Summer 2005

The Design And Implementation Of The Megacomm Media Center'S Extranet

Kenneth J. Quigley
Regis University

Regis University
School for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Disclaimer

To ensure the privacy of the organizations involved with this project, the author used fictitious names and removed any information or characteristics that could be used to identify or link this project to a particular organization. Any similarity to an actual organization is purely coincidental.

Abstract

The Purpose of this thesis is to document the project that designed, configured and implemented a network infrastructure that provided the capability to segment, current and future, non-MegaComm Media Center companies that need IT services from the MegaComm Media Center (MMC) and provided Business-to-Business connectivity.

The MegaComm Media Center, located in Littleton, Colorado, is a wholly owned subsidiary of the MegaComm Corporation. The MMC provides unique services to the cable industry. In support of these services, the MMC hosts several tenants. Prior to this project the tenants had access to internal MMC networks. The MMC also has several vendors that provide services or content for MMC programming. These vendors had unfettered access to MMC networks. This situation created concern with both the MMC network security department as well as MegaComm senior management. To mitigate the risks created by having external entities accessing MMC networks, the extranet project was commissioned.

The goal of the project was to design and implement an extranet that would provide the proper functionality for both the tenant and the vendors. The project followed the System Development Life Cycle and required approximately seven months to complete. The budget for the project was $350,000.00 and required a project team of four individuals. The author was the project manager as well as the network engineer for the project.

The project completed on time and within the established budget. The final deliverable was a functioning extranet that provided the necessary support for the

tenants and vendors. Additionally the extranet met all of the established networking and security requirements. The final network was flexible, expandable and extensible due to its modular design. The project was extremely successful.

CONTENTS

Table of Figures

List of Tables

Chapter 1

Introduction

1.1. Problem Statement

In the wake of the recent accounting scandals new legislation such as Sarbanes-Oxley has increased the complexity for those companies that provide shared IT services. The MegaComm Media Center (MMC) is one such company. Within the MMC there are several tenants, vendors and customers that receive IT services such as Email, storage and Internet access through the MMC IT infrastructure. Additionally, the MMC has undertaken several projects that require **Business-to-Business (B2B)** connectivity to both customers and vendors. In light of the current regulatory climate, it is necessary to ensure that not only are the non-MMC companies separated from the MMC networks, but that they are also sufficiently separate from each other. The MMC IT infrastructure was built on the shared services model and there is no immediate method for segmenting the non-MMC companies given the existing networks. There is also no current method to provide B2B connectivity to customers and vendors. This thesis documents the project that designed, configured and implemented a network infrastructure that provided the capability to segment current and future non-MMC companies that need IT services from the MegaComm Media Center and provided B2B connectivity.

1.2. Existing Situation

The MegaComm Media Center (MMC), located in Littleton, Colorado is a wholly owned subsidiary of the MegaComm Corporation. The MMC provides unique services to the cable industry. These services include the packaging and retransmission of over three hundred channels of content to MegaComm and other cable distribution companies.

The MMC also produces original content. Several TV shows, concert specials and even a movie have been filmed and produced at this facility. In compliment to this capability, the MMC provides office space and IT services for television networks and production companies.

In addition to the origination, packaging and distribution of television shows, the MMC is also MegaComm's main distribution facility for on demand content, which is previously produced and aired TV shows, movies, concerts, sports and etc. that are made available to the end consumer as an on demand product. This system impacts the network infrastructure of the MMC in that there are now additional content providers that have equipment on the MMC networks that the external companies control and to which the MMC has no access.

The On Demand content is distributed through the MegaComm Content Delivery Network (MCDN). The MCDN is a system for ingesting, processing and distributing content to local cable systems throughout the United States. The initial stages of the MCDN were confined to MegaComm cable systems only. Because all of the involved systems were connected through a common MegaComm business network, there were no problems with communications between the receiving devices at the local cable system and the distribution engine located at the MMC. Later, stages of MCDN development brought the On Demand capability to Non-MegaComm cable systems. Sending this type of B2B traffic across the MegaComm business network was not secure. The MMC had no existing method for facilitating this communication.

Prior to the implementation of the extranet gateway, the services provided for the tenants, business partners and vendors were co-mingled with the services used for the

day-to-day operation of the MMC and the rest of MegaComm. There was no logical or physical separation between the MMC networks and the external companies. Nor was there any separation between the external companies. Those systems that were on the MMC networks and not monitored or controlled by MMC personnel represented a significant security risk. Any type of malicious software could have been running on those systems.

A key factor in the design of a shared services model is the current regulatory climate. One piece of new legislation that potentially impacts this model is the Sarbanes-Oxley Act of 2002. This act deals primarily with financial controls and proper accounting practices within publicly traded companies. However, in section 404 of the act, a company's management is required to "include in their annual reports a report of management on the company's internal control over financial reporting". (Koch, 2004) Since the majority of financial controls and reporting have now been automated, this section has been interpreted by senior management within companies to mean that they may be liable if there are not sufficient IT controls in place to ensure the integrity of financial systems and reporting. A shared services model, like the one that was present at the MMC potentially violated this act due to the multiple companies sharing the same Email system or network storage.

The security issues of having systems that could not be accessed, the need to provide secure connectivity to non-MegaComm cable systems for the MCDN system and the regulatory situation led the senior management of MegaComm to require the development of a solution that adequately addressed all of these concerns. In response, the extranet gateway project was created.

1.3. Project Goals

This project had both business and technical goals. The business goals were to provide for the separation of MegaComm and non-MegaComm entities, while providing secure, isolated, as needed, access to MegaComm resources for non-MegaComm entities. A further business goal of the extranet gateway project was to maintain the current level of information system services for the MMC tenants. This included domain services, naming services, internet access, web hosting, email and etc.

The technical goals of the extranet gateway project included building a modular design that was flexible and extensible. The original requirements for the extranet gateway were to provide for two functional areas: the tenant segment and the content provider segment. However, there were a significant number of projects active within the MMC at the time of the initial design. To provide for economies of scale, it would be advantageous to design the extranet so that new projects could be added easily and at a minimal cost. A modular design for the gateway ensured that new projects could easily be added with minimal additional cost.

The extranet gateway was required to provide the tenants the existing level of services they were receiving. It was not difficult to predict that there would be additional services and functionality required in the future. Therefore, the extranet gateway had to be designed so that the services and functionality offered could be extended.

1.4. Project Barriers and Issues

The concept of providing secure independent access to the MMC for vendors, customers and tenants had been discussed for several years. There had been many architectures proposed. Like the previous designs, the extranet gateway faced several

barriers to implementation. First was the lack of funding. Although the businesses acknowledged the need for and the benefits of having a secure access method, none of the senior managers were willing to sponsor the project. The main argument for the lack of support was the initial cost. Senior management understood that, once built, the extranet would provide a very cost effective way of providing future projects secure external connectivity to the MMC. However, everyone thought the initial cost to provide the proper security and functionality too high. Finally, a project large enough came along to absorb the initial implementation costs.

A second barrier to implementation was the political battles over the extranet. The senior director that supported the initial design and cost of the extranet felt that it should only support his project and that any other project placed on the extranet needed his prior approval. One of the goals of this project was to provide a flexible modular design that would allow for the simple and cost effective addition of future projects that needed secure external connectivity. Requiring each project placed on the Extranet to be approved through a single director severely limited its functionality and curtailed the ability of the network engineers to provide cost effective flexible designs.

It is often humorously noted that there are really nine layers to the **Open Systems Interconnect (OSI)** model, the top two being politics and money. Interestingly, there were no real technical barriers to the implementation of this project. Both of the major barriers fell into either money or politics. One of the benefits of an education from Regis University is that in the Master's program they teach more than the technical side of networking. This came in very handy while overcoming the political barrier to implementation. The sponsoring director was concerned that others were benefiting from

equipment he paid for, and that his projects would not have the required bandwidth or processing resources. Acknowledging these concerns, the project manager presented a solution that was acceptable to the senior director. On any future projects that utilized the extranet gateway, the network engineer designing the connectivity would allocate a portion of the original extranet implementation cost to the new project. Thus the, sponsoring director would recoup some of his investment. Additionally, the project manager discussed the concept of Quality of Service and rate limiting with the sponsoring director, informing him that, if necessary, the network engineers could provide his projects with guaranteed bandwidth. Once all concerns were addressed, the director dropped his requirement of approving all future additions to the extranet gateway.

1.5. Project Scope

This project had two major focuses for its scope. First was the need to architect, design, implement and test a network that would provide controlled isolated external access to MMC vendors. Provisions needed to be made for multiple methods of connecting to the MMC including **point to point connections**, **Virtual Private Network (VPN) connections**, dial-up, and Internet access using standard Internet protocols such as **File Transfer Protocol**, **Secure Shell (SSH)**, and **Hyper Text Transfer Protocol**. The second focus was to architect, design, implement and test a network for MMC tenants. This portion needed to provide a method of isolating the tenants from MMC and MegaComm networks while still providing the capability to monitor and administer the devices on this segment. Also, the tenant portion of this project needed to leverage a common infrastructure while providing sufficient separation between tenants.

Conceptually, this meant that the project would provide a single structure for access control, naming services, email, and etc. while providing logical separation between the customers.

This project also needed to ensure the architecture and design was capable of being expanded and extended. It needed to expand to handle additional connectivity using the existing connectivity methods. For extensibility, it needed to be able to handle new connectivity methods and protocols.

Chapter 2

2. Literature Review and Project Research

2.1. Review of Existing Solutions

The terms **Intranet**, **Extranet**, **Demilitarized Zone (DMZ)**, VPN and B2B have received copious amounts of press and attention over the past few years. It is important to have an understanding of what these terms mean with relation to this project.

An Intranet is a private system of networks internal to a single organization that provides connectivity to all of that organization's business units. Where an Intranet provides connectivity to members within an organization, an Extranet extends a certain level of connectivity to external parties that have special relationships with the organization such as customers, suppliers, collaborators, shareholders and other stakeholders, but who do not have the same level of trust as internal users (Marcus, 1999). The term Demilitarized Zone (DMZ) comes from the military and denotes an area of lower security that acts as a buffer between your organization and a hostile environment such as the Internet. One of the key aspects of a DMZ is the need for monitoring. Just like the guard towers on the military DMZ in Korea, an organization's DMZ must have dedicated monitoring systems that ensure any hostile activity entering the DMZ is identified and mitigated prior to entering the higher security zones. Generally, servers that are open to the public and that are hard to secure, such as web servers, are placed in the DMZ. It is not uncommon for an organization to have multiple DMZ's, each with its own level of risk and security. Virtual Private Networks (VPNs) utilize cryptography, or the rendering of plain text unreadable, to establish private connectivity between organizations over a public network such as the Internet. By

utilizing the public Internet, VPNs eliminate the higher cost of dedicated point to point circuits between business partners. However, establishing a VPN requires establishing a connection between an organization's intranet and the Internet. This represents an increase in risk. Business-to-Business (B2B), sometimes also called E-Biz, is the exchange of products, services or information between businesses rather than between businesses and consumers (Definitions, 2004). Extranets are built to facilitate B2B operations. VPNs and DMZs are two main elements of Extranets. It was obvious that to solve the issues facing the MMC it would be necessary to build an Extranet. The crux of this portion of the project was to determine the best method for designing the Extranet. Companies have come and gone that promised unique and innovative solutions for extranet designs. The majority of these designs center on extranet applications not necessarily the underlying network that these "killer apps" would be running on. The MMC already had the applications that would be running on the Extranet. What was needed was a network design that would support those applications. Once all the hype over the "killer apps" was filtered out and the actual network designs were evaluated, they boiled down to only a viable few.

The cornerstone of a network design that allows non-MegaComm entities access to MMC resources, as well as providing for a shared services model was risk. The amount of risk acceptable to the MMC management dictated the network design. The simplest design, and consequently the one with the highest risk, was one that allows free access between MMC B2B partners and did not provide tenant segmentation. This was the design in place at the start of this project. Reducing the risk required the addition of methods to segment tenants, the termination of dedicated circuits to non-MegaComm

entities and the provision for VPNs to non-MegaComm entities. Figure 2-1 illustrates this type of design. Reducing the risk further required the implementation of a layered design where overlapping controls provided multiple levels of risk mitigation. An example of a layered design appears in figure 2-2.

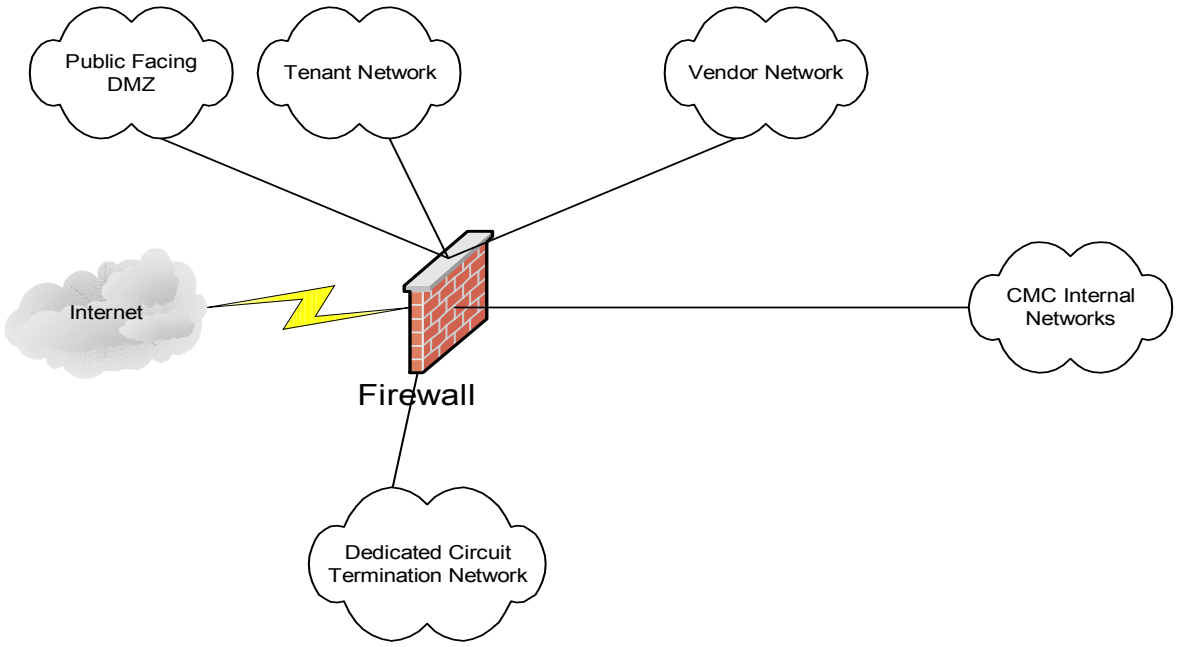

Figure 2-1 Single Firewall Design

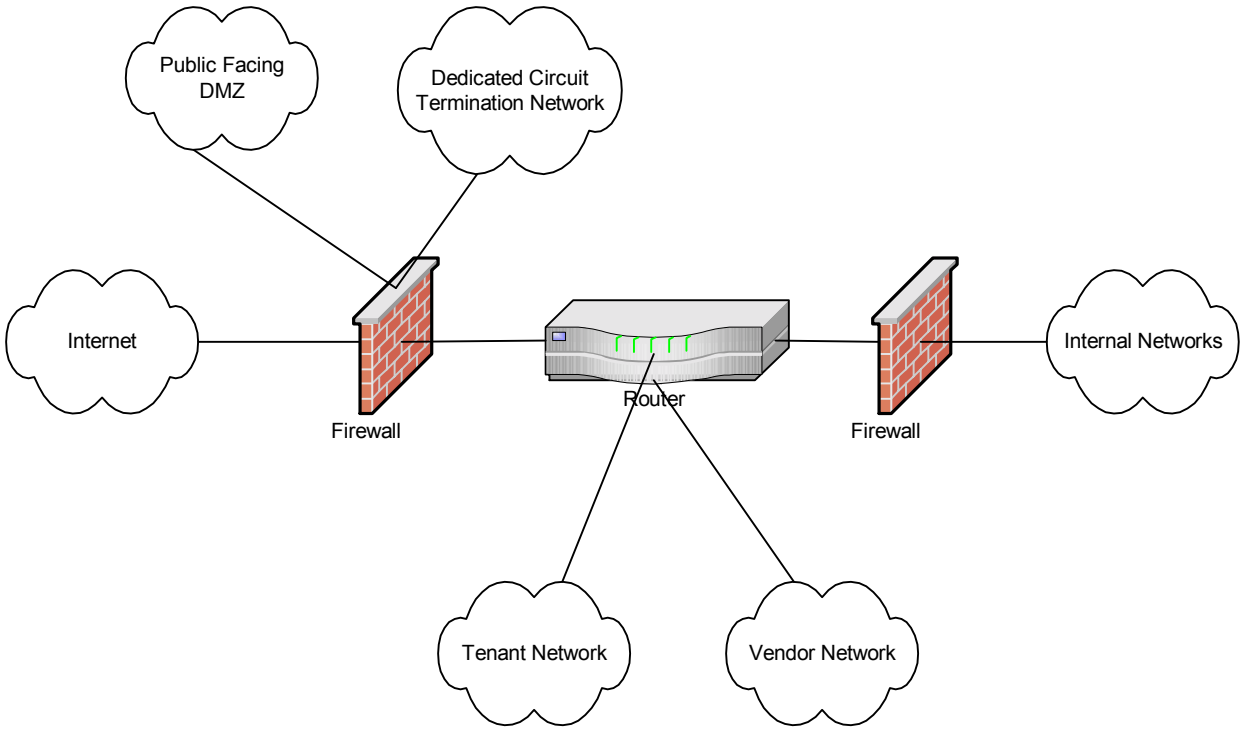

Figure 2-2 Layered Design

Yet a third design used an independent firewall for each separate element within the extranet. This was a very costly design requiring a great deal of administration. In some cases, this design could have represented more risk than the single firewall design due to the increased probability of a mis-configured firewall. An example of this design can be found in Figure 2-3.

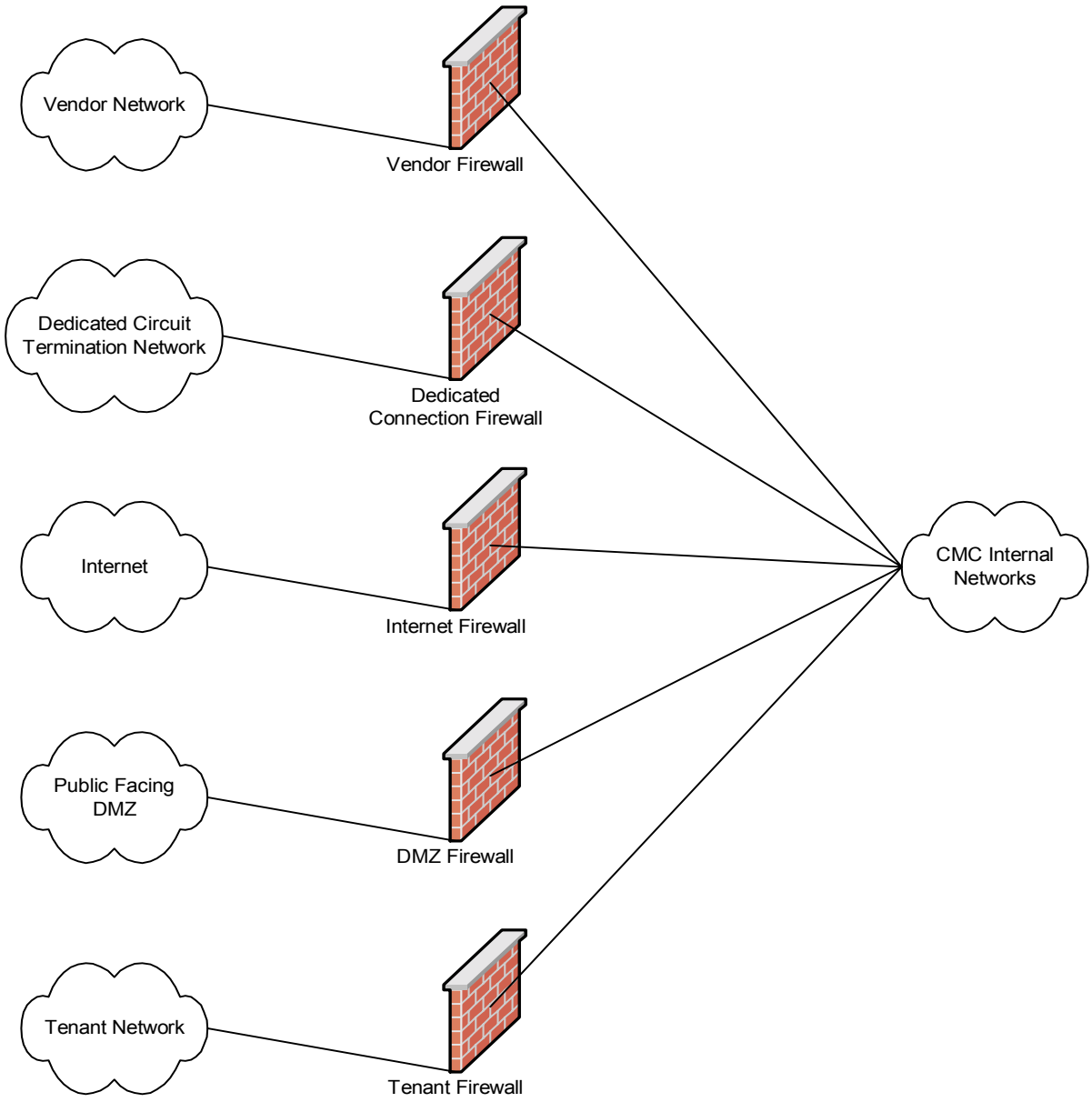

Figure 2-3 Multiple Firewall Design

Some would say that there was a final design; open communication without any firewalls. This entailed connecting all of the external networks directly into the internal networks. That design was not considered for this project.

2.2. Research Methods Used

Two main research methods were used for this project: interviews and literature review. The interviews conducted by the project manager fell into two categories. First he interviewed the internal stakeholders with the purpose of gathering requirements and expectations for the extranet. Also in these interviews, he obtained the relevant MegaComm policies and procedures for establishing external connectivity. The second interviews were with subject matter experts in order to establish and validate the appropriate design for the project.

The literature review required the consideration of many aspects of network design. The guiding principle behind this literature review was the Open System Interconnection (OSI) Model. The OSI Model defines a framework for implementing communication protocols in seven layers (The 7 Layers of the, 2004). The seven layers are:

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Applications Layer

Applicable literature was reviewed for each layer of this model with the goal of selecting the best architecture, given the requirements established during the interview

process. Ensuring the security of the deployed network was a significant requirement. Information security transcends all seven layers of the OSI Model; therefore, security received additional literature review. A complete bibliography of the research materials used can be found in the end material of this project.

2.3. What was Known and Unknown About This Topic?

What was known about this topic has filled volumes. The task of building an extranet required knowledge from several disciplines including networking, information security, application development, database administrations and design, as well as server administration and desktop support. The technology necessary to build an extranet did not differ from the technology necessary to build an intranet or, for that matter, the Internet. What makes any extranet unique is how the technology is deployed.

This project relied on proven technologies such as Ethernet, TCP/IP, static routing, Microsoft and Linux operating systems, Web, email and DNS servers, Firewalls and Intrusion Detection systems. These were all well documented technologies. What was unknown was how these technologies would be combined to form an extranet that met the requirements set forth by the MMC. No canned or "off the shelf solution" was available that would have solved the issues facing the MMC. Solving these issues was the cornerstone of this project.

