3-2005

Exploratory Inquiry: Disparate Air Force Base Area Network Architectures

Charlie W. Boyd Jr.

EXPLORATORY INQUIRY: DISPARATE AIR FORCE BASE AREA NETWORK ARCHITECTURES

THESIS

Charlie W. Boyd Jr., 1Lt, USAF

AFIT/GIR/ENV/05M-01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENV/05M-01

EXPLORATORY INQUIRY: DISPARATE AIR FORCE BASE AREA NETWORK ARCHITECTURES

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Charlie W. Boyd Jr., BS

First Lieutenant, USAF

March 2005

AFIT/GIR/ENV/05M-01

EXPLORATORY INQUIRY: DISPARATE AIR FORCE BASE AREA NETWORK ARCHITECTURES

Charlie W. Boyd Jr., BS
First Lieutenant, USAF

Approved:

_____/signed/_____	_14 March 2005___
Kevin Elder, PhD (Chairman) Assistant Professor of Information Resource Management Department of Systems and Engineering Management	date
_____/signed/__	_14 March 2005___
Michael Grimaila, PhD (Member) Assistant Professor of Information Resource Management Department of Systems and Engineering Management	date
_____/signed/_____	__15 February 2005_
Marc Grayson (Member) PKI Lead Command Manager, Information Assurance Air Force Communications Agency	date

Abstract

Joint Vision 2020, the Department of Defense (DoD) blueprint for development and transformation, identifies information and technology as critical enablers for our nation's military and calls for the development of a joint force capable of integrated information sharing to provide decision superiority, the ability to make and implement better decisions before enemies can react (DoD, 2000). Networks have been identified as the single most important element for transforming our current military forces. Ironically, Air Force base-level communications networks have been identified as a weakness.

This research follows the qualitative approach to increases the current understanding of base level communications networks by conducting a multiple site comparative case study that includes practitioner interviews at four locations and the examination of existing literature and documented trip reports. This study determines if base- level networks are disparate, isolates sources of disparity, identifies advantages and disadvantages of disparity, and recommends an appropriate course of action.

This research is significant for members of the Air Force, DoD, and private citizens. Air Force networks support close to three-quarters of a million users, including active duty service members, Air Force Reserves, Air National Guard, civilians, and embedded contract employees (McCarter, 2003). In addition to potentially affecting many people and the larger DoD network, base-level networks provide support to deployed warfighters and provide the environment to train, organize and equip our forces. Additionally, these networks provide critical information to key decision makers.

Acknowledgements

First, I thank God for all the blessings he has given me today and everyday. The lord's presence and blessings greatly enhance my life and make success possible; all my failures are mine. Next, I thank my late parents for their love, support, dedication, and guidance. Because of them, I have confidence and a strong work ethic. I also thank my three sisters for giving me strength and providing support throughout this research project and other endeavors throughout my life. Most importantly, I thank my wife and children for their understanding and sacrifices during this project and at other times due to serving our country.

Additionally, I thank my academic advisor, Dr. Kevin Elder, for his patience, understanding, and ability to guide my progression throughout this project. His methodical approach and demeanor helped me get the most out of this experience. I am truly grateful for his assistance. I thank Lieutenant Marc Grayson for lending his experience, insight, and friendship. Lastly, I also thank my fellow students for their help and support along the way. The teamwork and friendships enriched my academic journey. According to an old Greek saying, friendship is essential to the soul.

Table of Contents

Page

Page

Page

List of Figures

Figure Page

List of Tables

Table Page

EXPLORATORY INQUIRY: DISPARATE AIR FORCE BASE AREA NETWORK ARCHITECTURES

I. Introduction

Joint Vision 2020, the Department of Defense (DoD) blueprint for development and transformation, identifies information and technology as critical enablers for our nation's military. Currently, these key enablers provide a tremendous advantage over our adversaries and must be cultivated, protected, and employed effectively in the future (DoD, 2000). Joint Vision 2020 calls for the development of a joint force capable of integrated information sharing to provide decision superiority, the ability to make and implement better decisions before enemies can react (DoD, 2000). The synergy gained by the interdependence of the Services makes it clear that jointness is more than the simple combination of Service capabilities (DoD, 2000:42). The following comment by the current Secretary of Defense, Donald Rumsfeld, supports the guidance found in Joint Vision 2020 and highlights the importance of networks:

> "Possibly the single most transforming thing in our forces will not be a weapons system, but a set of interconnections and a substantially enhanced capability because of that awareness" (DISA, 2004).

