Project Part VII: Final Project Paper with Final Budget Recommendations

Sharon C. Perelman

Northwestern University School of Continuing Studies

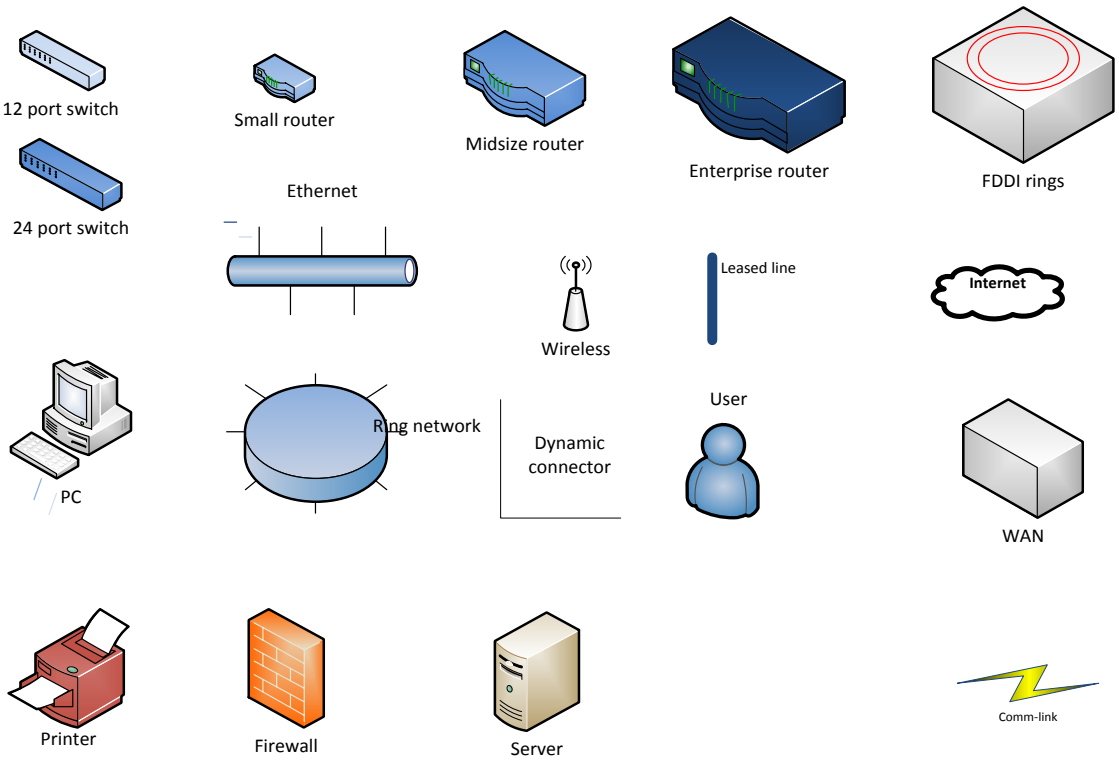
CIS 313-DL

Dr. Ken Woo

August 16, 2011

Project Part VII: Final Project Paper with Final Budget Recommendations\

Project part I: Network Legend



Project Part II: Local Area Network

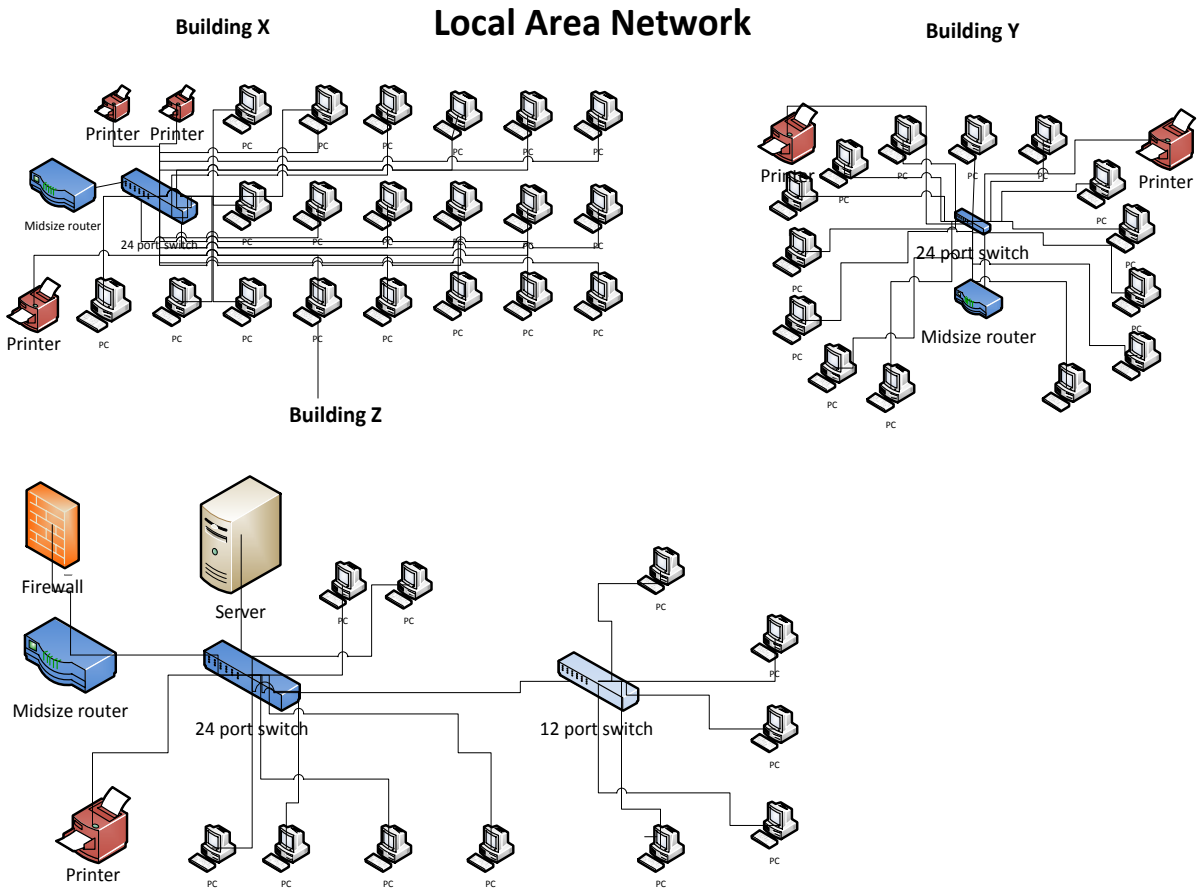
The first thing that I did prior to designing the LAN (Local Area Network) network diagram for scenario number four, was to look at the number of buildings, and the requirements from the client regarding the number of computers, printers, etc. I added those cost along with some of the fixed expenses such as LAN cabling. My thought process was to give me some idea of what type of revenue would be available for the remainder of the project.

Next, I explored options for the network topology; different topologies require different Ethernet standards. My first choice was the mesh network topology; it was the direct connections that appealed to me. If there is a problem at one site, an alternative pathway is available, thus the entire network does not go down.

I decided to use a Star and Extended Star topology since I felt the cost of additional switches in the Mesh network would be cost prohibitive at this phase. In the Star topology, all of the peripherals will be transmitting information through the center hub of the network, and then to the other users. If there is a problem with one of the users or connection lines, it remains isolated to that area, thus the network will still be up and running for the remainder of the users. I would be more concerned with this topology between the buildings, since a failure there could take the entire building off line.

In scenario number four, the buildings are new; therefore we may have some flexibility determining the location of the switches. We can strategically place the switches throughout the buildings, for current use as well as planning for expansion. Looking at the Ethernet physical layer standard, we may use either 100-BASE –TX or 1000 BASE-TX UTP cabling. In addition make certain that the switches are not greater than 100 meters apart.