2.4. Contribution the Project Will Make to the Field

It is rare that any two extranets will be designed exactly the same. After all, extranets are designed to solve unique situations faced by each company. There may be many similarities. However, as each business is unique, so their extranet solutions will also be unique. Although it is the author's belief that the actual design of the MMC

extranet may provide some contribution to the field, it is the process of designing the extranet that the author believes will be of most value.

This project followed the System Development Lifecycle which is well documented and can be applied to many situations. Most often, however, it is used in the development of software, databases and etc. Applying it to the design of an extranet will hopefully provide insight and guidance to other network engineers.

2.5. Discussion of Alternative Designs and Solutions

In section 2.1 the basic designs for extranets were discussed. The three main designs, the single firewall, the layered design and the independent firewall design present the network engineer with different levels of complexity in implementation, administration, security extendibility, extensibility and support. It will be helpful in understanding the final design if each of the basic designs is discussed.

2.5.1. The Single Firewall Design

This is by far the simplest design to implement and relatively simple to administer. A single firewall with multiple interfaces is deployed to protect the internal networks (see figure 2-1). Network switches are deployed off of each firewall interface to provide connectivity to the hosts belonging to each network.

The ease of implementation, however, is offset by the difficulties experienced in administration, security, expandability, extensibility and support. Deploying a single firewall will require a significant amount of administration. The firewall engineer must ensure that all of the proper rules are in place to allow only permitted traffic to pass from the Internet to any of the connected networks. Having only one firewall reduces the number of rule sets the administrator needs to maintain, however, even a minor

configuration mistake could allow unwanted traffic to traverse the firewall. Administering the switches off of each of the firewall interfaces requires an additional administrative burden.

A single firewall is inherently dangerous from a security point of view. The purpose of this extranet was to provide limited access to companies that had special relationships with the MMC; this, necessarily, included access from the public Internet. Having a single point that protected the internal networks from the Internet represented a significant amount of risk. Once the firewall was breached, an attacker would have unencumbered access to the MMC internal networks.

Expandability represents the ease with which new elements can be added to the extranet to provide more of the same type of services. With the single firewall model expandability is limited to the number of interfaces supported by the firewall. Additionally, firewalls will need to be deployed should all of the interfaces be used. Extensibility is a close cousin to expandability. Where expandability allows for the addition of elements that provide the same type of services, extensibility allows for the addition of elements that bring new or different services. This design supports extensibility as the networking equipment usually does not care what services it transports. However, should there be a need for incompatible services on the same network; this design would not provide any method for supporting them.

Any support needed for this network must pass through the firewall. There are several protocols used for supporting application, such as NetBIOS, that generate a great deal of traffic. Additionally, they broadcast a significant amount of information to the entire sub-network. This information can be used to attack these systems. It is, therefore,

best practice not to allow these types of protocols through a firewall. Here there is a dilemma; if the protocols are not permitted through the firewall the system administrators cannot properly support the hosts. If the protocols are allowed, valuable information could be leaked to attackers.

2.5.2. The Individual Firewall Design

The individual firewall design requires a separate firewall for each network requiring access to the internal networks. There is very little to recommend this design. Unfortunately, quite often this is the design companies are stuck with. This usually results from lack of planning. A company will experience the need to provide connectivity to an external entity; most likely a vendor that connects over a dedicated circuit. A low end firewall is deployed to protect the connection. The low end firewall is not expandable; so that, when additional external connectivity is required, another firewall must be purchased. This is costly both in equipment and manpower. Having multiple firewalls creates an administration nightmare. Since each firewall is a single point of egress, a breach on any one will result in a complete compromise of all systems. This design is expandable and extensible as additional firewalls can be added for more functionality. Support will be extremely challenging. This design suffers from the same problem with protocols as the single firewall design.

2.5.3. The Layered Design

The layered design utilizes multiple levels of networking gear including routers, switches and firewalls. This design is by far the hardest to implement requiring a great deal of planning prior to deploying any equipment. The multiple layers present challenges in physical layer connectivity, network layer addressing and routing, security

domain design and application support. Once designed and properly implemented however, these difficulties are more than offset by the increased level of security, the extendibility and extensibility, as well as, the ease of support. With the single firewall design implementation was very easy while resulting in significant challenges once it was deployed. This design is the opposite. The majority of the challenges come in the design and implementation portion of the project.

Properly designed the extranet was implemented in layers. At the center was a core enterprise router that fed all of the necessary networks. The majority of the traffic on the extranet traversed this router. There were two firewalls between the Internet or other external connectivity and any internal or extranet networks. This dual firewall design eliminated the single breach point present in the other designs. The two firewalls were set up in a screening/choke configuration. In this configuration the screening firewall was placed at the edge of the extranet where the external connectivity entered the system. The choke firewall was located on the inside edge of the extranet between the internal or protected networks and the core of the extranet. This layered design allowed the choke firewall to compensate for any holes that may have been present in the screening firewall. Figure 2-4 illustrates this design.

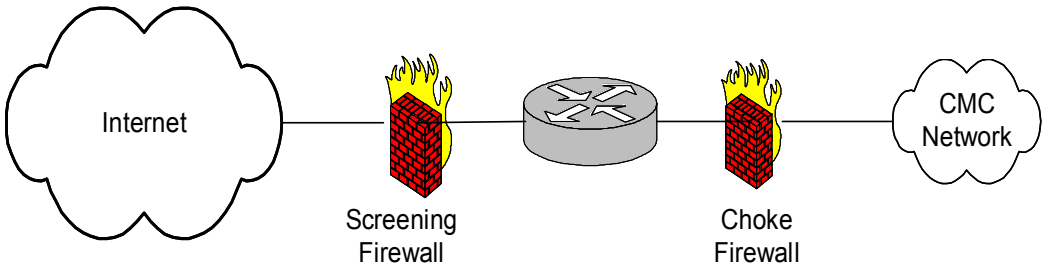

Figure 2-4 Screening Choke Design

Based on the established requirements, the project manager and the network architect chose to design and implement a variation of the layered network.

2.6. Why a Layered Network Design vs. Alternative Solutions?

This project had many requirements, chief among them were security, expandability and extensibility. The layered network design met these requirements far better than any of the other designs considered. A layered network was more secure than a single firewall or independent firewall design because the second or internal choke firewall compensated for any holes or mis-configurations that may have been present in the first or external screening firewall. Additional protection against a firewall breach due to a vulnerability in the firewall software was to be achieved by ensuring the two firewalls came from different vendors, Cisco and Checkpoint. The security of this design was further enhanced by deploying an **Intrusion Detection System (IDS)**. There are many points at which an IDS sensor could have been deployed in this model and they are discussed further in this document. However, two primary IDS placement points were important to the selection of the layered network design. A sensor placed directly inside the screening firewall acted as an early warning device should malicious traffic breach the external screening firewall. If this occurred that traffic could have subsequently been blocked on the internal or choke firewall. The second IDS placement point was directly inside the internal choke firewall. This sensor served to confirm that the choke firewall did indeed block the malicious traffic identified by the first IDS sensor.

The layered network provided for virtually unlimited expandability. Unlike the single firewall design, it was not limited by the number of interfaces on the firewall. The

core router ensured that addition of new segments could have been accomplished easily and uniformly. Each segment was a network unto itself yet was still able to take advantage of a shared services infrastructure. Each segment used, if needed, a common access method, email system DNS and etc. Conversely, if a segment required independent services this could also have been accommodated. The multiple firewall design also provided for expandability in that any new connectivity could have been added by implementing a new firewall. This model, however, limited the economies of scale realized by a common services infrastructure.

The ability to add new services or extensibility was also a requirement for this project. The layered design supported this requirement by ensuring that if incompatible services needed to be deployed on the extranet they could have been segmented either at the firewall or at the core router. A new incompatible service could have been placed on its own segment off the core router or off a separate interface on the firewall. This design could have been further expanded by adding routers to the firewall interface. This capability was not present in the single firewall design. Although it was present in the independent firewall design, the addition of firewalls for incompatible services would further increase the administrative and support burden.

2.7. Summary

Extranets are as unique as the companies that deploy them. No one solution will meet the needs of all or even many of the organizations with the need to extend their intranet to their business partners. Most companies providing designs for an extranet concentrate on the application that will be providing the services to the business partners. At the MMC, the applications were already designed and in use throughout MegaComm.

The challenge of this project was to design an extranet that would support the existing application. A few basic networks were considered. First was the single firewall, flat network model, second was the layered network, and third was the independent firewall, multiple network design. Providing improved security, virtually unlimited expandability and extensibility, the layered network was the only design to meet all of the project requirements.

Chapter 3

3. Project Methodology Followed

3.1. Development Model Followed

This project followed the **System Development Life Cycle (SDLC)** Model. This model consists of five phases: project planning, analysis, design, implementation and support. Each of these phases will be fully discussed throughout this chapter. There are several variations of the SDLC. The traditional, The Information Engineering, and The Rational Unified Process (RUP) are three of the variations. The project manager chose the traditional variation of the SDLC because it was the best fit for the project. Each of these variations can in turn be implemented using either the waterfall or iterative approach. Each phase in the waterfall method directly follows its predecessor so that the planning phase is completed prior to beginning work on the analysis phase and so on. A different approach is used with the iterative process. As the name implies, the system is developed in interactions. Each iteration contains the development phases. However, the complete system is not developed in a single iteration. Instead, each iteration builds on the results from the previous one until the project is complete. The idea is that not all of the requirements will be known until some portion of the system has been developed. This project used the waterfall approach to the SDLC, although some phases did overlap.

3.2. Project Planning Phase

3.2.1. Problem Definition

During this phase, the project manager determined the origins of the project. They were important because they revealed the initial business needs. There were two originating events for the MMC extranet. First, the manager of network security for the

MMC identified a significant security issue with the content provider catchers located on MMC production networks being remotely accessed by the content providers. Additionally, the MMC had no way of verifying the security and integrity of those systems. This same manager documented his concerns and presented them to the Senior Director responsible for the MCDN system. The Senior Director commissioned him to develop a solution that would mitigate the risk.

The second originating event occurred shortly after the manger of network security made his presentation to the senior director. The MegaComm lawyers recognized a problem with having the MMC tenants share MegaComm information systems. They communicated this issue to MegaComm senior management and then mandated that the tenants be removed from the MMC networks.

This resulted in two main business drivers. First was the securing of the content provider catchers and second, the removal of the tenants from the MMC networks. Once the project origins were identified, the scope of the problem was further defined through interviews with the stakeholders. This process produced a good understanding of the dilemma facing the MMC. It was defined as follows: Due to the regulatory environment as well as significant security concerns, it is necessary to create an information system that will provide the current level of services and support to the MMC tenants while isolating them from the MegaComm network. Additionally, a system needs to be developed that will permit MMC business partners limited access to MMC networks while ensuring the security and integrity of the network accessed.

3.2.2. Establish the Project Budget

In section 1.4 the author discussed the barriers to the extranet. One was financial. For quite a while there were no projects at the MMC large enough to absorb the entire cost of the extranet. Finally, one large enough and with enough visibility was established, the MegaComm Content Deliver Network (MCDN). Available budget for the extranet was also favorable impacted by MegaComm Corporate's mandate to segregate the tenants. These two factors ensured that there would be available funding.

The Initial budget developed for the project was $375,000. This included hardware, software and labor. Table 3-1 gives a high level breakdown of the initial anticipated costs. This led to the establishment of a working budget of $375,000.

Hardware	$278,107.65
Software	$33,625.00
Internal Labor	$30,000.00
Infrastrucure Upgrades	$10,000.00
Total	$351,732.65

Table 3-1 Project Budget

This budget included costs for both the MCDN vendor portion of the extranet, as well as, the tenant portion. However, for the presentations to the senior director responsible for MCDN and the corporate IT group, the budget was customized to reflect only the portions of the extranet they were interested in.

3.2.3. Produce the Project Schedule

The author chose to utilize the waterfall approach to the System Development Lifecycle. A series of phases that mapped to the SDLC were followed. These phases were:

- Planning
- Analysis
- Design
- Implementation
- Support

With these phases in mind the schedule was developed. The planning phase began after the initial problem presentation to the senior director in charge of the MCDN system. This presentation occurred on March 5, 2004. The project was completed on August 27, 2004, with the completion of final acceptance testing and the transition from implementation to support. Table 3-1 gives an overview of the high level schedule. The complete schedule is attached as part of the end material to this paper.

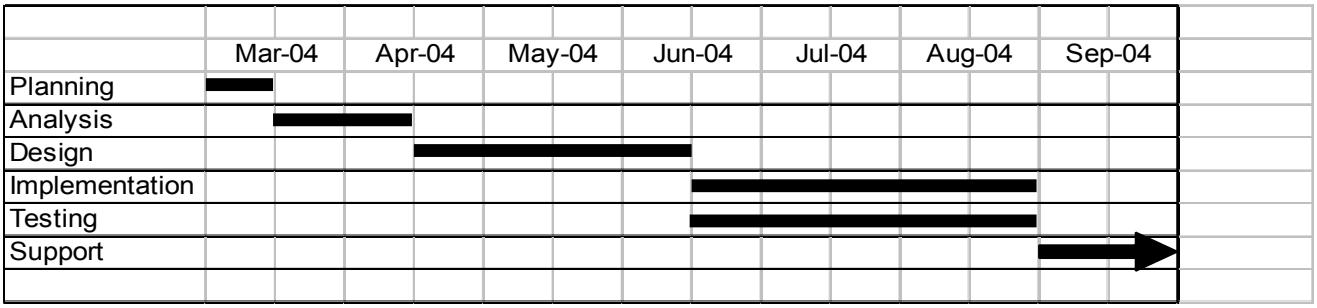

Table 3-2 Project Timeline

Milestones were developed for each phase of the project. They were used to ensure the project remained on schedule and that all of the pertinent steps for each phase were satisfactorily completed. All of the milestones can also be found as part of the end material to this paper.

3.2.4. Confirm the Feasibility of the Project

Feasibility can be measured in several ways, financially being the most common model. This project, however, followed a different model, that of reduction of risk. As pointed out by the Manager of Network Security there was significant risk with having external vendors controlling systems on MMC production networks. There was additional risk, identified by MegaComm Corporate, in having MMC tenants operating on MegaComm networks. Added to this were the regulatory requirements of Sarbanes-Oxley.

The feasibility analysis for this project consisted of ensuring that the proposed design would reduce the stated risks and comply with the regulatory requirements. To accomplish this, the author conducted a risk analysis and presented the design to the corporate IT group. "Risk analysis is a method of identifying risks and assessing the possible damage that could be caused in order to justify security safeguards" (Harris, 2002). The safeguard the author was attempting to justify was the Extranet. The risk analysis consisted of the following steps:

- Identify asset
- Identify the potential threat
- Determine the probability of threat occurrence
- Identify the safeguard

- Determine the probability of threat occurrence after safeguard deployment
- Compare the probabilities of occurrence

Table 3-3 presents the risk analysis.

Identify Asset	Identify Potential Threat	Probability of Threat Occurring	Identify Safeguard	Probability of Threat Occurring After Safeguard Deployment	Compare Probabilities of Occurrence
MCDN	System Failure due to Vendor actions	High	Extranet	Low	Before Safeguard - High After Safeguard - Low

Table 3-3 Risk Analysis

The risk analysis identified that the probability of a system failure due to vendor actions was high. The extranet was identified as the proposed safeguard. After deployment of the extranet the probability of system failure due to vendor actions was reduced to low. The extranet reduced the risk to acceptable levels. Based on this analysis the project was feasible.

The second test for feasibility was to determine if the proposed design would satisfy the regulatory requirements. These requirements were imposed by the MegaComm Corporate IT department; therefore, they were responsible for evaluating the design for regulatory compliance. At the end of April 2004, the extranet design was presented to the corporate IT department and it was approved. This satisfied the second feasibility requirement. Based on the results of the risk analysis and the approval of the

corporate IT department, the author concluded that it was feasible to proceed with this project.

3.2.5. Staff the Project

The magnitude of the extranet required expertise from several areas including network architecture, network engineering, security engineering and server administration. Proper staffing required resources from each of these areas. Table 3-3 shows the staffing for this project.

Requested Staff Position	Quantity Requested	Quantity Approved	Position Filled By	Responsibilities
Project Manager	1	1	Ken Quigley	Overall project management
Network Architect	1	1	Mike Walker	Network design review and approval
Network Engineer	1	1	Ken Quigley	Design, and implementation of the network security plan
Network Security Engineer	1	1	Adam Hajila	Design and implementation of the network security plan
Server Administrator	1	1	Jon Jones	Design the server architecture including domain, DHCP, DNS and etc

Table 3-4 Project Staffing

Mike Walker, the Network Architect, was responsible for reviewing the extranet network design and ensuring that it complied with MMC network engineering standards. Mr. Walker was also responsible for ensuring that the extranet design would integrate with existing MMC networks.

Adam Hajila, the network security engineer, was responsible for the development and deployment of the network security plan for the extranet. This included the selection

of firewalls, development of the firewall rule set, placement of the Intrusion Detection System and etc.

Jon Jones, the server administrator, was responsible for design and implementation of the server architecture. This included the selection of operating system, the domain design, the DHCP scope, the DNS design and etc.

The author, Ken Quigley, was the project manager and the network engineer. He was responsible for the overall management of the project. This included the initial proposal to MMC senior management, the development of the scope, methodology, schedule, milestones, and etc. He was also responsible for the management of the assigned staff. This included assigning the roles and responsibilities to each member of the team, ensuring the team had the resources necessary to complete their tasks, monitoring the team's progress against the established milestones and etc. As the network engineer, the author was also responsible for designing and implementing the network portion of the extranet. This included the physical, data link, network, and transport layer designs, selection of the networking equipment to be used and etc.

The above staff was responsible for the technical implementation of the extranet. To accomplish their assigned tasks they required support from several other departments within the MMC. It was the project manager's responsibility to secure support from the corporate IT group, the MMC finance department, the MMC purchasing department, the IT administrative assistants and the UNIX and Windows administrators.

3.2.6. Launch the Project

To launch the project several milestones had to be met. The high level extranet design had to be approved by the MMC senior management, the corporate IT group and

the network architect. Next, the budget had to be approved through both MMC senior management and corporate IT. Once the budget was approved the funds had to be released. At the MMC this was accomplished through the Capital Authorization process. A Capital Authorization Form (CAF) had to be submitted for each vendor supplying equipment, software or services for the extranet.

The final step in the launch process was to submit the project to the oversight team. At the MMC, all IT projects are approved and monitored by an IT oversight team made up of the Information Technology VP and all of the IT directors. There is a weekly status meeting where managers provide updates to the team. This provides an opportunity for the team to ask any questions and for the managers to bring up any concerns they might have. The extranet project manager submitted the project to the oversight team; it was approved and placed on the tracking status sheet.

3.3. Analysis Phase

3.3.1. Gathering Information

The goal of this portion of the analysis phase was to gather all the pertinent information necessary to establish requirements for the extranet. This differs from the information gathering documented in section 2.2 of this document. That research centered on the appropriate solution to the business problems. This research dealt with the functional requirements the extranet needed to meet.

There were two initial functional areas the extranet was to address: the MCDN vendors and the tenants. These two areas had very disparate requirements. The project manager, along with the project team, conducted interviews with the stakeholders of both the MCDN system and the tenants. The goal of these interviews was to establish the

functionality that would need to be duplicated on the extranet. The two functional areas were handled separately. The MCDN system stakeholders were handled first followed by the tenant stakeholders.

The methodology used by the project team was to break the MCDN vendor systems down into four component parts: the inputs, the processing, the outputs and the security requirements. The team was concerned with whom and what were accessing the vendor systems utilizing what software and protocols. This would provide valuable information as to the input to the system. This was established by interviewing the MCDN operators, as well as, the MCDN vendors. Additionally, network sniffers were used to confirm the information obtained through interviews. Once the inputs to the systems were established, the team focused on what the processing on the vendor systems entailed. Again the MCDN operators and the vendor's were interviewed. All information was verified through the use of network sniffers. Finally, the outputs to the systems were determined. Once again the team interviewed the MCDN operators and vendors using network sniffers for verification. The following list illustrates the information gathered from this process.

System Inputs

- Terminal Services – Some of the vendors utilized Microsoft terminal service for remote connections to the systems.
- VNC – VNC is similar to Microsoft terminal services and was used for remote control of the system.
- PC Anywhere – Like terminal services and VNC this was a remote control application that allowed the vendor to control the system.

- FTP – The vendor utilized FTP to transfer files to and from the system.
- SNMP – The vendor enabled SNMP monitoring for the systems. This required inbound SNMP queries as well as outbound SNMP Traps.
- NTP – The systems were configured to pull time from the local subnets.
- DNS – Some of the systems were configured to utilize DNS servers at the vendor's site.
- HTTP – All of the systems utilized HTTP, however it was enabled on the non-standard port of 8080.

System Processing

- SQL – The systems were configured to query SQL databases on the vendor's home network.
- Port 9191 – This was the back channel communications between the vendor server located on the vendor's network and the system located at the MMC.

System Output

- Samba – This was a file sharing protocol that allowed interoperability between Linux and Windows systems.
- Windows SMB and NetBIOS – These protocols were used to share files between the vendor server and the input system on MCDN.

To evaluate the security requirements, the team reviewed the relevant MegaComm security policies, and interviewed the MCDN operators, vendors and the MMC manager of network security. The security policies required that all 3rd party connectivity be accompanied by a 3rd party connectivity agreement. The team ensured

that all of the vendors had the appropriate agreements. The security policies did not put any restrictions on the type of traffic between the vendors and their systems.

The MCDN operators provided little input with regards to security. They were more concerned with system functionality. The MMC Manager of Network Security established the following security requirements for these systems:

- Isolation – If MMC employees were not to have control over these systems they must be isolated from all other MMC networks.
- Monitoring – These systems would need to be monitored for malicious activity.
- Controlled Access – Only the specified vendor would be able to access their system.
- Accountability – Vendors would be held accountable for any malicious activity originating from their systems. There had to be the capability of eliminating connectivity to any given system.

The team conducted one final interview with the Senior Director in charge of the MCDN. He was the business sponsor for the vendor portion of the extranet. The goal of this interview was to gather information on his business expectations. The following information was gathered as a result of this meeting:

- There would be up to 500 content vendors.
- Content would be delivered through a variety of methods.
- There were possible new non-traditional content delivery methods that had not been implemented yet.
- The extranet could afford to be down no more than 2% of the time.

Gathering information for the second functional area of the extranet, the tenant portion, required the team to interview representatives from each of the tenants, the corporate IT group, the MMC server administration group, the MMC Network Security Manager and the MMC Network Engineering and Operations Manager. The goal of these interviews was to gather information about the functional and business expectations for the tenant portion of the extranet.

The main driver behind moving the tenants onto the extranet was a requirement from the corporate IT group. This was initiated by concerns about compliance with existing regulations, specifically Sarbanes-Oxley. As no one on the project team was familiar with this regulation, they relied on the corporate IT group to provide the necessary information. The interviews with corporate IT resulted in the following:

- All tenant networks must be logically separated from MegaComm networks.
- Tenant networks could not utilize the same infrastructure as MegaComm networks. This meant that the tenant networks must have their own domain structure, DNS, Email, storage, backup, databases and etc.
- It was important to ensure that no tenant data was co-mingled with MegaComm Data.
- MMC employees could access the Tenant network, however, if any of the tenants needed access to MegaComm networks the connectivity must be supported by a 3rd party connection agreement.

