Anna Winkowski

CIS 313 Telecommunications and Computer Networks

June 4, 2008

There were four different scenarios that were available for the students to select. Since I have no experience with networking, I opted for Scenario 1 which was deemed appropriate for people like me. If Scenario 1 is less challenging, I can just imagine how difficult the other scenarios are. Although I must admit, I did learn a lot. The following are the deliverables for this project:

A. Diagram Justification

Although Scenario 1 called for an FDDI ring, which is an obsolete 100 Mbps token-ring network, I decided to use a PSDN, which would only require one private line running from each site to the PSDN carrier's nearest POP. Obviously in the real world, I would not do this without first explaining to my customer the reason for my actions. You might notice that there are two ISP connections in Building A. In the event that one of my ISP connections experience some technical issues, my other ISP connection should be able to provide the service without any interruptions. Because Building A was the only site with a firewall, it made sense to have the ISP connection from that site so that my network would be protected from attack packets.

B. Thought-process/Decision-making

Although Building B only had 23 users and 3 networked printers, I thought it would be to my customer's best interest to install a 48-port switch to accommodate for future growth. The same thought-process was used for Building C with only 9 users and 2 networked printers. Because a router is required in order to connect outside the building and to the Internet, I had to make sure that Building A is equipped with one. I used an enterprise-sized router for Building A because of the number of users in that building. Even though Building D only have 15 users and 3 networked printers at the moment, there is a potential to expand to 15 additional users and 2 more networked printers, therefore I used an enterprise-sized router as well. Because Building B and Building C do not have a lot of users at this time, I thought it would be best to use a midsize router. A PSDN, which is a carrier WAN, would allow the

facilities to access each other. The PSDN would also allow the other facilities to have access to the Internet even though the ISP connection is only in Building A. I have also equipped all four buildings with wireless LAN in order to have a competitive edge.

C. Budget/Cost Analysis

With a set budget of $130,000, I had to make sure that my purchases are not only aimed at the network's current needs but also set the stage for future expansion. All four buildings are equipped with a 48-port switch, with two spares available in case the other switches encounter some problems. Opting out of the obsolete FDDI ring which would have costs $14,000 freed some cash for other high dollar purchase such as another server. Although Building A has a back-up server and was sharing its existing server with Building C and Building D, I thought having another server which would be dedicated to Building C and Building D is a good investment. The goal to stay within budget was achieved based on the $2,300 remaining cash which I could use towards the purchase of Permanent Virtual Circuits.

D. Redundancy /Reliability

As my network diagram shows, there are two ISP connections in Building A. The reason for this is to make sure that the access to the Internet is not interrupted. In case one ISP connection fails, the second ISP connection will hopefully still be running. The PSDN is used to provide leased line connections between the local networks and the Internet. The PVCs allow communication between each site. Therefore, if there is a disruption in communication between Building B and Building C, Building A can still communicate with Building C using the PVC. Having some redundancy in my network will certainly help ensure the reliability of my data since there are alternate ways that a packet could reach its destination.

E. Change/Future Growth/Capacity Analysis

All four sites should be able to accommodate additional users and networked printers as each site is equipped with a 48-port switch. As previously mentioned Building D has a potential to expand to 15 additional users and 2 networked printers. In the event that additional support staffs are needed, they would be assigned to either Building B or Building C since it appears that both buildings have room for more people. As for the bandwidth, a V 9.0 modem is able to support a theoretical bandwidth of 56 Kbps but a Fast Ethernet supports a theoretical maximum bandwidth of 100 Mbps. It makes sense to start looking at modems that would support greater capacity in order to have greater performance.

F. Security Analysis

To address security risks in my network, the following security measures will be implemented:

I. Authentication – Typed to identify use of a username (account) on a computer.

A. Password Authentication

1. Passwords should be complex with mixed case, digits and other keyboard characters ($, #, !)
2. Passwords should be long
3. Use different passwords for different sites

B. Digital Certificate Authentication

1. Public and private keys
2. Digital certificate
3. Operation
4. Appraisal

II. Firewall – Drop provable attack packets

III. Hardening Servers and Client PCs – Setting up computers to protect itself

A. Server Hardening
   1. Back-up so restoration is possible
   2. Patch vulnerabilities
   3. Use host firewalls

B. Client PC Hardening
   1. Implement back-up
   2. Patch vulnerabilities
   3. Minimize applications
   4. Regular update of a good antivirus program

Because my network only has 1 firewall which is on Building A in Skokie, my proposal for the future would be to invest a firewall positioned at a each building to protect the network from cyber attacks.

G. Analysis of any other relevant factors related to hardware or systems

System upkeep is important to improve operating profitability, enhance productivity and reduce costs. Knowing what systems are deployed and what are operational, as well as knowing what measures are available to track each system will help gain visibility into the components that support the applications used by the network. Bandwidth optimization is also necessary as WAN users usually require more bandwidth than what is available on the circuit.

H. Recommendations

The following are recommendations that will be submitted to the board to further improve the system and give the network a competitive edge:

1. Invest in Firewalls for each site to protect it from cyber attacks
2. Purchase an additional server for Building C
3. Purchase enterprise size router for Building B and Building C
4. Purchase two additional 48-port Switch so each site has a spare switch
5. Optimize bandwidth to relieve congestion
6. Invest in Service Level Agreements for guarantees in throughput, availability, latency and error rate
7. Invest in a network shared storage which all buildings could have access to
8. Encourage use of dual security authentication by combining biometric authentication such as fingerprint scanning with digital certificate authentication
9. Assign dedicated staffs to manage the network and its security needs

I. Conclusion

It is my intention to create a network that is not only able to provide the services that is needed at the moment but one that will be able to accommodate future expansion in hardware and additional support staff. Requests for additional funding will be submitted to the board, if necessary.