2013

The implementation of a thin client in the Department of Defense network system

Sung Ju In

THE IMPLEMENTATION OF A THIN CLIENT IN THE DEPARTMENT OF DEFENSE NETWORK SYSTEM

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Business Administration:

Information Assurance and Security Management

---

by

Sung Ju In

June 2013

THE IMPLEMENTATION OF A THIN CLIENT IN THE DEPARTMENT OF DEFENSE NETWORK SYSTEM

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Sung Ju In

June 2013

Approved by:

[redacted]

Frank Lin, Ph.D., Committee Chair, Information and Decision Sciences

6/6/2013

Date

[redacted]

Conrad Shayo, Ph.D.

[redacted]

Jake Zhu, Ph.D., Department Chair

ABSTRACT

The implementation of a thin client network architecture in an organization, is a strategic Information Technology (IT) decision that best serves and satisfies three main requirements, (a) access, (b) distribution, and (c) core. The thin client network design focuses on virtualization and centralization of systems as well as providing reliable continuity of organizational operations. This project goal is to introduce and analyze a thin client solution that could enhance the overall Department of Defense (DoD) network system as well as its IT security posture, minimize risk from external threats, and ease of network operations. The current Information Assurance (IA) and security measures in the DoD are mainly based on the conventional network architecture where major processing and storing are done on its own desktop system. It also requires its own setup and maintenance at the individual level. There are only few research studies that have investigated on the implementation of a thin client network architecture for the DoD. In addition to introducing and analyzing a thin client solution for the DoD network system, this project introduces and discusses other security policies,

plans, and measures that can be coupled with the thin client solution. We demonstrate that the thin client architecture is more cost effective and easier to management when it's compared to the conventional network system. Potential challenges of implementing a thin client solution as well as suggestions to mitigate concerns and issues are also discussed. The information presented here is not only limited to the DoD, but it could be applied through the wide range of business operations.

ACKNOWLEDGMENTS

I would like to take this opportunity to express my profound gratitude and deep regards to my professors, Dr. Frank Lin and Dr. Conrad Shayo, who gave me the golden opportunity to do this project under their supervision. I also would like to take this opportunity to express a deep sense of gratitude to my co-workers from the various organizations for their cordial support which helped me in completing this project through various stages. Finally, I would like to thank the Almighty for sustaining me, and my wife, Madoka, for her constant encouragement and support without which this project would not be possible.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

The father of the Internet was first introduced as ARPANET (Advanced Research Projects Agency Network) in 1969 which was funded by the Department of Defense (DoD). It first used the rudimentary level packet switching technology datagrams which allowed transferring information from one computer to another. The ARPANET laid the foundation for the new era of a Global Information Grid (GIG) by successfully demonstrating packet switching. By the late 1970s, the personal computer was introduced to the public and it became more popular in the 80s and demand for sharing information increased substantially. With the explosion of personal computing, private networks such as the ARPANET, evolved into the public Internet and other private networks. In the 90s, the dial-up modem became the most popular and publicly used technology to share information which gave birth to AOL, Yahoo, and Netscape. Users could search and gain access to open information on the Internet. Until then, the public had never been exposed to so much information and their hunger for more information

increased exponentially. This rapid growth of the Internet also contributed to a wide range of information gathering and sharing for the DoD. Each service branch started to establish its own network systems to its lowest level. As a result, by the late 90s, the broad internet technology such as DSL (Digital Subscriber Line) was introduced and successfully established its foothold, which opened a new internet age for the DoD. This new establishment within the DoD network system allowed components within the DoD to share large amounts of information such as videos, voice, and data files which can be seamlessly transferred and shared without much degradation and latency.

However, the birth of the Internet left one critical issue unresolved, security. The Internet and its related network systems were established without proper security measures, because the network was originally established as a private network setup to share information freely between authorized users without restrictions. This fast growing demand for shared information forced the DoD to focus on expansions rather than optimizing the network health and its security.

Today, the DoD service components rely on information technology and its related system much more profoundly than in the past. Thus, carelessly implemented network systems would have a serious impact and consequences for national security as well as other day to day operations. This heavy reliance on information systems highlights the significance of implementing secure, fault tolerant, efficient, and effective network systems within the entire DoD community.

In an attempt to enhance the current network health, security, and efficiency, a potential solution is a thin client network. The Conventional system, which is also known as a thick client or a fat client, is different from a thin client because its processing and storing is done on its local client machine. Hence, the processing speed and storage capability requirements of the local thick client machine are higher than the thin client machine. It also requires its own setup and maintenance at the individual level. Thus, it consumes more power to operate and requires more personnel to manage it. In contrast, the thin client concept is to move away from the conventional distributed thick client network architecture by centralizing the network and its related

systems into one. Under this thin client network architecture, all software and programs are designed to install and operate at a central server or a back-end server, which allows ease of management and operations of the network. In addition, it enhances the security aspects where external or internal threats can be properly monitored and controlled.

Purpose of Study

The DoD network has grown enormously since the birth of the Internet age. As a result, it added inevitable network complexity as well as layers of different network systems. Currently, the DoD is challenged by a plethora of issues and problems. First, the DoD is having difficulty sharing information with different entities or components (National Security Agency, the Department of Homeland Security, and defense contractors/companies) and its own service branches (Army, Navy, Marine and Air Force) within the DoD. For example, within the DoD, there are multiple layers of systems based on unique information security requirements and classifications which create delay or cause a complete stop of information sharing. To make the matter worse, each

entity and service branch needs to invest significant time and effort to establish and maintain each network system. This process is called Interim Approve to Operate (IATO) and Approved to Operate (ATO).

The IATO and ATO are processes for validating "networthiness" and obtaining a certificate to establish and connect to the DoD network. According to the Army Regulation (AR) 25-2 on Information Assurance; networthiness is defined as 'the operational assessment of systems, applications, or devices to determine whether candidate systems possess security validation, interoperability, sustainability, usability, and supportability as well as compliance with federal, DoD, and Combatant Command, Service or Agency (CC S/A) regulations.' The preparation of IATO or ATO process can take anywhere from six months to a year in order to obtain a final approval from the Designated Approving Authority (DAA). It also requires a recertification every three to five years depending on its system requirements and classification. (AR 25-2, 2007)

Furthermore, the recent implementation of the 2011 Budget Control Act requires the DoD to reduce future expenditures by approximately $259 billion over the next

five years and overall $487 billion over the next ten years. (Defense Budget Priorities and Choices, 2012). As a result, each service branch announced that they would cut back on spending, training, and personnel. For example, the Army is planning to reduce its current force strength by 10 percent. This will reduce the Army personnel strength from 570,000 active duty personnel to 483,000 which can result in saving $220 billion over the next ten years.

Table 1. Budget Cut and Personnel Reduction Plan

Department of Defense Proposed Spending Cuts	
Program	10-Year Savings ($ billion)
Reduce the size of the Army	$220
Reform maintenance and supply systems	$13
Reform command, support, and infrastructure	$100
Reduce research, development, testing, and evaluation	$73

(Derived from Friedman and Preble, 2010)

This new budget cut and personnel reduction plan (see Table 1) can be detrimental to the current DoD

operations as well as its infrastructure including operating and maintaining the DoD network systems. About two decades ago, the General Accountability Office (GAO) conducted a study that focused on issues related to downsizing of the DoD. It stated that

> Another consideration is the impact of personnel reductions on unit manning levels. Army officials acknowledge that, during the current drawdown, personnel reductions have occurred more quickly than have changes in unit force structure, creating some undesired under-manning of units. While they expect this problem to correct itself as future reductions in unit structure occur, they recognize the problem could be exacerbated with increases in personnel reduction targets unless these further reductions are correlated with additional structural reductions. (U.S. GAO, 1993, p. 8)

Similarly, as the GAO stated above, the current reduction plan could easily create the following issues:

1) Lack of personnel to maintain its network systems
2) Overloaded tasks for remaining personnel
3) Loss of know-how and continuity of operations

4) Deterioration of the network infrastructure due to the insufficient funding for repairs and maintenance.

As a result, it is inevitable for the DoD to start looking into other alternatives to properly operate and maintain its network systems at the optimum level.

The thin client's overall benefits derive from centralization of its network and management as Barrie David, an author of Thin Client Benefits, described in his white paper, "It can significantly lower your operating costs, increase the quality of your support and reduce your risk." (David, p. 17) This can reduce overall operations and maintain costs by reducing support personnel. Also, it can enhance overall security by centralized security monitoring of external and internal threats.

In addition, the IATO and ATO processes can be reduced significantly. Under a single Army division, the conventional network would require 21 IATOs or ATOs. On the other hand, the thin client would only expect to require 5. This is more than a 70 percent reduction by centralizing a system.

Overall, this project will demonstrate how thin client implementation can effectively replace the current DoD's conventional network systems by forming a centralized network system. In addition, we analyze financial and non-financial benefits that can be derived from the thin client implementation.

The project is comprised of six chapters. Chapter one is focused on the introduction and purpose of the project. Chapter two is a brief discussion of the literature review of the conventional network architecture vs. thin client architecture implementation. Chapter three will review the basic DoD network system, scope, and goals. Chapter four will discuss thin client implementation. This chapter will introduce the DoD acquisition framework that describes functional activities throughout the life cycle of the DoD network system. Chapter five will analyze both financial and non-financial benefits of implementing thin clients. Lastly, chapter six will close the paper with the summary of the analysis and findings as well as a conclusion of implementation of thin clients in the DoD network systems.

CHAPTER TWO

LITERATURE REVIEW

There are very few research studies that focus on thin client implementation for the DoD. There are a few white papers that have been produced by the Defense Information Systems Agency (DISA), but they are merely recommendations for consolidating Multi-National Information Sharing (MNIS) systems or other coalition network systems under the thin client network system. Other thin client research studies have been focused on private sectors or universities.

According to 2X, a cloud computing software company, a thin client is one of the best computing solutions that can provide both financial and operational benefits. It described a thin client as the best cost cutting solution. It also stressed that a thin client has higher reliability (longer meantime before failure) and less risk of viruses at the user level. (2X, 2010) In addition, according to Barrie David, the conventional workstation is designed to store applications locally and store data centrally. Due to this, when the user is accessing data that are stored centrally, it transfer and

receive the entire file to the user's workstation. Thus, it consumes higher bandwidth. In contrast, thin clients use bandwidth more efficiently, because the central server allows each client to carry out only requested task without receiving the entire file which only consumes the minimal bandwidth. (David, 2002)

Furthermore, Steve Greenburg, Christa Anderson, Jennifer Mitchell-Jackson, authors of the Comparing Power Usage for PCs and Thin Clients in an Office Network Environment, revealed that thin clients reduce the cost of energy consumption, because it is based on server-based computing. They described that thin clients have lower microprocessor and memory requirements. Thus, it consumes less power. (Greenberg, Anderson, Mitchell-Jackson, 2001) In addition, there is another energy consumption research conducted by Initiative for Global Environmental Leadership (IGEL). They revealed that thin clients consume as much as 88% less power than conventional workstations. (IGEL, 2012)

Although, there are a plethora of advantages that are related to the thin client solution, there are also disadvantages that are associated with it. The 2X's white paper pointed out that thin clients use lower processing

resources that may hinder users who require operating under high performance environments such as Computer-Aided Design (CAD) or Desk Top Publishing (DTP). (2X, 2010) Moreover, David described that user acceptance can become an issue when all access becomes centralized. This will deny users from adding favorite screensavers and installing programs on their own workstations. David also pointed out that a thin client relies on constant network connectivity between the server and client. Thus, when there is a network failure, the client cannot be operational until the network regains its connection with the server. (David, 2002) Also, a thin client may offer no assistance to a user in accessing remote systems and web-applications. Thus, substituting a thin client may reduce user effectiveness in performing required tasks.

Sinclair and Merkow's "Thin Client Clearly Explained" supports and shares the thin client's advantages to the examples above. They described that the thin client's central management can provide efficient manageability and control as well as increased security. Implementation of the thin client simplifies the maintenance and support of the entire system which reduces the workload of IT personnel. Thus, the entire

thin client network can be operated and maintained with a smaller number of personnel. In addition, they also pointed out that power savings are one of main benefits of the thin client.

This project will develop thin client implementation for the DoD with the Sinclair and Merkow's approach. Their approach clearly aligns with the DoD's need for centralization as well as operating the network system with effective and efficient ways (Sinclair & Merkow, 2000). The fundamental approach of a thin client is to allow applications to run centrally, minimum usage of bandwidth, and operate network system with reduced support personnel as well as its associated costs.

Thin client network system is a great option to consider for the DoD in order to deal with the current budget cuts (sequestration) including the reduction of both military and government personnel. In addition, the DoD may enhance its current security and operations by centralizing the network which provides improved control and more efficient management of the network.

CHAPTER THREE

DEPARTMENT OF DEFENSE NETWORK 101

Prior to the introduction of the thin client study, it is important to understand how the DoD network system is designed and implemented. The conventional private sector network systems may resemble the DoD network systems. However, the DoD network was designed in more extensive ways in order to connect various branches and other components throughout the world (see Figure 1).

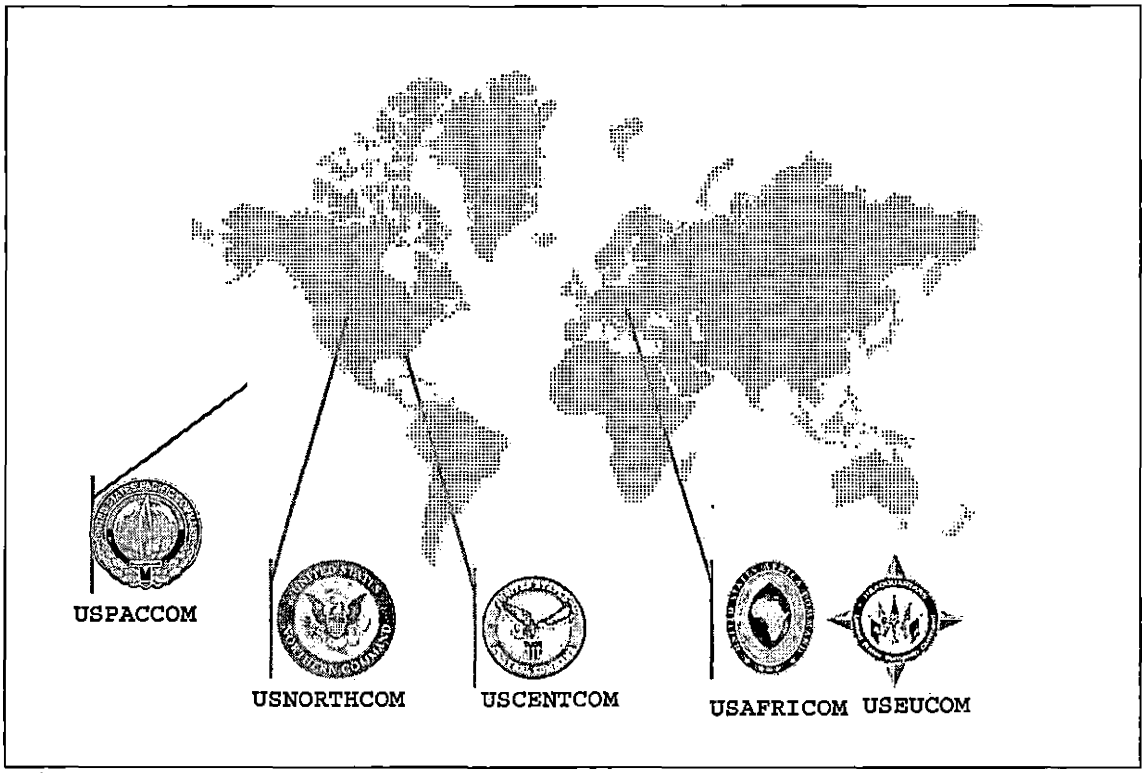


Figure 1. Department of Defense Components Map

As it is illustrated above, the DoD operates and maintains five main components throughout the world:

Table 2. Department of Defense Components Breakdown

Component Command	Area of Responsibility (AOR)
United States Pacific Command	Responsible for the DoD operations and military relations with the countries of Asia-Pacific
United States Northern Command	Responsible for the DoD operations and military relations with the countries of North America
United States European Command	Unified combatant command; responsible for the DoD operations and military relations with the countries in Europe
United States Africa Command	Responsible for the DoD operations and military relations with the countries in Africa
United States Central Command	Unified combatant command; responsible for the DoD operations and military relations with the countries in Middle-East

The DoD operates in the entire world and it requires network connectivity from anywhere in its area of responsibility (AOR). As a result, it requires rapid and reliable communication/network system and services to be deployed where the DoD personnel can obtain and share information in a timely manner.

First, let's review the general DoD network architecture. There are many requirements that the DoD formation system must meet. For example, an airplane or a vehicle could move you from San Diego to Washington D.C. However, the airplane would be the more effective and efficient mode of transportation when increased safety, speed, or number of users is desired. Similarly, when designing the DoD network, those factors (safety, speed, or number of users) need to be taken into consideration. Let's use typical methods of transportation to better illustrate this. For example, what are the speed limitations on the protocol or media sending the information? Most freeways and roads have speed limits. Moreover, a bad weather or traffic condition may alter transportation speed. Likewise, each type of equipment or protocol used for the transportation of information has unique security and speed restrictions. How much information can be sent in a certain timeframe? Larger freeway lanes can handle more traffic than single-lane street roads. Similarly, higher bandwidth connections allow more information traffic to move back and forth freely without any interruptions.