The goal of the interviews with the tenants was to determine what functionality they were currently using that was provided by MegaComm assets. This required

interviewing a representative sample of tenant employees, the senior management from each tenant and the IT group, if available, from each tenant. As a result of these interviews the project team established the following tenant network aspects:

- The tenants utilized the MegaComm email system.
- Although they utilized the MegaComm Email, they also had external email they wanted forwarded to their MegaComm email addresses.
- The tenants utilized MMC resources to perform post production editing on shows they produced. This required access by the post production editors to the tenant systems.
- The tenants relied on the MMC networks for Internet access.

Although the tenants were able to provide a great deal of information about their expectations for the extranet, there were still underlying MMC systems providing them with the day to day computing environment. To understand these underlying systems it was necessary to talk with the MMC server administration group. They provided the following information:

- The tenants utilized the MMC Windows domain structure.
- The tenants relied on the MMC systems for authentication.
- File sharing was provided by the MMC.
- MMC file, application and database servers were utilized by the tenants.
- All system backups were conducted through the MMC backup system.

Understanding the tenant requirements and the underlying computing environment lead the team to investigate the layer two and three connectivity that provided the communications infrastructure on which all the systems were running.

Interviewing the Network Engineering and Operations Manager provided valuable information:

- The tenants utilized the same network gear as the rest of the MMC networks.
- This network gear consisted of layer two access switches and layer three routers.
- This gear was located in several wiring closets throughout the building.
- In some cases the tenants had access to the network gear to perform moves, adds or changes.
- Port security was enabled on all tenants switches.
- Tenants had connectivity to Data Center 3 where the shared servers, as well as, tenant owned servers resided.

The final interview for this area of the extranet was with the MMC network security manager. The purpose of this interview was to gather information about any additional security requirements above those established by the corporate IT group to comply with Sarbanes-Oxley. The Security Manager provided the following security requirements:

- All tenant networks having Internet access must be protected by the screening and choke firewall configuration.
- All systems on the tenant domain must be managed through a push scenario. This required that all connectivity between MMC systems and tenant systems must be originated by the MMC system. A good example was the DNS system. The DNS administrators wanted to centrally

manage the DNS system. Unfortunately, the DNS resolver placed on the tenant network had to initiate connections to the central management console to pull zone updates. The updates were not pushed from the central console. The Security Manager did not permit this and the extranet DNS had to be managed separately from the MMC DNS.

- All areas of the extranet had to be logically separate. This required firewalls between the different areas.

3.3.2. Define the System Requirements

From the information gathered the team was able to begin defining the system requirements. These were broken down into four areas: business, technical, pre-implementation and training requirements.

3.3.2.1. Business Requirements

The business requirements for the vendor system portion of the extranet were driven by the rapid nature of the information flow within MCDN, as well, as the rapid development of new vendor systems and new methods for moving the information. Table 3-5 enumerates the major business requirements for the vendor portion of the extranet.

Vendor system business requirements
Flexibility – The extranet must be able to accommodate several types of vendors and several different delivery methods.
Rapid Response – The extranet must allow for the rapid response to the needs of existing vendors and to the addition of new vendors.
Expandability – The extranet must be able to handle up to 500 content providers.
Extensibility – Currently, the communication method used by the vendors are known. The extranet will be built to accommodate those methods. Also, the extranet must be capable of handing methods outside the original set. In some cases, these new methods may not currently exist.

Table 3-5 Vendor Business Requirements

Where the vendor portion of the extranet was concerned with rapid response and flexibility, the business requirements for the tenant network were more driven by ensuring the current functionality experienced by the tenants was duplicated on the extranet and that the regulatory requirements were met. Table 3-6 illustrates the tenant portion of the extranet major business requirements.

Tenant Business Requirements
No loss of functionality - The extranet must duplicate the functionality the tenants experienced while on the MMC networks.
No loss of service levels - The tenants must have the same level of service on the extranet that they did while on the MMC networks.
No commingling of data - Data from the tenants must not be co-located in any way. This included separate file, application, backup servers and etc.
No Shared Services - The extranet must provide all the necessary services to the tenants. No services could be provided from the MMC networks.

Table 3-6 Tenant Business Requirements

3.3.2.2.Technical Requirements

The technical requirements were generated by the MMC Manager of Network Operations, the MMC Manager of Network Security, the governing MegaComm policies on connections to external third parties and generally accepted network design principles. The primary technical requirements can be found in table 3-7.

The extranet design had to conform to Cisco's tiered architecture. The design had to include an access, distribution, and core layer.
The extranet design had to be modular. Although there were only two business units/segments slated for the initial implementation of the extranet, there were several other proposed projects that could take advantage of the extranet.
The extranet had to segment the different business units. Although all traffic would traverse a common distribution and core layer, only traffic destined for a specific segment should be permitted to the access layer.
The extranet, where possible and not prohibited by policy or regulation should rely on a common application layer infrastructure. This would include common domain services, email, DNS, and etc.
No traffic originated on the extranet would be allowed to pass to the internal MMC networks without first being proxied through a MMC controlled device.
The extranet must conform to the dual screening/choke firewall design. No segment, including the MMC internal networks should be less than two firewalls away from the Internet or other external connectivity. Where possible,

the screening and choke firewalls should come from different manufacturers.
Connectivity from the internal MMC networks to extranet segments would be on an as needed basis and be controlled to the layer four port level.
An intrusion detection system had to be deployed to monitor the extranet.
Under no circumstances would the extranet be used for Internet connectivity for internal MMC user networks.

Table 3-7 Technical Requirements

3.3.2.3.Pre-implementation Requirements

As the name implies, the pre-implementation requirements were those items that had to be in place prior to the final implementation of the extranet. These were items that were primarily external to the extranet; however, they were necessary to ensure the extranet functioned and was used properly. Table 3-8 covers the main pre-implementation requirements.

Tenant agreements had to be in place that detailed the MMC's responsibilities given the new connectivity.
Partner connection requests had to be in place with each vendor requesting access to the extranet.
A costing model had to be developed to amortize the initial cost of the extranet to new projects that would be added to the extranet.
A standard configuration model must be in place for new projects that were to be added to the extranet. This allowed for standardized deployment of equipment for all projects across the extranet.

Table 3-8 Pre-Implementation Requirements

3.3.2.4.Training Requirements

Fortunately, the extranet was deployed with well known technology. This reduced the technical training requirements for the network and security engineers and the server administrator assigned to the project. There were, however, some initial training requirements for some of the tenants and vendors being placed on the extranet. Table 3-9 describes the training requirements.

The security engineer assigned to the project needed Checkpoint training in support of the multiple firewall manufacturer requirement.
Training for the tenants was needed to ensure their IT personnel understood the new network connectivity.
Training for the MMC sales force was needed so that they understood the importance of Service Level Agreements that now needed to be included in all new tenant leases.
Vendor training was needed to ensure vendors could connect through the extranet.

Table 3-9 Training Requirements

3.3.3. Prioritize the Requirements

The project manager solicited input from the stakeholders, as well as the project team while prioritizing requirements. As with most projects each individual group was convinced their priorities should take precedence over all others. In the end, the project manager decided that the extranet project was created to solve a set of business requirements therefore, they should take priority. Table 3-10 takes a look at the prioritized requirements.

Business Requirements
1. Expandability
2. Extensibility
3. Flexibility
4. Rapid Response
5. No Loss of Functionality
6. No Loss of Service Levels
7. No Commingling of Data
8. No Shared Services
Technical Requirements
1. Must Conform to Cisco's Tiered Architecture
2. Dual Screening/Choke Firewall Configuration
3. Deploy IDS
4. Must be Modular
5. Inbound Connections to MMC Must be Proxied
6. Must Provide for Segmentation
7. Connectivity from MMC to Extranet on an as Needed basis
8. No MMC user networks internet access through Extranet
9. Shared Services on Extranet where possible
Pre-Implementation Requirements
1. SLAs included in Tenant leases
2. Partner Connection Requests with Vendors
3. Standard Configuration for New Projects

4. Costing Model for New Projects
Training Requirements
1. Tenant Training
2. Vendor Training
3. Sales Training
4. Technical Training

Table 3-10 Prioritized Requirements

3.3.4. Develop Initial Design

Given the prioritized requirements, an initial design was created that attempted to accommodate as many of the requirements as possible. This design would be fleshed out during the actual design phase of the project. The goal of this initial design was to present a working model to senior management for approval. Figure 3-1 illustrates the initial design.

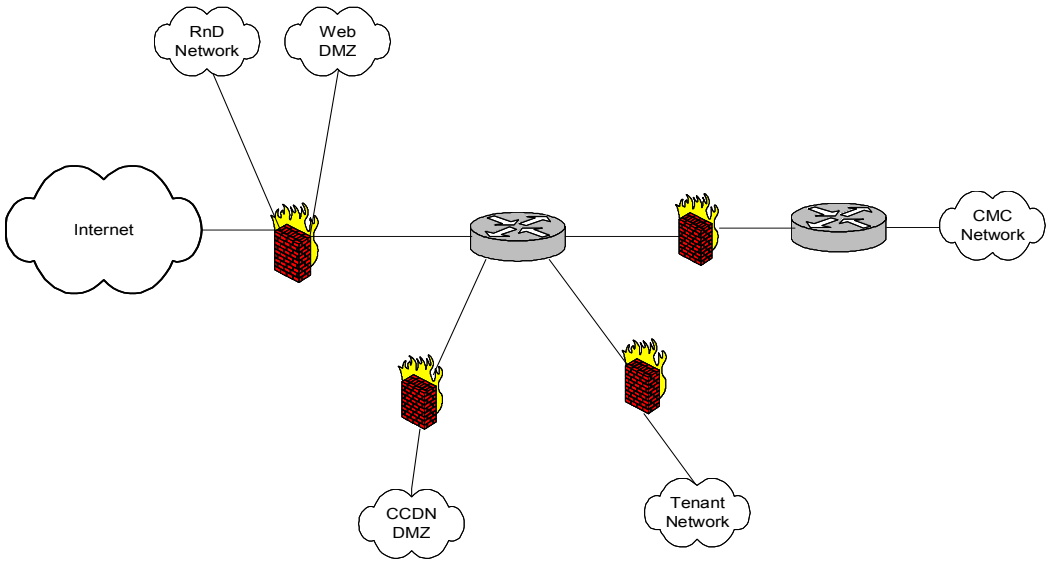

Figure 3-1 Project Initial Design

This initial design was created with the goal of meeting as many of the prioritized requirements as possible. The primary business requirement of expandability and extensibility were met through the use of a core router that allowed for segmentation. This also created a modular design so that new businesses could easily be added to the extranet. The initial design consisted of three main segments: the web DMZ that would provide Internet services such as mail relays, external DNS and etc, the MCDN DMZ that would provide an environment to place the vendors and a Tenant Network that would provide an environment for the tenants. Within the Tenant network there would be further segmentation that would provide a place for shared services such as domain service, internal email, internal DNS and etc. This design also met the technical requirements, as it was designed using the Cisco tiered architecture, it had a screening and choke firewall, it was modular and etc.

3.3.5. Management Review and Buy Off of Initial Design

Once the initial design had been documented, a meeting was scheduled with the Senior Director responsible for the MCDN project, as well as a separate meeting with the MegaComm corporate IT group. The purpose of these meetings was to present the documented requirements and the initial design. The project manager presented how the initial design would meet the prioritized requirements. Chief among the concerns of the Senior Director in charge of MCDN was that the extranet would be able to handle up to 500 content vendors and be flexible enough to support unknown connectivity methods. The project manager assured the Director that these requirements were accounted for in the design mainly due to the tiered architecture and the modular design. At the

completion of these meetings both the Senior Director and the MegaComm corporate IT group gave approval of the design and gave permission to proceed with the project.

3.4. Design Phase

The purpose of this phase was to take the approved initial design and develop working documents. These working documents were the major deliverables from this phase and consisted of designs for the physical, data link, network, transport, and application layers, security and plans for support and training. A complete set of Visio design drawings for each layer, and the written plans for support and training can be found in the appendices. The OSI Model was followed as a guideline while completing the design phase. The separate designs are discussed below.

3.4.1. Physical Layer Design

Quite often networking project managers look at the physical layer of their network design as the cabling they will use to connect all of the systems together. Cabling is definitely a major player in the physical layer design. However, this time, the project manager decided to incorporate several other factors he felt belonged in the physical layer design. These included the power infrastructure, the location of the networking and server equipment, the temperature and humidity controls for the facility and etc. Table 3-11 covers a few of the physical layer considerations the project team explored.

By its nature, the extranet required a connection to the Internet. The MMC had an existing connection to the Internet that was to be used for the Extranet. Although the Internet connection could be extended to any of the three MMC data centers, it was primarily located in data center three.
The MMC has three independent power legs entering the facility. Each of these power legs is supported by battery and generator backup. When the extranet was designed, the only data center with all three legs of power was data center three.
To accommodate the tenant portion of the network, the Extranet had to be extended to several Intermediate Data Frames (IDFs) throughout the facility. Regardless of the chosen data center the distance to the IDFs required the use of Fiber Optic cable for transport.
For the tenant portion of the Extranet, where possible, a shared application infrastructure was to be used. For this, rack mounted servers were to be used. The servers chosen were too long to fit in a standard telco rack. These racks were prevalent in data center three. The other two data centers contained deeper racks that would easily hold the chosen servers.
All three data centers had surplus air temperature and humidity controls.
Of the three data centers, data center three was most centrally located.

Table 3-11 Physical Layer Considerations

After reviewing these factors the project team decided on the physical layer design. This included the placement of the extranet in data center three. Racks to accommodate the servers would be moved from one of the other two data centers. Two of the three power legs would be used to provide redundant power where needed on the extranet. For the network connectivity, enhanced category five and fiber optic cabling would be used. Fiber optic cabling would be used to tie the IDFs to the Data Center. Also, within the Data Center, fiber would be used to provide connectivity between rows of racks. Figure 3-2 illustrates the extranet physical layer.

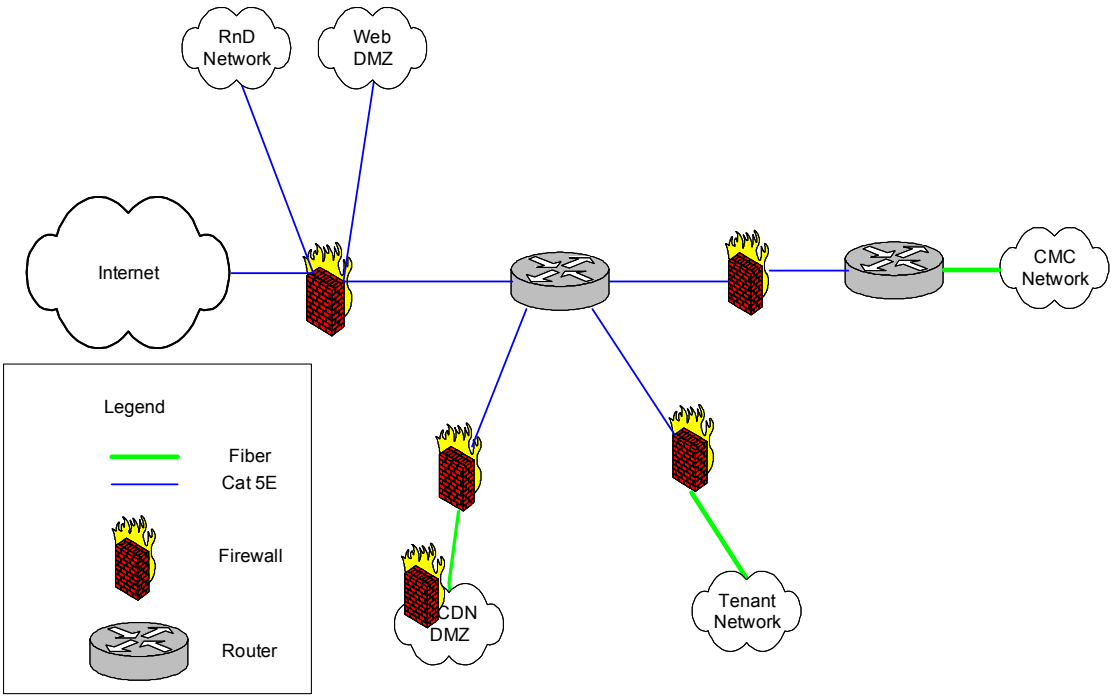

Figure 3-2 Physical Layer Diagram

3.4.2. Data Link Layer Design

Once the design was complete for the physical layer, the team moved on to the data link layer. This is the second layer of the OSI model and is responsible for utilizing

hardware addresses to ensure messages are delivered to the proper device. Additionally, the data link layer translates the message from the upper layers of the OSI model into bits, then delivers those bits to the physical layer for transmission (Lammle, 2001, 24). There were three main data link layer elements the project team needed to decide upon. The first and second (which data link protocol to choose and whether to use switches or hubs), had a direct bearing on the third, the use of **Virtual Lans (Vlan)**. One of the main factors in choosing the data link layer protocol was the projected speed of the network. The speed requirements for the extranet were for an initial 100 Mbps with the capability of upgrading to 1 Gbps. There were several well known data link protocols to chose from, however the three main contenders were Ethernet, Fiber Data Distribution Interface (FDDI) and Token Ring. FDDI was quickly dismissed as there was a mix of both fiber and copper cabling at the physical layer. The team could have chosen to implement FDDI on the copper cabling (CDDI). However, this was beyond the expertise of the team and would have required additional training. Although Token Ring is still used on some networks, it has primarily been superseded by Ethernet. Additionally, Ethernet was the existing protocol in use at the MMC. The project team chose to implement the Ethernet data link protocol on the extranet.

The next decision to be made dealt with choosing between switches and hubs. Both are layer two devices, however, they work in completely different ways. Hubs act as repeaters. Traffic coming in on a specific port is sent out all ports except the one the traffic entered on. Hubs have no capability of discerning on which port the intended destination resides. Switches, on the other hand, have the capability of learning the location of each system to which they are connected. They accomplish this by

associating the systems hardware address with a specific port. These associations are contained in the MAC address table. As hubs flood incoming traffic out all but one port and switches only send traffic out a specific port, they are much more efficient. Switches reduce the amount of traffic traversing the network. Additionally, hubs do not support Virtual Lans (Vlans). If the team decided to use hubs, Vlans could not be used. The last factor in deciding the data link layer devices was the required speed. Switches were far more capable of the higher speeds needed for the extranet. Once all of the factors were considered, the team decided to deploy switches instead of hubs.

The last decision was on the use of Vlans. Vlans provide several benefits; the team was primarily concerned with two of them. First was the segmentation of the extranet, and second was the added flexibility offered. Vlans segment networks by grouping systems together based on any number of factors including, similar functionality, department membership, or in the case of the extranet, vendor or tenant membership. Vlans on the extranet allowed the team to group the systems that belonged to each vendor or tenant together. The second benefit the team was concerned with was the flexibility Vlans offer. To group all of the systems belonging to each vendor or tenant would be a challenge without Vlans as the systems were spread throughout the MMC. Without the use of Vlans each separate network would need to be extended to multiple locations to accommodate all of the vendors and tenants. This would have significantly increased the cost of the project. Through the use of Vlans, all of the appropriate networks were able to be extended to the needed location with a minimum investment in hardware and cabling.

After making the decisions on the protocol, the choice between switches and hubs, and the use of Vlans, the project team selected the layer two switches that were used on the extranet. Cisco equipment is used almost exclusively at the MMC. The discounts granted by Cisco, as well as the compatibility with the other Cisco devices throughout MegaComm drove this requirement. The team considered several factors when selecting the switches:

- Port density
- Interface speed
- Compatibility with existing equipment

The actual data link design called for the use of Ethernet as the protocol, the use of switches and the use of Vlans. Due to the distance requirements switches were chosen that supported fiber optic connectivity. The Vlans were designed so that there was a separate one for management of the networking equipment, one for each tenant and one Vlan for each vendor.

3.4.3. Network Layer Design

The next step for the project team in the design process was to tackle the network layer, or the third layer of the OSI model. Several decisions faced the team: which layer three protocol to use, to build a flat or routed network, the addressing scheme, the choice of using static or dynamic routing, the routing protocol to use if dynamic routing was chosen and etc. Many of the subsequent decisions hinged on the choice of layer three protocol. Fortunately, this decision was all but made for them. Although there have historically been a couple of layer three protocols to choose from, Internet Protocol (IP)

and Internet Packet Exchange (IPX), IP has emerged as the clear leader. It was also the protocol in use at the MMC, therefore it was chosen as the layer three protocol.

TCP/IP is so ubiquitous in the industry today it might be assumed that all that needs to be done for the network layer is to hand out the IP addresses. First, however, the choice between building a flat network (where all systems would be on the same subnet), or a building a routed network (creating multiple subnets and segmenting traffic), needed to be made. One of the main business drivers behind building the extranet was the segmentation and isolation of traffic generated by the MMC tenants. This requirement precluded the use of a flat network. Figure 3-3 shows the layer three devices and the initial design of the routed subnets.

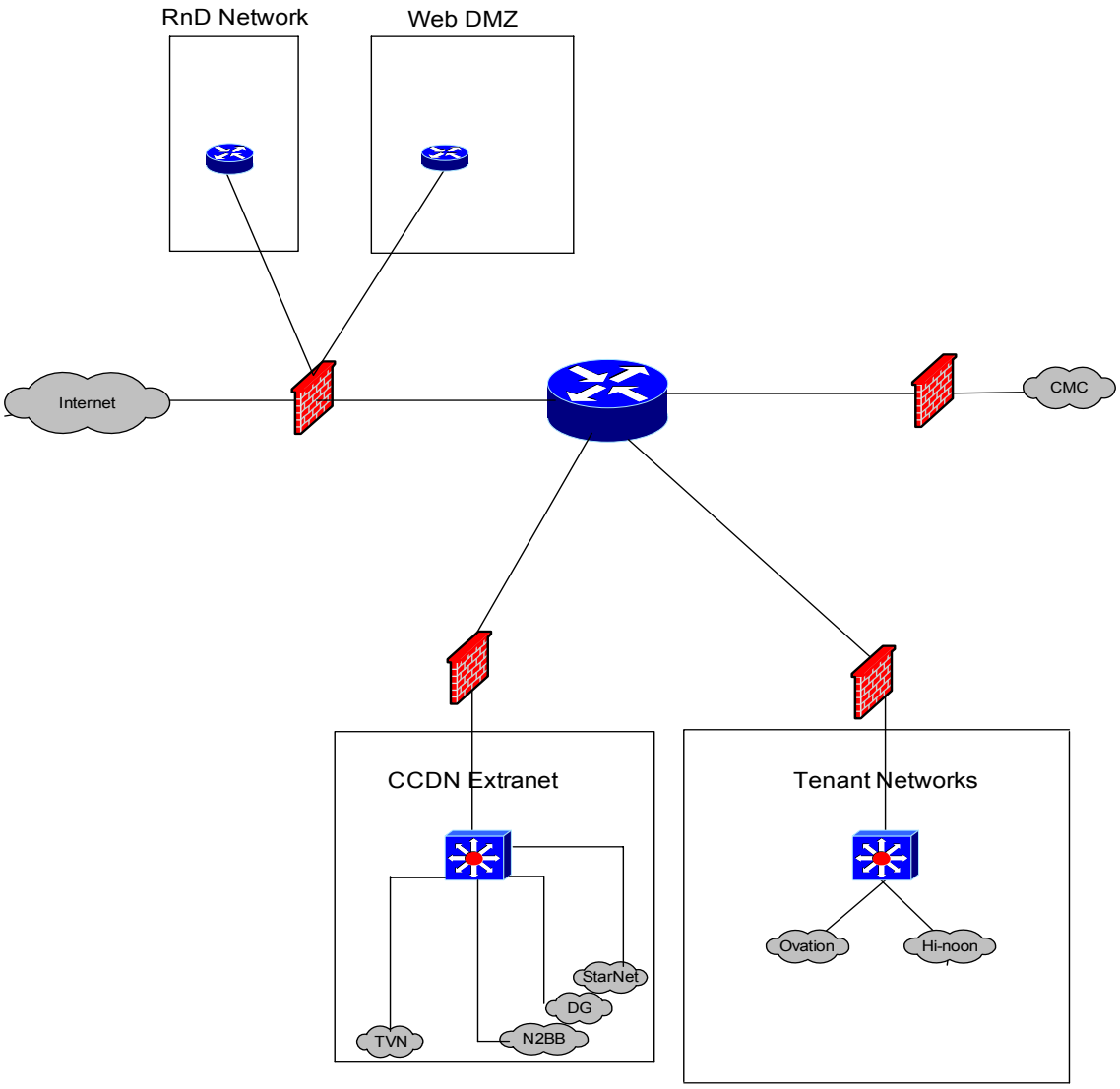

Figure 3-3 Initial Layer Three Design

Using the initial layer three design as a template the addressing scheme was developed. On these networks, only the devices on the web DMZ would be accessed from the Internet. The MMC also had a limited number of public addresses so a private address scheme was chosen. Those devices on the web DMZ that needed to be accessed from the Internet would have public addresses assigned on the firewall. Network Address Translation would be used to permit access to the actual devices. For security reasons, the first three octets of the actual addresses used have been changed in this

document. The modified scheme accurately reflects what was implemented on the extranet.