In order to provide the environment for decision superiority, Joint Vision 2020 requires the development of a Global Information Grid (GIG); a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting processing, storing, disseminating, and managing information on demand to

warfighters, policy makers, and support personnel (DoD 2000). According to Mr. Rob Thomas, the Air Force Assistant Deputy Chief of Staff for Warfighting Integration, existing network architectures require transformation to provide warfighters with a globally integrated battle-space (Thomas, 2004). Effective integration within the Air Force and across joint operating mission areas necessitates abandoning traditional barriers to take advantage of new technological capabilities (Thomas, 2004). To achieve decision superiority, DoD systems must be interoperable, supportable, and exchange relevant information in a timely manner (DoD, 2004a:23). An August 2002 Secretary of the Air Force policy memo tagged architectures as the "key construct in visualizing mission information relationships and promoting interoperability" (Cabrera, 2004). To summarize, Joint Vision 2020 provides a roadmap for the development of a joint force capable of sharing information and integrated operations beyond the simple combination of capabilities (DoD, 2002). A GIG will provide the information environment required by the joint force and outlined in Joint Vision 2020. Establishment of a GIG requires transformation of existing network architectures. The DoD and the individual services are currently taking action to increase interoperability and achieve optimal integration as outlined in Joint Vision 2020, the DoD blueprint for development and transformation (USSTRATCOM, 2004). This study examines Air Force installation-level networks that contribute greatly to DoD interoperability and integration.

Installation-level wide area and local area networks, WANs and LANs respectively, represent the lowest Air Force portion of the GIG and are critical to joint force interoperability and integration (Brewin, 1997). The services cannot support the DoD blueprint for development and transformation without addressing installation-level

networks (Brewin, 1997). Although the two previous citations are a few years old, the researcher believes these sentiments are still true today. This research study explores these Air Force installation-level or base area network (BAN) architectures, referred to as BANs throughout this study. In the context of this research study, the following definition defines a BAN:

> "The BAN provides interconnectivity within and between systems and networks in the defined campus area. The BAN also provides access for the attached systems and networks to external networks, such as Non-classified Internet Protocol (IP) Network (NIPRNET), Secret IP Network (SIPRNET), and the Internet" (AFCA, 2002).

In this research study, the defined campus area is the area serviced by the local communications organization on a typical Air Force Base and identifies the BAN coverage area. The campus area or BAN includes transmission facilities; switching and routing components; links from the backbone to buildings; interfaces to external and internal networks; and the components required to provide voice, data, and imaging (AFCA, 2002).

In 1997, the Air Force program executive for battle management labeled installation-level networks or BANs as the service's "Achilles' heel" and promoted Air Force plans to establish standard BANs (Brewin, 1997). This study investigates whether BANs are still the service's "Achilles heel". Specifically, this study explores whether BANs are different throughout the Air Force, reasons for existing differences, and advantages and disadvantages of disparate networks.

This research study follows a qualitative approach using a comparative multiple site case study and focused interviews to identify patterns and increase understanding concerning BANs. Information is verified through triangulation, the researcher's values

and bias are reported, and the nature of the research is exploratory. The qualitative approach is appropriate for exploratory research efforts that report the researcher's values and biases (Creswell, 1994).

Background

The Clinger-Cohen Act of 1996 requires the Department of Defense to establish and maintain sound and integrated information technology architectures (US Congress, 1996). Additionally, the nature of military engagement has changed; future wars will be fought with coalitions in a joint service environment (DoD, 2000). Unilateral operations are a thing of the past. The Clinger-Cohen Act mandate and a change in the nature of military engagements acknowledge the importance of the key enablers, information and technology, mentioned in the introduction. Achieving the DOD goal of increased interoperability and integration by exploiting these key enablers fully requires each military service to ensure their respective service-level networks are interoperable and integrated (USSTRATCOM, 2004). Air Force BANs are a key component of the Air Force Enterprise Network (AFEN) and provide a vehicle for mission information exchange between key functional areas supported by an Air Force Base. Figure 1 reflects common BAN connections. The figure shows a high-level example, but is not intended to show a complete set of connections supported by all BANs (AFCA, 2002).