When designing the network, it also deals with costs. How will cost affect the choice of a network/communication system? Larger organizations, such as the DoD, with ample funding can use dedicated network for its intranet, Internet, and other communications such as Voice Over Internet Protocol and Voice Over Secured Internet Protocol. How far will the information travel? One might choose an airplane for traveling long distances. For long distance transportation of information, you may choose satellite technology or fiber optic cable. For shorter distances, microwave technology might be used such as Asynchronous Transfer Mode (ATM) or Integrated Digital Network Exchange (IDNX).

An appropriate protection of information has to be considered. Does the information require any protections? For example, an upper-armored car is probably the best avenue to protect the transportation of money. A secure protocol is the best avenue to protect information on the Internet or use an encryption device that can harden or add another layer of security measure. Let's briefly review the types of information security assurances or services (including the CIA triad): (Andress, 2011, p. 6)

Table 3. Types of Information Security Assurances and Services

Services	Description
Confidentiality	Allows only the intended recipient views messages. If an unauthorized person is reading an email message or listening to phone conversations, the system may be compromised.
Integrity	Need to ensure that the received information is correct and free from alteration. For example, a slight manipulation to a refueling database for an airplane could lead to a disaster.
Availability	Availability means that information can be accessed when the user needs it. It is imperative to get the right information to the right decision-maker.
Authentication	Must validate the user of the system. This is done with passwords and other authentication techniques.
Non-repudiation	Must make sure that the sender cannot deny sending the information, and the receiver cannot deny receiving it.

Various types of media are used for sending messages within the DoD network infrastructure. They vary from conventional dial-up connections to high-speed fiber optic data lines. The choice of media influences other considerations, such as cost, speed, and throughput.

The different types of media that are being used by the DoD and its service components daily operations today are: satellite, radio, microwave, fiber optic, and coaxial cable.

The choice of media will be depend on the volume of information to be sent, the distance to the intended recipient, and the timeliness and security of delivery. For example, to mail a box of documents from San Diego to New York City, we may choose a carrier such as FedEx based on the size, shipping costs and timeliness of delivery. Thus, the choice of media is important to accommodate the users need when designing the network. If the rapid deployment of the network system is required, satellite communications can be used. Fiber optic lines can be more effective to accommodate larger number of users as well as provide faster data services.

Designing the DoD network can be a difficult task due to special circumstances such as additional security requirements and to run and execute other non-commercially available software. When designing the DoD network, each of the two major components of a network is vital and must be well understood in order to

design a reliable and scalable network: 1) network architecture and 2) modeling.

The DoD depends on the common network architecture to provide accurate and timely control of the other critical network systems. Here is a basic layout of the DoD network architecture (see Figure 2):

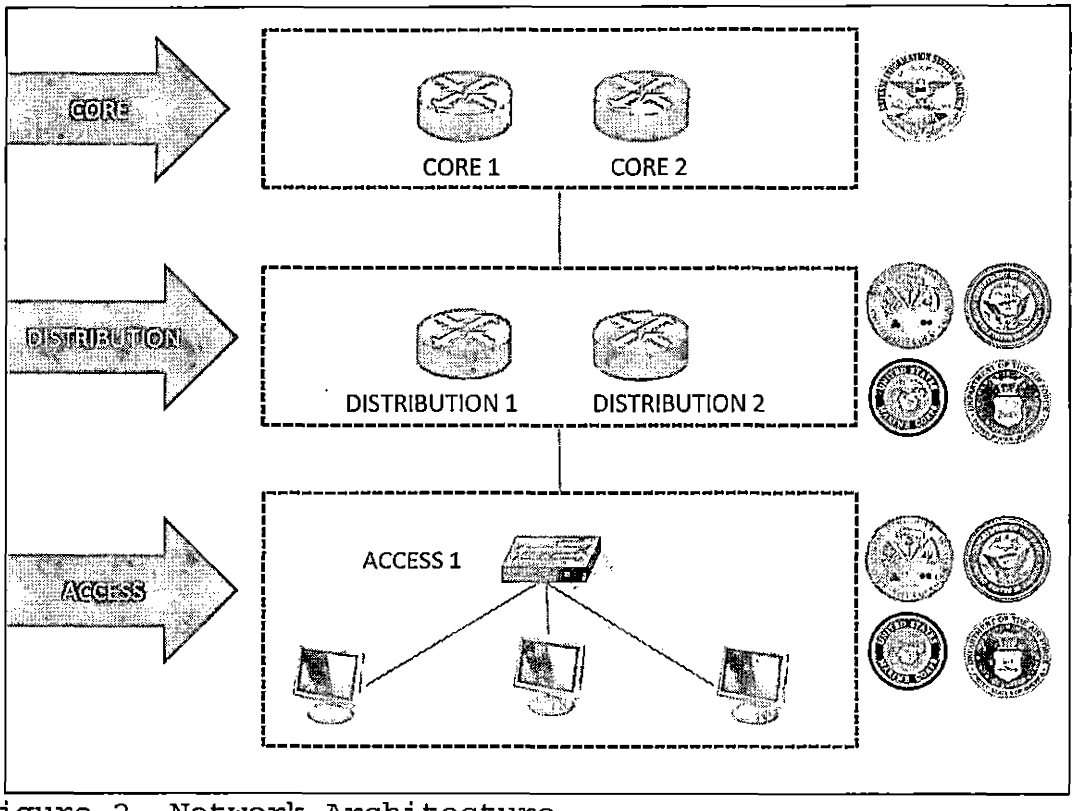


Figure 2. Network Architecture

Access - Allow users to access information via various end devices including programs and software. This

is operated and maintained by each service branch (i.e. Army, Navy, and Air Force).

Distribution - Act as the DMZ (Demarcation Zone) between the core and the access layers of the network that enable routing and security policy enforcement features. This is operated and maintained by each service branch (i.e. Army, Navy, and Air Force).

Core - Allow distribution layer of different network to communicate each other. This is operated and maintained by DISA as part of its DISN (Defense Information Systems Network) services that form world-wide GIG. DISA's main mission is to provide long-haul transmission services including satellite and optical fiber cable. (DISA, n.d.)

Now, let's briefly review the DoD network modeling components (see Table 4). The network modeling is a simple representation of complex real-world network structures which can be useful in understanding complexities of the real work environment. Similar to the public or business network modeling, the DoD shares the four main parts of network modeling, hardware, software, and policies and regulations.

Table 4. Department of Defense Network Modeling Components

	Description	Example
Hardware	Collection of physical components that comprise a network system	Laptop, Desktop, Router, and Encryption Device
Software	Collection of programs that enable a computer or related peripheral to exchange information or execute tasks	Microsoft Office, Email, and Encryption Software
Policies and Regulations	Collection of set of rules and guidance to operate and maintain network and its related systems	IEEE standards, Army Regulation 25-2, and Security Technical Implementation Guide (STIG)

So, why use models? Models can reduce overall operating and maintenance costs by simplifying assumptions, clarifying requirements, and validating architectures. (Guizani, Mohsen, Rayes, Ammar, Khan, Bilal, and Al-Fuqaha, Ala, 2010)

Today, the DoD information infrastructure is very complex. No single organization controls the protocols, the use of the infrastructure, or even the physical lines. For example, as mentioned earlier, there are multiple layers of infrastructure within the DoD based on

its classification needs (see table 5). Today's DoD is supported by an interrelated set of critical network infrastructures and these are identified as different service branches (i.e. Army, Navy, Air Force, and Marine Corps) as well as other DoD related components such as Department of Homeland Security (DHS).

Table 5. Department of Defense Network Types

Network Type	
SIPR Network	Secured Internet Protocol Routing
NIPR Network	Non-secured Internet Protocol Routing
GCCS	Global Command and Control Systems
JWICS	Joint Worldwide Intelligence Communications System
CENTRIX	Combined Enterprise Regional Information Exchange System

These systems support applications such as:

- E-mail with attachments
- Common Microsoft Office software
- A Common Operating Picture
- A Common Intelligence Picture

- Web page hosting, posting, and producing
- Voice Over IP (VOIP) Phones

In addition, most of these systems use National Security Agency (NSA) approved Type-1 encryption devices to establish an encrypted channel between strategic or tactical locations to a forward point of presence or command headquarters site. Let's briefly review the crypto categories (see Table 6) that are assigned by the NSA (CNSSI No. 4009):

Table 6. National Security Agency Crypto Categories

Type 1	Classified cryptographic equipment and algorithms approved by the NSA for securing classified U.S. Government information.
Type 2	Unclassified cryptographic equipment endorsed by the NSA, for use in national security systems.
Type 3	Encryption algorithm that has been adopted as a Federal Information Processing Standard (FIPS) for use with Sensitive, But Unclassified (SBU) information on non-national security systems.
Type 4	Defined as Best Commercial Practices. Encryption algorithm has been registered with NIST but is not a Federal Information Processing Standard (FIPS). The type 4 algorithms may not be used to protect classified information.

(Derived from CNSSI No. 4009)

The DoD depends on the information infrastructure to provide accurate and timely control of its readiness, missions, tasks, and security. To achieve this, the Global Information Grid (GIG) was born. This is roughly equivalent to the Internet and its supporting elements (core level). It provides connectivity between one location to another in the United States as well as other foreign countries that have U.S presences.

Next, let's briefly review the policies and regulations that deal with the DoD information assurance and security (see Table 7). In general, the DoD or service branch specific policies do not encompass all aspects of information assurance and securities. There are three components of policies and regulations that help the DoD or its service branches to form its network and security regulations and policies. First, the DoD specific directives and guidance from DISA which provide requirements to connect to the core (GIG) of the network. Second, the NSA directives and guidance that are designed specifically for information assurance which applies to the all three of components of the DoD architecture. Third, each service branch maintains its specific regulations and policies that are mainly tailored at the

access level. Here are brief examples of regulations that are applicable to the respective DoD network architecture.

Table 7. Department of Defense Policies and Regulations

DoD Architecture	Entities	Policies and Regulations
CORE	DISA & NSA	CJCSI (Chairman of the Joint Chief of Staff Instruction) 6211.02D, CJCSI 6210.01F, NSA (National Security Agency)/CSS (Central Security Service) 1-5, and NSA/CSS 1-30
DISTRIBUTION	Army, Navy, Marine, and Air Force	AR (Army Regulation) 25-2, MCO (Marine Corps Orders) 5239.1 AFI (Air Force Instruction)33-200, and SECNAVINST (Secretary of Navy Instruction) 5239.3B
ACCESS	Army, Navy, Marine, and Air Force	AR 25-2, MCO 5239.1 AFI 33-200, and SECNAVINST 5239.3B

At the core level, the instructions provide basic guidance and policies regarding the network and its security. At the distribution and access levels, each service branch provides its own regulations and instructions to further tailor the DoD guidance and policies that fit and satisfy their own requirements.

The current DoD network is decentralized all the way down to the access/user level. This decentralization increases vulnerability from both the internal and external perspectives. From the internal perspective, the user can compromise the overall network security. The threat can be simply introduced from the user's USB drive, internet sites, and specific ports such as File Transfer Protocol (FTP) and Peer to Peer (p2p). Externally, points of entry or attack increases due to the number of decentralized computers that are operating within the network. The decentralization of network results in the threat of operations setbacks from the intrusion or loss of important data and information (Sinclair & Merkow, 2000).

Scope and Goals

Scope of this project is limited based on the amount of study and research that was conducted on this particular subject of thin client implementation in the DoD network. In addition, the information available to the public regarding this subject is also limited, because the subject is specifically dealing with the DoD network information and its security which are considered

to be sensitive and often classified in order to protect its own security interests. Thus, the scope will mainly focus on areas that can be implemented on the DoD network based on information that is readily available to the public.

The overall goal of this project is to identify and recommend areas that can be implemented as thin clients as well as illustrate resulting benefits to the DoD. The benefits include centralization of the network which enhances performance and security of the network as well as financial and non-financial gains that are derived from implementation.

CHAPTER FOUR

THIN CLIENT IMPLEMENTATION

The Internet was originally funded and developed to connect universities, so they could share their research for the DoD. This network gradually grew. With the invention of the World Wide Web, the Internet expanded into the massive system we have today. In addition, the Internet is a system of systems - a worldwide connection of universities, businesses, and other computer sites, all using the same set of protocols. Today, the Internet is physically linked through high-speed networks.

Unlike the conventional workstation and its network design, the thin client can be referred to as a system that relies heavily on a centralized computer (or known as a backend server) to do most of its user required work including saving and sharing files and information. In most cases, the client software or the small size computer acts as an interface, while the centralized computer does all the real work. This network design eliminates all hard disks that are installed in every workstation. Thus, each work station does not have to be installed and monitored individually. As a result, it

streamlines the network complexities and designs. It also allows more robust and reliable network security that enables ease of operations for both network administrator and users. This aligns with the vision of the DoD's joint network operations (NetOps).

NetOps is the DoD wide operational and technical capabilities for maintaining, operating, and defending the Global Information Grid (GIG). NetOps has main operational and management components, enterprise management, net assurance, and content management. These three main components allow management and leadership to make appropriate decisions based on the latest and timely available situational awareness information. Those components assure system and network availability and delivery as well as its protection. (DoD Instruction 8410.02, 2008.) All those NetOps components can be best achieved by implementing the thin client system into the DoD network based on its own unique capabilities and its benefits.

First, the DoD has to go through the budget cuts based on the Budget Cut Act of 2011. The thin client system will allow the DoD to accomplish this commitment and goal by using resources more effectively and

efficiently. Thin clients are less expensive and less complex than the conventional workstations, which require more training and experience. In addition, thin clients are smaller and provide creative configurations that the DoD community can use in a variety of ways such as mobile or remote work offices.

Secondly, thin clients enhance the overall network assurance because it does not store data locally which can introduce viruses or compromise the security of the entire network. Since thin clients manage all assets centrally, it is much easier to manage and take actions to any potential threats and exploitations.

Lastly, content management is much easier, because data will be stored at the central or backend server where all users will store their data and files. This allows other users to share information more easily and efficiently which creates greater user experiences and ease of content management. (Sinclair & Merkow 2000)

On the other hand, as it was discussed earlier, thin clients have their own shortfalls due to their unique operating environment. Thin clients heavily rely on the back-end server to process the majority of requested tasks from the user. Thus, thin clients have lower

processing resources such as a processor and a memory. This could hinder users who require operating graphic intensive programs such as Computer-Aided Design (CAD) or Desk Top Publishing (DTP). Since the back-end server provides all services and applications that are necessary to run thin clients, when there is an issue with the server or the network, the user clients cannot be operational. In addition, user acceptance can become an issue in the beginning phase of the implementation, because it denies all users from adding favorite screensavers and installing programs.

However, these shortfalls can be mitigated by implementing a redundant server and a network path. For those users operate graphic intensive programs, a hybrid (consists of both thin clients and conventional workstations) network solution can be considered and integrated. Also, early user training could mitigate user resistance.

So, how this thin client network can be implemented in the DoD network? Let's quickly review how the DoD set up its core, distribution, and access network. The diagram (see Figure 3) below is an example of a notional network diagram of one of the DoD network systems. The

core level, a Synchronous Optical Networking (SONET) provides a connection in and out of the Internet. The distribution level, Asynchronous Transfer Mode (ATM) provides a connection between the core and the users (access level).

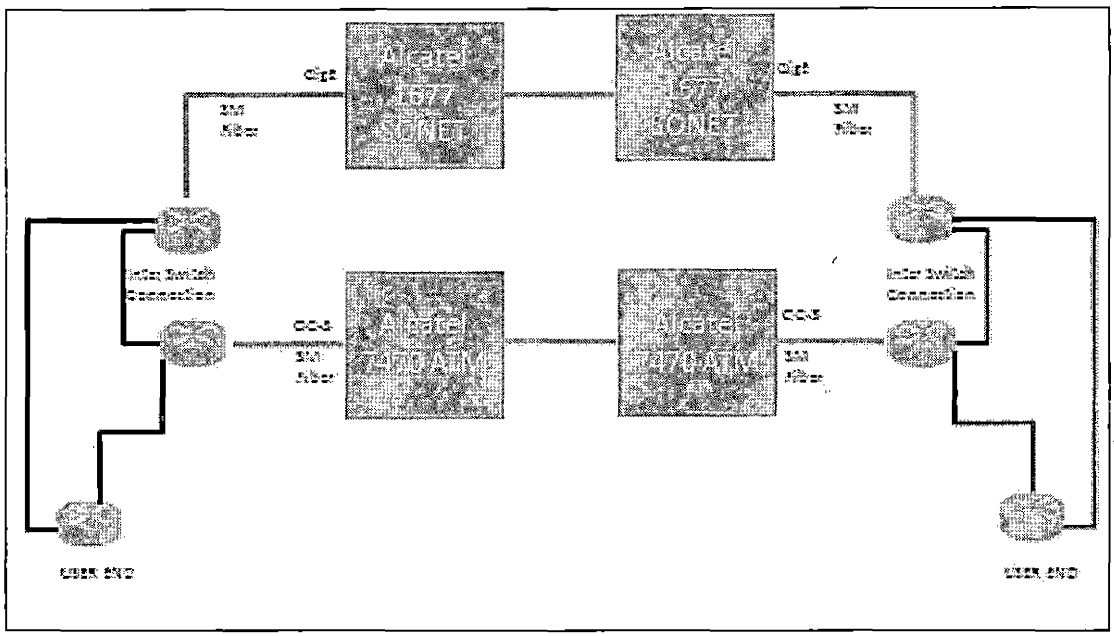


Figure 3. Core and Distribution Architecture of the Department of Defense Network

The DoD core and distribution networks are often consist of SONET and ATM architectures. The SONET is a connection of fiber optic transmission system and it is one of the fiber optic connection standards of the American National Standards Institute (ANSI). The ATM is

considered as a legacy network technology that enables users to transport data, voice, and video at the same time. The ATM is considered as the legacy system due to the limited bandwidth capability of maximum 155 Mbps, but it is still widely used within the DoD community. For this particular case, the SONET act as a CORE while ATM act as a distribution to support a smaller network.

