Assignment 10 Final Project Part VII:
Scenario 4 Project Summary, Budget and Recommendations

Frank C. Lynch, M.D.

David M. Schlossman, M.D.

Northwestern University
CIS 313 DL
Spring 2011

June 5, 2011

Final project scenario 4 involves the LAN and MAN connection of three new buildings (X, Y, and Z), none of which currently have networks. Each building will have its own wireless LAN only, and each building will require a new router. Building X will have 20 users and three networked printers. Building Y will have 14 users and two networked printers with a planned expansion to a user number that is unknown at this time. Building Z will have 11 users and one networked printer with an expected expansion by 14 users and one networked printer at some time in the near future. Building Z will also house a server and a firewall through which WAN connection and internet services will be provided for all three buildings.

A lack of in-depth understanding of the company's business and environment significantly limited all aspects of our network planning. In a real life network planning project, these subjects would be researched in depth and much more specific recommendations would be made. In order to proceed with the network design, we made three assumptions. The first is that all three buildings are on a company owned property such that there are no obstructions or legal right of way issues preventing cabled connections from building to building. The second is that building schematics will be supplied to allow calculation of the number and placement of wireless access points (WAPs) to provide a strong 802.11n Wi-Fi signal throughout each building. The final assumption is that the overall network demands for the enterprise in question will represent typical moderate business usage. Although the network will be designed for future growth in user base and application bandwidth requirements, we have not assumed that the network will need to support extremely high bandwidth time sensitive applications such as streaming video, VoIP, or online commerce. This capacity could be added later with hardware upgrades.

The attached Visio document shows our proposed LAN and WAN design using a physical connection scheme. The three buildings are connected using a campus wide MAN with the router in each building connected to the other two routers in a full mesh topology for redundancy. The routers will be interconnected using 10 Gbps Ethernet over optical fiber cables which will provide excellent throughput at distances up to 5 km and should be sufficient for the distances typically involved. Each building's router also connects by 1 Gbps wired Ethernet to a central switch which provides subsequent connection to the building’s wireless LAN access points and, in the case of building Z, to the server. Since building Z houses the server and firewalled connection to the ISP and Internet, it will require an enterprise level router to deal with the increased network demands funneled through it. All non-optical cable connections in the three buildings will be category 6a or 7 to match the campus MAN 10 Gbps capacity over shorter distances and allow maximum potential for future network growth.

No information concerning ISP services available to the firm was provided with the given scenario. Since the types of services offered vary greatly by location, two options will be considered. In each case, a single access line from building Z's firewall will connect the Campus to the ISP. The nature of the line (copper wire or optical fiber) will vary depending on the type of service selected. Ideally the ISP would provide and manage the additional hardware (FRAD& CSU/DSU or FTU/CPE) which will be required between the fire wall and the trunk line.

A traditional solution for WAN connection beyond the campus would be through a carrier that offers a frame relay type public switched data network. This type of service is relatively inexpensive and offers incremental speeds between 256 Kbps and 40 Mbps. The initial contracted service could be slower to contain costs with flexibility to increase service speed to accommodate future company needs. Robust quality of service agreements are typically offered with this type of service. Many carriers who offer this service also offer management services outside of the PSDN cloud to include management of on-site equipment, monitoring of network traffic, and network trouble shooting. Depending on pricing this could be an attractive alternative to internal network support personnel.

The major alternative to the Layer 2 frame relay solution is to use IP at Layer 3 for WAN transmission. Simply using the Internet as a WAN can produce very low cost per bit transmitted and grant access to other companies, but lack of security/reliability, absence of quality of service guarantees, and lack of management tools are major concerns with this approach. An IP carrier grade WAN would solve these problems, and provide much higher maximum speed than frame relay (up to10 Gbps), provide better convergence with internet services, and provide a more straightforward upgrade path to a unified communications strategy. For these reasons, we prefer the IP approach for WAN technology and will focus on this technology henceforth.

The network plan accounts for future growth. A 45 client capacity wireless network will be installed in each building. Based on planned expansion in building Z and a reasonable allowance for expansion in Building Y, all buildings still provide capacity for at least 30% growth in client numbers. This should be adequate for a five year time horizon, and it is very difficult to forecast accurately beyond that range. If future network demands require more than 45 wireless clients in any one building and such expansion cannot be allocated to one of the other buildings, the installed switches already have open ports for additional access points needed to upgrade network capacity. Depending on the size of the expansion, additional switches and segmentation into subnets may also be required. Maintenance and expansion of the network will require a significant ongoing and long term company investment well beyond the costs described in the initial budget. For example, the presence of only a single server creates significant network vulnerability from both mechanical and security standpoints. An upgrade adding servers in Buildings Y and Z should be an early high IT priority.