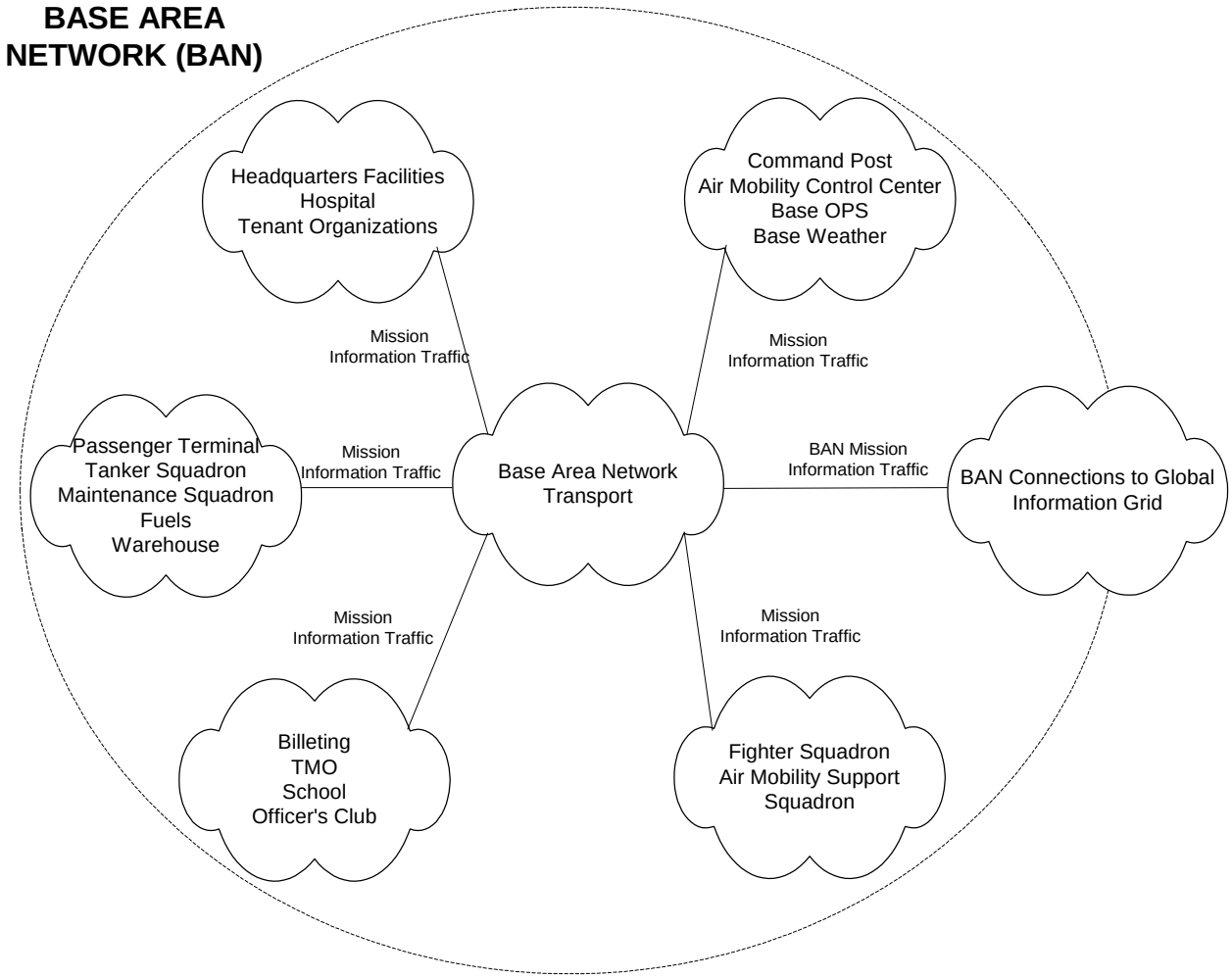

Figure 1, Base Area Network High-level Operational Concept (AFCA, 2002)

Air Force BANs evolved over the years from simple disjointed networks into intricate and essential components of a critical weapons system, the AFEN (DoAF, 2004). These networks provide the critical link between users, information, and technology in support of Air Force and joint operations (DoAF, 2004:4). Accordingly, BANs directly affect our ability to fly, fight, and win (Williams, 2004). The Combat Information Transport System (CITS) program effectively standardized the way individual bases connect to the larger AFEN; chapter II covers this program in more

detail. However, BANs should receive more attention and focus because a loss of service for BAN users could result in mission failure at home or abroad. A briefing provided to senior Air Force leaders in the communications field reflected the standardization of regional control centers, but failed to address installation-level networks (Bruns, 2004).

According to a former director of the Defense Information Systems Agency shared, for far too long people just thought of BANs as plumbing, but they are critical part of the Defense Information Infrastructure (Brewin, 1997). The researcher has encountered Air Force IT leaders that believe standardized BANs are critical to success, and others who believe BAN standardization holds less significance. Base Area Networks are a vitally important element of enhancing combat strength through the synergy created by joining the strengths of individual components (AFCA, 2003).

The researcher has also encountered many IT leaders that believe unique mission requirements or local factors require the development of specialized systems. This line of thinking is outdated and does not support Joint Doctrine requiring increased interoperability and integration. In order to transform doctrine into operational capabilities, leaders must select synergy over specialization to achieve optimal effects. Solutions based on commercial open-systems technology should replace legacy systems whenever possible. This study provides solutions and insight while recognizing the divergent environments and actions dictated by various missions, procurement strategies, and development histories present at bases throughout the Air Force.