Now, in attempt to put this thin client into an overall picture, here is a basic thin client diagram (see Figure 4) that includes all three main network architectures:

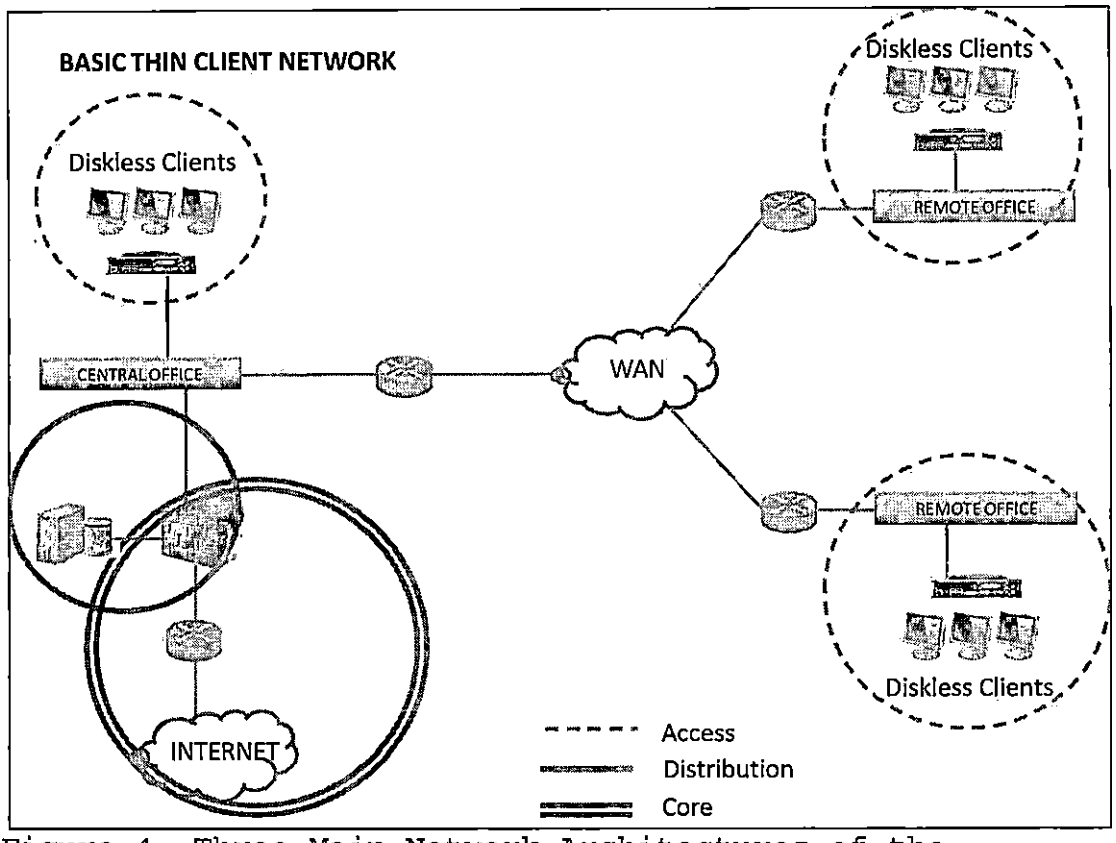


Figure 4. Three Main Network Architectures of the Department of Defense

As it is depicted in the diagram above, a remote office, which is operated at the access level, has multiple diskless clients connected to the router. Then, the server(s), which is operated at the core or distribution level, will host thin client session for multiple diskless clients and its users. The server will maintain all necessary programs and services such as an Operating System (OS) and its related office tools. The

access to those programs and services are tailored to each individual and it is based on user requirements and credentials. Since, the server can host dozens of diskless clients, it allows IT personnel to maintain applications and services on the single server (backend server) without having to install or repair the programs and services on each individual workstation.

Thin client network is simple to design and implement because all necessary programs and services run from the central server. Thus, thin client diskless workstations have lower microprocessor and memory requirements than the conventional workstations, which consume less power to run and operate. Since it is diskless workstation, it reduces risk of introducing malicious code and viruses as well as compromising the network security at the individual client level. As it was described earlier, the thin client network environment shares plethora of benefits. These benefits will be further explained in the later chapter.

In order to implement a new system in the DoD network environment, a particular acquisition framework should be used as a baseline to seamlessly integrate thin clients. The DoD has established an acquisition framework

(see Appendix A) that help its subordinates and entities to obtain an optimum system that satisfy the DoD and users requirements and needs. Based on the DoD acquisition framework, the implementation of thin clients should take place through the following phases which can help the DoD to integrate a new system more efficiently and effectively.

Within a life cycle of the system, four main phases can be identified (see Figure 5). First, the life cycle of the thin client system should begin with a concept refinement phase where the implementation plan should begin with identifying the goals and requirements. It is important to get user input to and acceptance of the formal output of this phase. Once the goals and requirements were identified, the network design and planning should follow. Then, an adequate budget should be in place to support the implementation and testing. The second phase should be procurement of the system and demonstration. This phase should identify the correct vendors who can provide all necessary equipment to create a small test bed of the thin client network. Once all equipment is procured, then it is necessary to test the system in order to evaluate and validate the successful

integration of the thin client network. Once the test bed evaluation is completed, a full integration of the equipment will be followed. The last phase will be the operation, support, and maintenance phase.

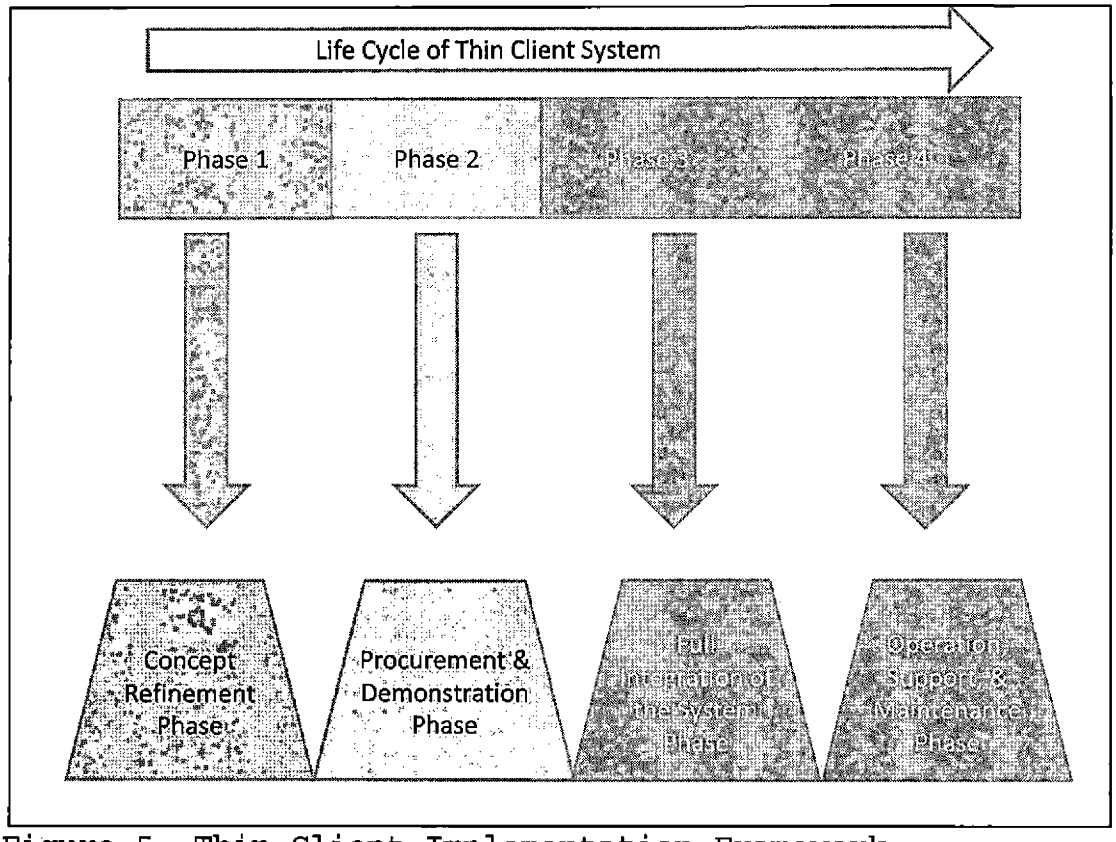


Figure 5. Thin Client Implementation Framework

Concept Refinement Phase

According to Sinclair and Merkow, thin clients are easier to implement and manage, but they are more difficult to purchase than those conventional

workstations due to a variety of configurations and options. Therefore, they emphasize careful evaluation of thin clients that will satisfy users' needs (Sinclair and Merkow, 2000). During the concept phase (see Figure 6), it is important to analyze capabilities and constraints of a new system.

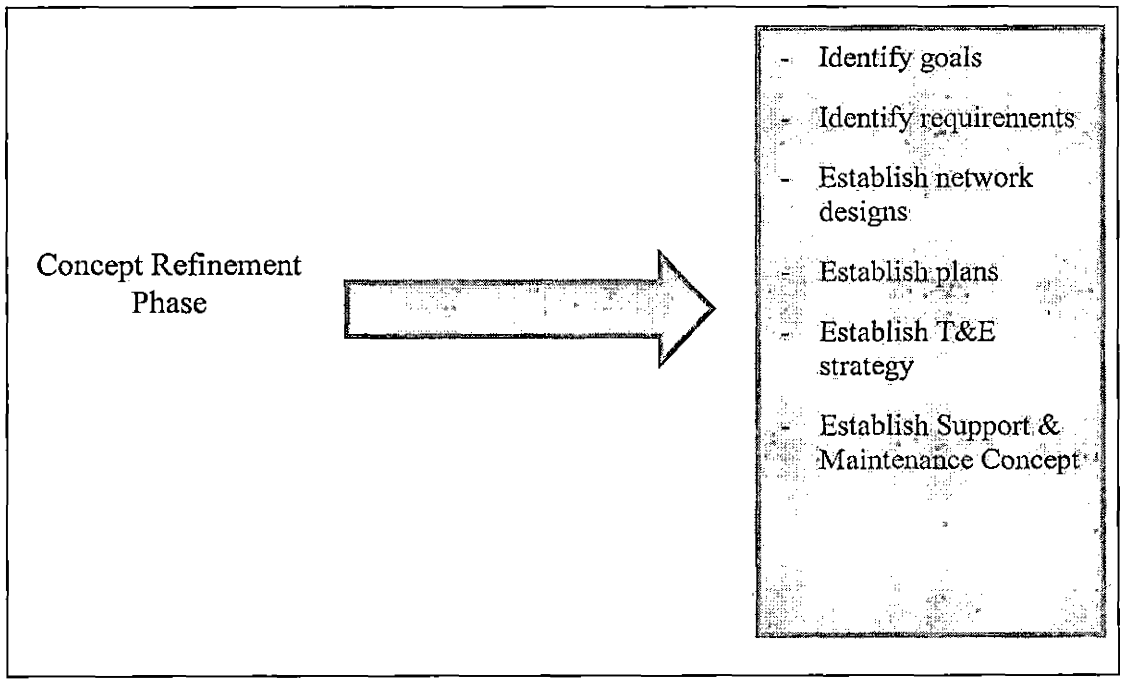


Figure 6. Concept Refinement Phase

Also, it is important to interpret and understand the user requirements. This is one of the most important elements of a successful implementation of a new system, because the system needs to focus on user requirements

and their needs that ensure ease of operations as well as maintaining the effective and efficient NetOps. Once the user requirements are finalized, a confirmation should be followed during the demonstration phase that assures and verifies user's needs. The user's buy in is necessary to move on to the next phase.

Prior to the implementation, a Test and Evaluation (T&E) strategy should be established which will assist a network manager to evaluate and validate all appropriate functions and capabilities that are derived from user requirements. The DoD maintains a Test and Evaluation Management Guide (TEMG) that can be used to conduct T&E activities in order to satisfy the DoD specific policies and standards. The results from the test and evaluation may be used for refining requirements that will later fulfill user requirements.

In addition, a support and maintenance concept strategy should be considered that will continue to support the system throughout its life cycle. This strategy should include a training plan for both users and system administrators and support personnel.

Similar to the DoD acquisition framework, IGEL found that clarifying requirements are one of the main

ingredients of successful implementation of thin clients. There are key aspects to consider such as number of clients planned on run through the back-end server, types of software and applications, and security requirements.

Sinclair and Merkow also described that the network design should include physical layout and logical diagrams. Then, proper wiring for network connectivity should be implemented. In addition, physical access control procedures for network and server hardware should be established. (Sinclair & Merkow, 2000). In addition, the article from Nippon Electric Company (NEC) stressed that all proper system migration steps should be established and performed to ensure the successful integration of thin clients. The most important step would be preliminary examinations of software template (NEC, n.d). Chris Almond, Jeroen van Hoof, Nick Lassonde, Ben Li, and Kurt Taylor, authors of Linux Client Migration Cookbook, discussed that migration goals have to be clearly defined which ensures seamless transition from conventional workstations to thin clients. Also, they noted a good planning is a major part of the migration which requires supports from all levels of management. (Almond, et al., 2006)

Procurement and Demonstration Phase

This procurement and demonstration phase (see Figure 7) will be involved with identifying appropriate suppliers or vendors to provide a thin client system.

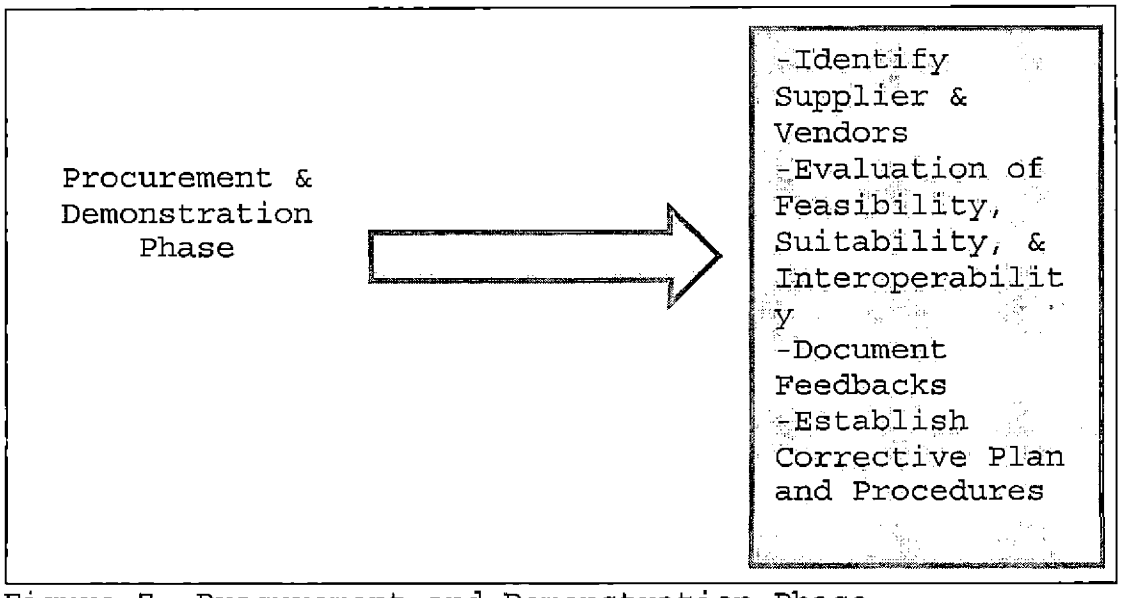


Figure 7. Procurement and Demonstration Phase

The DoD mandates all organization to follow and comply with the Federal Acquisition Regulation (FAR) for acquiring any goods and services for the DoD. In addition, the procurement should go through the appropriate DoD contract officer and procurement channel which will assure timely delivery of all equipment to perform a demonstration of the system. The demonstration will be based on test and evaluation strategy which will

first test the system using the small sample of thin clients. Sinclair and Merkow provided the following simplified checklist (see Table 8) that can be used to assist the system administrator to conduct its activities and tasks. (Sinclair & Merkow, 2000)

Table 8. A Simplified Administrator's Checklist

Activities	Tasks
Define and Create Disk Structures and Partitions	
Install Server Operating System	
Define Server Devices	-Disk Devices -Ethernet Devices -Device Controllers -Device Drivers
Define File System	-File system implementation -Data Areas -Making and Mounting File Systems
Develop Startup and Shutdown Procedures	
Configure Operating Systems Kernel (to support new devices and for packaged software configuration, as required)	
Configure Special Files	-Block and Character Devices -Major and Minor Devices

Activities	Tasks
Define Create System Directories	-System and Network Configurations -System Programs and Libraries
Establish User Accounts	
Establish Daily System Administration Procedures	-User and Group Administration -Communicating with Users as Required -Running Programs Automatically
Package Administration	-SVR4 Packages -Third-Party Packages
Develop Backup Strategies and Procedures	-Define Full and Incremental Backup Schedules
Network Administration	-Network Initialization -Configure Host Names and Addresses -Configure Network Services -Configure Network Diagrams
Distributed File System Administration	-Network File System (NFS) -Remote File System (RFS)
Network Information Services	-Define Domains -Configure Objects -Configure Names -Define Authorization and -Authentication Procedures
Configure UserNet	
Configure Print Services	
Configure Email and User Accounts	
Configure World Wide Web Services	

Activities	Tasks
Define System Security Strategies and Procedures	-Understand What Needs to be Secured -Install, Configure, and Operate Security Programs -Establish Security Response Teams and Procedures -Protect the Password and Group Files -Establish File and Directory Permissions -Secure the Server Console Port

(derived from Sinclair, J., & Merkow, M. (2000). *Thin client clearly explained*, Morgan Kaufmann.)