In addition to accommodating increased personnel (number of clients), a growth plan should also consider enhanced productivity (more work product on the network per unit time), enhanced software applications and new network capabilities (requiring more bandwidth), and client geographic expansion (requiring communication with other campuses). This requires an analysis of bandwidth. Our previous LAN specification called for the wireless network to be implemented on dual band gigabit access points running under the 802.11n standard. While the standard describes individual client throughputs up to 300 Mbps at short range using 40 MHz channels, typical throughput for each client under real world conditions and distances is unlikely to be more than 100 Mbps. If the entire 45 client capacity in a building were transmitting simultaneously, the required “worst case scenario” throughput at the wired switch and router in that building would be 4.5 Gbps. However, this situation is very unlikely to occur since typical network activity at each device consist of short bursts of data transmission intermixed with long periods of silence, and since 802.11 media access control protocols (such as CSMA/CA+ACK and RTS/CTS) put limits on simultaneous transmission. As long as large file downloads, media streaming for entertainment, and other high bandwidth activities are controlled, each client connection is only in use for about 5% of its rated capacity (Panko, 2008). At this utilization rate, a very rough estimate of the average combined throughput for a maximum of 45 clients in each building would be only 225 Mbps, well under 30% of the capacity of the cables, switches, and routers, which will be minimum 1 Gbps in all network hardware. The planned 10 Gbps fiber optic connection from building to building would be sufficient to support even the hypothetical worst case.

As with the other stages of this network plan, it is difficult to make concise and cost appropriate security plans without a full understanding of the nature of the company's business, its threat environment, and the subsequent consequences of a security breach. However, the provided scenario details and general security principles such as authentication, cryptography, use of firewalls, and host hardening can guide the formulation of a reasonable security plan.

Scenario 4 relies exclusively on a wireless LAN configuration and therefore presents a unique

set of security challenges. These challenges require careful judgment to achieve the correct balance of usability and security. Security starts with the design and installation of network. It is vital to carefully plan access point placement for strong signal coverage in all areas and to verify the calculations with a site survey when the network is activated. From a security standpoint, this process is also vital in order to minimize signal bleed beyond the intended area of network coverage. Defining the edge of the WLAN as closely as possible to the company secure premises reduces the network's vulnerability to security threats from unauthorized wireless access.

The first line of security within each building's LAN will be WPA2 enterprise level encryption with a strong password required to gain connectivity to the network. Access to the corporate network under the 802.1X standard will be supervised by a Radius Server running PEAP or one of the other extensible authorization protocols. The system will be designed to provide authentication, authorization, and accounting (AAA) for all users on the network, including user activity logs which meet applicable regulatory requirements for individual audit trails if necessary. To achieve even more stringent wireless security, on-site wireless access to the network could also require a VPN connection. In the event that the WPA2 encryption is compromised, VPN security protocols would remain active. Company policy will rigorously enforce the use of strong passwords changed every 90 days.

As shown in the network diagrams, there will be an enterprise-level firewall between the main campus server and the ISP. Without knowing the nature of the company's business, it is difficult to plan for an appropriate firewall functionality and topology. The scenario calls for a single server on the network. If the purpose of that server is to provide services exclusively to the on-site employees, it should be placed behind the firewall. If the purpose of the server is to also provide network services to its off-site customers or employees (such as web based services or FTP), it may be wise to place the server in a demilitarized zone (DMZ) such that those services alone would be exposed to the internet without exposing the entire LAN. In either case, the firewall will be capable of stateful filtering and intrusion prevention system (IPS) filtering. Off-site access to the LAN through the firewall will be supported only via VPN.

The server and other network hosts will require shielding against the consequences of a successful breach through the firewall, against threats introduced by user activities that violate security policy (e.g. plugging a personal thumb drive into a network host), and against equipment failure. The first and most important line of defense will be a plan for server data backup at intervals that make sense in the context of the company's business, likely on a daily basis. The daily backup of changed and critical files will be supplemented by total server backups at longer intervals with a copy of the data also stored off-site to insure against data loss due to physical damage to company premises. Comprehensive Internet security software which incorporates a host firewall, real time virus and malware protection and cleaning, e-mail scanning, web site rating for security threats, and other necessary capabilities will be installed and run on every company networked device capable of supporting it. The on-site IT personnel will be tasked with maintaining and updating this security software as well as updating operating systems and application software with patches that eliminate security vulnerabilities.

Explosive growth in the use of tablets, smartphones, and other network-capable small mobile devices adds new dimensions to the problem of network security. Although security issues used to be less frequent with such devices, their wide adoption has now made them targets for all the same malware and exploitation used against more traditional computing platforms. An infected device connecting to the LAN either on-site or over the Internet can create a security breach and potentially expose sensitive information. Although various devices run differing operating systems, many major security software vendors have developed mobile security suites, and one of these will be required on

all company provided small mobile devices. Company policy will also require such devices to be protected by a password or PIN at logon, to implement data encryption, to support local data wipe in case of excessive logon attempts, and to enable remote services (remote lock, remote wipe, GPS location) for use should the device be lost. Employees' personal mobile devices not managed by the company IT department will be restricted from sensitive parts of the LAN. Those wishing full access would agree to install recommended security software and allow IT staff to confirm that their devices comply with all applicable protocols.