Building X and Building Y each have a 24- port switch, which allows for significant growth in building Y, yet minimal in X. Building Z has 2 switches and will be capable of the anticipated additional users.



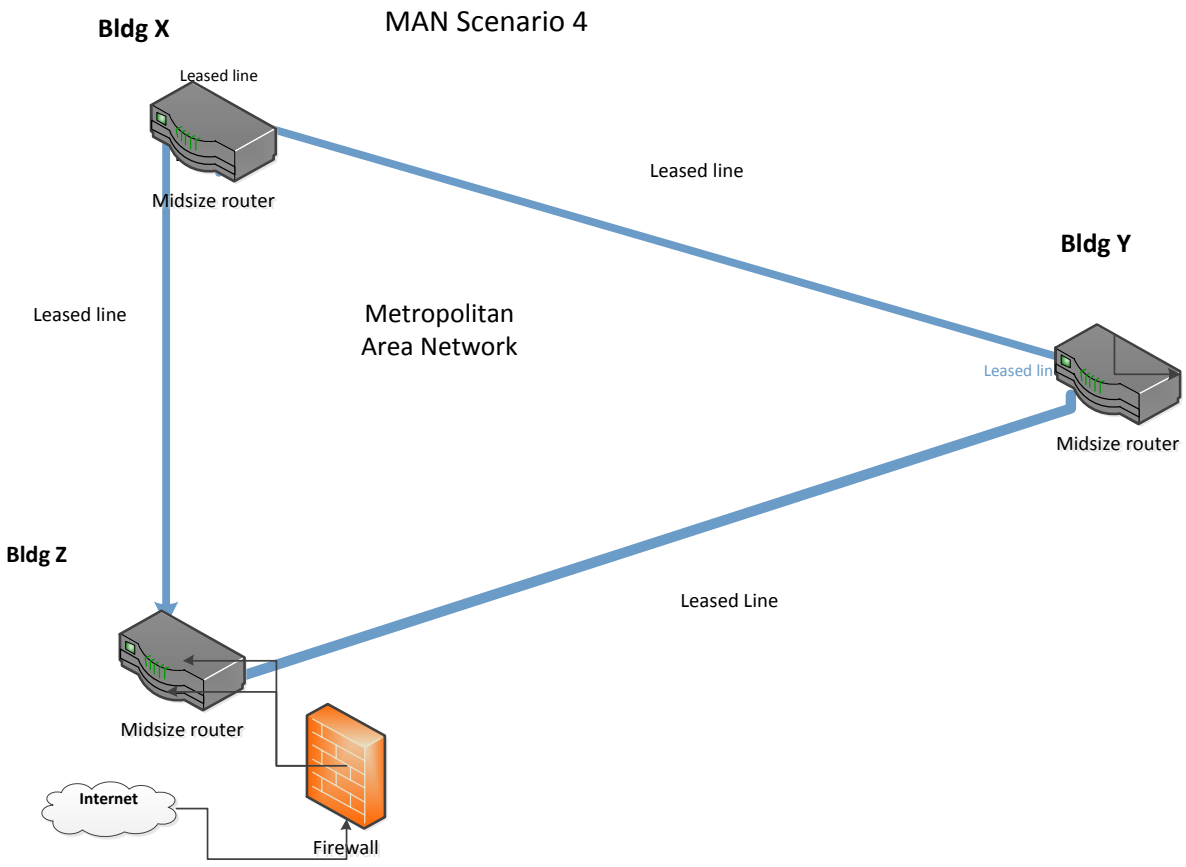
Project Part III: Wide Area Network

When determining how to set up my WAN (wide area network) that will connect the three buildings in my project, there were several factors that I took into consideration. The options I had to choose from were a WAN or a MAN (metropolitan area network). A MAN is actually a WAN yet its scope is on a smaller scale. WAN's can be used on a larger scale, even internationally; as a result, most WAN's operate at 256kbps-50Mbps, compared to MAN speeds of 1Mbps to 100Mbps.