This phase's main purpose is to evaluate feasibility, suitability, and interoperability of thin client network. Sinclair and Merkow also described that testing phase will be the most vital and important process of all. Because, the behavior of the system can be predicted, including the server and thin client, this test bed will involve actual users since it is hard to predict how they will use the thin clients. Thus, this process will require multiple changes in order to adapt the network to users using thin clients. (Sinclair & Merkow, 2000) The results from the test are normally reflected as user feedback, which should be properly

documented and reflected in the later integration phase. Once the demonstration and evaluation of the test bed is completed, a corrective plan and procedure should be developed and documented. It will record all adjustments and changes that were made during the evaluation. These changes and adjustments should document when a full system is integrated in the later phase.

In addition, a corrective plan and procedures should include risk assessment that is derived from accepting changes and adjustments. The risk assessment will help the organization to avoid future issues and problems ahead of time by establishing its own mitigation plan and solutions. This risk assessment should be thoroughly reviewed and when finalized, take all necessary actions to minimize or mitigate those risks that are identified. Furthermore, risk assessment can also reveal cost and benefit analysis in terms of how the budget or resource would be best spent to make necessary corrections or actions. Through a proper risk assessment process, the system can be integrated and managed more effectively and efficiently.

Full Integration of the System Phase

In this phase (see Figure 8), the organization will go through the procurement of a full range of thin of client system and all related equipment.

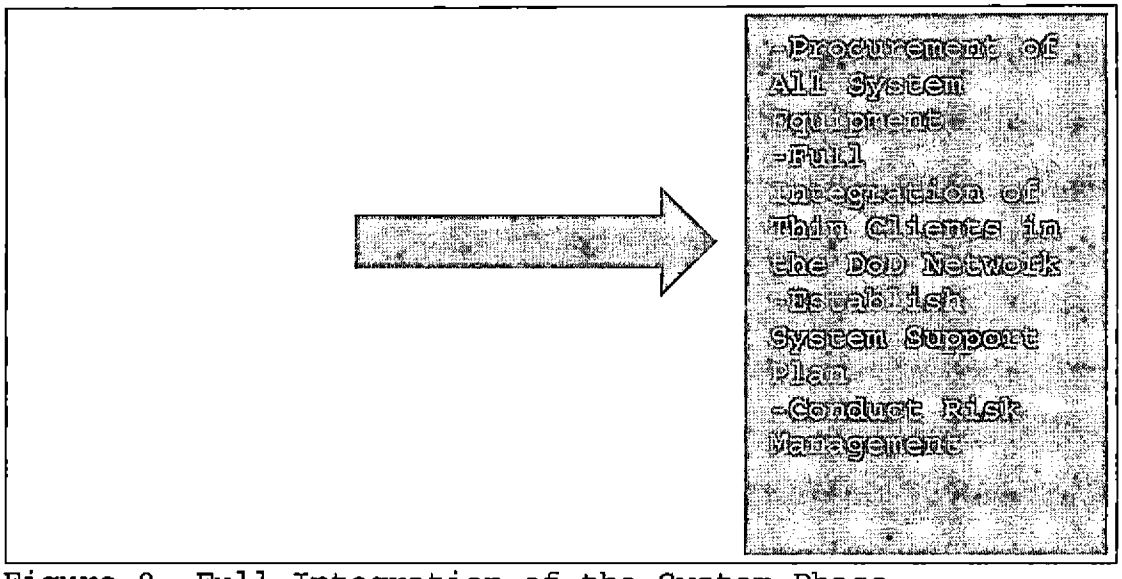


Figure 8. Full Integration of the System Phase

The system should maintain the minimum down time that allows users to continue to operate without much interference. In an attempt to minimize the down time, the implementation of the system can be integrated by small sections or units. While the new system is getting integrated, the organization can provide user training that will help first time users get acquainted to the new

system as well as reduce the volume of trouble tickets or calls.

A system support plan should be created to ensure continuous operations of the new system. The system support plan should include all necessary personnel to manage and operate the system as well as all required maintenance and updates that are needed to sustain the system.

A proper risk management plan should be followed based on the risk assessment from the previous phase. This will help the organization to prioritize its resources to maintain the system at an optimum level. Any future changes or modifications should be properly documented and reviewed in order to prevent potential down time or failures.

Operation, Support, and Maintenance Phase

After the full integration of thin clients is successfully implemented, an operation, support and maintenance phase of the system life cycle begins (see Figure 9).

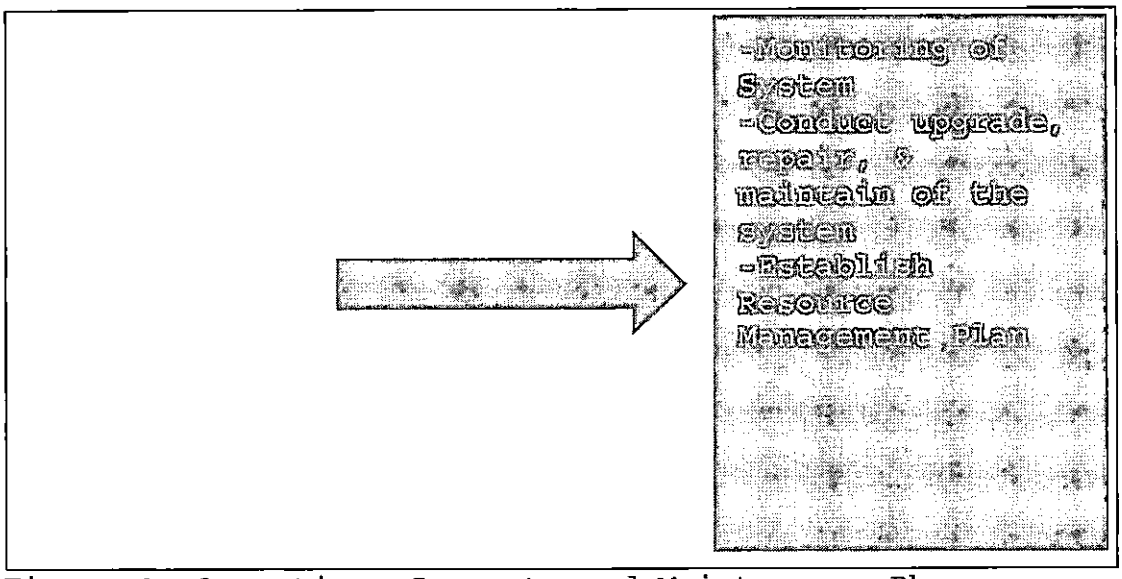


Figure 9. Operation, Support, and Maintenance Phase

This is the longest phase among those mentioned above, because the system normally stays operational until it become obsolete or the cost of maintaining the system exceeds the cost of obtaining a new system. Thus, understanding the characteristics of this phase is critical because it will help system support personnel and users to enjoy benefits that are derived from this new system. This phase will continue in existence until the termination of the system's life cycle.

During this phase, the system support personnel must monitor the system continuously and collect all data, especially anomalies and errors and then apply patches and fixes. After the system is fully operational, it will

be required to have continuous maintenance. This maintenance will ensure the system operates at its peak performance levels.

A proper resource management plan should be created which can fund and support (including personnel, license, and repair parts) all necessary repairs and maintenance activities to keep the software current and the system operating at the optimum level.

Other Consideration of Classified Thin Clients (Tunneling, Black Core and Cross Domain Solution)

As mentioned earlier, the thin client system can be implemented in different classifications of systems within the DoD network. According to Sinclair and Merkow, they described the extranets which are bridging the Internet and the intranet together in order to transfer intranet data to a remote or distant intranet network location. This can be done by tunneling through the Internet. (Sinclair & Merkow, 2000)

Tunneling is creating a secure pipe within the Internet, thus using part of the Internet as a private secure network to transmit sensitive information. For the DoD network, this approach can be used to combine

classified and unclassified network together. As mentioned earlier in Chapter Three, there are multiple layers of network systems with different levels of security classifications. For example, NIPR, SIPR, GCCS, CENTRIX, and JWICS use its own access, distribution, and core system to transport information from one end to another. Except the NIPR network system, which is considered as the unclassified network, SIPR, GCCS, CENTRIX, and JWICS are encrypted at each respective end point to form classified network systems. Those classified networks are designed to protect their own sensitive information from unauthorized activities and entities. However, those networks can be possibly combined in order to minimize redundant access, distribution, and core systems, which can help the DoD to reduce overall costs of maintaining those systems. Under Sinclair and Merkow's theory, the DoD classified and unclassified networks can be combined using a tunneling method.

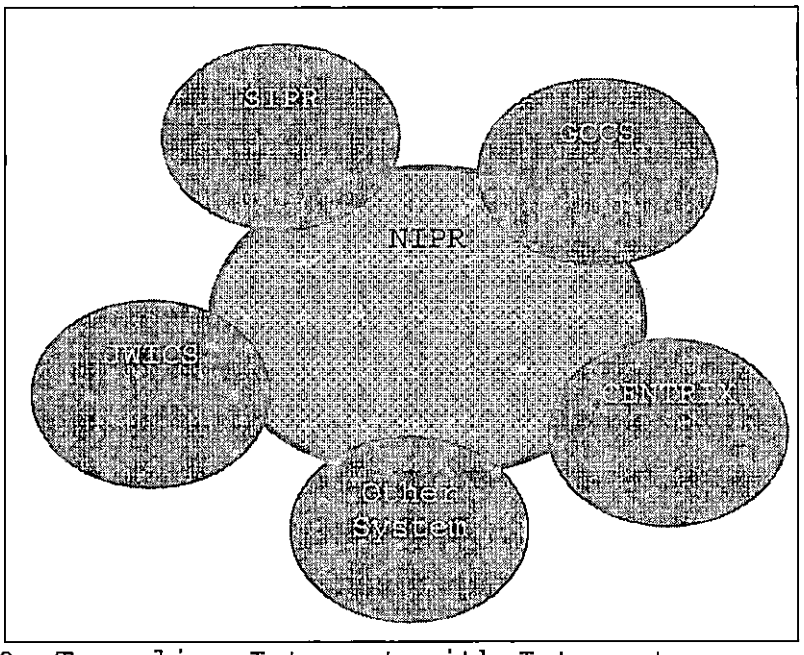


Figure 10. Tunneling Internet with Intranets

A tunneling is based on a Virtual Private Network (VPN) or often established in Secure Shell (SSH) environment. However, the SSH does not provide all the features of the VPN. The VPN tunneling can be established by setting up the VPN server using an encrypted path which protects data from exploitations and spoofing. Once the VPN server is established, the users can access the private network over the Internet. Based on this concept, the classified networks can be replaced by its own backend servers. The tunneling (see Figure 10) will allow a single data transmission path to be shared by multiple network systems. Ultimately, this allows the DoD to

operate and maintain the effective and efficient network architecture.

Cross Domain Solution

Similar to the tunneling concept, another potential solution that thin client based system can adopt is a Cross Domain Solution (CDS). The CDS is no different from tunneling the Internet in support of transporting private and sensitive information. It only utilizes the unclassified bandwidth to transport sensitive information.

To further define the CDS, the CDS is geared towards sharing non-U.S. classified information with other coalition organizations such as North Atlantic Treaty Organization (NATO) and Combined Forces Command (US and Korea). If CDS is successfully implemented, it could also consolidate and standardize current operational services to improve supportability and interoperability and align the vision for NetOps of the DoD. According to the DoD Instruction (DoDI) 8110.1, Multinational Information Sharing Networks Implementation, signed on February 6, 2004, initiated the establishment of the Multi-National Information Sharing (MNIS) Program within the DoD. The

directive describes multinational as including all interactions between the United States and foreign nations whether referred to as combined, coalition, allied, bilateral, multilateral, or similar terminology. (DoDI 8110.1, 2004)

Under the CDS, consolidating coalition services and co-locating them with identical or similar US-only services (GCCS, SIPR, and JWICS) has the potential to reduce operating and maintaining costs. Other benefits of centralization include allowing the integration of coalition information-sharing capabilities into a single network environment to be possible. This also provides the integration, configuration management, and synchronization, of coalition capabilities as well as providing the foundation for the DoD-wide NetOps.

Over the longer term, centralization has the potential to reduce the implementation time and associated costs of installing, updating, and maintaining network services. This effort could help the DoD to move coalition services away from the heavy reliance on multiple, discrete, and costly NSA's Type-1 encrypted networks and move toward greater net-centricity.

Black Core

In addition to the CDS, there is a concept call "Black Core Network" which is designed to transport of sensitive data using the Internet. This method has been used widely by commercial organizations for years in order to transport their sensitive information and data safely and securely.

Currently, the DoD network is operating similar to the early version of propriety online services such as AOL which cannot accommodate and interoperate multiple classifications of networks due to its own security parameters and encryption requirements. In attempt to combine those classified networks, the black core could replace its current encryption requirements. According to DeSimone, the Johns Hopkins Applied Physics Lab, "the black core would substitute cryptographic associations among network endpoints for the physical segregation of data on separate networks. Ultimately, there might be no need to maintain a rigid separation between, for example, Secure IP Router Network and the Unclassified but Secure IP Router Network." (DeSimone, 2009)

This process (see Figure 11) can be achieved by assigning packet headers to identify as either

unclassified or classified information with prioritize packet transmission. The classified packet header will maintain higher prioritization that allows the packet to go ahead of unclassified packets. This also enables each user's packets to be isolated into its own virtual circuit which allows logical separation of two different traffics.

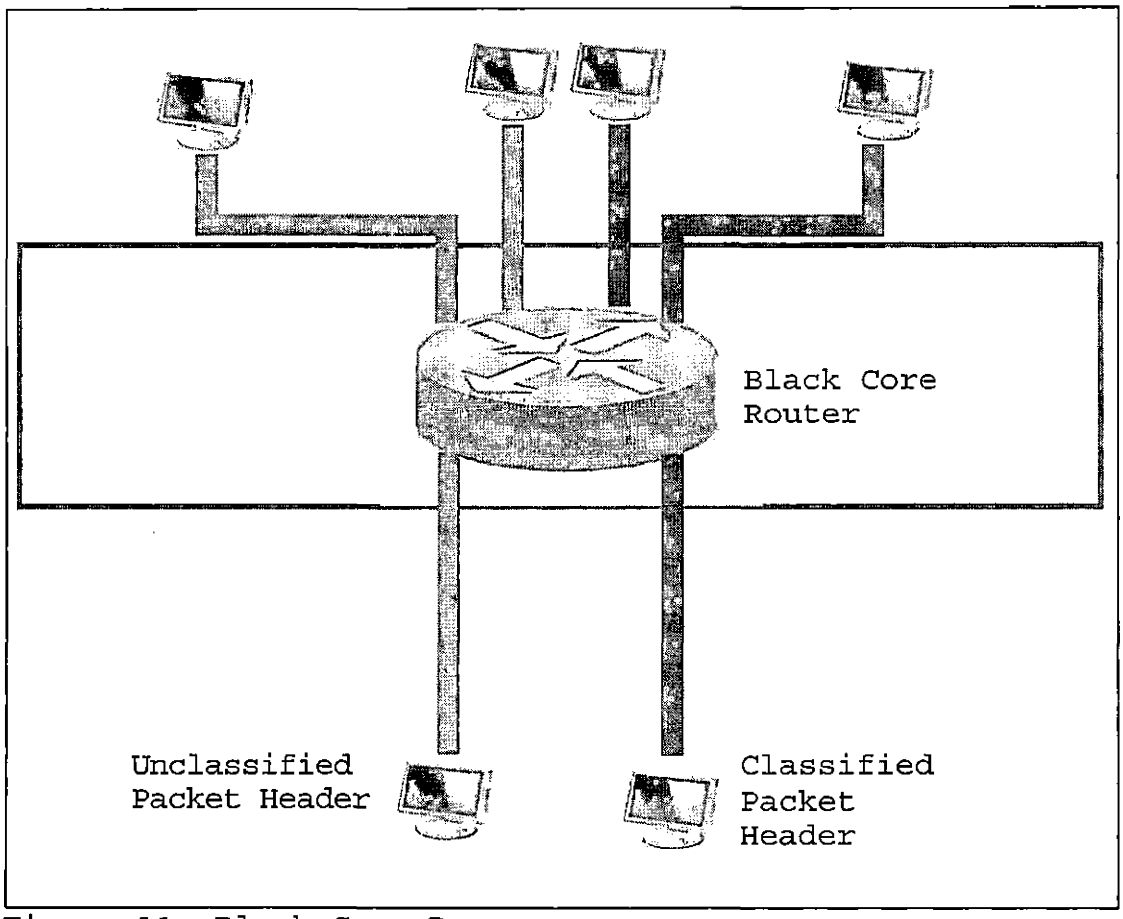


Figure 11. Black Core Process

In addition, this black core routing solution could combined both classified and unclassified bandwidth together to provide more throughput and bandwidth availability for users.