In looking at the network design as well as the business requirements, the project team developed the following addressing criteria:

- There would be several transport networks used solely for interconnecting layer three devices. No actual users would need access to these networks, therefore only a large number of networks with few hosts would be needed.
- There were only a few tenant networks. However, there would be a large number of users accessing these networks.
- On the MCDN subnet there would be an even mix between the number of networks and the hosts on those networks.
- The Web DMZ would start with a few hosts and may grow over time.

It was clear from the requirements that one subnet scheme would not fit all of the subnets contained within the extranet. It was decided to start with a class B private space. The 10.17.0.0 network was chosen as the initial class B network. This network would then be subnetted into class C networks for the different subnets within the extranet. Table 3-12 outlines the addressing scheme:

SubNet Description	Network Address	Subnet Mask	Number of Networks	Number of Hosts per
Class B Address:	10.17.0.0	255.255.0.0		
Administrative Tranpsort Networks:	10.17.0.0	255.255.255.240	16	14
CCDN Subnets	10.17.10.0	255.255.255.224	8	30
Reserved for CCDN Growth	10.17.11.0			
Reserved for CCDN Growth	10.17.12.0			
Reserved for CCDN Growth	10.17.13.0			
Reserved for CCDN Growth	10.17.14.0			
Reserved for CCDN Growth	10.17.15.0			
Reserved for CCDN Growth	10.17.16.0			
Reserved for CCDN Growth	10.17.17.0			
Reserved for CCDN Growth	10.17.18.0			
Reserved for CCDN Growth	10.17.19.0			
Web DMZ	10.17.20.0	255.255.255.0	1	254
Reserved for Web DMZ Growth	10.17.21.0			
Reserved for Web DMZ Growth	10.17.22.0			
Reserved for Web DMZ Growth	10.17.23.0			
Reserved for Web DMZ Growth	10.17.24.0			
Tenant Networks	10.17.100.0 and Higher			
Ovation	10.17.103.0	255.255.255.0	1	254
Hi-Noon	10.17.104.0	255.255.255.0	1	254

Table 3-12 Layer Three Addressing Scheme

The administrative subnet 10.17.0.0 255.255.255.0 was further sub-divided into 16 smaller subnets. This allowed all of the transport networks to be contained within the same class C network. This made it easier when developing the access control lists. Also four additional class C networks were reserved for future expansion of the administrative subnets. Ten class C networks were reserved for the MCDN subnets, however, only the

first class C network was utilized. This class C was sub-divided into 8 smaller subnets with 30 hosts per subnet. This allowed for each vendor to have their own subnet where they could place up to 30 hosts. The tenant network required large number of hosts per subnet; therefore, it was decided to give each tenant a complete class C network. This allowed for up to 254 hosts per network. Additionally, the tenant networks started at 10.17.100.0. Starting the tenant networks with this address allowed for a significant amount of future expansion.

The decision to build a routed network necessitated the need to choose the routing method to be used on the extranet. Static or dynamic routing could be used. Static routing requires the addition of each route to all layer three device by the network engineers. With dynamic routing each layer three devices learns about the routes it has access to, and then forwards that information onto the other layer three devices. Routing protocols include Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP). Routing protocols are separated by the two methods used to determine routes, distance vector and link state. A distance vector protocol uses distance or "hop count" as the method for determining the best route to a destination. RIP is a distance vector protocol. Link state protocols use the status of each link to determine the best route to a destination. OSPF is an example of a link state protocol. To determine whether to use static routes or dynamic routing, the project team consulted the Manager of Network Engineering. It was determined that because only static routing was used at the MMC the routing on the extranet would also be static. It was, therefore, not necessary to choose a routing protocol.

3.4.4. Transport Layer Design

The transport layer is the fourth layer of the OSI model. The main purpose of the transport layer is to segment and re-assemble data into a data stream (Lammle, 2001, 14). Additionally, this layer provides end to end data transport services and establishes logical connections between the sending and receiving host (Lammle, 2001, 15). Network dependent information is hidden from upper layer applications by the transport layer.

The Internet Protocol (IP) is actually a family of protocols. IP is at the network layer. There are other protocols within this family at the transport layer. The two best known are TCP and UDP. TCP provides reliable transport between source and destination host by creating a session. UDP, on the other hand, is not a reliable protocol; it does not create a session between source and destination hosts.

Fortunately for the project team, little design was required for this layer. The choice to utilize Cisco equipment for both layer two and three ensured that all of the layer four protocols within the IP suite would be supported. The choice of which layer four protocol to use would be determined by the applications run over the network. Regardless of the application, the underlying layer two and three equipment would be able to support it.

3.4.5. Network Security Design

The extranet gateway was built for several reasons; many of which required access to the Internet, or segmentation of non-MegaComm traffic. Securing this connectivity was the major driver behind the design and implementation of this network. This portion of the design was critical to the success of the extranet.

The goals of the security design were:

- Isolate tenant network traffic from MMC and/or MegaComm networks
- Isolate MCDN vendor connectivity.
- Deploy a layered security model that includes a screening and choke firewall configuration.
- Prevent MMC users from accessing the Internet via the extranet.
- Limited connectivity from MMC networks to the extranet on an as needed basis.
- Inbound connections from the extranet to the MMC must be proxied.
- Intrusion detection must be deployed on each segment.

One of the requirements was to deploy a layered security design. Layered security involves the use of compensating countermeasures where one countermeasure compensates for necessary holes in other countermeasures. For example it was necessary to open World Wide Web access over port 80 to the Web DMZ servers. To compensate for this hole, a host network intrusion detection system was deployed monitoring port 80 traffic. There were several components of a layered security design, including the application of security patches to hosts, maintaining updated antivirus on all hosts, deploying multiple firewalls (screening/choke configuration), hardening the network equipment, deploying host based and network based intrusion detection, implementing security policies that define the type of access permitted to and from the extranet, and etc.

The layer three design provided the basis for segmenting the extranet and isolating the tenant and MCDN vendor traffic. The routers within the layer three design did not provide any traffic control. Any sources on the network could get to any

destinations. This did not meet the requirements of ensuring that traffic from the tenant network did not traverse or access MMC or MegaComm networks. Additionally, without some method of access control all segments would be exposed to inbound traffic from the Internet. The access controls implemented were in the form of firewalls. Keeping with the screening/choke firewall design, a screening firewall was placed between the Internet and the extranet. Choke firewalls were placed between the extranet and the MMC networks, between the extranet and the MCDN subnets and between the extranet and the tenant network. This ensured that all segments were isolated from each other, by two firewalls (screening and choke) and two firewalls away from the Internet. Figure 3-4 highlights the placement of the firewalls.

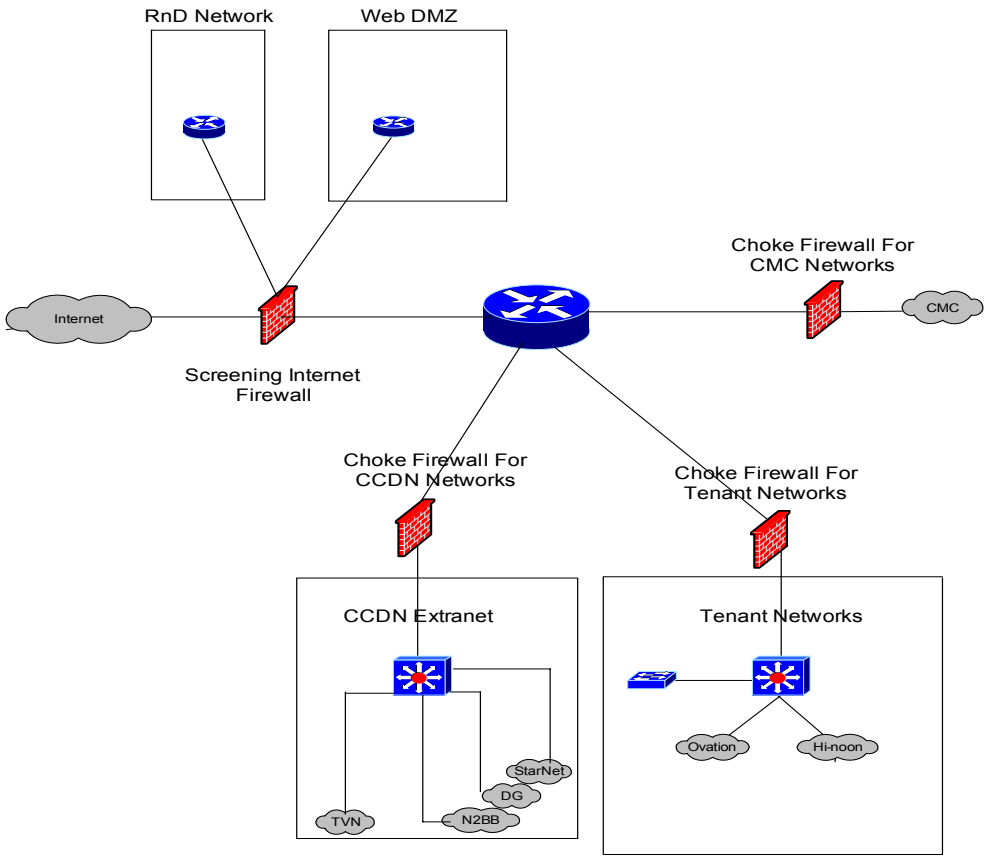

Figure 3-4 Firewall Placement

With this design, if traffic needed to pass from the MCDN extranet into the MMC networks, the screening/choke firewall model would still be met. The screening firewall was responsible for only permitting authorized traffic into the extranet. The choke firewall ensured that only authorized traffic from the extranet could pass into the protected subnets.

The project team implemented basic access control lists on each of the firewalls that permitted only administrative traffic into each of the protected subnets. Further access into the protected subnets would be on a limited "as needed" basis. There was no open access permitted from the MMC networks into the extranet subnets or between the

subnets. The MMC security department utilized an online firewall request system that enabled users within the MMC to request access through firewalls. This enables tracking and documentation of firewall requests. This system was used to process access requests to the extranet.

The only inbound traffic from the extranet permitted was snmp traps sent from the networking devices to the MMC snmp monitoring system. Here, the addressing scheme played a significant role. All of the networking equipment was on the same class C network 10.17.0.0 255.255.255.0. Even though this class C had been subnetted, the ACLS on each of the firewalls could permit traffic to and from the single class C. This ensured proper control over traffic bound for the networking equipment.

Before moving on to host based security and the implementation of an Intrusion Detection System, the project team developed a design for hardening the networking equipment. This is a step that is often overlooked when deploying a new network. Quite often it is met with less than enthusiastic support from networking groups as it makes it slightly more difficult to access their equipment. However, if the networking equipment is not hardened an intruder can use this equipment to launch additional attacks on the more sensitive servers.

Hardening the networking equipment included:

- Ensuring the Cisco IOS code was stable and did not have any known vulnerabilities.
- Limiting ICMP messages.
- Restricting remote access to the equipment.
- Requiring external authentication when accessing the equipment remotely.

- Setting a difficult to guess local username and enable password.
- Disabling CDP neighbor.

Although Cisco utilizes proprietary code, vulnerabilities are still often reported. It was important to ensure the code deployed did not have any known vulnerabilities. Internet Control Message Protocol (ICMP), if not restricted, can provide valuable information to a potential intruder. By limiting the type of ICMP message each piece of network equipment was permitted to send, this threat was mitigated. Only the network engineers needed access to the networking equipment. Limiting this access involved developing an access list on each piece of the networking equipment. This control went hand in hand with requiring external authentication when accessing the equipment remotely. This was accomplished by utilizing an authentication server running special software that bridged between the networking gear and the Windows domain authentication system. This allowed for the use of domain login information and for the tracking of access and accounting information.

Normally on Cisco equipment a connection to the console port does not require a password. Although the rights granted through the console session will be limited until the enable password is provided, this access could still enable a malicious person enough information to compromise the network. For this reason the project team implemented the use of a local username and password for the console connection. This, in addition to, the enable password, ensured that only authorized individuals could gain access to the networking equipment.

By default Cisco also enables the Cisco Discovery Protocol (CDP). This protocol exchanges information between networking devices. During initial configuration and

deployment this feature is extremely useful. Once in production, this feature must be disabled to limit the amount of information that can be obtained by any intruders. For all of the network equipment on the extranet, CDP was disabled.

Designing the security for the host layer required the involvement of the Windows server administrators, as well as the UNIX administrators. Host based security involves ensuring that all of the latest operating system and application patches are deployed, turning off all unnecessary services, installing and maintaining current anti-virus software, and deploying host based intrusion detection software on critical servers. Table 3-13 is a checklist designed by the project team to be used by the system administrators while implementing host security.

	Task Description	Initials
	Deploy the most current operating system patches	
	Deploy the most current application patches	
	Deploy the latest anti-virus software (Windows only)	
	Disable all unnecessary services	
	Enable logging	
	If critical server, install host based intrusion detection software	

Table 3-13 Host Security Checklist

The final portion of designing the layered security architecture was the Intrusion Detection System design. Intrusion detection systems (IDS) are deployed on critical hosts and networks to monitor for suspicious traffic. The project team along with the

system administrators had to identify the critical servers. The team also had to identify the appropriate choke points for deploying the IDS sensors. Once the locations of the sensors were determined, the team had to identify the traffic each sensor would monitor. It was decided to deploy host based IDS sensors on all of the servers on the Web DMZ as they were internet facing. Host based sensors were also deployed on the domain controllers and the critical database servers. Figure 3-5 shows the placement of the network based IDS sensors.

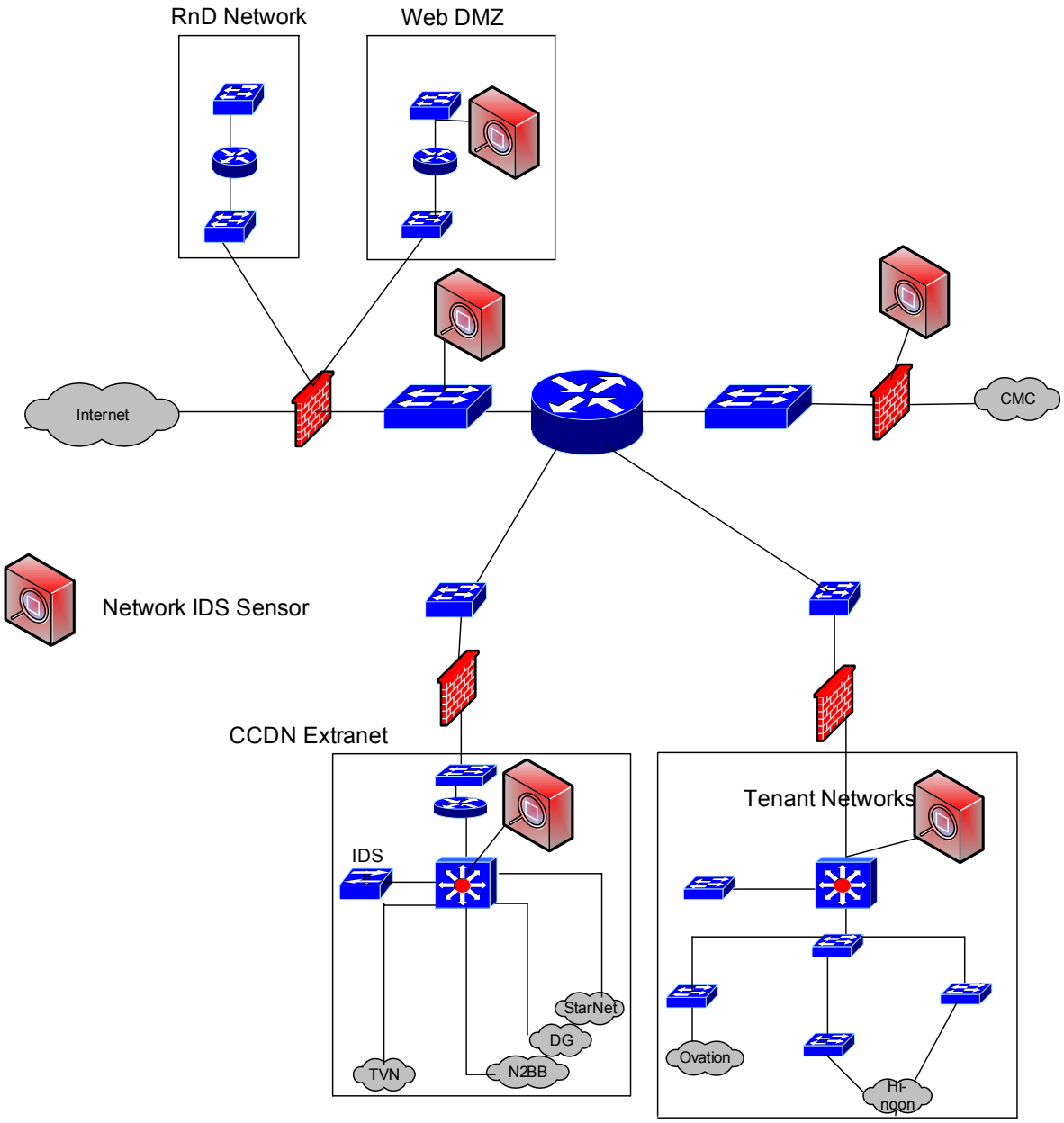

Figure 3-5 Placement of Network Based Sensors

3.4.6. Application Deployment Design

Designing the application deployment plan, once again, involved input from the Windows and UNIX systems administrators. Initially, the majority of the applications deployed were Windows based. The only system administered by the UNIX group was a

Linux FTP server on the Web DMZ. The Windows applications included IIS web, Active Directory, email, database and file servers. There were also specialized Windows applications deployed for the MCDN content providers. The deployment design involved determining which applications needed to be deployed in what order. Table 3-14 gives the deployment order:

Sequence	Application	Deployed by
1	Active Directory Controllers	Windows Admins
2	DNS Servers	Windows Admins
3	Email Servers	Windows Admins
4	IIS Web Servers	Windows Admins
5	FTP Server	UNIX Admins
6	Database Servers	Windows Admins
7	File Servers	Windows Admins
8	MCDN Specialized Applications	Windows Admins

Table 3-14 Application Deployment

The priority of the applications was determined with input from the administrators and the users. It was imperative to have the active directory controllers up first as all other Windows systems would rely on them. Next was the rest of the Windows infrastructure including the DNS and Email servers. The IIS Web Servers and FTP server were scheduled next, followed by the database and file servers. As there were already systems in place for MCDN the specialized applications were scheduled last.

This priority list was provided to the Windows and UNIX administrators for use during the installation phase.

3.4.7. Support Plan Design

The MMC supports several systems for MegaComm, External Customers as well as internal MMC organizations. The project team leveraged this expertise when developing the support plan. As many support systems were already in place; developing the plan was a matter of ensuring that the existing support infrastructure was capable of supporting the extranet.

The support plan for the extranet encompassed application, server operating system, network and security support. At the MMC application support is provided by two groups, the System Support Technicians (SST) who provide tier one support, and the production support team that provide tier two and three support. For applications developed within the MMC additional support is available from the developers. The support plan called for the SSTs and the production support team to support the extranet applications. Server operating support was provided through the respective administrators. Both the Windows and UNIX administration groups had an on call schedule for after hours support. Similarly, networking support was provided by the network engineering group which also had an on call function. The security group provided support 8x5x5 due to the fact that they did not have an on call function. After hours support for security was provided through the networking group.

3.4.8. Training Plan

Very little training was necessary for the extranet. This was due to the use of standard or existing applications, standard Cisco gear running industry standard protocols

and the use of security systems that were already in use at the MMC. A small amount of orientation and training was necessary for the support groups. The training plan called for the project team to provide a hands on orientation of the network and the supported applications once the extranet was deployed. Table 3-16 shows the training plan:

Training	Group Trained
Orientation to the network	Network Engineering
Microsoft applications (Active Directory, Email, IIS, Database)	Windows Admins, SSTs Production Support
FTP application	UNIX Admins, SSTs, Production Support
MCDN specialized applications	SSTs, Production Support

Table 3-15 Extranet Training Plan

3.5. Implementation Phase

The purpose of the implementation phase was to take the created designs and perform the necessary tasks to build the extranet. These tasks included purchasing the required equipment and material, receiving the equipment and material, installation of the physical, data link, network, transport and application layers. The major deliverable from this phase was a fully functional extranet. Additional deliverables were the "as built" diagrams for each of the physical, data link and network layers.

3.5.1. Physical Layer Implementation

Three main tasks made up the physical layer implementation: installing the copper and fiber cabling necessary to support the network, running the electrical circuits necessary to power the equipment, and finally, the placement of the racks to hold the equipment. Installing the copper and fiber cabling, as well as placing the cabinets was accomplished by the project team. Running the electrical circuits required the support of the MMC facilities department.

As stated in the design phase, Data Center 3 (DC3) was the chosen location for the implementation of the extranet. Within DC3 a great deal of attention had been paid to the physical cabling. There was a centralized structure that included end-caps in each row. These end caps all had cabling that came back to a centralized distribution point. For the most part, this infrastructure was used for the extranet. There were only two places where there was not sufficient capacity to allow for installation of equipment. In these two places, it was decided to utilize direct connectivity between the network devices (known as a home run). These two runs of cabling consisted of one pair of fibers and two cat 5e cables.

Also mentioned in the design phase, DC3 contained only standard telecommunications racks that did not have enough depth to support the servers purchased for this project. Fortunately, the other two MMC data centers contained plenty of the correct size. For this project a total of seven racks would be used. Of the seven, four needed to be retrieved from the other data centers and placed in row K of DC3. The remaining three existed in DC3 and were in the proper locations.