Although the cost of a MAN is considerably higher the WAN, I chose the MAN for the following reasons. First I was already using Ethernet technology within the buildings for my

LAN's (local area network). Ethernet technology is fairly common therefore the learning curve in minimal. Making changes to the service can be accomplished fairly expeditiously, typically within a day or two. MAN will support both Data and Voice; if we decide to use VoiP that option would be available. Within a metropolitan area, I thought that a MAN was the best option for this project.

The next consideration is which type of topology I should use to connect the three buildings. The network topology is within the physical layer and there are different standards for each topology. As I stated in the previous phase of the project, I am concerned that I choose the best topology. I examined the Pure Hub-Spoke topology and quickly discounted it, since a problem with one of the leased lines could knock out service to an entire building. After careful consideration, I decided on the Mesh topology. Although it will be more expensive (due to the number of leased lines needed) I feel that it is the best option. If the company decides to add sites in the future, additional buildings can be added with leased lines expanding on this Mesh topology. Leased lines will connect the sites to each other and here we have several to choose from. Since I do not have information on cost, it is difficult to make a determination at this time. The options I am evaluating are T1, T2, Fractional and SONET (Synchronous Optical Network). T1 speeds are 1.544Mbps and use 2 pair Data Grade UTP, T3 is faster at 44.73 Mbps using optical fiber. Depending on cost, my choice would be SONET, OC3/STM1 or OC3/STM 4 at speeds of 155.2 Mbps and 622.08 Mbps respectively, and both using optical fiber.



Project Part IV: Capacity / Future Growth Plan

Prior to designing this network, I carefully analyzed the information given to me by the client. As I prepared my design, I evaluated the current needs along with the immediate growth requested, keeping in mind the budget as well. I wanted to use this design to maximize the potential for growth within the organization.

At the start, we know that Building X has 20 users and 3 network printers, in this building; I placed a 24 port switch. Not much growth is allowed in this current configuration, unless another switch is added. Building Y has 14 users and 2 network printers; the 24 port

switch will allow for additional users and printers. Although Building Z has the least number of users the anticipation is 14 additional users. My plan is to use Building Z as the primary location for additional users. Providing this building with a 24 and 12 port switch will allow for this expansion.

The mesh network topology I initially chose was in anticipation of future expansion. Although my initial set up cost using a mesh topology as my network design was a bit more expensive since it required 3 leased lines; my thought process was to allow for expansion of the organization and the ability to add locations. We could add a building with 2 leased lines connecting it via the expansion of this mesh topology. If one of the leased lines is to go down, the redundancy in the design allows the network to continue running.

Not knowing what type of organization I am working with makes it difficult to determine the type of bandwidth needed, therefore I am going to make some assumptions. First of all, my previous paper discusses the MAN network and I looked at T1, T2, and Fractional T lines. Considering the number of user, I would suggest T1 lines and can fractionate later if desired. I will assume all of the buildings will want Internet access, so this is where we need to look at bandwidth. The future is tending towards cloud computing services so we would want WAN bandwidth. This will allow for VoiP, and telepresence conferencing. Optimally with the number of users I would like to see one IT person minimal per location.

Project Part V: Security Plan

Now that our network design is complete, we need to consider security of this network. I asked myself what exactly is network security, why do we need it, and who is responsible for it? A proactive, not reactive approach to security will serve this organization well. Surely, it is the IT department that is responsible; however this is only partially correct. The IT people will

implement and monitor security, yet it is primarily a managerial responsibility.