Policies and Procedures

According to Sinclair and Merkow, the thin client will not create a revolution overnight in the way that a firm organizes its work and writes its policies. Likewise, this applies to the DoD network when implementing a new system. (Sinclair & Merkow, 2000) The careful establishments of policies and procedure have to be in place. Then, the implementation should be followed by user awareness and training. Especially, the network security is one of the vital areas that must be focused in order to protect sensitive information while maintaining optimum network performance and user access.

Security Policy

In order to protect the thin client system integrity and security, the DoD Computer Emergency Response Team (CERT) issues alerts, bulletins, and technical tips based on IAVA (Information Assurance Vulnerability Alert) messages and alerts. These messages and alerts direct

specific actions and give mandatory suspense compliance in order to maintain the system's integrity and its security. (AR 25-2, 2007) All classified information will be protected in transmission by approved technique unless a waiver is granted under procedures established by Chief of Information Officer (CIO). Approved techniques, which may be used separately or in various combinations, to protect the transmission of classified information, are as follows:

a. Encryption - Approved cryptographic products.

b. Products used to protect both classified information.

c. Products used to protect sensitive (but unclassified) information only

d. Data encryption standard equipment - Unclassified cryptographic equipment employing the Data Encryption Standards (DES) algorithm, which meets the requirements of Federal Standard 1027.

e. Government approved commercial equipment

f. Unencrypted cable circuits - Unencrypted cable circuits can be employed to transmit sensitive information when the cables are used only

within the geographic boundaries of the United States or within areas totally within U.S. control overseas

The Information Assurance (IA) program will consists of three parts:

a. Training. All personnel will receive IA training. The role of user will determine what level of IA training the user receives. In addition, ensure all section personnel receive periodic IA training conducted by the IASO.

b. Identification. IA personnel will proactively identify known vulnerabilities on a thin client system by using tools such as antivirus and firewalls suites.

c. Prevention. IA personnel will ensure that all identified severe and medium vulnerabilities are removed from a thin client system in order to prevent exploitation.

Security Procedures

When vulnerability or threat is notified, the following procedures should be taken in order to protect the network system:

a. Notify the Information Assurance Security Officer (IASO) of vulnerability and provide initial information.

b. Upon notification of an IAVA, the IASO or IA personnel coordinate with the System Administrator to access the vulnerability.

c. There are three categories of vulnerability and each category has its own procedure to be followed:

- High Vulnerabilities - Remove the vulnerability immediately.
- Medium Vulnerabilities - Remove the vulnerability within specified time given by the CERT.
- Low Vulnerabilities - Removing a low vulnerability can cause the functionality of the system to degrade. Therefore, remove the vulnerability when directed.

d. Once the vulnerability is identified, remove the vulnerability and perform a rescan using the appropriate scanning tool.

e. Once the removal of vulnerability is completed, document the event.

f. When reportable event (such as intrusion) occurs before IAVA was issued, the following actions must be performed:

- Isolate the system by disconnecting the LAN cable and do not turn off the system
- Check if other systems are affected by similar intrusion signs
- Document the following information:
  - System Type
  - Operating System and Version
  - System Network IP and Hostname
  - System Audit Logs
  - Description of Incident
    - How was the problem brought to your attention?
    - What occurred?
    - Where was the attack coming from?
    - What are the Network address and the user Id?

    - When did the incident occur?
    - Was the system compromised?
- Notify the IASO and provide the information above
- IASO must advise all users of the potential intrusion signs and problems

Handling Sensitive and Classified Information

Transmission of sensitive and classified information should be transmitted securely by using methods approved by the NSA. When information transits an area not under access controls as rigorous as required for that classification of the information, it need be secured by a protected distribution means such as an encryption device or a program. The security safeguards applied to sensitive and classified information during transmission will be consistent with the need for protection against disclosure, loss, exploitation, modification, and destruction. (AR 25-2. 2007)

CHAPTER FIVE

FINANCIAL AND NON-FINANCIAL BENEFITS ANALYSIS

Finance Benefits

Every year, energy costs are going up constantly which impact day to day operations of private businesses and government activities, which result in higher energy bills. Especially in support of the current defense Budget Cut Act of 2011, the DoD leadership needs to find areas to reduce overall budget and other operational related costs while maintaining and operating the current defense posture. A major cost of running the DoD comes from supporting an information technology infrastructure. The DoD can enjoy financial benefits when thin clients are implemented in the DoD network system. The thin clients can contribute to the overall cost savings in the area of power usage, overall equipment cost, and operating/manning of the network equipment.

In order to fulfill this information, the study was conducted by obtaining information from Dell and Southern California Edison Power Company. Those two company provided information based on a notional test bed

environment of a thin client backend server and 11 thin client workstations.

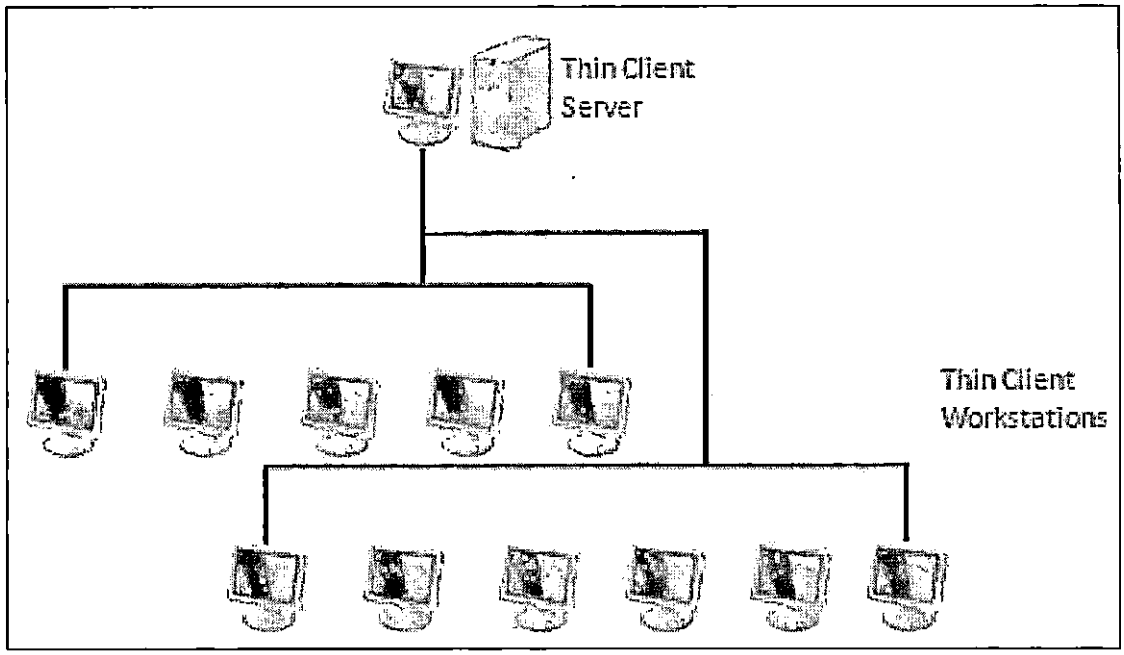


Figure 12. Test Environment Diagram

The Figure 12 above is simply illustrating how the test bed would set up to demonstrate its integration into the DoD network.

Price Comparison Study

The following price (see Appendix B) is from Dell Federal Systems who is authorized supplier of DoD computer equipment, network equipment, and its related peripherals through the DoD acquisition process.

The table 9 below is showing an estimate of 11 conventional workstations. The total procurement cost would be $11,366.

Table 9. Conventional Workstation Price Quote

Product	Quantity	Price	Total
OptiPlex 9010 Minitower	11	$1,033.29	$11,366.19

The table 10 below is showing an estimate of 11 thin client workstations. The total procurement cost would e $3,929.

Table 10. Thin Client (Diskless Workstation) Quote

Product	Quantity	Price	Total
Wyse P25	11	$357.27	$3,929.97

When the estimated total price of thin clients is compared with the estimated total price of conventional desktops, it is clear that thin clients will only cost one third or only 34% percent of a conventional desktop price.

For the DoD, it is not always easy to track and monitor its own power requirements and usages, given the flood of equipment running around the clock. Thus, this analysis is only focuses on the differences between two systems. The table 11 shows a total power usage between thin clients and conventional workstations. Based on the report (Appendix C), thin clients power usage would range from 563 watts (minimum usage) to 833 watts (maximum usage) for all the hardware including its backend server. If a single thin client is measured alone, it would only consume 8 watts. Under the test bed environment, 11 thin clients would only draw 88 watts. In contrast, the desktop alone for the conventional network environment is 2200 watts. This measurement is based on the 11 units of conventional workstations.

Table 11. Power Consumption Comparison

	Desktop	Thin Client
Minimum Usage	200 watts per x 11 workstations	(8 watts per x 11 workstations) + (475 watts per x 1 backend/central server)
Total	2200 watts (2.2 kw)	563 watts
Maximum Usage	200 watts per x 11 workstations	(8 watts per x 11 workstations) + (745 watts per x 1 backend/central server)
Total	2200 watts (2.2 kw)	833 watts

When you compare the power usages between the two systems, 11 thin clients would only consume merely 4% of the desktops' total power usage. Even with the backend/central server running as a set, it would only consume 40% of the power. This is a significant cost saving that the DoD can certainly enjoy.

Now, let's take this cost savings study into another level. Under a typical single military division unit, at its own headquarters level, it is estimated to have roughly 460 unclassified workstations (see Figure 13). This number is based on number of workstations that are

assigned to its commanders and staff members and does not include other network systems.

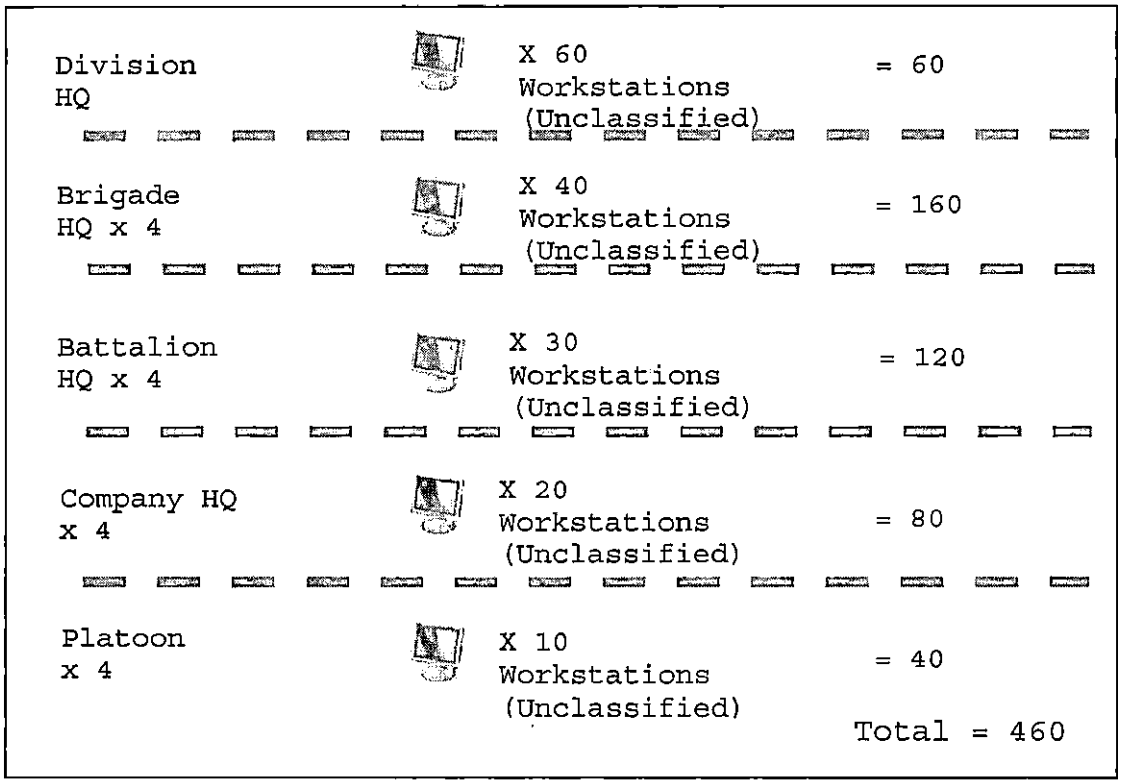


Figure 13. Estimated Number of Workstations (Under a Single Division)

Based on the estimated number of workstations in the division, the estimated cost of two systems shows a significant difference (Table 12 and Figure 14). Under a thin client system, the total cost of 460 workstations would be $164,347.88. In contrast, the total cost of conventional workstions would be $475,313.40.

Table 12. Price Comparison (Under a Single Division)

	# of WS	Thin Client	Conventional	Cost Delta
Test Bed	11	$3,929.97	$11,366.19	$7,436.22
Platoon	40	$14,291.12	$41,331.60	$27,040.48
Company	80	$28,582.24	$82,663.20	$54,080.96
Battalion	120	$42,873.36	$123,994.80	$81,121.44
Brigade	160	$57,164.48	$165,326.40	$108,161.92
Division	60	$21,436.68	$61,997.40	$40,560.72

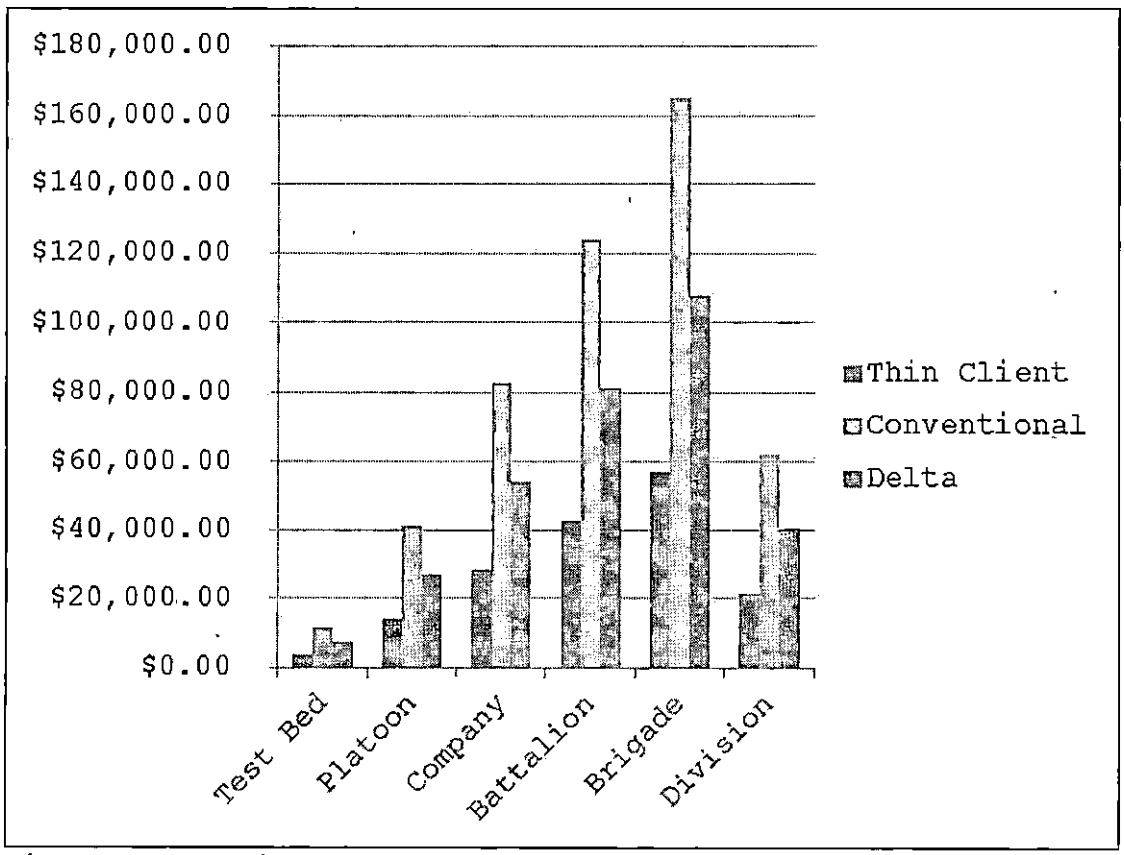


Figure 14. Price Comparison (Under a Single Division)

The total purchasing price of the thin client (see Figure 15) would be $164,347 for the single division and the workstation would cost $475,313. By implementing the thin client the division can achieve a total saving of $310,965 or a saving of $676 per thin client unit.