At the completion of the design phase, a circuit order was placed, with the facilities department, for fourteen new 110v circuits. These circuits were split into groups of seven. One of the groups of circuits came from a separate power leg. This provided redundant power to each of the seven racks. The facilities department had the circuits in place shortly after the racks were moved into the proper location. With the power installed, the project team utilized the rack elevation diagram to install the appropriate shelving, power strips and cable management in each of the seven racks.

3.5.2. Data Link Layer Implementation

As indicated in the data link layer design section, Cisco switches were chosen as the extranet layer two devices. The project team also decided to use Vlans to help segment the network. Although switches are relatively simple devices, they did require some configuration. This configuration included updating the Cisco IOS to the stable version currently in use at the MMC, assigning a management IP address to each switch, configuring the needed switch ports for the proper speed and duplex, assigning the switch ports to the appropriate Vlans, enabling the ports, and etc. To facilitate the configuration of the switches, the network engineers utilized a checklist. This checklist included both the standard switch configuration and the steps necessary to harden the switches. An example checklist can be found in the appendices.

With the installation of the physical layer cabling, it was possible to deploy the data link layer devices. It was also decided to deploy the layer three routers and firewalls at this time. This would enable proper placement of all of the networking equipment in the racks, as well as provide end to end data link layer connectivity. The deployment of

the layer three devices required the network engineers to perform a basic configuration on these devices also.

Installation of the data link layer devices, the routers and firewalls proceeded in an outside in manner. The switches and routers that bordered the ISP connectivity were placed in the racks first, and the network diagram was followed until all of the equipment had been placed. The physical layer cabling was connected to each device in turn with the exception of the connectivity to the ISP. For security reasons, this cabling remained disconnected until the entire network was installed and tested. As each cable was connected, the device configuration was verified to ensure the interface was enabled, and that the switch ports were assigned to the appropriate Virtual Lan. Connectivity between devices was verified by inspecting the layer two link light on each device. Further connectivity was verified using Cisco's CDP neighbor protocol. This phase was complete when there was complete end to end layer two connectivity.

3.5.3. Network Layer Implementation

Although the network layer routers and firewalls were physically deployed during the data link layer implementation, the initial configuration of these devices was completed prior to physical deployment. The initial configuration on the routers was similar to the initial switch configuration and included the updating of the Cisco IOS to the stable version currently in use at the MMC, assignment of a management IP address, configuration of IP addresses on each of the required interfaces, setting speed and duplex on the interfaces, enabling routing, configuring the required static routes, assigning any necessary Vlans, and etc.

The firewalls also required an initial configuration. Although somewhat similar to routers, the initial configuration for firewalls is slightly more complicated. It included updating the operating system to the MMC standard for both Cisco and Checkpoint, assigning IP addresses, speed, duplex, name and security level (Cisco only) on each interface, assigning static routes, setting up Vlans where appropriate, enabling address translations on the Checkpoint firewalls, and etc.

The final step prior to physical deployment was to develop the initial **Access Control List (ACL)** on each firewall. ACLs define what traffic is permitted through each firewall. They are based on the IP address and transport layer port of the source and destination host. For implementation purposes, the only traffic permitted by the ACLs was administrative traffic including Internet Control Message Protocol (ICMP) used to test connectivity. End-to-End layer three connectivity was verified by utilizing the ping command throughout the network. At the end of this phase the project team was able to utilize ping and telnet to access all devices on the network.

3.5.4. Transport Layer Implementation

The transport and network layers had to be implemented together. The implementation of the transport layer involved configuring the routers and firewalls to pass the appropriate layer four traffic. This traffic was determined during the planning phase. The applications that were to be used on the extranet were evaluated. Each application uses transport layer protocols to communicate between systems. For example, an ftp host connecting to an ftp server will use ports 20 and 21 to communicate. The ports used by the extranet applications were identified and the appropriate **Access Control Entries** were added to the ACLs on the firewalls.

Until the servers and applications were deployed, testing the transport layer implementation was limited. Telnet was used to simulate connections over the permitted protocols and firewall logs monitored for any denied traffic. Full testing was conducted once the application servers were installed.

3.5.5. Network Security Implementation

Although the layer three firewalls were deployed with the data link layer and configured with the network layer, there were still additional steps that needed to be taken to fully implement network security on the extranet. These steps included developing access control lists on the switches and routers, limiting communication to the network equipment to secure shell only and limiting remote connectivity to the network engineers only, requiring external authentication for remote access, setting a difficult to guess local user name and password, controlling ICMP messages, enabling port security on the switches, disabling Cisco's CDP protocol and deploying the Intrusion Detection System Network Sensors.

Once again, an outside in approach was taken to configuring the devices. Work started on the border routers and switches and proceeded to the equipment separating the MMC networks from the extranet. Access lists were deployed on all of the devices to ensure that only users from the network engineering and security groups were permitted to access the networking equipment. The ACLs verified the IP address of the originating system to ensure it belonged to the proper groups. The network equipment was also configured to only allow inbound secure shell communications. This was to eliminate the exchange of user names and passwords in the clear.

Normally, Cisco equipment does not require a user name and password to access the console port. This is an added security measure that is most often taken when equipment is placed in a shared environment. Although the extranet equipment would solely be under the control of the MMC networking group, it is standard operating procedure at the MMC to require the added security level of a difficult to guess local username and password. This was configured on all of the networking equipment.

The **Cisco Discovery Protocol (CDP)** is a very useful tool during the initial implementation of a network. However, the information exchanged between devices is not secure and can be used to attack a network. Therefore, once layer two and three communication was established this protocol was disabled on the extranet network gear.

Like CDP, Internet Control Message Protocol (ICMP), is very useful while deploying and trouble shooting a network. Unfortunately, it can also be used by malicious individuals to gather information about a network. To ensure that ICMP did not become a tool for hackers, its use was limited. Only ICMP messages from network engineering or network administrative IP addresses were permitted. Although the capability to use ICMP was limited to network engineers only, ICMP tends to be a very helpful protocol. Two messages in particular are not controlled through access lists. These are the network unreachable and administratively prohibited response messages. The proper way to ensure these messages are not sent is to disable them through the IOS configuration. This was done on all of the equipment.

On Cisco switches the IOS provides switch port security. This turns off all unneeded switch ports and limits the number of systems that can connect to active ports. This prevents a malicious individual from connecting to unused switch ports, or from

disconnecting a legitimate system from an active port and connecting an authorized system.

The final step in deploying security on the routers, switches and firewalls was to establish external authentication. Anytime a user logs onto a network device, that device has the capability of authenticating the user locally or externally. Local authentication requires an account for each user be established on the network equipment. External authentication uses a database to verify the user's credentials. A separate account on each device is not necessary. Additionally, the external server can record the user's logon attempts and, in most cases, all actions the user takes on the network equipment. For these reasons external authentication was used on the extranet equipment. This involved using the **Tacacs+** protocol. Tacacs+ is used throughout the rest of the MMC networks; therefore the required server was already in place. The network gear was configured to pass the authentication off to the appropriate Tacacs+ server. This was tested by logging into each of the network devices using the account registered with the Tacacs+ server.

The next step in deploying the network security was to deploy the network intrusion detection systems. Internet Security Systems' Real Secure was the IDS used throughout the MMC. This same system was deployed on the extranet. Network IDSes work best when they are deployed at choke points such as firewalls or routers. The placement of the network IDSes was determined during the planning phase. Implementing them involved placing the equipment in the racks, spanning the appropriate ports, registering the network sensors with the IDS control system and deploying the initial rule set to the sensor. Spanning a port involves enabling a switch port to copy all

of the traffic from one switch port to another. This allows the Network Sensor to see all of the traffic passing through the original port. This is accomplished in real time, and no latency or loss is introduced through this process. Registering the sensor with the control systems requires the administrator to instruct the control system to go out and attach to the sensor. This is done by IP address and user account. Once communication between the control system and the sensor is established, the initial rule set is pushed to the sensor. The rule set pushed to the extranet sensors included all of the rules currently being monitored on the rest of the MMC sensors as well as specific rules for internet connectivity.

3.5.6. Deployment of the Supporting Network Applications

The supporting network applications consist of the operating systems, the network naming service, Simple Mail Transport Protocol and Internet services. During the planning phase, priorities were established for the deployment of the applications. Table 3-15, located earlier in this chapter, illustrates these priories.

3.5.6.1.Windows Operating System and Active Directory Controllers

The majority of the devices placed on the extranet were Windows based. They required an active directory infrastructure. Therefore, the first priority in installing the supporting network applications was to set up the Windows active directory controllers. Two controllers were placed on the extranet. This involved installing and patching the operating system and anti-virus software, configuring the servers as primary and secondary active directory controllers, and finally, physically deploying the servers.

3.5.6.2.Domain Name Service Servers

The Domain Name Service is critical for all applications. It is used to map a user friendly system name to an IP address. For example, ExtraMailServer.priv might be mapped to 10.17.20.10. For the extranet a specialized DNS appliance from InfoBlox was used. The appliance, DNS one, has a hardened Linux operating system. The implementation of this device involved ensuring that the latest revision of proprietary code was deployed on the system and that all security patches were properly applied, configuring the IP address, configuring the Domain Name Zones and physically deploying the appliance.

3.5.6.3.Email Servers

The next critical application deployed was the Email system. During the planning phase, Microsoft Exchange was selected as the email system. This required the installation of the Windows operating system, as well as, the exchange software. The operating system and applications were properly patched. Anti-virus was deployed and updated. The operating system and Exchange were configured. Finally, the server was physically deployed.

3.5.6.4.Internet Services

Next on the priority list were servers to support internet services. These included a World Wide Web server and an FTP server. The World Wide Web (WWW) server selected during the planning phase was Microsoft's Internet Information Server (IIS). This, of course, required the installation of the Windows operating system. As with the email server, the operating system was installed, patched, and configured, followed by the installation and patching of IIS.

The FTP application selected was a secure ftp application that ran on Linux. Therefore, the UNIX administrators installed and configured the operating system and application. The MMC used Red Hat as the standard Linux operating system. As with the Windows applications, all of the appropriate security and operating system patches were also deployed. Unlike the Windows systems however, anti-virus was not required on the Linux system.

3.5.6.5.Database and File Servers

Microsoft SQL was selected as the database application. The Windows operating system, along with the SQL application was installed, patched and configured. Additional development was required to set up the appropriate databases on this server. These were primarily tenant databases and already existed on servers residing on the MMC networks. This eased the configuration as the existing database schema and data could be copied to the new server.

The only requirement for file servers was on the tenant network. The storage requirements on the file servers were limited enough that a separate network attached storage device was not necessary. All of the storage requirements were met with a standard Windows server with a moderately sized redundant array of disk. A standard installation of the Windows operating system provided the controls necessary to facilitate the file shares. The operating system was properly configured and patched, and the anti-virus software was installed, patched and configured.

3.5.7. Host Based Security

As stated in the security design section of this document, one of the requirements for the extranet was layered security. Several layers of this design have already been

discussed; these include the deployment of firewalls, the hardening of the network equipment and the deployment of an intrusion detection system. One of the most important layers, however, was host based security. Two important aspects of host based security occurred during the server installation and configuration. This was the patching of the operating system and the deployment of anti-virus software. Additional steps taken to harden the hosts were to disable all unnecessary services, enable appropriate logging and deploy host based intrusion detection sensors on critical hosts.

By default, most Windows operating systems have all available services enabled. This makes it very easy to configure and deploy the system; however it makes them very insecure. To eliminate the unneeded services, the project team had to review the purpose of each server, determine the underlying services the system needed to properly function and turn off all other unnecessary services. The servers were reviewed individually. The active directory controllers required only the standard Microsoft active directory services, all other services were shut down. The DNS server was a purpose built appliance; therefore, it was already hardened. The only services running on the appliance were the DNS service and a small web server for administration. On the email servers, only the SMTP service was allowed to run. The IIS server had several services enabled by default, these included: WWW, FTP, Telnet and etc. All services except WWW were turned off. The FTP server was a Linux system; therefore, the majority of the services were off by default. The only service running on the system was Secure FTP and Secure Shell for administration. On the database server only SQL was enabled. The file server required the standard Windows file sharing services.

Logging on most servers can be configured to monitor important events. Again, each server was reviewed and appropriate logging enabled. On all systems administrative access was recorded. This included successful administrative activity, as well as, failed activity. Other items of interest on the systems included domain related events for the active directory controllers, Email logging on the exchange servers, web access activity on the IIS server, successful and failed FTP attempts on the ftp server, SQL transactions on the database server and file access successes and failures on the file server.

The last step in host security was to select the critical servers and deploy host based intrusion detection sensors. The project team identified the critical servers as all servers on the Web DMZ as they would be internet facing and the active directory controllers. Real Secure host based sensor applications were installed on each of the critical servers. These applications were configured to communicate with the Real Secure management module. On this module, entries were made for the new sensors and communication between the sensors and the management station was established. Real Secure has several rule sets native to a standard installation. Three of these standard rule sets were deployed to the host sensors; these were the Windows web, the Linux web and the Windows Active Directory rule sets.

3.5.8. Implementation Testing

Testing the implementation consisted of two steps. First, was the connectivity testing. This ensured that all of the appropriate connectivity was in place for all of the systems to communicate properly. The second step was security testing. This ensured that all of the appropriate security measures were in place to protect the network.

3.5.9. Connectivity Testing

It was important for the project team to ensure that all of the devices on the network could communicate properly. In the data link and network layer implementation phases, initial connectivity testing was conducted. This consisted of, at the data link layer, ensuring that all devices had link lights on the appropriate interfaces and at the network layer, that ICMP could be used to communicate throughout the network. Further connectivity testing involved placing a workstation on each of the subnets, logging on to the workstation using the Active Directory, and then connecting to email, SQL and file servers. Connectivity from the tenant subnets to the Internet and between the servers was also tested.

3.5.10. Security Testing

As important, if not more important than the connectivity testing, was the security testing. The purpose of these tests was to ensure that only permitted traffic traversed the network, and that only authorized users could gain access to specific devices. Testing occurred from the outside in. Access to the extranet and the MMC network was tested from outside the Internet screening firewall. The only inbound Internet traffic permitted should have been WWW and Secure FTP traffic bound for the servers on the web DMZ. This was confirmed. All other access attempts other than to the web DMZ failed.

Next, connectivity between the segments on the extranet was tested. The only permitted traffic should have been to the active directory controllers, the email, database, file and SQL servers and the Internet. No traffic should have been allowed between segments or from the extranet to the MMC networks. This was tested by placing a host on each of the segments and attempting to connect between the hosts and to the servers.

Traffic between the hosts was denied and traffic to the servers was permitted. An additional test was conducted to ensure that workstations on the segments could only access the appropriate services on the servers. For example, only DNS traffic should have been allowed from the workstation to the DNS appliance. This was tested by attempting to telnet, ftp, http and etc. to the different servers. The test results showed that only connectivity to permitted services was successful. All other connection attempts failed.

3.5.11. Project Documentation

Documentation is often the least favorite task when building a new network. However, due to the significant work load at the MMC, documentation is vital. Although the engineer that builds the network understands the inner workings of what has been built, that engineer is not always the one troubleshooting the network should a problem occur. The standard method for ensuring that everyone on the networking team has the information needed about each and every network is through documentation. Table 3-16 illustrates the required documentation.

Documentation	Purpose
Network Logical Drawing	Illustrate the physical, data link and network layers Gives logical locations of subnets Illustrates IP addressing scheme
Network Physical Drawing	Illustrates the physical location of the network equipment
IP address scheme	Documents the IP addressing scheme and serves as a central location for assigning addresses
Initial Configuration of network equipment	Documents the original configuration of all network gear Serves as a benchmark to measure configuration changes

Table 3-16 Documentation Requirements

3.6. Support Phase

When the extranet was built, the MMC had no formal hand-off procedure for transitioning a project from the development/implementation phase to the operations and support phase. When the project team was satisfied that the network was deployed properly and in accordance with MMC standards and all of the documentation was complete and thorough, they scheduled a meeting with the network engineering group. At this meeting, the project team requested that they conduct a review of the network including the documentation. The outcome of the review was suggestions from the

engineering group on modifications they wanted made prior to supporting the network. These changes were made. The network group agreed that the extranet was ready to be supported.

The last step before final transition to the operations/support phase was final acceptance by the internal customers. Meetings were scheduled with the senior director sponsoring the project and tenant representatives. At these meetings the documentation for the network was presented along with the results from the connectivity and security testing. The senior director recommended placing the MCDN test systems on the network to verify proper functionality. Also, a few trial users from the tenant networks were placed on the extranet. After a trial period of two weeks, the customers certified the extranet as ready for operation.

The transition was made from development to operation. The network engineering group added the extranet to the "on call" support duties. The UNIX and Windows administrator groups began supporting the operating system, and the production support group began supporting the extranet applications.

The final wrap up involved meetings with the team to discuss the project outcome, and lessons learned. These lessons are detailed in later sections of this document.

3.7. Review of Deliverables From Each Phase

This project consisted of five main phases. They were the planning, analysis, design, implementation and the support phases. The project manager also believed that testing was extremely important, and therefore decided to include testing as a major component of the implementation phase. The deliverables from each phase were:

Planning Phase

- Initial Design
- Project Budget
- Project Schedule
- Feasibility Analysis
- Staffing Plan

Analysis Phase

- Business Requirements
- Technical Requirements
- Pre-Implementation Requirements
- Training Requirements
- Management Review and Buy Off

Design Phase

- Physical Layer Design
- Data Link Layer Design
- Network Layer Design
- Transport Layer Design
- Network Security Design
- Application Deployment Design
- Support Plan
- Training Plan
- Test Plan

Implementation Phase

- Functional Extranet
- Physical Layer "As Built Diagram"
- Data link Layer "As Built Diagram"
- Network Layer "As Built Diagram"
- Test Results
- Network Engineering Buy Off
- Internal Customer Buy Off
- Tenant Buy Off

Support Phase

- Acceptance of Extranet by Support Organizations

3.8. Review of Milestones From Each Phase

The project manager utilized the established schedule to track the major milestones for each phase. These included:

Planning Phase

- Problem Definition
- Feasibility Study Results
- Project Staffing Plan

Analysis Phase

- Definition of Requirements
- Initial Design Selection
- Management and Customer Review and Buy Off of Initial Design

Design Phase

- Physical Layer Design
- Data Link Layer Design
- Network Layer Design
- Transport Layer Design
- Network Security Design
- Application Deployment Design
- Support Plan Design
- Training Plan
- Design Review

Implementation Phase

- Capital Authorization Form Creation
- Request for Purchase Order Creation
- Capital Authorization Form Approval
- Request for Purchase Order Approval
- Submission of Purchase Orders to Vendors
- Delivery of Equipment
- Category Five Copper Cable Installation
- Fiber Optic Cable Installation
- Power Installation
- Rack Installation
- In Rack Power Installation
- In Rack Wiring Guide Installation

- Layer Two Switch Configuration and Installation
- Layer Three Router Configuration and Installation
- Layer Three Firewall Configuration and Installation
- Layer Two and Three Connectivity Testing
- Installation and Configuration of Applications
- Network Security Implementation
- Connectivity, Functionality and Security Testing
- Review and Buy Off

Support Phase

- Transition of the Extranet to the MMC Support Organizations

3.9. Project Outcomes

The major outcome of this project was a fully functional extranet that met the original design goals of segmentation, flexibility, extendibility, extensibility and security. The project also was completed on schedule and within the established budget. The completed extranet conformed to the Cisco tiered architecture design, ensuring that there was an access layer, a distribution layer and a core layer. This resulted in a modular network that could easily be expanded in the future. The extranet security conformed to a layered design where overlapping countermeasures compensated for necessary holes. The concept of layered security was fully realized with the implementation of dual firewalls from different manufacturers, host based security, network hardening and network and host based intrusion detection.

The completion of this project gave the MMC a badly needed platform for business expansion. The extranet provided the MMC a place to isolate vendors and business partners while granting them controlled access to MMC resources. Although the extranet was built to meet the needs of two main business objectives, upon completion, there were several additional MMC projects inquiring as to how the extranet could meet their needs.

3.10. Summary of Project Methodology

This project followed the system development lifecycle. Traditionally, this methodology utilizes five phases for managing a project. Although this methodology is not normally used for the development of a network, the project manager felt that using it would provide a systematic approach that might become a standard in the future.

The system development lifecycle was implemented using the waterfall approach where each phase led into the next subsequent one. In many cases the deliverables from one phase became the inputs to the next. This allowed the manager to run the project by following the schedule and ensuring that the deliverables from each phase were completed on time.

Although the SDLC is not traditionally used for the deployment of networks, it is the project manager's opinion that it worked very well for this project. With a little adaptation this method could be used for all future network deployments at the MMC. The project team recommended that this methodology be adopted by the MMC Information Technology Department.

Chapter 4

4. Project History

4.1. How the Project Began

The origins of this project actually stretch back two years prior to the project manager's initial proposal to the senior director in spring of 2004. The concept of an extranet had been pitched in multiple forms numerous times to senior management. The need for an extranet was anticipated by the Information Technology Department as early as 2001. Unfortunately, due to the large initial investment, no one on the senior team wanted to sponsor the project. Two major factors combined to push the need for an extranet to the forefront. These were the need to comply with the regulatory environment, especially Sarbanes-Oxley, and the need to secure vendor and business partner connectivity to MMC resources. The MMC Manager of Network Security identified the security needs and found a project sponsor on the senior team. The director responsible for the MCDN accepted the need for the extranet and commissioned the project.

4.2. How the Project Was Managed

The project methodology used, the SDLC, is documented in multiple sections of this paper. Employing the waterfall method with the SDLC allowed the use of industry standard management techniques. The main tools used were the schedule, the list of deliverables and the milestones. The schedule was managed with Microsoft Project. A weekly Integrated Project Team (IPT) meeting was held. Prior to the meeting, the team updated the schedule to accurately reflect the weekly status. At the meeting, the status

was reviewed, constraints were discussed and solutions developed for any constraint that jeopardized the project. The manager was responsible for ensuring that any constraints jeopardizing the schedule were solved.

The team was made up of employees from multiple departments. This necessitated the use of a matrix management approach. The manager was responsible for coordinating with the team member's department heads to ensure the employee was available, when needed. Due to the heavy work load at the MMC, the team members were not dedicated to this project. They were also members of other IPTs. Therefore, the manger was responsible for coordinating with other team leaders to ensure there were no conflicts.

4.3. Was the Project Considered a Success?

The extranet was definitely considered a success. A functional network was delivered that fulfilled the goals of the project. This was done on time and within budget. The objectives were to build an extranet that was flexible, extendible and extensible. Additionally, the extranet had to segment the tenants and business partners from the MMC networks while providing controlled access to MMC resources. A layered security model also had to be used. All of those objectives were met. By implementing Cisco layered architecture with the access, distribution and core layers, the extranet was able to support multiple business, as well as, connectivity methods.

4.4. What Changes Occurred to the Plan?

Very few changes occurred to the original plan until the extranet was completed. Minor changes occurred to the IP addressing scheme, as well as the logical location of

some of the devices. The original IP addressing scheme called for the management interface on the networking devices to be on the same subnet as the equipment connecting to it. This was modified, and all management interfaces were placed within the same subnetted class C network. This simplified the access control lists. Initially, the Web DMZ was located off of the core router with a separate firewall. This was modified early in the planning phase to place the Web DMZ off of the screening firewall. This was reflected in all of the design documentation.