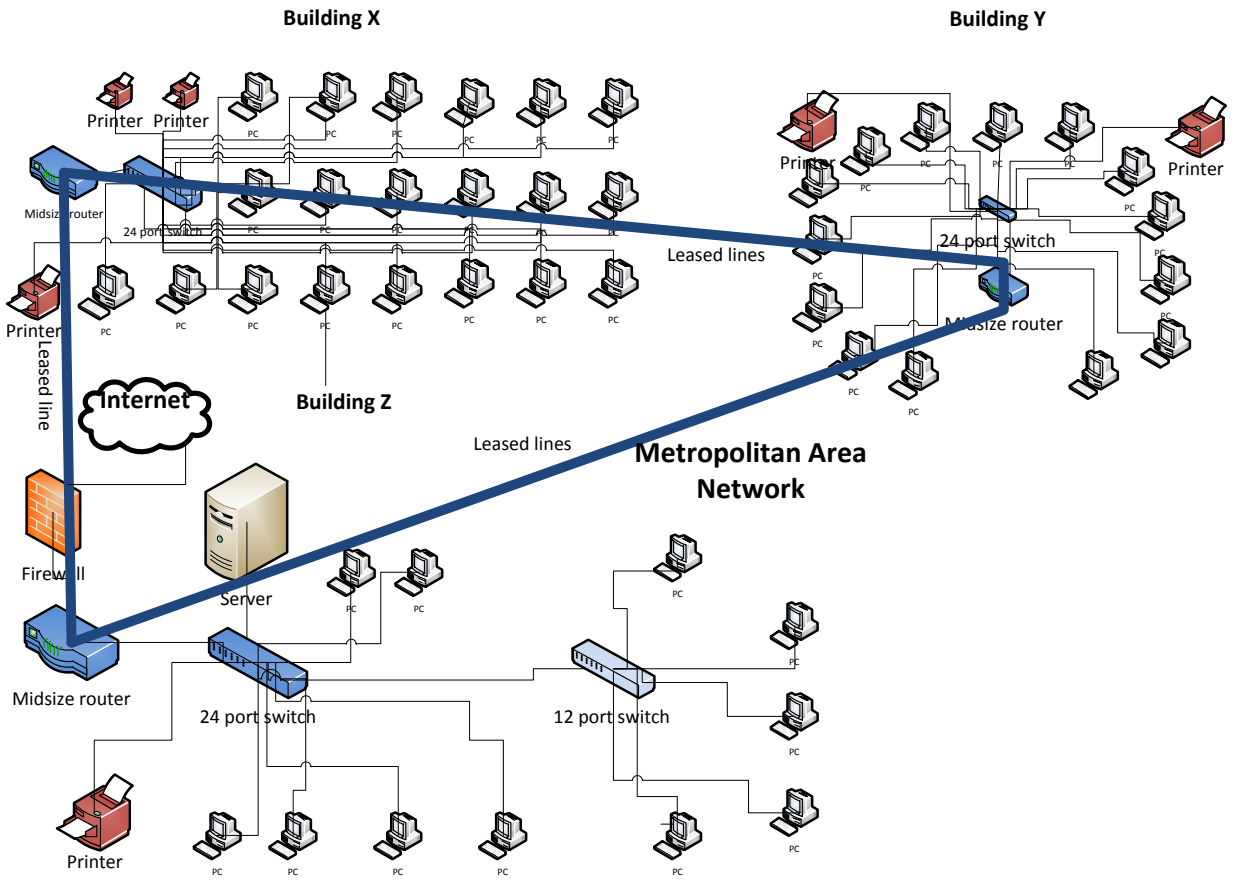
One must begin the process of securing a network with a Risk Analysis, asking how important is security to this enterprise and what the possible sequela of breaches to the system. It would be excessive for a mom and pop office to use iris scans to access their computers, yet this technology may be appropriate for the military. We need to be aware that the goal of security is not to eliminate the risks but to reduce them.

Different organizations require different levels of security. This particular company will have multiple locations. It is imperative that there are written policies regarding security protocols including Internet use, and opening attachments from email. A place to begin the security process is at the user level. Educating the staff on security matters ranging from password selection, to logging off their account when stepping away from a desk is imperative. The user authentication should not be a re-usable password. It should have a minimum of eight characters with a combination of letters and numbers. Anti-virus and antispyware software must be not only installed, but also maintained. Common threats include viruses, Trojan horses, worms and spyware. A firewall will block access to our network and it is located in the building with the server. In addition to all of these measures, a system should be in place to restore and recover data if there is a breach to the system.