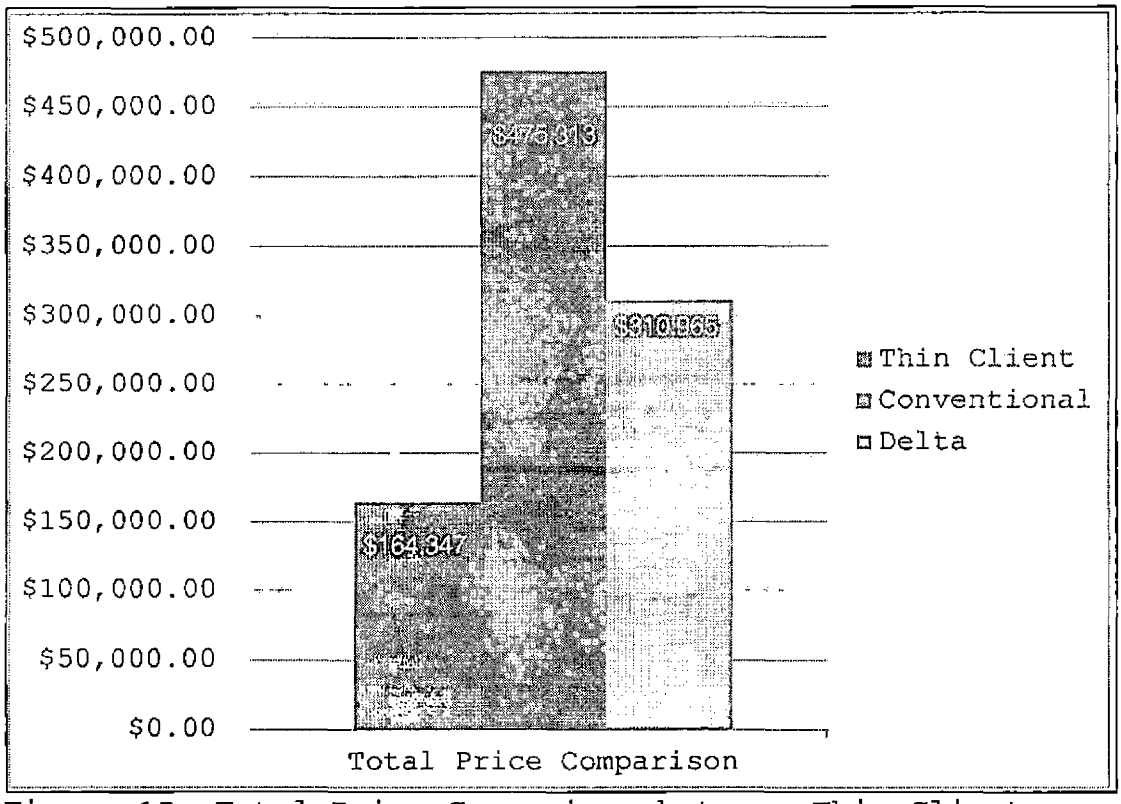


Figure 15. Total Price Comparison between Thin Clients and Conventional Desktops

Under this calculation, if the DoD replaces 10,000 conventional workstations with thin clients, it would

save approximately $6,760,000. The Figure 16 shows incremental cost savings by units.

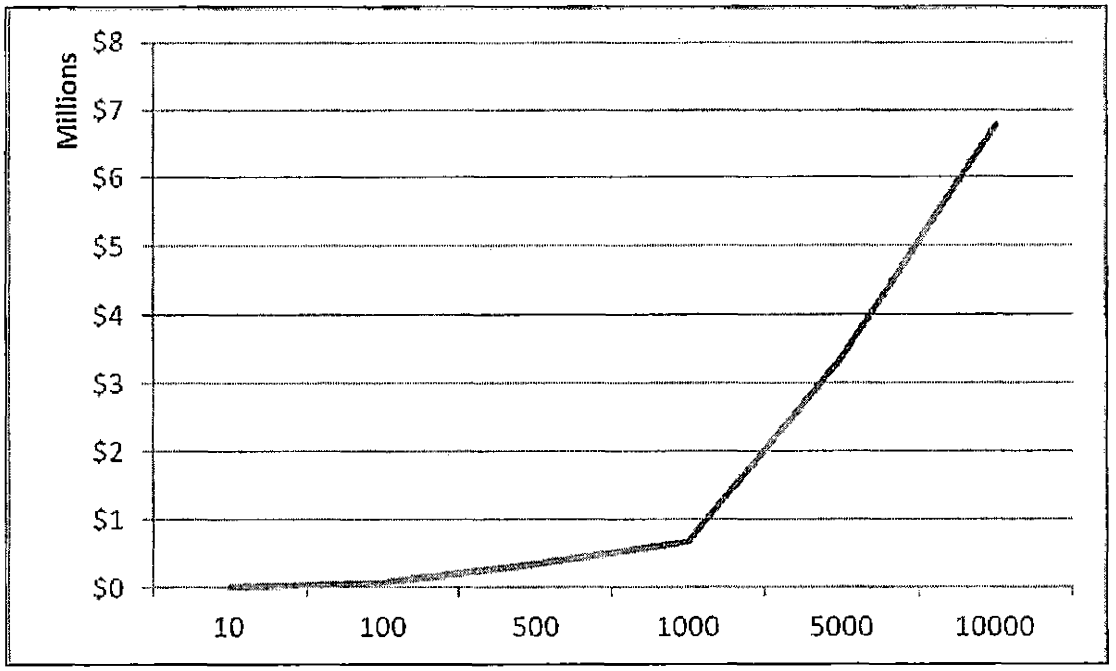


Figure 16. Incremental Savings ($676 per Unit)

It is unclear to find out a total number of workstations in the DoD. Therefore, an accurate projection of the total savings would be difficult. But, it is clear that thin clients can certainly ease the burden of an IT budget, which can support the Budget Cut Act of 2011.

Power Consumption and Cost Study

As it was mentioned above, the thin client network environment uses significantly less power than the

conventional desktop network. In attempt to understand the total cost savings from the power usage, the power consumption rate was converted into the local power company's charging rate using Dell's estimated power consumption information.

This study was supported by Southern California Edison Power Company (Appendix C) in order to provide estimated charges and fees based on the usage of thin clients and conventional desktops. The estimated cost report was generated based on the following assumptions:

1. Cost based on 1000 workstations
2. Cost based on 24 hours of workstation operations
3. Cost based on three categories of demand charge rates (On-Peak, Mid-Peak, and Off-Peak)

The cost of powering a thin client network is divided into two categories, maximum and minimum power usage. This estimated total cost include customer service charge per month, reliability charge per month, and demand and energy charges based on on-peak/mid-peak/off-peak. If all thin clients are using at the maximum power (see Table 13) rate, the usage of thin client workstations and its backend server would

cost $62,072. At the minimum power (see Table 14) rate, the total cost would be $42,537.

Table 13. Thin Client under the Maximum Power Usage Rate

	Rate	Monthly Usage	Avg. Monthly Charge
Customer Service Charge ($/month)	$704.66		$704.66
Reliability Charge ($/month)	$1,100.00		$1,100.00
Demand Charge - On Peak ($ per KW)	$6.88	833.0	$5,731.04
Demand Charge - Mid Peak ($ per KW)	$2.74	833.0	$2,282.42
Demand Charge - Off Peak ($ per KW)	$1.31	833.0	$1,091.23
Energy Charge - On Peak($/kWh)	$0.10330	152,022.5	$15,703.92
Energy Charge - Mid Peak($/kWh)	$0.08280	228,033.8	$18,881.19
Energy Charge - Off Peak($/kWh)	$0.07270	228,033.8	$16,578.05
	Average Monthly Bill		$62,072.52

Table 14. Thin Client under the Minimum Power Usage Rate

	Rate	Monthly Usage	Avg. Monthly Charge
Customer Service Charge ($/month)	$704.66		$704.66
Reliability Charge ($/month)	$1,100.00		$1,100.00
Demand Charge - On Peak ($ per KW)	$6.88	563.0	$3,873.44
Demand Charge - Mid Peak ($ per KW)	$2.74	563.0	$1,542.62
Demand Charge - Off Peak ($ per KW)	$1.31	563.0	$737.53
Energy Charge - On Peak($/kWh)	$0.10330	102,747.5	$10,613.82
Energy Charge - Mid Peak($/kWh)	$0.08280	154,121.3	$12,761.24
Energy Charge - Off Peak($/kWh)	$0.07270	154,121.3	$11,204.61
		Average Monthly Bill	$42,537.92

For the conventional workstation (see Table 15), the total cost would be $160,975 based on monthly usage of 2,200 KW.

Table 15. Conventional Desktop Under the Maximum Power Usage Rate

	Rate	Monthly Usage	Avg. Monthly Charge
Customer Service Charge ($/month)	$704.66		$704.66
Reliability Charge ($/month)	$1,100.00		$1,100.00
Demand Charge - On Peak ($ per KW)	$6.88	2200.0	$15,136.00
Demand Charge - Mid Peak ($ per KW)	$2.74	2200.0	$6,028.00
Demand Charge - Off Peak ($ per KW)	$1.31	2200.0	$2,882.00
Energy Charge - On Peak($/kWh)	$0.10330	401,500.0	$41,474.95
Energy Charge - Mid Peak($/kWh)	$0.08280	602,250.0	$49,866.30
Energy Charge - Off Peak($/kWh)	$0.07270	602,250.0	$43,783.58
	Average Monthly Bill		$160,975.49

The results are illustrated in the figure below (see Figure 16). It shows the conventional workstations cost almost 4 times more than the minimum usage of thin clients and almost 2.5 times more than the maximum usage of thin clients.

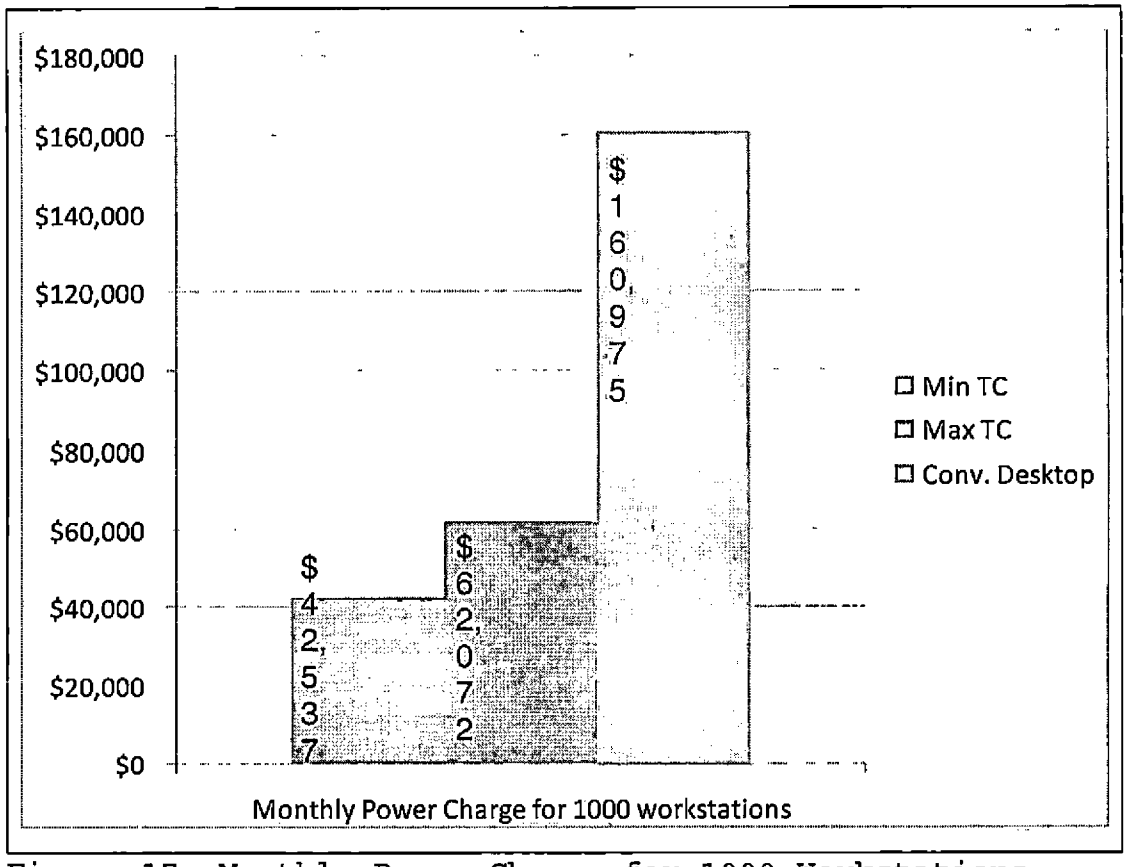


Figure 17. Monthly Power Charge for 1000 Workstations

Based on the result above, one can conclude that power and cost savings increase as the size of the network increases under the thin client environment. For each conventional workstation replaced by a thin client workstation, there will be a significant cost savings that the DoD can benefit and enjoy.

In addition, the Total Cost of Ownership (TCO) can be one of the major cost saving factors. There are other costs that are associated with maintaining the system

(operations, support, and maintenance phase). This phase includes updating software, repairing workstations and systems, and other IT infrastructural needs such as HVAC (Heating, Ventilation, and Air Conditioning). Since thin clients are based on the centralized network, it requires less resources and time to update software and other programs as well as any repairs that are required. There is plethora of other benefits, but in short, thin clients will cost much less than conventional workstations from the cradle to the grave.

Other Benefits

Reduction of Interim Approve To Operate and Approved To Operate

As mentioned earlier, all DoD network access has to go through either IATO or ATO process. Without an approved IATO or ATO, the network system is not allowed to join the DoD network. Although, the reduction of IATO and ATO under the thin client may not appear as a direct financial benefit, it can contribute to streamline the process and expedite overall approving processes. The Figure 17 below is a representation of IATO and ATO process.

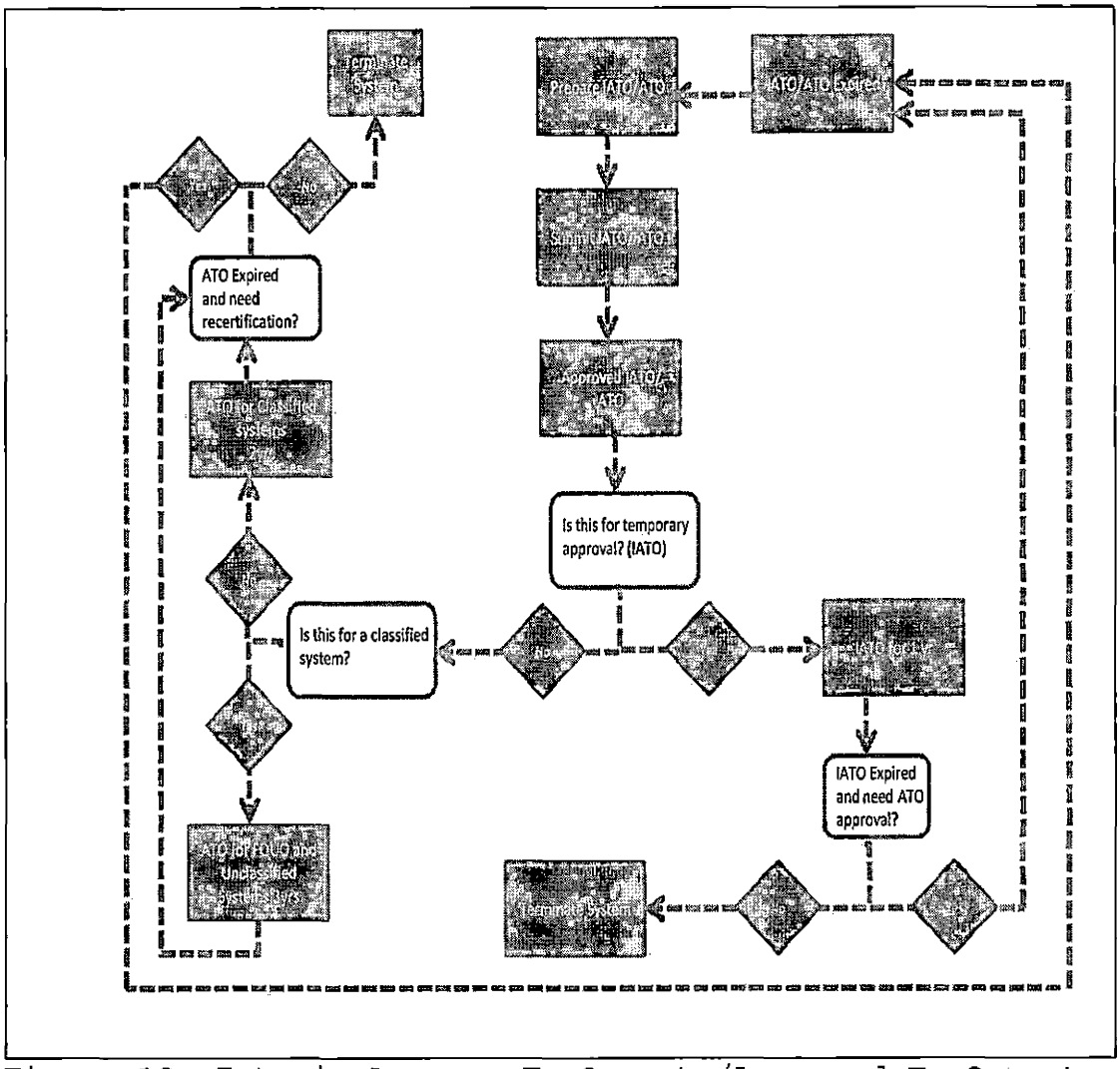


Figure 18. Interim Approve To Operate/Approved To Operate Processing Flow Chart

The user (at the command layer such as Battalion, Brigade, and Division) prepare IATO or ATO and submit all required information to the Designated Approving Authority (DAA). Once DAA approves the IATO or ATO, it gets finalized by a local Directorate of Information

Management (DOIM). If the approval is based on the IATO, then the access to the DoD network is only limited for a year and the user has to submit a complete ATO packet in order to gain access for additional 2 or 3 years based on its classification (unclassified or classified) level.