Major changes occurred once the extranet was placed into production. Multiple business units requested segments on the extranet. Some of the business units required alternative connectivity to the extranet including dedicated circuits and VPNs. The extranet was flexible enough to accommodate all of the new businesses, as well as the connectivity methods.

4.5. How did the Project End?

Officially the project ended when the network engineering department and application support departments took over responsibility for the operation of the extranet. Prior to this, there was an acceptance test period for both the support organizations and the customers. The support organizations performed acceptance testing first. Their goal was to ensure the extranet conformed to the MMC networking standards. With a few minor modifications, this testing was successful and the support groups accepted the network. The customer testing involved ensuring the extranet performed as needed. This was accomplished by placing systems on the extranet and allowing them to function normally for a two week period. This went flawlessly and the customers accepted the extranet. With this acceptance, the project team was dissolved and the project concluded.

4.6. What Went Right and What Went Wrong With the Project?

There were definitely more things that went right, than went wrong. There were only minor problems throughout the project. The first obstacle that had to be overcome was a problem with some of the switches on the tenant network. The plan called for using fiber optical cable to interconnect all of the switches to the routers. The only place copper connectivity was to be used was from the end devices to the switches and from the switches to the firewalls. Unfortunately, two incorrect switches were ordered. They did not have fiber interfaces. The project manager overcame this obstacle by identifying another project that could use the incorrect switches while trading fiber capable switches that could be used on the extranet.

One problem encountered by the network engineer was that the Cisco IOS differed depending on the capabilities of the switches even within the same switch family. The network engineer was upgrading the IOS on some switches; he had the proper IOS image for the 48 port fiber capable switches he was working with. He attempted to load this image on a switch with slightly different capabilities. This failed rendering the switch unusable. To fix the problem, the network engineer had to transfer the new image using the serial console port. This was a very long and difficult process.

During this project the MMC network engineering department maintained a spreadsheet of assigned IP addresses for the MMC networks. This spreadsheet was not shared. Therefore, only one individual could make changes to the sheet at a time. This caused an issue with entry of the extranet IP addresses. All of the addresses, except those for the Web DMZ management segment, were entered correctly. The Web DMZ management segment IPs were entered but did not get saved correctly. This ultimately

resulted in overlapping IP address space with a subsequent project. Since then, the IP address spreadsheet has been shared correctly so that multiple people can access it at the same time.

One of the most significant aspects that went right with the project was the cooperation and teamwork within the project team. Everyone worked exceptionally well together ensuring that any issues that did arise were quickly dealt with.

The MMC network engineering group standardizes on a Cisco IOS, and an initial router and switch configuration. This eased the job of configuring and deploying the switches. Although the network engineer could have directly loaded the standard configuration, then modified it for the extranet, he chose to manually configure the switches using the standard as a template. This provided the network engineer a great deal of experience in configuring switches and routers.

The underlying infrastructure present within the MMC made the deployment of the extranet much easier. There was existing infrastructure in place for the majority of the extranet. This included connectivity within the data center, from data center three to the other two data centers and to all of the IDFs. This minimized the amount of new cabling that needed to be installed. In most cases all that was needed was the addition of a few cross connect cables.

4.7. Project Summary

Although this project had a rocky beginning, once sponsorship was gained and budget approved, it went very well. The use of the waterfall method and the SDLC to design and implement a network worked exceptionally well. The structure provided by the project management techniques ensured that any problems that occurred were

identified early and solutions quickly enacted. The matrix management method for leading the team was at times challenging, but the team worked extremely well together and accomplished all of the goals for the project. The final product produced has become an indispensable addition to the MMC.

Chapter 5

5. Lessons Learned

5.1. What was Learned from the Project Experience?

The lessons learned fall into two categories, project management and technical. For project management, the use of the SDLC and the waterfall method provided the manager with valuable experience. Many organizations within the MMC use the SDLC for development of information systems. The author believes that this is the first time the SDLC was used to design and implement a network. The experience provided him with the knowledge and skills to work more closely with the other departments within the MMC that utilize the SDLC.

This was also the first time the project manager has lead a matrix team. He is normally the Manager of Network Security and has direct lines of responsibility and although he has been a member of a matrix team before, this was his first opportunity to lead one. This gave him experience in coordinating with multiple organizations including several departments and other project teams. The project manager had a great deal of experience managing and leading employees. He learned to use those management skills to lead a group of individuals that did not directly report to him.

This project gave the manager an opportunity to practice his presentation skills. Although the he has had positions where he gave presentations on a regular basis, since moving into the Information Technology field his opportunity for presentations has been limited. Additionally, this was a slightly different type of presentation. He had to present technical material to a non-technical audience.

There were many technical lessons learned from this project. One of the major reasons the author chose to pursue a master's degree in information technology was to increase his technical knowledge. The author was both the project manager and the network engineer. As the network engineer he was able to practice many of the technical skills learned through Regis.

The author learned to configure and deploy both routers and switches. He was also able to increase his skills in deploying firewalls. He gained a much better understanding of the overall network design, configuration and deployment process. Although he knew how to configure a firewall or router to perform routing, he was able to see the end-to-end process of routing through an entire network. The author also received first hand experience in designing and deploying layer two Virtual Lans. Conceptually, he understood how Vlans worked and what they were used for, but the extranet allowed him to put that knowledge to use.

5.2. What Would have Been Done Differently?

This was a very successful project. There is very little that could have been done differently. No project, though, is perfect. One thing the author would change is the method used at the MMC for tracking IP addresses. Although the duplicate IP addressing did not specifically impact the extranet project, it did have a major impact on subsequent projects. If a more robust system of IP address tracking had been used, these problems could have been avoided.

From a technical point of view the extranet was extremely successful. It met all of the requirements identified in the analysis phase. The project manager, however, encountered a non-technical problem after the extranet was completed. Many of the

MMC managers and business owners had expectations about the capabilities of the extranet that were not supported in reality. One of the major problematic expectations was with Virtual Private Network connectivity. Although the extranet needed to provide for this capability, the actual termination and management of VPNs was constrained by the limited staff available within the MMC network security department. The resources to terminate and manage large numbers of VPNs were never a requirement for the extranet project. During the planning phase, when the project manager asked about terminating significant numbers of VPNs on the extranet, he was told by the project customers that this was not a capability that was needed. Although it was clearly communicated to the project customers, other project managers and business owners within the facility had the mistaken understanding that the extranet would have the capability of terminating large numbers of VPNs. The project manager should have communicated the resource limitations of the security department more clearly to all of the interested business owners and project managers.

5.3. Did the Project Meet the Initial Expectations?

Based on the problem definition and requirements, this project fully met the initial expectations. The project manager did deal with a significant amount of expectation creep. As more people within the MMC became aware of the extranet project they all began to have plans for its use. Fortunately, it was built to be flexible, expandable and extensible so the majority of the business needs could be met. Adding businesses requirements to the extranet would, unfortunately, require a small amount of additional investment. This caused issues as many people believed that the extranet would support

their project as soon as it was complete. It did meet the expectations of the original project customers.

5.4. What Would be the Next Stage of Evolution for the Project if Continued?

The next logical step for this project would have been to move the tenants and the content providers to the network. This did occur, however, it was not as timely as it could have been. The tenant move was hampered by the service level agreements contained within their new leases. This took some time for the legal teams on both sides to resolve. The final move occurred three months after completion of the extranet.

Additional evolution could have been for content providers and business partners to have access to the FTP server. This occurred very quickly after the completion of the extranet. Within the first month after completion, seven content providers requested and were granted access to the FTP server.

One very logical next stage would have been to implement redundancy on the extranet. Given the original requirements for the extranet, redundancy was not necessary. On completion of the extranet there were several projects requesting functionality that included connectivity through the extranet. Based on these requests, and senior management's projections for growth, it was obvious that the extranet should be made redundant as soon as possible.

5.5. Conclusions

This project utilized the SDLC with the waterfall method to develop and deploy a network. This deviated from the traditional methods used at the MMC for network deployment. The project manager utilized knowledge and skills gained through his

master's degree program to accomplish this task. The most important conclusion that can be drawn from this project is that, with minor modifications, the System Development Life Cycle can be used to design and implement a variety of systems. It is not limited to software or database development.

A layered network design was chosen over several alternatives for this project. Based on the success of the tenant transition, the MCDN vendor transition, as well as the numerous projects requiring extranet access, it can be concluded that the correct design was chosen. Since completion of the extranet, several of the projects requesting access to it have been completed, requiring its expansion. Due to the layered and modular design these expansions were very successful. The extranet has given the MMC added capabilities it did not have prior to the completion of this project.

Included in the layered network was layered security. This layered security has allowed for the addition of secured connectivity from multiple sources. The decision to implement a layered security model with the layered network has resulted in the creation of a secure environment where multiple types of external connectivity can be terminated.

5.6. Project Summary

There were two major business drivers for the extranet project: securing external connectivity from content providers and vendors and providing a comparable networking environment for the tenants so that they could be removed from the MegaComm networks. This project satisfied both of those objectives. The System Development Life Cycle with the waterfall method was used as the project methodology. This was the first time they had been used at the MegaComm Media Center for this purpose. This provided

a very structured process for developing and deploying networks. This should become the standard method used by the MMC in the future.

The author was able to apply knowledge and skills learned through the master's degree program at Regis University. He believes that this project was instrumental in cementing his knowledge and skills. Not only did the project provide him the opportunity to hone his technical skills, it also gave him the opportunity to practice new management skills, and refresh his presentations skills. Looking at where the extranet project began, where it has come and where it is most likely to go, it is clear that this project was valuable and successful for both the MegaComm Media Center and the author.

References

Definitions. (2004). Retrieved October 7, 2004, from SearchCIO.com Web site: http://searchcio.techtarget.com/sDefinition/0,290660,sid19_gci214411,00.html

Harris, Shon. (2002). *CISSP All-in-one Certification Exam Guide*. Berkley, CA: McGraw-Hill/Osborne.

Koch, Christopher. (2004, July). The SarBox Conspiracy. *Cio*(July 15, 2005), 58-66.

Lammle, Todd. (2001). *Cisco Certified Network Associate Study Guide* (3rd ed.). Alameda, CA: Sybex, Inc.

Marcus, J. Scott. (1999). *Designing Wide Area Networks and Internetworks*. Reading, MA: Addison Wesley Longman, Inc.

Sarbanes-Oxley. (2005). Retrieved June 17, 2005, from www.webopedia.com Web site: http://www.webopedia.com/TERM/S/Sarbanes_Oxley.html

Satzinger, Robert G. Jackson, & Stephen D. Burd. (2002). *System Analysis and Desgin*. Boston: Course Technology, Inc.

The 7 Layers of the OSI Model. (2004). Retrieved October 12, 2004, from www.webopedia.com Web site: http://www.webopedia.com/quick_ref/OSI_Layers.asp

Bibliography

Ciampa, Mark. Security+ Guide to Network Security Fundamentals 2nd ed. Boston, MA: Course Technology Inc, 2005

Goldman, James and Phillip T. Rawles. Local Area Networks A business-Oriented Approach 2nd Ed. New York, NY. John Wiley & Sons, Inc 2000.

Greensberg, Paul. Customer Relationship Management at the Speed of Light. Emeryville, CA. McGraw-Hill/Osborne 2004.

Harris, Shon. CISSP All-in-One Certification Exam Guide. Berkley, CA: McGraww-Hill/Osborne, 2002.

Howlett, Tony. Open Source Security Tools A Practical Guide to Security Applications. Upper Saddle River, NJ. Prentice Hall 2005.

Koch, Christopher. "The SarBox Conspiracy." CIO 1 July 2004: 58 – 66.

Lammle, Todd. Cisco Certified Network Associate Study Guide 3rd ed. Alameda, CA: Sybex Inc, 2001.

Marcus, J. Scott. Designing Wide Area Networks and Internetworks a Practical Guide. Reading, MA. Addison Wesley Longman, Inc. 1999.

Microsoft. Windows Server System. Windows Server 2003 Active Directory. June 17, 2005 retrieved from: http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx

Satzinger, John W, Robert G. Jackson and Stephen D. Burd. System Analysis and Design. Boston, MA: Course Technology Inc, 2002.

SearchCIO.com Definitions. 2004 SearchCIO.Com. October 7, 2004 http://searchcio.techtarget.com/sDefinition/0,,sid19_gci214411,00.html

Skodis, Ed. Counter Hack A Step-by-Step Guide to Computer Attacks and Effective Defenses. Upper Saddle River, NJ. Prentice Hall 2002.

Stevens, Richard. TCP/IP Illustrated Volume 1 The Protocols. Indianapolis, IN. Pearson Education, 1994.

The Honeynet Project. Know Your Enemy Learning about Security Threats. Boston, MA. Pearson Education, Inc. 2004.

Tipton, Harold F. and Micki Krause. Information Security Management Handbook 4th ed. Boca Raton, FL. CRC Press 2000.

Treese, G. Winfield and Lawrence C. Stewart. Designing Systems for Internet Commerce 2nd ed. Boston, MA: Pearson Education Inc, 2003.

Webopedia. Sarbanes-Oxley. Webopedia.com retrieved on June 17, 2005 from: http://www.webopedia.com/TERM/S/Sarbanes_Oxley.html

Webopedia. The 7 Layers of the OSI Model. 2004 Webopedia.com. October 12, 2004. http://www.webopedia.com/quick_ref/OSI_Layers.asp

Whitman, Michael E. and Herbert J. Mattord. Principles of Information Security 2nd ed. Boston, MA: Course Technology Inc, 2005

Appendix A

Glossary of Terms

Access Control Entry - An Access Control Entry is an individual element contained within an Access Control List that grants a specific entity rights

Access Control List - A list of entities, usually either usernames or system addresses, that are granted specific permissions to access a computer system or device

Active Directory – A central component of the Windows platform that provides the means to manage the identities, rights, and relationships that make up a networking environment (Microsoft Windows Server System 1)

Application Layer – The seventh layer of the Open System Interconnect reference model, supplying services to applications like electronic mail or file transfer that are outside the OSI model (Lammle, 2001, 611)

Business-to-Business (E-Biz) –Business-to-Business is the exchange of products, services or information between businesses rather than between businesses and consumers (Definitions, 2004)

Category 5 Cable - A cable consisting of four twisted pair of copper wire terminated in an RJ-45 connector. Category 5 cable can support speeds up to 1 Gbps. Most often this cable is used for Ethernet networks.

CDDI (Copper Distributed Data Interface) - is a local area network standard used at the physical layer of the Open System Interconnect model and is closely related to Fiber Distributed Data Interface. It uses a token ring media access method and can Support speeds up to 200 mbps (Lammle, 2001, 636).

Cisco Discovery Protocol – The Cisco proprietary protocol that is used to tell a neighboring Cisco device about the type of hardware, software, version, IP information, and active interfaces that the Cisco device is using (Lammle, 2001, 621)

MegaComm Content Delivery Network – A network designed by the MegaComm Media Center for the distribution of digital content, usually video, to cable headends

Data Link Layer – The second layer of the Open System Interconnect model responsible for the trustworthy transmission of data over a physical link and is primarily concerned with physical addressing, line discipline, network topology, error notifications, ordered delivery of frames and flow control (Lammle, 2001, 628)

Demilitarized Zone – A separate network that operated between the un-trusted Internet and the trusted secure networks that provides access from the Internet to selected services such as a World Wide Web site.

Domain Name System – A network system designed to translate a human friendly system name to a network Internet Protocol address.

Ethernet - A Local Area Network standard operating at the data link layer of the Open System Interconnect model. Ethernet uses a Carrier Sense Multiple Access/Collision Detection method for accessing the physical media and operates over various cable at 10 Mbps

Extranet – a network for extending a certain level of connectivity to external parties that have special relationships with the organization – customers, suppliers, collaborators, shareholder and other stakeholders – but who do not have the same level of trust as internal users (Marcus, 1999)

FDDI (Fiber Distributed Data Interface) - is a local area network standard that uses token-passing media access on fiber optical cable to achieve operational speeds of 200 Mbps

File Transfer Protocol – One of the protocols within the TCP/IP suite of protocols, operating at the application layer it is responsible for moving files between systems

Firewall – A network device used to control access into and out of a network. The tree main types of firewalls are packet filtering, stateful, and application firewalls

Hyper Text Transfer Protocol – One of the protocols within the TCP/IP suite of protocols that operates at the application layer and is the underlying protocol used by the World Wide Web. HTTP is responsible for defining how messages are formatted and transmitted and what actions are taken by Web servers and Web browsers

Intranet – A private network usually built on the TCP/IP suite of protocols that belongs to a single organization

Intrusion Detection System – A networking device used to monitor, detect, analyze, and report potentially malicious activity on hosts and networks. An IDS is made up of network and host sensors and a management console. The sensors are responsible for activity detection. The management console analyzes monitors and reports suspicious activity.

Local Area Network – A network linking two or more computers or systems within a limited geographical region. They are typically high-speed, low-error networks within an organization.

Network Layer – The third layer of the Open System Interconnect model responsible for routing which enables connections and path selection between two end systems (Lammle, 2001, 655)

Open Systems Interconnect - A conceptual reference model developed by the International Organizations for Standards, describing how any combination of devices can be connected for the purpose of communication.

Physical Layer – The first layer of the Open Systems Interconnect model responsible for converting data packets from the Data Link Layer into electrical signals.

Point-to-Point – A network connection over private circuits. A point-to-point circuit does not use any public accessible network connectivity.

Presentation Layer – The sixth layer of the Open System Interconnect model that defines how data is formatted, presented, encoded and converted for use by software at the application layer (Lammle, 2001, 661)

Router – A network layer device that uses one or metrics to decide on the best path to use for transmission of network traffic (Lammle, 2001, 666)

Sarbanes-Oxley – A 2002 law designed to oversee financial reporting for finance professionals. Its purpose is to review legislative audit requirements and to protect investors by improving the accuracy and reliability of corporate disclosures (Sarbanes-Oxley, 2005)

Secure Shell – One of the application layer protocols in the TCP/IP family of protocols used to create an encrypted command shell connection between two hosts

Session Layer – The fifth layer of the Open System Interconnect model that is responsible for creating, managing, and terminating session between applications and overseeing data exchange between presentation layer entities (Lammle, 2001, 668)

Switch – A data link layer device that is responsible for multiple functions including filtering, flooding and sending frames. It utilizes the end systems hardware address to accomplish its tasks (Lammle, 2001, 675)

System Development Life Cycle – A planned undertaking, which is normally a large job that produces a new system (Satzinger, Robert G. Jackson, & Stephen D. Burd, 2002)

Tacacs+ - Terminal Access Controller access Control System is a protocol used to communicate between a device and a remote authentication server (Lammle, 2001, 676)

Token Ring – A token-passing local area network technology developed by IBM. It is capable of running at up to 16 Mbps over a ring topology (Lammle, 2001, 678)

Transport Layer – The forth layer of the Open System Interconnect model that is responsible for reliable communication between end nodes over the network. The Transport layer provides mechanisms for establishing, maintaining, and terminating connections as well as transport fault detection and recovery, and information flow control (Lammle, 2001, 678)

Virtual Local Area Network – A group of devices on a logically segmented local area network that allows devices to communicate as if they were attached to the same physical media (Lammle, 2001, 680)

Virtual Private Network – The use of encryption to secure private network communications that use public networks for transport

World Wide Web – A system of servers on the Internet that support special documents formatted using Hyper Text Markup Language and transported using Hyper Text Transport Protocol