The anticipation is that this company will experience rapid growth. I recommend a VPN. According to Panko, VPN's provides end- to-end protection between the client and the server along with end –to-end authentication. THE VPN will work well with the T1 lines that we established. In addition, we will be prepared if the organization would like users to have secure remote access to the network.

Project Part VI: Network Diagram

LAN/WAN Diagram



Final Recommendations

In Summary, I have completed the network project design based on Scenario number four. This scenario involved setting up the network plan for a new organization with three separate sites. Now that the plan is complete, and the budget has been evaluated, I have reviewed the entire project and have recommendations.

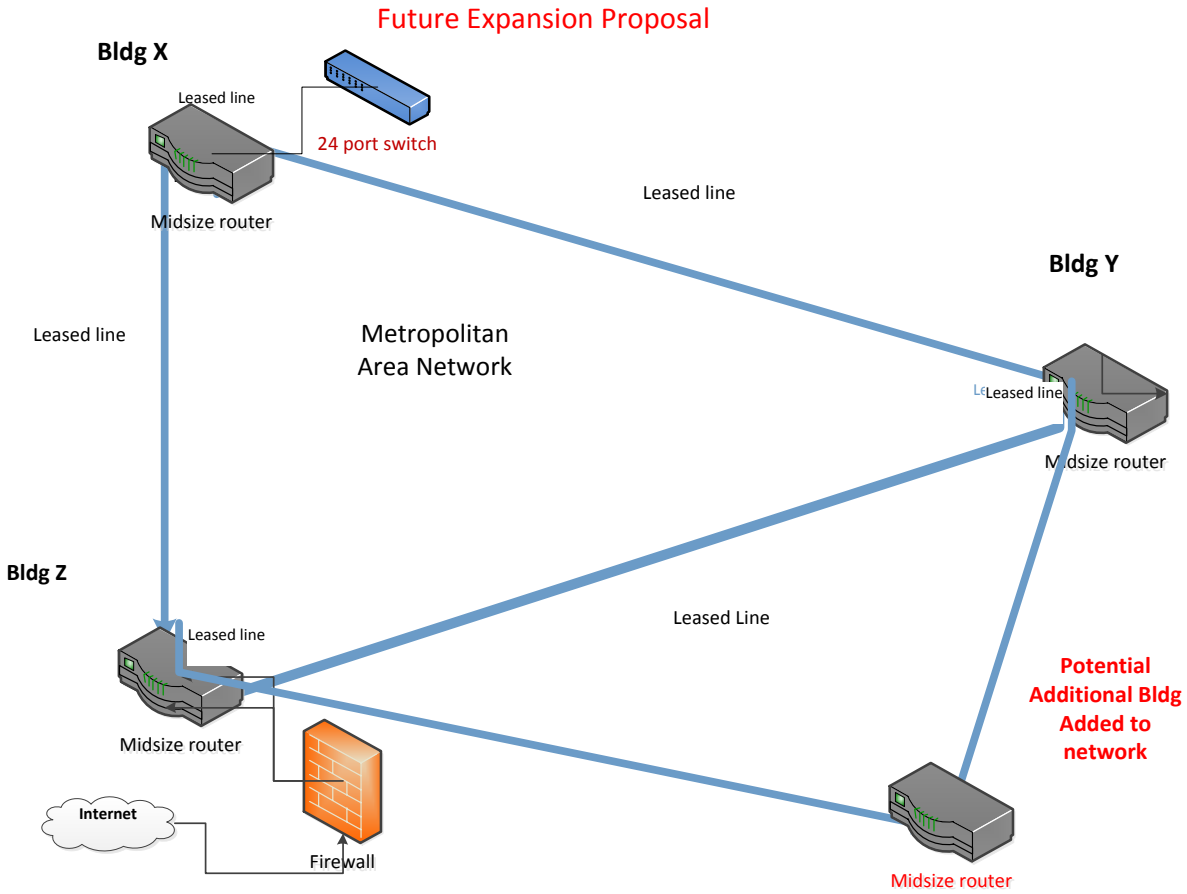
Although the overall growth capacity for the organization is good, one of the sites, building X, has limited ability for expansion in its current configuration. The simplest way to increase the capacity would be to add a 12 or 24 port switch, this will make the building on par with building Z as far as capacity. Beyond this, I pre-planned my network design for expansion once each location reaches capacity. Expanding on my mesh network topology, another location can easily be added with the addition of two leased lines connecting the location, along with a suitable router and switches, dependent upon the needs of this organization. With this expansion, I may think about adding an additional server and firewall to this new location. Another less expensive option is to accommodate the growth by allowing specified users to work from home and log into the network remotely; we prepared for this possibility by setting up a VPN that with will provide secure remote access.