The Figure 18 below shows the estimated number of total IATO or ATO to be approved by the DAA under the current conventional network architecture (under a single division).

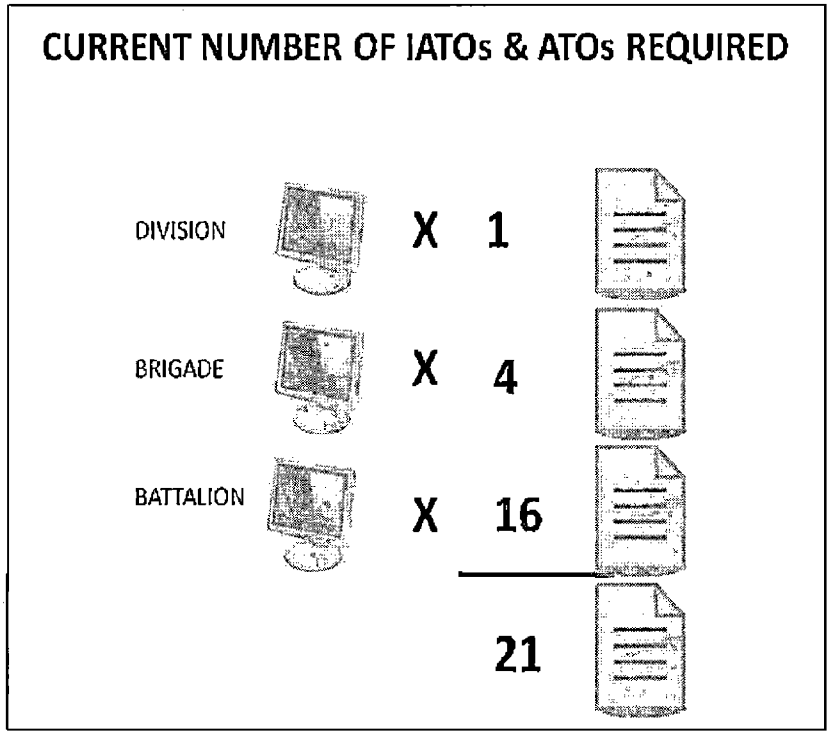


Figure 19. Current Number of Interim Approve To Operate/Approved To Operate Required (estimated)

Based on the number of units assigned to each layer of command (i.e. Battalion and Brigade) under one division, the required estimated number of total IATO or ATO would be approximately 21 which are all required to gain access to the DoD network with the DAA's approval.

As it is illustrated above, the IATO or ATO process can add tremendous work and time to the leadership or management as well as it supporting staff to prepare all necessary information and documentations. Thus, under the thin client network, this IATO or ATO process can be reduced significantly. In contrast to the Figure 18, the Figure 19 shows the estimated number of total IATO and ATO to be approved by the DAA under the new thin client concept.

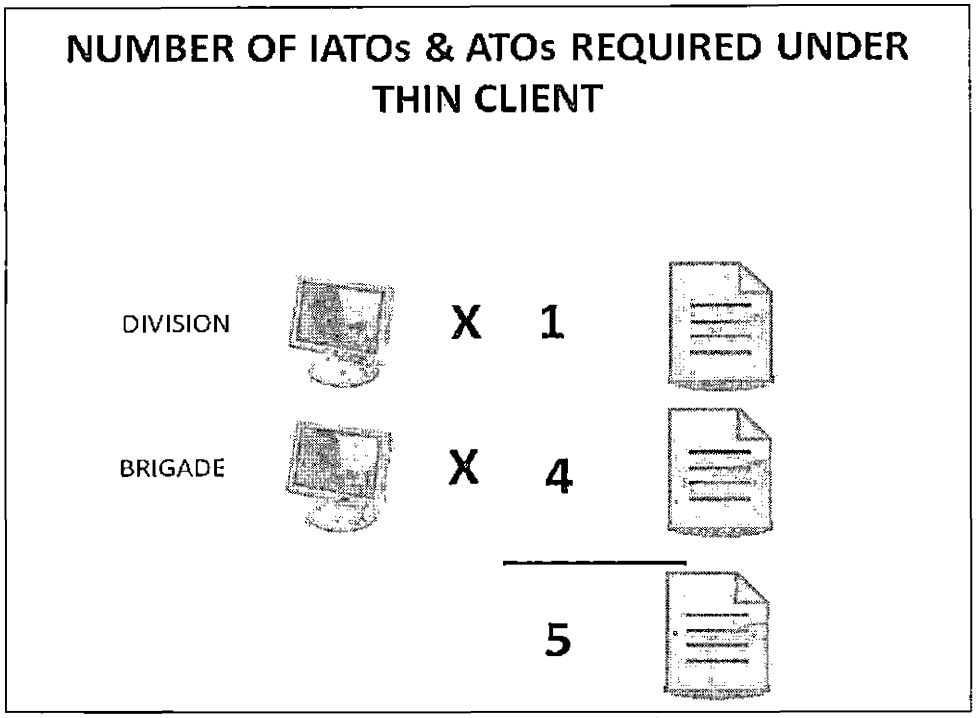


Figure 20. Interim Approve To Operate/Approved To Operate Requirement under a Thin Client (estimated)

The IATO and ATO requirements will be reduced significantly from 19 to 5, because the division and brigades will be only responsible for gathering IATO and ATO in order to obtain an approval by the DAA. This is a result of processing, file sharing, and accessing of all required work through the centralized network.

Supporting Personnel

When thin clients replace the conventional workstations, the number of support personnel requirements can be reduced as well. Since, the thin

client system manages all software and programs from the backend server (at the core and distribution), it reduces the number of trouble tickets or calls. Thus, it requires fewer personnel to maintain, operate, and troubleshoot each workstation.

Table 16. Estimated Number of Personnel Assigned to Each Unit

	Estimated # of IT Personnel Required for a Division (Under Conventional)	Estimated # of IT Personnel Required for a Division (Under Thin Clients)
Division	16	16
Brigade x 4 (ea)	40 (10 ea)	32 (8 ea)
Battalion x 4 (ea)	32 (8 ea)	16 (4 ea)
Company x 4 (ea)	16 (ea)	8 (2 ea)
Total	104	72

A total number of IT personnel (military) assigned to each unit can be varied based on a mission specific area and a task (see Table 16). Under the conventional network environment, the estimated number of total IT personnel can be 104. In contrast, under the thin client environment, the total personnel can be reduced to 72

(estimated). This is total savings of an estimated 32 IT personnel. The lower echelon units (battalions and companies) can reduce its personnel significantly, because all maintenance can be conducted at the core or distribution level. The remaining IT personnel at the lower echelon units can be remained in support of other tactical communication systems.

The differences in personnel between the conventional and the thin client environments can be converted into dollar amount in order to project its potential savings. According to Aurelio Locsin, he found the average salary of the active duty soldier based on a Congressional Budget Office report. In 2010, the average active duty soldier received an average of $99,000 per year. This includes 60 percent of non-cash compensation such as medical/dental care and tax advantages. (Locsin, n.d.) Based on this information, the thin client implementation can save $3,168,000 (32 personnel x $99,000) a year for one division.

Overall, the implementation of the thin client system within the DoD may serve at the global level that bring together critical service components, leverage system administration and maintenance resources including

different level of security systems. In addition, the merging of services and network promote increased sharing of information. As a result, the thin client system may provide the greatest impact and result with the following benefits:

- Economies of scale
- Ability to relieve redundant maintenance tasks
- A higher degree of optimization, operational efficiency, configuration management, interoperability, and compatibility
- Ability to provide consistent, reliable, uniform service using DoD standard IA tools
- 24/7 NetOps operational visibility, control, and monitoring of enterprise services, Information Assurance (IA), and Computer Network Defense (CND)
- Improved information sharing
- Better collaboration with the DoD components, allies, and coalition partners
- Better quality of service
- Improved security through elimination of ad hoc lash-ups of legacy systems and replacement with

an integrated suite of capabilities defined by regulations, policies, and procedures

- Integrated NetOps - information assurance, reporting and monitoring
- More rapid deployment and insertion of additional capabilities and services
- Potential to shorten implementation time
- Streamlined, standardized, and simplified connection approval process
- Potential to reduce infrastructure personnel and equipment

Potential Issues and Challenges

Every day, organizations (both government agencies and private sectors) deal with security breach, incidents, and other malicious attacks. According to Symantec, the U.S. Government was recorded as the top industry sector for data breach and other exploitations. Moreover, it was 12 percent increase from the previous year. (Symantec, 2008) The 12 percent increase is substantial and its impact cannot be measured in dollars because it deals with the national security and welfare of our citizens.

The issues with the Internet can be identified from its origin of the network concept where it was established to share information freely without any restrictions. However, this concept had to be modified and changed throughout the time due to the security threats from inside and outside. The security issues are not only limited to the logical, but also physical. The thin client system is not an exception from those issues.

Due to the nature of the network and its system, it is impossible to mitigate and detect all those threats to guarantee seamless day to day operations, There is no other system or network that guarantees 100 percent security. Only secured system known to the IT personnel is probably the stand alone computer. Therefore, it is important to streamline processes and its design, so the IT and IA professions can manage the network more securely and respond to a threat(s) or an incident(s) in a timely manner.

Other issues that are surrounding the thin clients would be a core problem of centralized networks. If the centralized or back-end server becomes inoperable or faces a total failure, the rest of the thin clients would not be operable or accessible. In order to mitigate this

issue, the management must look into implementing a back up backend server to provide a redundancy in case of a main server failure.

In addition, the performance of the thin client may become an issue. The thin client is a diskless workstation and has lower microprocessor and memory requirements than the conventional workstations. Thus, if the user require running and operating a heavy program or software, the thin client would not be feasible. This could be resolved by a hybrid network approach where thin clients and conventional workstations can be melded to form a network that satisfies different user requirements.

Lastly, the implementation of thin clients in the DoD network may face challenges by the external agency. This potential thin client implementation needs to be reviewed and tested by NSA in order to obtain security validation and approval. The NSA system approval and validation may take time. Thus, close coordination with the NSA security validation team are required. This coordination should begin during the initial phase of concept refinement.

In addition, one of the final steps of the full integration phase is obtaining a Joint Interoperability Test Center (JITC) approval. The JITC needs to validate its system interoperability in accordance with the DoD acquisition guideline. JITC will test the system to ensure this implementation allows seamless operations between different service branches such as Army, Air Force, Navy, and Marine Corps. This is to ensure that procuring system could interoperate within the service components and satisfy their requirements.

It is uncertain to find the longevity of a validation and a certification time from those two agencies. But, it is certain that those two agencies are one of the major stakeholders to approve the overall implementation of the thin client system.

CHAPTER SIX

CONCLUSION

When thin Clients are compared with the conventional workstations, they are not only different with appearances. It is also different how the system operates and managed. Thin clients operate based on centralization of all services including software and programs at the backend server. This is like utilizing a bank. The users deposit money at the bank for a security purpose as well as other helpful services such as loans and financial advices. Likewise, the user will leave all applications and services at the centralized or backend server and use it when required.

Thin client network is simple to design and implement because all necessary programs and services run from the central server. Thus, thin client diskless workstations have lower microprocessor and memory requirements than the conventional workstations, which consume less power to run and operate. The thin client is considered to be more secured than the conventional workstation, because thin client is a diskless workstation, and it reduces risk of introducing malicious

code and viruses as well as compromising the network security at the individual client level.

The analysis based on Dell and Southern California Edison Power Company information proved that the DoD can enjoy significant cost savings. The two main cost savings can be seen from per unit/workstation savings and cutback of power consumptions. Thin client network system is a great option to consider for the DoD in order to support and align with the Budget Cut Act of 2011.

There are also other non-financial benefits such as consolidating other network systems such as SIPR, GCCS, CENTRIX, and JWICS. In addition, the IATO or ATO process can be significantly reduced. The supporting personnel can be reduced at each command layer due to the centralization of the network where updates and repairs can be easily conducted at the server level.

However, there are other issues and potential challenges that the DoD has to realize. First, there is always a possibility of the central server failure of the central server. When it occurs, it could cripple the entire network and deny any access that prevent all day to day operations. In addition, there may be challenge imposed by external entities such as NSA and JTICS. In

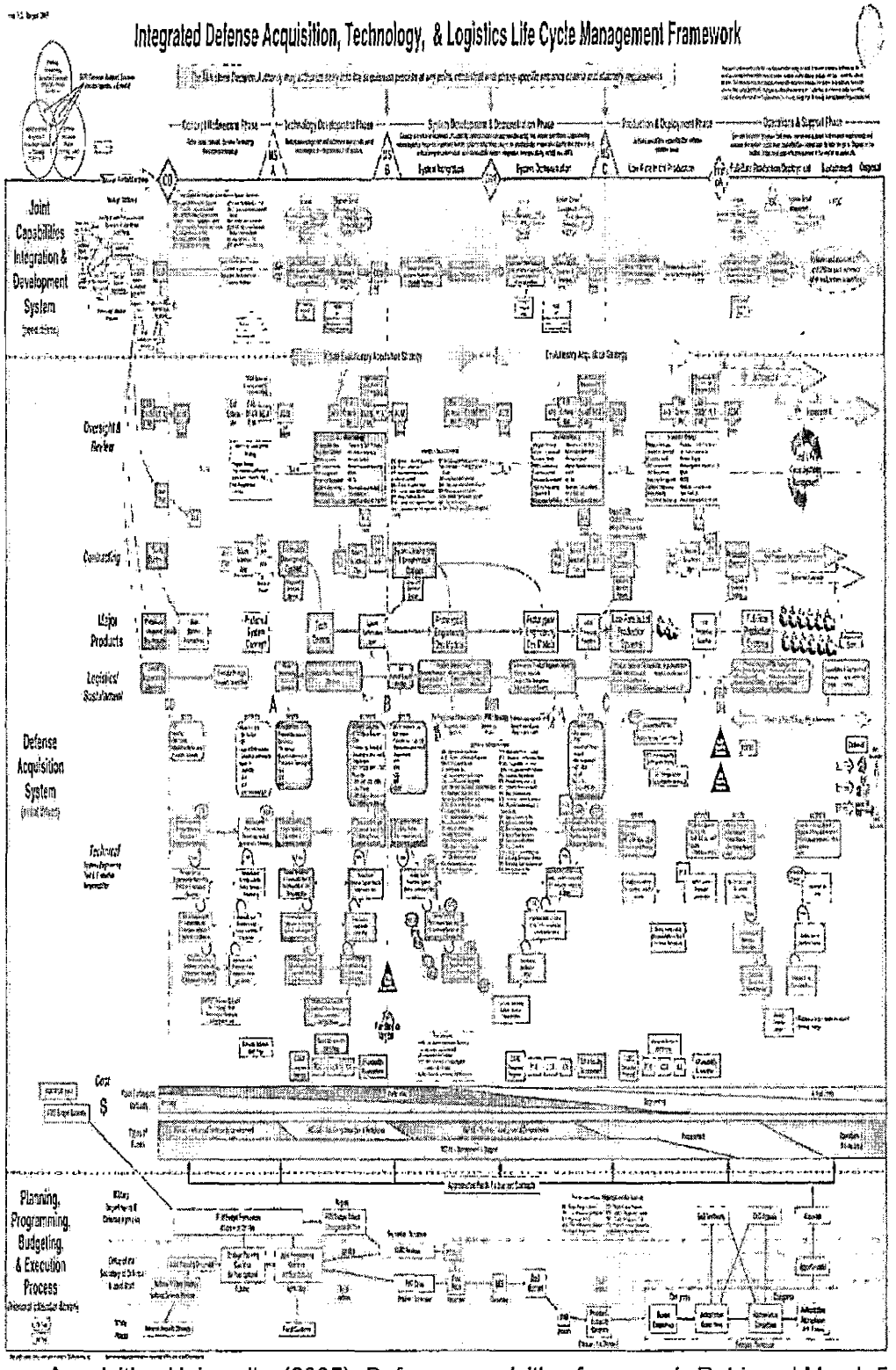
order to implement the thin client system successfully, close coordination are required with these external entities from the beginning to the end.