Access to each building's network equipment room will be locked and secured to prevent building visitors or intruders from adding unauthorized equipment to the network and to prevent employees from making unauthorized modifications to the network such as the addition of extra access points. The IT staff will carry out network intrusion detection activities as part of their regular duties with the capability of detecting unauthorized hardware (such as access points) added to the network and capability of detecting port scans and other activity indicating unauthorized attempts to access the network. Some of these capabilities may be available as features of smart switches or smart access points.

Perhaps the greatest technical challenge of this network security environment is the potential requirement to provide easy convenient temporary network access with appropriate privilege levels to visitors, contractors, vendors, and other nonemployee personnel authorized to enter the buildings. The need to provide these services should be closely examined since they present significant security risks and introduce significant complexity into management of the network. If this functionality is required, we would recommend that it be implemented either using a hardware WLAN controller or through a software guest management system which communicates with the AAA system via an API or which may even reside in the Radius Server. Both types of products are available on the market, and either can create a VLAN for guest users. The VLAN then assigns and enforces the appropriate restrictions (only a certain number of hours, only certain areas of the company campus) and privileges (Internet only, Internet plus VPN to home office, Internet plus limited access to company network, etc.) for each guest.

We fully expect the stringent security mechanisms described above to be quite effective against the vast majority of hacking attacks, but the weakest link in the security shield of most business networks is the human user. Employees are the only element within the secured environment that can be coerced or fooled by hackers skilled in social engineering or can consciously decide to violate security rules. In fact, the majority of serious network breaches can be traced to human action internal to the organization. Our security plan addresses these issues through the five core guiding principles ("pillars") defined and analyzed by Kritzinger and Von Solms (2005). These include buy-in and support of security initiatives by senior management, development of a comprehensive set of written network security policies, employee buy-in regarding the importance of their role in network security, establishment of an ongoing employee education program regarding network security matters, and periodic comprehensive reporting of the results of the network security efforts back to senior management.

Submitted with this document is an estimated budget for the proposed network plan based on a provided list of available network components. While we recognize that there are commercially available products not included on this list that combine multiple device functions (such as a wireless firewall router), devices representing each individual function have been diagrammed and budgeted separately. The proposed estimated budget for this project as stated in the scenario is $188,000. Using the pricing information provided with the scenario, our proposed budget for the project is $184,500. However, we believe that the actual cost of the project could be closer to $165,800. The largest line

item in the budget is for LAN cabling. Although some physical cabling will be required for the project, we anticipate the cost per building to be much less since the majority of each building's LAN will be wireless. As a conservative estimate, we have reduced the the per-building LAN cabling budget by 25% to $28,500. Part of the budget surplus will be directed into the cost of installing an optical fiber connection to the ISP to allow carrier class IP WAN service with 10 Gbps capacity to supply maximum room for growth. Extra funds to ensure a fully modern WLAN including smart switches and smart WAP's capable of centralized management would also be a good investment. Additionally, our security plan calls for a Radius server for authentication, access and accounting. If that server process cannot be hosted securely on the single physical server specified in the scenario, the cost of an additional server may need to be budgeted. The security plan also calls for an intrusion detection/protection system which will require purchasing sensors and an IPS appliance (or other equivalent hardware), and pricing for this is not listed in the scenario. If the cabling costs do not produce the predicted savings, negotiations with vendors in regards to combined purchases could further reduce costs. Ultimately, if a negative budget variance exists, requests for additional capital can be made to the company's chief financial officer.

Our initial plan calls for a minimum of one, but preferably two, IT support personnel. It is likely that this number will need to be expanded with any future network expansion either in number of clients or complexity of services. In addition, a network operation center (NOC) should be established on the premises, to not only serve as the home for the IT support personnel but also as the home for the equipment required to monitor the performance and security of the network. The costs of the NOC are not included in the initial budget, but if they cannot be assumed along with the initial network configuration, creation of a NOC should have a high priority in future network expansion plans. The logical place for the NOC would be in building Z since that is where the server, the firewall, and the enterprise level router are located. Finally, our plan heavily stresses the security issues inherent to a predominantly wireless network and recognizes that network security is primarily a management issue. Therefore, it will be vital to appoint a management level employee to serve as the company's chief security officer. The role of this person would be to serve as liaison between IT and non-IT employees in matters of security and to serve as an advocate for security matters at the highest levels of company leadership. With growth in the company and its information technology needs, such a position might eventually evolve into a Chief Informatics Officer in the company's management structure.

References

Kritzinger, E., & von Solms, S.H. (2005). Five Non-Technical Pillars of Network Information Security Management. *IFIP International Federation for Information Processing*, 175, 277-287.

Panko, R (2008). *Business Data Networks and Telecommunications, 7th Edition.* Upper Saddle River, NJ: Pearson Prentice Hall.