly at the present time. Based on the initial proposal due to market growth around Building D it has the immediate potential of adding an additional 15 users/computers and 2 printers without upgrading the network overall.

The capacity of the network is established, but the quantity of data throughput is not. After the system is in place and network statistics are obtained it will be possible to determine whether the switches chosen are sufficient to meet demand. Based on current assumptions of activity it is anticipated that throughput will be 25% below saturation, which would be 33% of total capacity (typical for Ethernet). Potential options when further data is obtained would be to unblock certain messages or develop alternative paths to smooth data throughput.

Other relevant factors related to hardware or systems:

All installations will comply with local and state fire and construction codes, including plenum cabling and conduit as needed.

Recommendations:

Hardware

Our recommendations include the purchase of additional routers for all buildings to increase the capabilities of the system. The purchase of additional routers will also allow future growth of the company. We would further recommend the purchase of an additional forty-eight port switch in building A or upgrading these switches to a higher capacity, with twenty four port switches in buildings B and D, with a twelve port switch added to building C. The cost of this would total $7,700.00. We recommended a lower capacity in the budget in order to allow about 10% flexibility in available funds at the time of installation. Implementing this decision will be based on the amount of aggregate throughput and the amount of blocking that may occur. Consideration may be given to 1000Base-T in the future.

Software

Security recommendations include the addition of AES cipher encryption for data transfer to the anticipated strong password requirements. An IT professional would have to be hired at company expense to oversee and manage the system. Their duties would include management of the servers, ensure protection of the system and troubleshoot immediate problems. The average cost per year would be approximately fifty to sixty thousand dollars for a salaried employee. If the company preferred an outside agency such as Symantec could provide this service on a contract basis. Additional management of the network will be need to be performed.

We would suggest a network management program. This program will be responsible for all managed devices on the network. These include but are not limited to printers, switches, routers, user personal computers and software. The program collects data from the devices and allows analysis from a central point. Once in use, an IT technician or agency would work with management to prioritize applications and shape traffic. High priority applications would be sent though the network without delay even during times of data congestion. Low priority traffic would be delayed during those times as well. Traffic would be managed at the network access points, shaping the traffic to filter unwanted traffic such as downloading music files, video files and the non business related software. These changes together will allow the network to function and fulfill the desired capacity for now and for the future of the corporation.