This brings me to the next issue which is security. In regard to physical security, building Z has the server and we want to ensure that it is maintained in a locked room with limited access. Some ideas for this admission to the server can range from access cards to Biometrics. If access cards are used a system must be in place to for rapid disabling of an access card if lost or stolen. Two factor authentications provide an added layer of security, by not only requiring the access card, but a PIN number as well. A concern regarding cards, PINs, passwords is that employees often lose the cards and forget passwords. Once an employee terminates employment, we must be certain that passwords are de-activated and access cards are returned. Another option that may alleviate these issues is to consider is Biometrics. The advantage is that the user always has what they need with them. The lowest level in this category is fingerprint scanning. This would prove beneficial if remote users are working with laptops. The higher end Biometrics would include

iris scanning and facial recognition software. Depending on the security needs of the organization these may be considered.

I would recommend that a security team is assembled. A Chief Security Officer should be chosen and this person shall reside in the location where the server is maintained. In addition to this a security officer shall be located in each building.

The overall design and implementation of this project came in under the designated budget. From the initiation of the project; I sketched a complete plan of the fixed cost for each location. This was instrumental in the ongoing choices that I made in the design. It is important to look at priorities during the design process along with providing a base to the design that anticipates future needs.



*** See Attached Excel File for Budget

Scenario 4: Connect LAN, WAN, and users
A new company wants three new buildings interconnected together.
None of these buildings currently have networks.
Approximate users in Bldg. X = 20 + 3 networked printers.
Approximate users in Bldg. Y = 14 + 2 networked printers. Additional users are expected, but the number of users and printers are unknown at this time.
Approximate users in Bldg. Z = 11 users + 1 networked printer. An additional 14 users are expected, and one additional networked printer is expected.
Approximate budget allowed is $188,000. Capital requests can be made to the CFO.
Only Bldg. Z site will need its own server.
All sites will be connected via WAN of your choice (FDDI, frame relay, leased lines, wireless WAN, or MAN).
All buildings will require new routers.
All buildings will need to have their own wireless LAN only.
Internet services will be required for all buildings, but only Bldg. Z will have the firewall installed.

Budget Considerations for all four scenarios (USD):
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): $2,900
Wireless LAN (can support 45 clients only): $1,500
Wireless WAN (single microwave): $3,000
MAN (metropolitan area network): $7,000
Leased line circuits: $1,000 per used circuit
Frame relay circuits: $600 per permanent virtual circuit (PVC)
FDDI rings: $14,000
Server: $5,500
Firewall: $5,000
ISP connection fee: $700
LAN cabling costs: $38,000 per building
PC costs: $500 each computer
Printer costs: $100 each printer

References

Panko, R., & Panko, J. (2011). . In (Ed.), *Business Data Networks and Telecommunications* (8 ed.,). New York: Prentice Hall.