Appendix B

Diagrams

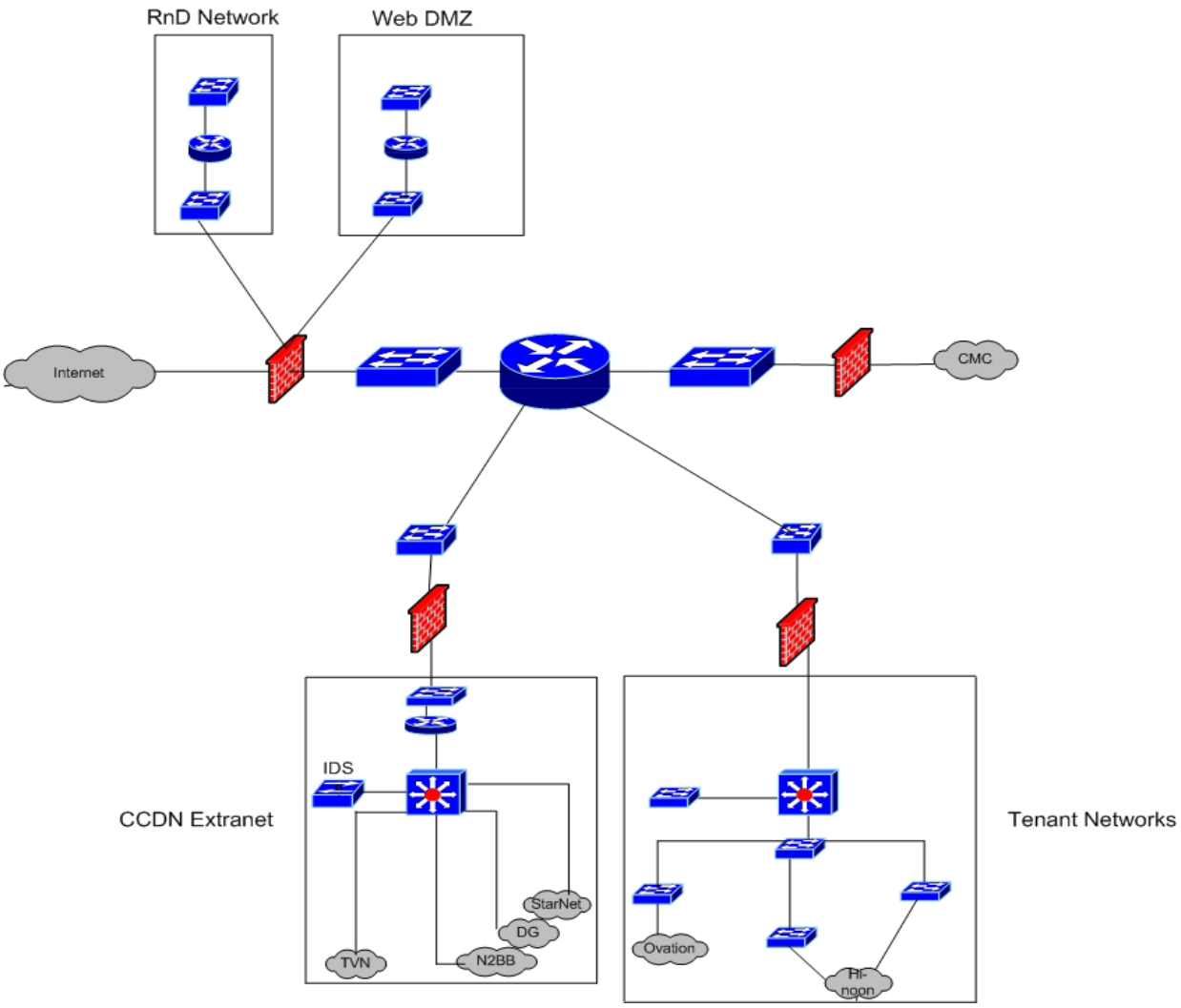

Figure B-1 Proposed Extranet Design

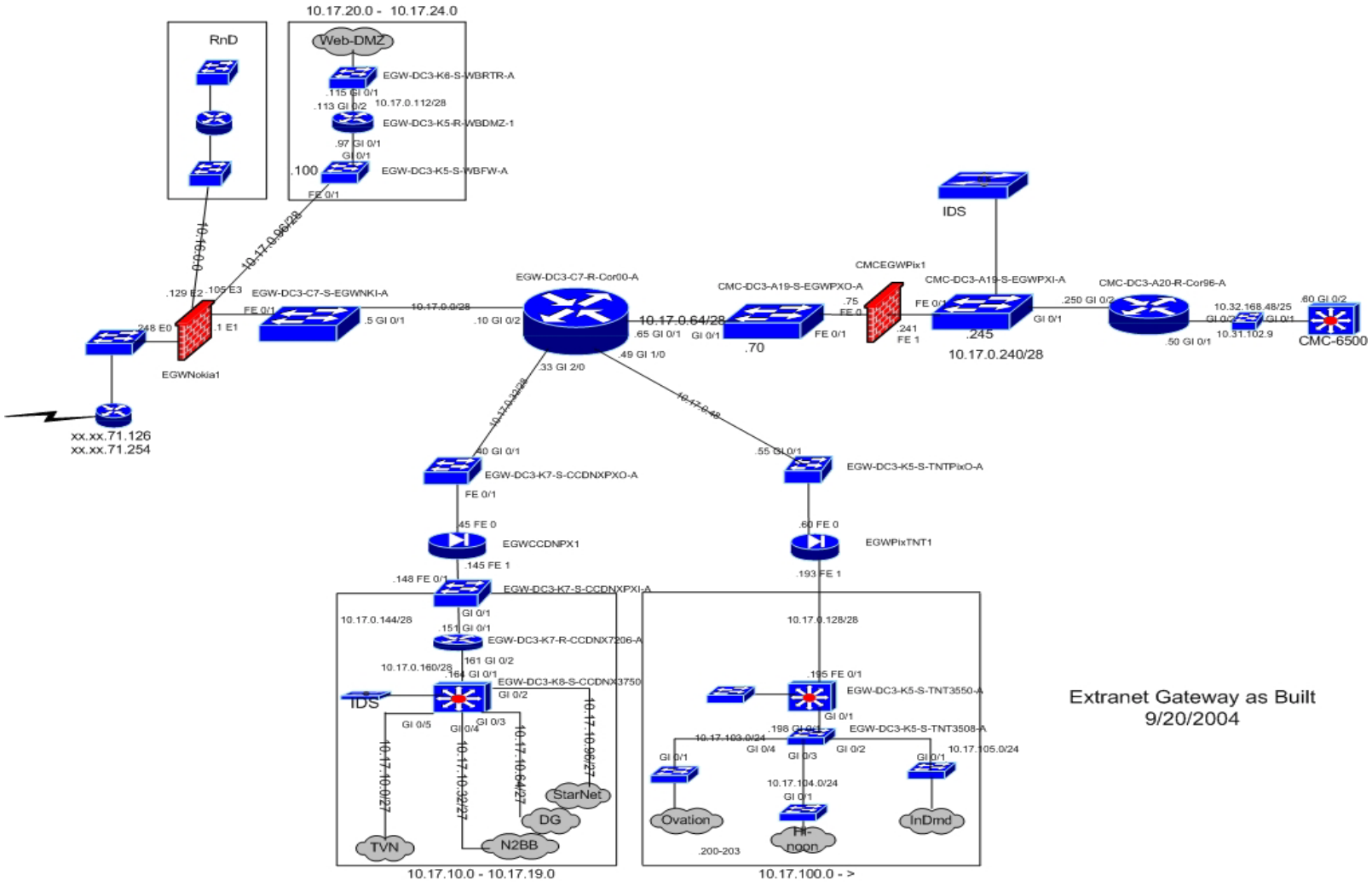

Figure B-2 Extranet As Built

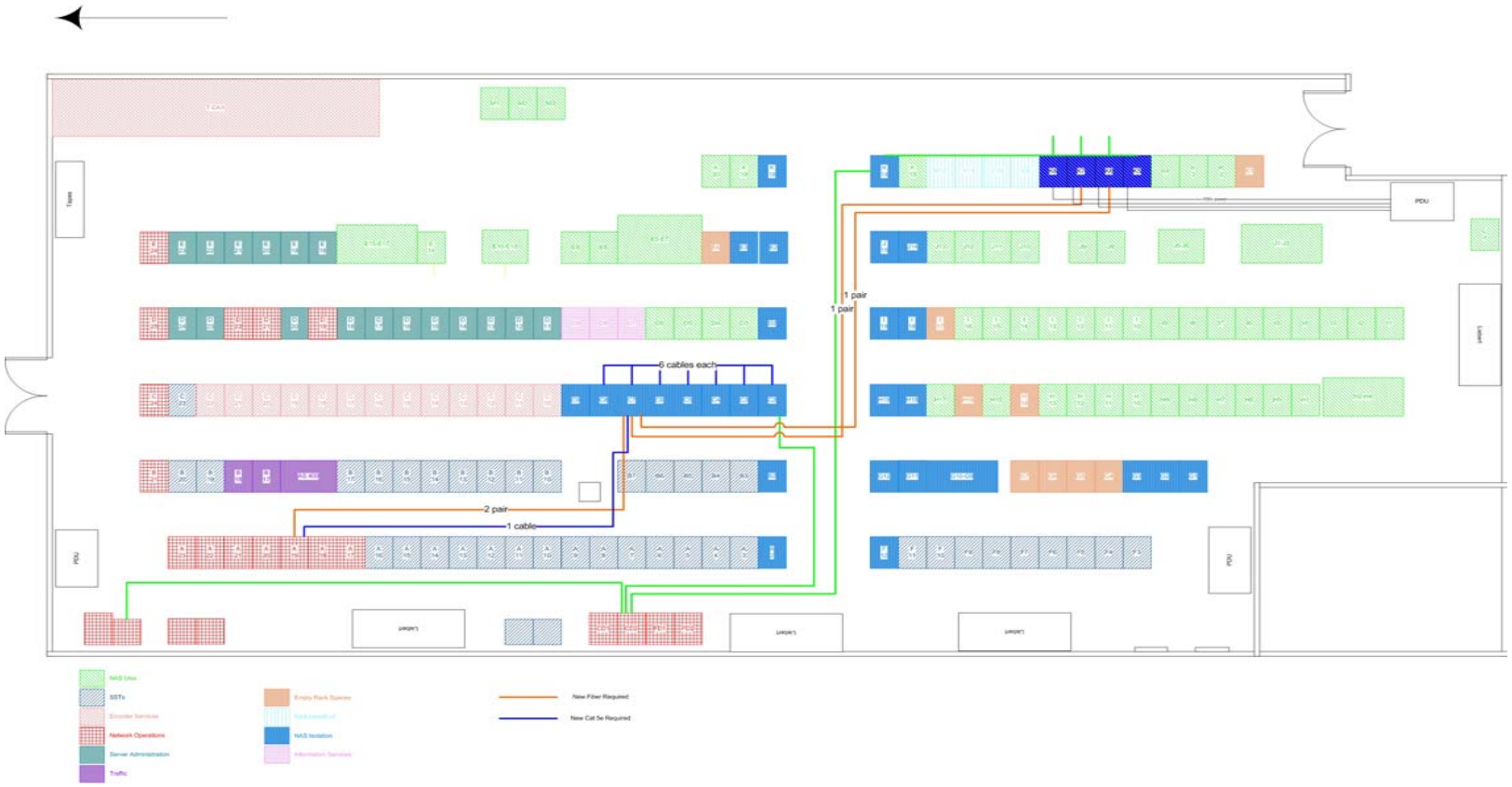

Figure B-3 Extranet Physical Layer

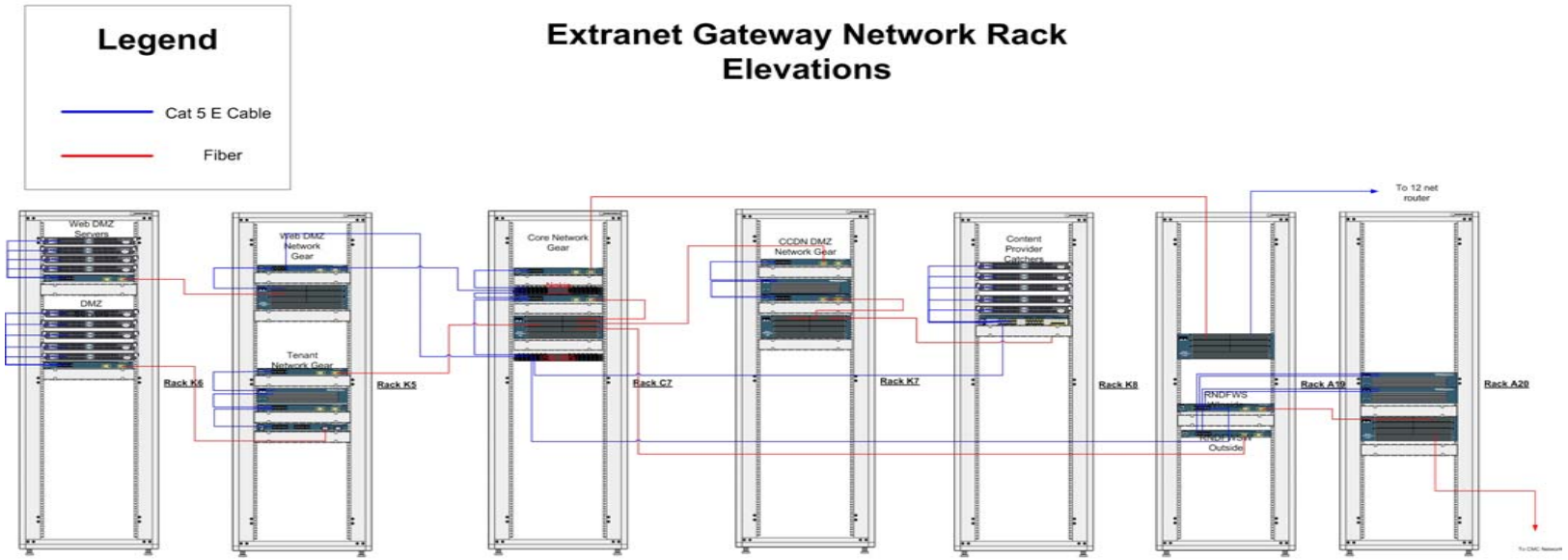

Figure B-4 Rack Elevations

Appendix C

Project Plan

Project Start Date: Fri 3/5/04
Project Finish Date: Wed 9/22/04

Extranet Gateway Project Plan

Name	Percent Complete	Start Date	Finish Date
Extranet Gateway	100%	Fri 3/5/04	Wed 9/22/04
Planning	100%	Fri 3/5/04	Mon 3/15/04
Problem Definition	100%	Fri 3/5/04	Fri 3/5/04
Determine Feasibility	100%	Fri 3/5/04	Fri 3/5/04
Develop Budget	100%	Fri 3/5/04	Fri 3/5/04
Produce The Project Schedule	100%	Fri 3/5/04	Thu 3/11/04
Staff The Project	100%	Fri 3/12/04	Fri 3/12/04
Project Launch	100%	Mon 3/15/04	Mon 3/15/04
Analysis	100%	Tue 3/16/04	Tue 4/13/04
Information Gathering	100%	Tue 3/16/04	Fri 4/2/04
System Requirements Definition	100%	Mon 4/5/04	Tue 4/6/04
Requirement Prioritization	100%	Wed 4/7/04	Wed 4/7/04
Alternative Generation And Selection	100%	Thu 4/8/04	Thu 4/8/04
Management Review	100%	Tue 4/13/04	Tue 4/13/04
Design	100%	Fri 3/5/04	Fri 6/18/04
Physical Layer Design	100%	Tue 5/25/04	Thu 6/17/04
Determine Equipment Location	100%	Tue 5/25/04	Tue 5/25/04
Rack Elevation Design	100%	Wed 5/26/04	Tue 6/1/04
Create Physical Wiring Diagram	100%	Wed 5/26/04	Tue 6/1/04
Determine Power Requirements	100%	Tue 6/1/04	Wed 6/2/04
Create A Power Diagram	100%	Thu 6/3/04	Mon 6/14/04
Determine If Current Infrastructure Exists	100%	Wed 5/26/04	Tue 6/15/04
Copper	100%	Wed 5/26/04	Wed 5/26/04
Fiber	100%	Wed 5/26/04	Wed 5/26/04
Power	100%	Fri 6/11/04	Tue 6/15/04
Racks	100%	Wed 5/26/04	Wed 5/26/04

Shelves	100%	Wed 5/26/04	Wed 5/26/04
Wire Management	100%	Wed 5/26/04	Wed 5/26/04
Other Hardware	100%	Wed 5/26/04	Wed 5/26/04
Determine Need For New Infrastructure	100%	Wed 6/16/04	Wed 6/16/04
Copper	100%	Wed 6/16/04	Wed 6/16/04
Fiber	100%	Wed 6/16/04	Wed 6/16/04
Power	100%	Wed 6/16/04	Wed 6/16/04
Racks	100%	Wed 6/16/04	Wed 6/16/04
Shelves	100%	Wed 6/16/04	Wed 6/16/04
Wire Management	100%	Wed 6/16/04	Wed 6/16/04
Other Hardware	100%	Wed 6/16/04	Wed 6/16/04
New Infrastructure Deployment Plan	100%	Thu 6/17/04	Thu 6/17/04
Copper	100%	Thu 6/17/04	Thu 6/17/04
Determine Category Of Cable	100%	Thu 6/17/04	Thu 6/17/04
Design Infrastructure	100%	Thu 6/17/04	Thu 6/17/04
Fiber	100%	Thu 6/17/04	Thu 6/17/04
Determine Type Of Fiber	100%	Thu 6/17/04	Thu 6/17/04
Design Infrastructure	100%	Thu 6/17/04	Thu 6/17/04
Power	100%	Thu 6/17/04	Thu 6/17/04
Determine New Circuit Types	100%	Thu 6/17/04	Thu 6/17/04
Determine Type Of Power Strip	100%	Thu 6/17/04	Thu 6/17/04
Racks	100%	Thu 6/17/04	Thu 6/17/04
Shelves	100%	Thu 6/17/04	Thu 6/17/04
Wire Management	100%	Thu 6/17/04	Thu 6/17/04
Other Hardware	100%	Thu 6/17/04	Thu 6/17/04
Design Physical Layer Security	100%	Wed 5/26/04	Wed 5/26/04
Limited Access Area	100%	Wed 5/26/04	Wed 5/26/04
Rack Locks	100%	Wed 5/26/04	Wed 5/26/04
Surveillance	100%	Wed 5/26/04	Wed 5/26/04
Data Link Layer	100%	Wed 4/7/04	Mon 6/7/04
Determine Layer 2 Devices	100%	Wed 4/7/04	Wed 4/7/04
Determine Layer 2 Devices Port Density	100%	Wed 4/7/04	Wed 4/7/04
Determine Vlan Requirements	100%	Tue 6/1/04	Fri 6/4/04
Determine VTP Domains	100%	Mon 6/7/04	Mon 6/7/04

Design The Vlans	100%	Mon 6/7/04	Mon 6/7/04
Determine Layer 2 Protocols (Trunking And Etc)	100%	Mon 6/7/04	Mon 6/7/04
Network Layer	100%	Wed 4/7/04	Wed 6/16/04
Determine Layer 3 Protocol	100%	Wed 4/7/04	Wed 4/7/04
Determine Layer 3 Address Scheme	100%	Mon 6/14/04	Mon 6/14/04
Determine Layer 3 Devices	100%	Wed 4/7/04	Wed 4/7/04
Determine Routing Method (Static Vs. Dynamic)	100%	Wed 4/7/04	Wed 4/7/04
If Dynamic Routing Is Used Determine Routing Protocol	100%	Wed 4/7/04	Wed 4/7/04
If Dynamic Routing Is Used Determine Routing Domains	100%	Wed 4/7/04	Wed 4/7/04
If Static Routing Is Used Determine The Static Routes	100%	Tue 6/15/04	Wed 6/16/04
Design Layer 3 Security	100%	Wed 4/7/04	Tue 6/15/04
Firewalls	100%	Wed 4/7/04	Wed 4/7/04
Acls	100%	Tue 6/15/04	Tue 6/15/04
Ids	100%	Wed 4/7/04	Wed 4/7/04
Transport Layer	100%	Wed 6/16/04	Thu 6/17/04
Determine The Level Of Layer 4 Port Security Needed	100%	Wed 6/16/04	Wed 6/16/04
Design The Layer 4 Port Security	100%	Thu 6/17/04	Thu 6/17/04
Upper Layers (5-7)	100%	Fri 3/5/04	Wed 4/7/04
Determine The OS For Each Server	100%	Wed 4/7/04	Wed 4/7/04
Determine The Applications For Each Server	100%	Wed 4/7/04	Wed 4/7/04
Email	100%	Wed 4/7/04	Wed 4/7/04
Dns	100%	Wed 4/7/04	Wed 4/7/04
Wins	100%	Wed 4/7/04	Wed 4/7/04
Aaa	100%	Wed 4/7/04	Wed 4/7/04
Www	100%	Wed 4/7/04	Wed 4/7/04
Web Access	100%	Wed 4/7/04	Wed 4/7/04
Design The Domains For Each Application/Service	100%	Fri 3/5/04	Fri 3/5/04
Windows Domain/Active Directory	100%	Fri 3/5/04	Fri 3/5/04
Organizational Units	100%	Fri 3/5/04	Fri 3/5/04

Service Accounts	100%	Fri 3/5/04	Fri 3/5/04
User Accounts	100%	Fri 3/5/04	Fri 3/5/04
Shared Directories	100%	Fri 3/5/04	Fri 3/5/04
Directory Permissions	100%	Fri 3/5/04	Fri 3/5/04
User Permissions	100%	Fri 3/5/04	Fri 3/5/04
Email Domain	100%	Fri 3/5/04	Fri 3/5/04
Email Accounts	100%	Fri 3/5/04	Fri 3/5/04
Email Groups	100%	Fri 3/5/04	Fri 3/5/04
Public Folders	100%	Fri 3/5/04	Fri 3/5/04
Shared Email Resources	100%	Fri 3/5/04	Fri 3/5/04
Conference Rooms	100%	Fri 3/5/04	Fri 3/5/04
Calendars	100%	Fri 3/5/04	Fri 3/5/04
DNS Domain	100%	Fri 3/5/04	Fri 3/5/04
Design Zones	100%	Fri 3/5/04	Fri 3/5/04
Static Host Records	100%	Fri 3/5/04	Fri 3/5/04
Wins Domain	100%	Fri 3/5/04	Fri 3/5/04
Backup Domain	100%	Fri 3/5/04	Fri 3/5/04
Printing	100%	Fri 3/5/04	Fri 3/5/04
Determine The Network Management Software	100%	Wed 4/7/04	Wed 4/7/04
Acs	100%	Wed 4/7/04	Wed 4/7/04
Cisco Works	100%	Wed 4/7/04	Wed 4/7/04
Determine The Anti-Virus System	100%	Wed 4/7/04	Wed 4/7/04
Determine Project Milestones	100%	Fri 6/18/04	Fri 6/18/04
Design Review	100%	Fri 6/18/04	Fri 6/18/04
Implementation	100%	Fri 5/7/04	Fri 8/27/04
Purchasing	100%	Fri 5/7/04	Mon 6/21/04
Create Capital Authorization Form	100%	Fri 5/7/04	Fri 5/7/04
Create Rpos	100%	Fri 5/7/04	Fri 5/7/04
Caf Approval	100%	Fri 5/14/04	Fri 5/14/04
RPO Approval	100%	Fri 5/14/04	Fri 5/14/04
Create Pos	100%	Mon 5/17/04	Tue 5/18/04
Submit Pos	100%	Wed 5/19/04	Wed 5/19/04
Receive Layer 2 Equipment	100%	Thu 5/20/04	Mon 6/21/04
Receive Routers	100%	Thu 5/20/04	Thu 5/20/04

Receive Firewalls	100%	Thu 5/20/04	Thu 5/20/04
Receive Upper Layer Equipment	100%	Thu 5/20/04	Thu 5/20/04
Physical Layer	100%	Thu 5/27/04	Thu 6/24/04
Run Copper As Necessary	100%	Thu 6/17/04	Wed 6/23/04
Run Fiber As Necessary	100%	Thu 6/17/04	Wed 6/23/04
Run Power As Necessary	100%	Wed 6/16/04	Thu 6/24/04
Circuits To Rack Locations	100%	Wed 6/16/04	Tue 6/22/04
Power Strips In Racks	100%	Wed 6/23/04	Thu 6/24/04
Place Racks As Necessary	100%	Wed 6/16/04	Thu 6/17/04
Install Rack Equipment (Shelves, Wire Management And Etc) As Necessary	100%	Fri 6/18/04	Mon 6/21/04
Install Physical Security As Necessary	100%	Thu 5/27/04	Fri 6/18/04
Card Readers	100%	Thu 5/27/04	Thu 5/27/04
Rack Locks	100%	Fri 6/18/04	Fri 6/18/04
Surveillance	100%	Thu 5/27/04	Thu 5/27/04
Extranet Gateway Core	100%	Tue 6/22/04	Fri 8/6/04
Data Link Layer	100%	Tue 6/22/04	Fri 8/6/04
Mmc-Dc3-A19-S-Egwpxi-A	100%	Tue 6/22/04	Fri 6/25/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Tue 6/22/04	Tue 6/22/04
Configure Switch (Use Checklist)	100%	Wed 6/23/04	Wed 6/23/04
Label Devices	100%	Tue 6/22/04	Tue 6/22/04
Label Cables	100%	Tue 6/22/04	Tue 6/22/04
Rack Devices	100%	Thu 6/24/04	Thu 6/24/04
Connect Devices	100%	Fri 6/25/04	Fri 6/25/04
Egw-Dc3-A-19-S-Egwpxo-A	100%	Tue 7/6/04	Thu 7/8/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Tue 7/6/04	Tue 7/6/04
Configure Switch (Use Checklist)	100%	Wed 7/7/04	Wed 7/7/04
Label Devices	100%	Tue 7/6/04	Tue 7/6/04
Label Cables	100%	Tue 7/6/04	Tue 7/6/04
Rack Devices	100%	Thu 7/8/04	Thu 7/8/04
Connect Devices	100%	Thu 7/8/04	Thu 7/8/04
Egw-Dc3-C7-Egwnki-A	100%	Wed 7/14/04	Fri 7/16/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Wed 7/14/04	Wed 7/14/04