In addition, this paper not only presented benefits of thin clients, but also illustrated developing processes of the implementation of thin clients using the DoD acquisition framework as a baseline.

Based on findings and analysis, a full implementation of the thin client system in the DoD network is highly recommended.

APPENDIX A

DEPARTMENT OF DEFENSE ACQUISITION FRAMEWORK



Defense Acquisition University. (2005). *Defense acquisition framework*. Retrieved March 5, 2013 from https://acc.dau.mil/CommunityBrowser.aspx?id=30503

APPENDIX B

DELL QUOTATIONS

QUOTATION

	Quote #:	643289808
	Customer #:	119829978
	Contract #:	10000
	CustomerAgreement #:	FAR 52.212-4 T & C
	Quote Date:	01/24/2013
Date: 01/24/2013	Customer Name:	US ARMY

Thanks for choosing Dell! Your quote is detailed below; please review the quote for product and informational accuracy. If you find errors or desire certain changes please contact your sales professional as soon as possible.

ACCOUNT TEAM

Account Manager

Name	Amanda Knittel	Phone	1-800-259-3355
Email	Amanda_Knittel@dell.com	Ext.	5138161

Account Manager

Name	Amanda Knittel	Phone	1-800-259-3355
Email	amanda_knittel@dell.com	Ext.	5138161

SOFTWARE & ACCESSORIES — GROUP TOTAL: $5,896.77

Product	Quantity	Unit Price	Total
P25 32MB (256MB) FLASH/512MB (4GB) DDR3 RAM FIBER READY TAA (A6504140) non-TAA	11	$357.27	$3,929.97
KIT SC SIMPLEX OPTICAL MODULE FOR P20 (A5562154)	11	$178.80	$1,966.80

***Total Purchase Price:**	$5,896.77
Product Subtotal:	$5,896.77
Tax:	$0.00
Shipping & Handling:	$0.00
State Environmental Fee:	$0.00
Shipping Method:	STANDARD GROUND

(Amount denoted in $)*

Please review this quote carefully. If complete and accurate, you may place your order at www.dell.com/qto (use quote number above). POs and payments should be made to *Dell Federal Systems L.P.* For TAA: http://tcbox.us.dell.com/slc/Federal/army/delltaalist.xls.
If you do not have a separate agreement with Dell that applies to your order, please refer to www.dell.com/terms as follows: If purchasing for your internal use, your order will be subject to Dell's Terms and Conditions of *Sale-Direct* including Dell's U.S. Return Policy, at www.dell.com/returnpolicy#total. If purchasing for resale, your order will be subject to *Dell's Terms and Condition of Sale for Persons or Entities Purchasing to Resell*, and other terms of Dell's PartnerDirect program at www.dell.com/partner. If your order includes services, visit www.dell.com/servicecontracts for service descriptions and terms. Quote information is valid for U.S. customers and U.S. addresses only, and is subject to change. Sales tax on products shipped is based on "Ship To" address, and for downloads is based on "Bill To" address. Please indicate any tax-exempt status on your PO, and fax your exemption certificate, with seller listed as *Dell Federal Systems L.P.*, to Dell's Tax Department at 800-433-9023. Please include your Customer #.
For certain products shipped to end-users in California, a State Environmental Fee will be applied. For Asset Recovery/Recycling Services, visit www.dell.com/assetrecovery.

QUOTATION

Quote #:	643286231
Customer #:	119829976
Contract #:	IDIQ6680
CustomerAgreement #:	W91QUZ-07-D-0006
Quote Date:	01/24/2013
Customer Name:	US ARMY

Date: 01/24/2013

Thanks for choosing Dell! Your quote is detailed below; please review the quote for product and informational accuracy. If you find errors or desire certain changes please contact your sales professional as soon as possible.

ACCOUNT TEAM

Account Manager

Name	Amanda Knittel	Phone	1-800-289-3355
Email	Amanda_Knittel@dell.com	Ext.	5138161

Account Manager

Name	Amanda Knittel	Phone	1-800-289-3355
Email	amanda_knittel@dell.com	Ext.	5138161

GROUP: 1 QUANTITY: 1 SYSTEM PRICE: $1,033.29 GROUP TOTAL: $1,033.29

Base Unit	OptiPlex 9010 Minitower (225-2583)	1
	3rd Gen Intel Core i5-3570 Processor (6MB, 3.4GHz) w/HD2500 Graphics, Dell Optiplex 9010 (319-0809)	1
	8GB, NON-ECC, 1600MHZ DDR3,2DIMM,OptiPlex (317-9987)	1
	Dell Smartcard Keyboard with Detachable Palmrest,OptiPlex (330-3944)	1
	Activate Dell Data Protection Access Software to enable authentication selection (469-2656)	1
	No Monitor Selected, Dell OptiPlex (320-3704)	1
	Intel® Integrated Graphics w/o Adapters, OptiPlex (320-3184)	1
	320GB 2.5,Opal SED with FIPS,S,3.0Gb/s,16MB DataBurstCache,OptiPlex 990 Minitower (342-3057)	1
	Windows 7 Professional,No Media, 64-bit, Optiplex, English (421-6606)	1
	Windows 7 Label, OptiPlex, Fixed Precision, Vostro Desktop (330-6228)	1
	Dell Client System Update (Updates latest Dell Recommended BIOS, Drivers, Firmware and Apps),OptiPlex (421-5334)	1
	Dell Data Protection Access, OptiPlex x010 (421-6276)	1
	Dell MS111 USB Optical Mouse,OptiPlex and Fixed Precision (330-9455)	1
	Intel vPro Technology Enabled, Dell OptiPlex 9010 (331-5542)	1
	16X DVD-ROM SATA,Data Only,Dell OptiPlex 990 Desktop and Minitower (318-0483)	1
	Thank you for Choosing Dell (318-2231)	1
	Heat Sink, Performance, Dell OptiPlex Minitower (331-5538)	1
	Internal Speaker, OPtiplex (318-0319)	1
	OptiPlex 9010 Minitower Standard Power Supply (331-5536)	1
	Regulatory label, Mexico, for OptiPlex 9010 MiniTower (331-6253)	1
	Enable Low Power Mode for EUP Compliance,Dell OptiPlex (330-7422)	1
	Power Cord,125V,2M,C13,Dell OptiPlex (330-1714)	1
	Documentation,English and French,Dell OptiPlex (331-2030)	1
	No RAID, Dell OptiPlex (341-8035)	1
	No ESTAR Settings, OptiPlex (331-5325)	1

No Resource DVD for Dell Optiplex, Latitude, Precision (312-3673)	1
Chassis intrusion switch, DellOptiPlex (310-6719)	1
No Quick Reference Guide,Dell OptiPlex (310-9444)	1
Shipping Material for System,Minitower,Dell OptiPlex (331-1268)	1
Microsoft Office Trial (410-0702)	1
Dell Limited Hardware Warranty Plus Service Extended Year(s) (939-1018)	1
Dell Limited Hardware Warranty Plus Service Initial Year (935-6167)	1
ProSupport: Next Business Day Onsite Service After Remote Diagnosis 2 Year Extended (998-1182)	1
ProSupport: Next Business Day Onsite Service After Remote Diagnosis Initial Year (939-2511)	1
Thank you choosing Dell ProSupport. For tech support, visit http://support.dell.com/ProSupport or call 1-866-516-3115 (989-3449)	1
ProSupport : 7x24 Technical Support , 2 Year Extended (998-1342)	1
ProSupport : 7x24 Technical Support , Initial (939-3131)	1
Core i5 vPro Sticker (331-1564)	1

***Total Purchase Price:**	**$1,033.29**
Product Subtotal:	$1,033.29
Tax:	$0.00
Shipping & Handling:	$0.00
State Environmental Fee:	$0.00
Shipping Method:	STANDARD GROUND

(Amount denoted in $)*

Please review this quote carefully. If complete and accurate, you may place your order at www.dell.com/ciq (use quote number above). POs and payments should be made to *Dell Federal Systems L.P.* For TAA: http://fpbox.us.dell.com/sb/Federal/army/dellskuSL.xls.

If you do not have a separate agreement with Dell that applies to your order, please refer to www.dell.com/terms as follows: If purchasing for your internal use, your order will be subject to Dell's Terms and Conditions of *Sale-Direct* including Dell's U.S. *Return Policy*, at www.dell.com/returnpolicyctod. If purchasing for resale, your order will be subject to *Dell's Terms and Condition of Sale for Persons or Entities Purchasing to Resell*, and other terms of Dell's PartnerDirect program at www.dell.com/partner. If your order includes services, visit www.dell.com/servicecontracts for service descriptions and terms. Quote information is valid for U.S. customers and U.S. addresses only, and is subject to change. Sales tax on products shipped is based on "Ship To" address, and for downloads is based on "Bill To" address. Please indicate any tax-exempt status on your PO, and fax your exemption certificate, with seller listed as *Dell Federal Systems L.P.*, to Dell's Tax Department at 800-433-9023. Please include your Customer #.

For certain products shipped to end-users in California, a State Environmental Fee will be applied. For Asset Recovery/Recycling Services, visit www.dell.com/assetrecovery.

APPENDIX C

CALIFORNIA EDISON POWER COMPANY

(CITY OF RIVERSIDE) POWER RATES

SCHEDULE TOU

LARGE GENERAL AND INDUSTRIAL SERVICE

Applicability:

Applicable to service for all types of uses, including lighting, power and heating, alone or combined. Beginning on January 1, 2007, this schedule is applicable for new customers whose service is designed for a 150 kW load or greater per Electric Rule 11 as determined by the Department, or for existing customers with a monthly demand level equal to or exceeding 150 kW for any two of the preceding 12 months. Customers that do not meet or exceed the monthly demand under this schedule shall be transferred to the applicable rate schedule.

Character of Service:

Alternating current; regulated frequency of 60 cycles; single phase or three phase service as may be specified by the Department.

Territory:

City of Riverside

Rates:

	Per Meter Per Month
Customer Charge	$704.66
Reliability Charge	$1,100.00
Demand Charge (to be added to Customer and Reliability Charges):	
All kW of on-peak billing demand, per kW	$6.88
Plus all kW of mid-peak billing demand, per kW	$2.74
Plus all kW of off-peak billing demand, per kW	$1.31
Energy Charge (to be added to Demand, Reliability and Customer Charges):	
All on-peak kWh, per kWh	$0.1033
All mid-peak kWh, per kWh	$0.0828
All off-peak kWh, per kWh	$0.0727

For all customers served on Schedule TOU with Thermal Energy Storage (TES) equipment installed and operating to reduce on-peak charges, all energy delivered during any Sunday through Thursday, including holidays from 11 p.m. to 8 a.m. will be charged at the rate of $0.0610 per kWh.

Special Conditions:

1. **Voltage:** Service will be supplied at one standard voltage.

   Three phase and single phase normally will be served through one meter installation. The customer shall provide, subject to the Department's approval, means for combining two or more existing meter installations if he desires to convert existing separately metered power and light service to a combined service that will be billed under this schedule.

2. **Daily Time Periods are Defined as Follows:**

   On-Peak: 12:00 p.m. to 6:00 p.m. summer weekdays except holidays
   5:00 p.m. to 9:00 p.m. winter weekdays except holidays

   Mid-Peak: 8:00 a.m. to 12:00 p.m. and 6:00 p.m. to 11:00 p.m. summer weekdays except holidays
   8:00 a.m. to 5:00 p.m. winter weekdays except holidays

   Off-Peak All other hours
   Off-peak holidays are: New Year's Day, Washington's Birthday, Memorial Day, Independence Day, Labor Day, Veteran's Day, Thanksgiving Day, and Christmas.

   Summer shall commence at 12:01 a.m. on June 1 and continue through September 30 of each year. Winter shall commence at 12:01 a.m. on October 1 of each year and continue through May 31 of the following year.

3. **Billing Demand:**

   Separate billing demands for the on-peak, mid-peak and off-peak time periods shall be established for each monthly billing period. The billing demand for each time period shall be the maximum demand for that time period occurring during the respective monthly billing period.

4. **Maximum Demand Measurement:**

   Maximum demands shall be established for the on-peak, mid-peak and off-peak Period. The maximum demand for each period shall be the measured maximum average kilowatt input indicated or recorded by instruments to be supplied by the Department, during any 15-minute metered interval in the month. Where the demand is intermittent or subject to violent fluctuations, a 5-minute interval may be used.

REFERENCES

2X White Paper. (2010). *Thin clients: Benefits and savings of using thin clients*. Retrieved April 30, 2013 from http://www.2x.com/docs/en/whitepapers/pdf/WPthinclient.pdf

Administration's Budget Projections. (2010). *Budget of the U.S. government, fiscal year 2011*. Washington DC: Government Printing Office.

Almond, C., Hoof, J., Lassonde, N., Li, B., & Taylor, K. (2006). *Linux client migration cookbook,* Version 2, IBM Corp.

Andress, J. (2011). *The basics of information security: Understanding the fundamentals of infosec in theory and practice*. San Diego, CA: Syngress Press.

Committee on National Security Systems. (2010). *National information assurance glossary: CNSS instruction No.4009*. Retrieved January 22, 2013 from http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

David, B. (2002). *White paper on thin client benefits*. Retrieved April 30, 2013 from http://www.thinclient.net/pdf/Thin_Client_Benefits_Paper.pdf

Defense Acquisition University. (2005). *Defense acquisition framework*. Retrieved March 5, 2013 from https://acc.dau.mil/CommunityBrowser.aspx?id=30503

Defense Information Systems Agency. (n.d.), *DISA services*. Retrieved February 2, 2013 from http://www.disa.mil/Services/SATCOM/Teleport-System

Department of Defense. (2004). *Multinational information sharing networks implementation*. Retrieved February 3, 2013 from http://www.dtic.mil/whs/directives/corres/pdf/811001p.pdf

Department of Defense. (2008). *NetOps for the global information grid (GIG)*. Retrieved January 20, 2013 from http://www.dtic.mil/whs/directives/corres/pdf/841002p.pdf

Department of Defense. (2012). *Defense budget priorities and choices*. Retrieved February 3, 2013 from http://www.defense.gov/news/Defense_Budget_Priorities.pdf

Department of the Army. (2007). *Information management: Information assurance, Army regulation 25-2.* Washingtin DC: Author.

DeSimone, T. (2009). *IA newsletter: Defining the GIG core*. Retrieved December 11, 2012 from http://iac.dtic.mil/csiac/download/Vol11_No2.pdf

Friedman, B., & Preble, C. (2010). *Department of defense proposed spending cuts*. Retrieved December 20, 2012 from http://www.downsizinggovernment.org/sites/downsizinggovernment.org/files/pdf/defense-spending-cuts.pdf

Greenburg, S., Anderson, C., & Michell-Jackson, J. (2001). *Power to the people: Comparing power usage for PCs and thin clients in an office network environment*. Retrieved April 30, 2013 from http://www.lamarheller.com/technology/thinclient/powerstudy.pdf

Guizani, M., Rayes, A., Khan, B., & Al-Fuqaha, A. (2010). *Network modeling and simulation: A practical perspective*. United Kingdon: John Wiley & Sons Ltd.

Initiative for Global Environmental Leadership (IGEL). (2012). *Less power, pollution and CO2: Thin clients have a lower environmental impact*. Retrieved April 30, 2013 from https://www.igel.com/fileadmin/user/upload/documents/PDF_files/White_Paper_EN/WP_Green_99-EN-44-1.pdf

Locsin, A. (n.d.), *The average salary of a U.S. soldier*. Retrieved April 30, 2013 from http://work.chron.com/average-salary-us-soldier-9060.html

Sinclair, J., & Merkow, M. (2000). *Thin client clearly explained*. Cliltion, NY: Morgan Kaufmann.

Symantec. (2008, April 8). *Symantec report reveals malicious attacks focused toward trusted web sites.* Retrieved February 20, 2013 from http://www.symantec.com/about/news/release/article.jsp?prid=20080407_01

United States General Accounting Office. (1993). *Military downsizing: Balancing accessions and losses is key to shaping the future force.* Retrieved December 14, 2012 from http://www.ntis.gov/search/product.aspx?ABBR=ADA271349