Configure Switch (Use Checklist)	100%	Thu 7/15/04	Thu 7/15/04
Label Devices	100%	Thu 7/15/04	Thu 7/15/04
Label Cables	100%	Thu 7/15/04	Thu 7/15/04
Rack Devices	100%	Fri 7/16/04	Fri 7/16/04
Connect Devices	100%	Fri 7/16/04	Fri 7/16/04
Egw-Dc3-C7-Egwnko-A	100%	Wed 8/4/04	Fri 8/6/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Wed 8/4/04	Wed 8/4/04
Configure Switch (Use Checklist)	100%	Thu 8/5/04	Thu 8/5/04
Label Devices	100%	Thu 8/5/04	Thu 8/5/04
Label Cables	100%	Thu 8/5/04	Thu 8/5/04
Rack Devices	100%	Fri 8/6/04	Fri 8/6/04
Connect Devices	100%	Fri 8/6/04	Fri 8/6/04
Network Layer	100%	Tue 6/22/04	Tue 8/3/04
Mmc-Dc3-A20-R-Cor96-A	100%	Tue 6/22/04	Fri 6/25/04
Ensure The Proper IOS Image Is On Each Router	100%	Tue 6/22/04	Tue 6/22/04
Configure The Router (Use Checklist)	100%	Wed 6/23/04	Wed 6/23/04
Label Routers	100%	Tue 6/22/04	Tue 6/22/04
Label Cables	100%	Tue 6/22/04	Tue 6/22/04
Rack Routers	100%	Thu 6/24/04	Thu 6/24/04
Connect Routers	100%	Fri 6/25/04	Fri 6/25/04
Egw-Dc3-C7-R-Cor00-A	100%	Fri 7/9/04	Tue 7/13/04
Ensure The Proper IOS Image Is On Each Router	100%	Fri 7/9/04	Fri 7/9/04
Configure The Router (Use Checklist)	100%	Mon 7/12/04	Mon 7/12/04
Label Routers	100%	Mon 7/12/04	Mon 7/12/04
Label Cables	100%	Mon 7/12/04	Mon 7/12/04
Rack Routers	100%	Tue 7/13/04	Tue 7/13/04
Connect Routers	100%	Tue 7/13/04	Tue 7/13/04
Mmcegwpix1	100%	Thu 7/1/04	Mon 7/5/04
Ensure The Proper IOS Is Each Cisco Firewall	100%	Thu 7/1/04	Thu 7/1/04
Configure The Firewalls (Use Checklist)	100%	Fri 7/2/04	Fri 7/2/04
Label Firewalls	100%	Mon 7/5/04	Mon 7/5/04
Label Cables	100%	Mon 7/5/04	Mon 7/5/04

Rack Firewalls	100%	Mon 7/5/04	Mon 7/5/04
Connect Firewalls	100%	Mon 7/5/04	Mon 7/5/04
Egwnokia1	100%	Mon 7/19/04	Tue 8/3/04
Ensure The Proper OS Revision And Software Level	100%	Mon 7/19/04	Mon 7/19/04
Configure The Firewalls (Use Checklist)	100%	Tue 7/20/04	Mon 8/2/04
Label Firewalls	100%	Tue 7/20/04	Tue 7/20/04
Label Cables	100%	Tue 7/20/04	Tue 7/20/04
Rack Firewalls	100%	Tue 8/3/04	Tue 8/3/04
Connect Firewalls	100%	Tue 8/3/04	Tue 8/3/04
Tenant Network	100%	Wed 7/14/04	Thu 8/19/04
Data Link Layer	100%	Wed 7/14/04	Thu 8/19/04
Egw-Dc3-K5-S-Tntpxi-A	100%	Wed 7/14/04	Fri 7/16/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Wed 7/14/04	Wed 7/14/04
Configure Switch (Use Checklist)	100%	Thu 7/15/04	Thu 7/15/04
Label Devices	100%	Wed 7/14/04	Wed 7/14/04
Label Cables	100%	Wed 7/14/04	Wed 7/14/04
Rack Devices	100%	Fri 7/16/04	Fri 7/16/04
Connect Devices	100%	Fri 7/16/04	Fri 7/16/04
Egw-Dc3-K5-S-Tntpxo-A	100%	Mon 7/19/04	Thu 7/22/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Mon 7/19/04	Tue 7/20/04
Configure Switch (Use Checklist)	100%	Tue 7/20/04	Wed 7/21/04
Label Devices	100%	Mon 7/19/04	Mon 7/19/04
Label Cables	100%	Mon 7/19/04	Mon 7/19/04
Rack Devices	100%	Wed 7/21/04	Thu 7/22/04
Connect Devices	100%	Thu 7/22/04	Thu 7/22/04
Egw-Dc3-K5-R-Tnt3550-A	100%	Tue 7/27/04	Thu 8/5/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Tue 7/27/04	Wed 7/28/04
Configure Switch (Use Checklist)	100%	Wed 7/28/04	Wed 8/4/04
Label Devices	100%	Tue 7/27/04	Tue 7/27/04
Label Cables	100%	Tue 7/27/04	Tue 7/27/04
Rack Devices	100%	Wed 8/4/04	Thu 8/5/04
Connect Devices	100%	Thu 8/5/04	Thu 8/5/04

Egw-Dc3-K5-S-Tnt3508-A	100%	Thu 8/5/04	Mon 8/16/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Thu 8/5/04	Fri 8/6/04
Configure Switch (Use Checklist)	100%	Fri 8/6/04	Fri 8/13/04
Label Devices	100%	Thu 8/5/04	Thu 8/5/04
Label Cables	100%	Thu 8/5/04	Thu 8/5/04
Rack Devices	100%	Fri 8/13/04	Mon 8/16/04
Connect Devices	100%	Mon 8/16/04	Mon 8/16/04
EGW-IDF-S-Tntovation1-A	100%	Mon 8/16/04	Thu 8/19/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Mon 8/16/04	Tue 8/17/04
Configure Switch (Use Checklist)	100%	Tue 8/17/04	Wed 8/18/04
Label Devices	100%	Mon 8/16/04	Mon 8/16/04
Label Cables	100%	Mon 8/16/04	Mon 8/16/04
Rack Devices	100%	Wed 8/18/04	Thu 8/19/04
Connect Devices	100%	Thu 8/19/04	Thu 8/19/04
EGW-IDF6-S-Tnthinoon1-A	100%	Mon 8/16/04	Thu 8/19/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Mon 8/16/04	Tue 8/17/04
Configure Switch (Use Checklist)	100%	Tue 8/17/04	Wed 8/18/04
Label Devices	100%	Mon 8/16/04	Mon 8/16/04
Label Cables	100%	Mon 8/16/04	Mon 8/16/04
Rack Devices	100%	Wed 8/18/04	Thu 8/19/04
Connect Devices	100%	Thu 8/19/04	Thu 8/19/04
EGW-IDF7-S-Tnthinoon1-A	100%	Mon 8/16/04	Thu 8/19/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Mon 8/16/04	Tue 8/17/04
Configure Switch (Use Checklist)	100%	Tue 8/17/04	Wed 8/18/04
Label Devices	100%	Mon 8/16/04	Mon 8/16/04
Label Cables	100%	Mon 8/16/04	Mon 8/16/04
Rack Devices	100%	Wed 8/18/04	Thu 8/19/04
Connect Devices	100%	Thu 8/19/04	Thu 8/19/04
Network Layer	100%	Mon 7/19/04	Tue 7/27/04
Egw-Dc3-K5-R-Tnt3550-A	100%	Thu 7/22/04	Tue 7/27/04
Ensure The Proper IOS Image Is On Each Router	100%	Thu 7/22/04	Fri 7/23/04

Configure The Router (Use Checklist)	100%	Fri 7/23/04	Mon 7/26/04
Label Routers	100%	Thu 7/22/04	Thu 7/22/04
Label Cables	100%	Thu 7/22/04	Thu 7/22/04
Rack Routers	100%	Mon 7/26/04	Tue 7/27/04
Connect Routers	100%	Tue 7/27/04	Tue 7/27/04
Egwpixtnt1	100%	Mon 7/19/04	Wed 7/21/04
Ensure The Proper IOS Is Each Cisco Firewall	100%	Mon 7/19/04	Mon 7/19/04
Configure The Firewalls (Use Checklist)	100%	Tue 7/20/04	Tue 7/20/04
Label Firewalls	100%	Mon 7/19/04	Mon 7/19/04
Label Cables	100%	Mon 7/19/04	Mon 7/19/04
Rack Firewalls	100%	Wed 7/21/04	Wed 7/21/04
Connect Firewalls	100%	Mon 7/19/04	Mon 7/19/04
Egw Web Dmz	100%	Wed 7/14/04	Mon 7/26/04
Data Link Layer	100%	Wed 7/14/04	Mon 7/26/04
Egw-Dc3-K5-S-Wbfw-A	100%	Wed 7/14/04	Fri 7/16/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Wed 7/14/04	Wed 7/14/04
Configure Switch (Use Checklist)	100%	Thu 7/15/04	Thu 7/15/04
Label Devices	100%	Wed 7/14/04	Wed 7/14/04
Label Cables	100%	Wed 7/14/04	Wed 7/14/04
Rack Devices	100%	Fri 7/16/04	Fri 7/16/04
Connect Devices	100%	Fri 7/16/04	Fri 7/16/04
Egw-Dc3-K5-S-Wbrtr-1	100%	Thu 7/22/04	Mon 7/26/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Thu 7/22/04	Thu 7/22/04
Configure Switch (Use Checklist)	100%	Fri 7/23/04	Fri 7/23/04
Label Devices	100%	Thu 7/22/04	Thu 7/22/04
Label Cables	100%	Thu 7/22/04	Thu 7/22/04
Rack Devices	100%	Mon 7/26/04	Mon 7/26/04
Connect Devices	100%	Mon 7/26/04	Mon 7/26/04
Network Layer	100%	Mon 7/19/04	Wed 7/21/04
Egw-Dc3-K5-R-Wb7206-A	100%	Mon 7/19/04	Wed 7/21/04
Ensure The Proper IOS Is On Router	100%	Mon 7/19/04	Mon 7/19/04
Configure The Router (Use Checklist)	100%	Tue 7/20/04	Tue 7/20/04
Label Rotuer	100%	Mon 7/19/04	Mon 7/19/04

Label Cables	100%	Mon 7/19/04	Mon 7/19/04
Rack Firewalls	100%	Wed 7/21/04	Wed 7/21/04
Connect Firewalls	100%	Wed 7/21/04	Wed 7/21/04
Mcdn Providers	100%	Wed 7/14/04	Tue 8/3/04
Data Link Layer	100%	Wed 7/14/04	Tue 8/3/04
Egw-Dc3-K7-S-Mcdnxpxi-A	100%	Wed 7/14/04	Fri 7/16/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Wed 7/14/04	Wed 7/14/04
Configure Switch (Use Checklist)	100%	Thu 7/15/04	Thu 7/15/04
Label Devices	100%	Wed 7/14/04	Wed 7/14/04
Label Cables	100%	Wed 7/14/04	Wed 7/14/04
Rack Devices	100%	Fri 7/16/04	Fri 7/16/04
Connect Devices	100%	Fri 7/16/04	Fri 7/16/04
Egw-Dc3-K7-S-Mcdnxpxo-A	100%	Thu 7/22/04	Mon 7/26/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Thu 7/22/04	Thu 7/22/04
Configure Switch (Use Checklist)	100%	Fri 7/23/04	Fri 7/23/04
Label Devices	100%	Thu 7/22/04	Thu 7/22/04
Label Cables	100%	Thu 7/22/04	Thu 7/22/04
Rack Devices	100%	Mon 7/26/04	Mon 7/26/04
Connect Devices	100%	Mon 7/26/04	Mon 7/26/04
Egw-Dc3-K8-S-Mcdnx3750-A	100%	Fri 7/30/04	Tue 8/3/04
Ensure Proper IOS Image Is On Each Layer 2 Device	100%	Fri 7/30/04	Fri 7/30/04
Configure Switch (Use Checklist)	100%	Mon 8/2/04	Mon 8/2/04
Label Devices	100%	Fri 7/30/04	Fri 7/30/04
Label Cables	100%	Fri 7/30/04	Fri 7/30/04
Rack Devices	100%	Tue 8/3/04	Tue 8/3/04
Connect Devices	100%	Tue 8/3/04	Tue 8/3/04
Network Layer	100%	Mon 7/19/04	Thu 7/29/04
Egwmcdnpx1	100%	Mon 7/19/04	Wed 7/21/04
Ensure The Proper IOS Is Each Cisco Firewall	100%	Mon 7/19/04	Mon 7/19/04
Configure The Firewalls (Use Checklist)	100%	Tue 7/20/04	Tue 7/20/04
Label Firewalls	100%	Mon 7/19/04	Mon 7/19/04
Label Cables	100%	Mon 7/19/04	Mon 7/19/04

Rack Firewalls	100%	Wed 7/21/04	Wed 7/21/04
Connect Firewalls	100%	Wed 7/21/04	Wed 7/21/04
Egw-Dc3-K7-R-Mcdnx7206-A	100%	Tue 7/27/04	Thu 7/29/04
Ensure The Proper IOS Image Is On Each Router	100%	Tue 7/27/04	Tue 7/27/04
Configure The Router (Use Checklist)	100%	Wed 7/28/04	Wed 7/28/04
Label Routers	100%	Tue 7/27/04	Tue 7/27/04
Label Cables	100%	Tue 7/27/04	Tue 7/27/04
Rack Routers	100%	Thu 7/29/04	Thu 7/29/04
Connect Routers	100%	Thu 7/29/04	Thu 7/29/04
Transport Layer	100%	Tue 6/22/04	Fri 8/27/04
Configure Intrusion Detection System	100%	Thu 8/19/04	Fri 8/27/04
Ensure Proper Level Of OS Is On Each IDS	100%	Thu 8/19/04	Fri 8/20/04
Install IDS Software	100%	Fri 8/20/04	Tue 8/24/04
Connect Sensor To Management Station	100%	Tue 8/24/04	Wed 8/25/04
Configure The Sensor Policy	100%	Wed 8/25/04	Thu 8/26/04
Deploy The Sensor Policy	100%	Thu 8/26/04	Fri 8/27/04
Upper Layers (5-7)	100%	Tue 6/22/04	Thu 8/26/04
Configure Network OS And Application Servers	100%	Tue 6/22/04	Tue 6/22/04
Install OS On Servers	100%	Tue 6/22/04	Tue 6/22/04
Patch OS	100%	Tue 6/22/04	Tue 6/22/04
Install Anti-Virus	100%	Tue 6/22/04	Tue 6/22/04
Update Anti-Virus	100%	Tue 6/22/04	Tue 6/22/04
Load Applications On Servers	100%	Tue 6/22/04	Tue 6/22/04
Email	100%	Tue 6/22/04	Tue 6/22/04
Create Email Accounts	100%	Tue 6/22/04	Tue 6/22/04
Dns	100%	Tue 6/22/04	Tue 6/22/04
Create Zones	100%	Tue 6/22/04	Tue 6/22/04
Create Records For Static Hosts	100%	Tue 6/22/04	Tue 6/22/04
Wins	100%	Tue 6/22/04	Tue 6/22/04
Configure Domains	100%	Tue 6/22/04	Tue 6/22/04
Create Organizational Units	100%	Tue 6/22/04	Tue 6/22/04
Create Service Accounts	100%	Tue 6/22/04	Tue 6/22/04
Label Servers	100%	Tue 6/22/04	Tue 6/22/04

Label Cables	100%	Tue 6/22/04	Tue 6/22/04
Rack Servers	100%	Tue 6/22/04	Tue 6/22/04
Connect Servers	100%	Tue 6/22/04	Tue 6/22/04
Configure Network Management Applications	100%	Thu 8/19/04	Thu 8/26/04
Cisco ACS	100%	Thu 8/19/04	Thu 8/26/04
Cisco Works	100%	Thu 8/19/04	Thu 8/26/04
Snmpc	100%	Thu 8/19/04	Thu 8/26/04
Openview	100%	Thu 8/19/04	Thu 8/26/04
Migration	100%	Wed 8/4/04	Mon 8/9/04
Migrate 12 Net Connectivity To Nokia	100%	Wed 8/4/04	Thu 8/5/04
Migrate Existing 172.16 Network To Nokia	100%	Fri 8/6/04	Mon 8/9/04
Test	100%	Fri 6/25/04	Fri 8/27/04
Physical Layer	100%	Fri 6/25/04	Fri 6/25/04
Cable Tester	100%	Fri 6/25/04	Fri 6/25/04
Link Lights	100%	Fri 6/25/04	Fri 6/25/04
Data Link Layer	100%	Wed 8/4/04	Wed 8/4/04
Check Protocol On Switch	100%	Wed 8/4/04	Wed 8/4/04
Cisco CDP/CDP Neighbor	100%	Wed 8/4/04	Wed 8/4/04
Network Layer	100%	Wed 8/4/04	Wed 8/4/04
Ping The Following:	100%	Wed 8/4/04	Wed 8/4/04
Local Host	100%	Wed 8/4/04	Wed 8/4/04
Default Gateway	100%	Wed 8/4/04	Wed 8/4/04
Remote Host	100%	Wed 8/4/04	Wed 8/4/04
Ping Or Trace Router Across Entire Network	100%	Wed 8/4/04	Wed 8/4/04
Deploy A Workstation On Each Subnet And Test The Following:	100%	Wed 8/4/04	Wed 8/4/04
Ping Each Workstation From Each Router	100%	Wed 8/4/04	Wed 8/4/04
Ping From Workstation To Authorized Destinations (Testing Firewalls And Acls)	100%	Wed 8/4/04	Wed 8/4/04
Transport Layer	100%	Thu 8/5/04	Fri 8/27/04
With A Host On Each Subnet Test Connectivity To:	100%	Thu 8/26/04	Fri 8/27/04

Email	100%	Thu 8/26/04	Fri 8/27/04
Dns	100%	Thu 8/26/04	Fri 8/27/04
Wins	100%	Thu 8/26/04	Fri 8/27/04
Domain	100%	Thu 8/26/04	Fri 8/27/04
Internet	100%	Thu 8/26/04	Fri 8/27/04
Printers	100%	Thu 8/26/04	Fri 8/27/04
File Shares	100%	Thu 8/26/04	Fri 8/27/04
From Outside The Screening Firewall	100%	Thu 8/5/04	Thu 8/5/04
Scan The Internal Networks	100%	Thu 8/5/04	Thu 8/5/04
Monitor The IDS And Firewall Logs	100%	Thu 8/5/04	Thu 8/5/04
From Inside The Screening Firewall	100%	Fri 8/6/04	Fri 8/6/04
Scan The Internal Network	100%	Fri 8/6/04	Fri 8/6/04
Monitor The IDS	100%	Fri 8/6/04	Fri 8/6/04
From Outside The Choke Firewall	100%	Mon 8/9/04	Mon 8/9/04
Scan The MMC Internal Networks	100%	Mon 8/9/04	Mon 8/9/04
Monitor IDS And Firewall Logs	100%	Mon 8/9/04	Mon 8/9/04
Upper Layers (5-7)	100%	Thu 8/26/04	Fri 8/27/04
Ensure The Workstation On Each Subnet Can Connect To:	100%	Thu 8/26/04	Fri 8/27/04
Domain	100%	Thu 8/26/04	Fri 8/27/04
Wins	100%	Thu 8/26/04	Fri 8/27/04
Dns	100%	Thu 8/26/04	Fri 8/27/04
Email	100%	Thu 8/26/04	Fri 8/27/04
Printing	100%	Thu 8/26/04	Fri 8/27/04
File Shares	100%	Thu 8/26/04	Fri 8/27/04
Internet	100%	Thu 8/26/04	Fri 8/27/04
Perform A Vulnerability Scan On All Servers	100%	Thu 8/26/04	Fri 8/27/04
Troubleshooting And Contingency	100%	Fri 8/27/04	Tue 9/21/04
Support (Support Will Be Handled In Accordance With Current MMC Procedures)	100%	Tue 9/21/04	Wed 9/22/04
Network (Network Operations)	100%	Tue 9/21/04	Wed 9/22/04
8 - 5 On Site Support	100%	Tue 9/21/04	Wed 9/22/04
After Hours On Call Support	100%	Tue 9/21/04	Wed 9/22/04
Server (NT And UNIX Administration)	100%	Tue 9/21/04	Wed 9/22/04

8 - 5 On Site Support	100%	Tue 9/21/04	Wed 9/22/04
After Hours On Call Support	100%	Tue 9/21/04	Wed 9/22/04
Application (Ssts)	100%	Tue 9/21/04	Wed 9/22/04
24 X 7 For Supported Applications	100%	Tue 9/21/04	Wed 9/22/04
Security	100%	Tue 9/21/04	Wed 9/22/04
8 - 5 On Site Support	100%	Tue 9/21/04	Wed 9/22/04
After Hours On Call Support	100%	Tue 9/21/04	Wed 9/22/04

Appendix D

Supporting Document

1.1. Requirements

Vendor system business requirements
Flexibility – The extranet must be able to accommodate several types of vendors and several different delivery methods
Rapid Response – The extranet must allow for the rapid response to the needs of existing vendors and to the addition of new vendors
Expandability – The extranet must be able to handle up to 500 content providers
Extensibility – Currently the communication method used by the vendors are known and the extranet will be built to accommodate those methods. In addition, the extranet must be capable of handing methods outside the original set. In some cases these new communication methods may not currently exist.
Tenant Business Requirements
No loss of functionality - The extranet must duplicate the functionality the tenants experienced while on the MMC networks
No loss of service levels - The tenants must have the same level of service on the extranet that they did while on the MMC networks

No commingling of data - Data from the tenants must not be co-located in any way. This included separate file, application, backup servers and etc
No Shared Services - The extranet must provide all the necessary services to the tenants. No services could be provided from the MMC networks
Technical Requirements
The extranet design had to conform to Cisco's tiered architecture. The design had to include an access layer, a distribution layer, and a core layer.
The extranet design had to be moduler. Although there were only two business units/segments slated for the initial implementation of the extranet. There were several other proposed projects that could take advantage of the extranet.
The extranet had to segment the different business units. Although all traffic would traverse a common distribution and core layer, only traffic destined for a specific segment should be permitted to the access layer.
The extranet, where possible and where not prohibited by policy or regulation, should rely on a common application layer infrastructure. This would include common domain services, email, DNS, and etc.
No traffic originated on the extranet would be allowed to pass to

the internal MMC networks without first being proxied through a MMC controlled device.
The extranet must conform to the dual screening/choke firewall design. No segment, including the MMC internal networks should be less than two firewalls away from the Internet or other external connectivity. Where possible, the screening and choke firewalls should come from different manufacturers.
Connectivity from the internal MMC networks to extranet segments would be on an as needed basis and be controlled to the layer four port level.
An intrusion detection system had to be deployed to monitor the extranet.
Under no circumstances would the extranet be used for Internet connectivity for internal MMC user networks.
Pre-Implementation Requirements
Tenant agreements had to be in place that detailed the MMC's responsibilities given the new connectivity.
Partner connection requests had to be in place with each vendor requesting access to the extranet.
A costing model had to be developed to amortize the initial cost of the extranet to new projects that would be added to the extranet.
A standard configuration model must be in place for new projects

that were to be added to the extranet. This allowed for standardized deployment of equipment for all projects across the extranet.
Training Requirements
The security engineer assigned to the project needed Checkpoint training in support of the multiple firewall manufacturer requirement.
Training for the tenants was needed to ensure their IT personnel understood the new network connectivity.
Training for the MMC sales force was need so that they understood the importance of Service Level Agreements that now needed to be included in all new tenant leases.
Vendor training was needed to ensure vendors could connected through the extranet.

1.2. Configuration Checklist

Switch Name:

	Host Name	
	Domain Name	
	Service password-encryption	
	Set passwords	
	VTY 04	
	Set vty password	
	Set login	
	Set transport modes	
	VLAN 502	
	Create Vlan	
	IP address on Vlan	
	No shut on Vlan interface	
	VTP client mode	
	Assign ports to Vlans	
	Ensure port mode is access	

	Assign necessary ports to Vlan 502	
	Set Time Zone and summer-time	
	Logging	
	Set logging buffer to warning	
	Turn logging monitor and console off	
	Set logging trap to warning	
	Add logging servers	
	Set ip subnet zero	
	Set no domain lookup	
	Create ACL 90	
	Apply ACL 90 to VTY interfaces	
	SNMP	
	Banner	
	Tacacs+	
	AAA	
	Generate Cypto Keys	
	No CDP Neighbor	