Research Significance

This research is significant for members of the Air Force, DoD, and private citizens. Air Force networks support close to three-quarters of a million users, including

active duty service members, Air Force Reserves, Air National Guard, civilians, and embedded contract employees (McCarter, 2003). Currently, the Air Force has 108 connections into the DoD network enterprise (AFCA, 2004:10). In addition to potentially affecting many people and the larger DoD network, BANs provide support to deployed warfighters and provide the environment to train, organize and equip our forces. Today's operating concepts require deployed personnel to obtain logistic and administrative support from home, referred to as reachback capability, and deployed locations (DoD, 2003:1). The term "battlespace" describes an environment where far removed participants and individuals on the battlefield both help shape the battlefield (AFCA, 2003:7). The battlespace construct recognizes the synergy achieved by reachback and distributed operations to increase situational awareness, flexibility, and speed of execution (AFCA, 2003:6). Warfighters, regardless of their location, must be able to obtain and use intelligence from national and theater assets that may be widely dispersed (DoD, 2003). The kill chain (find, fix, track, target, engage, and asses) is where networks as a weapons system can be most effective (Williams, 2004). illustrates the kill chain and the enhancements provided by the GIG. Base area networks play a pivotal role in executing the Air Force mission. Base area networks provide critical voice, data, video, sensory, and imagery to decision makers (CITS, 2004). In light of the facts mentioned in this paragraph, increased understanding and the development of BANs are very important and served as the catalyst for this research project.

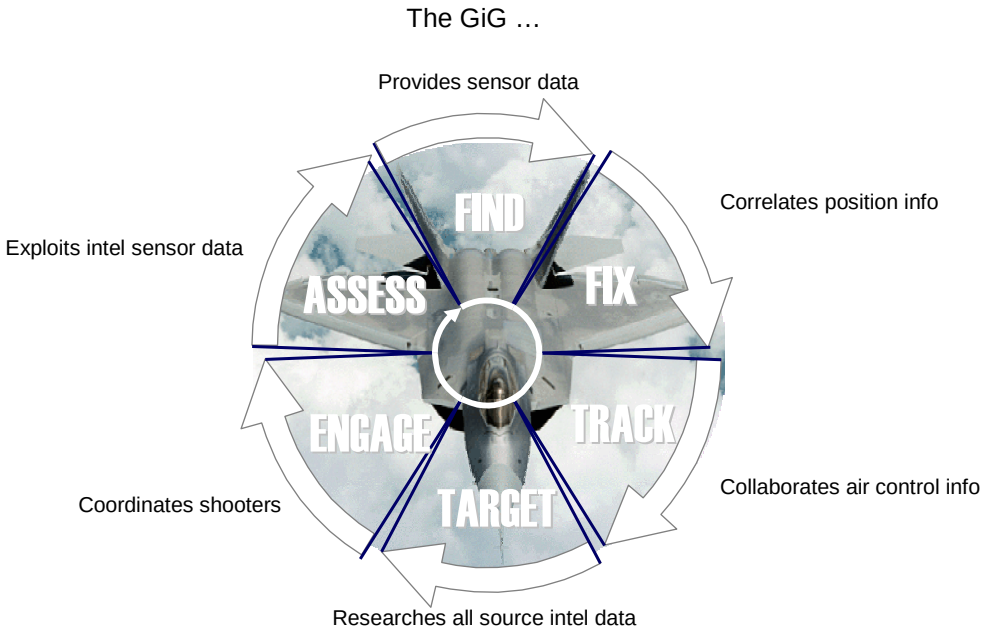

Figure 2, Kill Chain

According to former Secretary of the Air Force, James Roche, "We must preserve and enhance our ability to get and use quality, timely, actionable information to shorten the kill chain." (Williams, 2004) The United States of America is the only superpower in the world, but our nation is still vulnerable to threats now and in the future (DoD, 2000). Few adversaries will take on the United States military directly; however, they will attempt to offset our military superiority by exploiting information and technological vulnerabilities (AFCA, 2003). Future success against enemies and discovering new capabilities depends heavily on our ability to share information and conduct integrated operations. BANs provide a critical link between warfighters, technology, and the information required for mission accomplishment. The Air Force estimates $5 billion in

network upgrades are required to implement Joint Vision 2020 capabilities (USAF/XORI, 2004). Failing to manage base level resources effectively forfeits technological advances implemented at the Department of Defense, Air Force, and Major Command levels.

This comparative multiple site case study, with accompanying focused interviews, provides benefits by uncovering and qualitatively validating valuable patterns and insights from the field. Reviewing pertinent literature combined with the comparative multiple site case study results will increase the existing body of knowledge and provide a foundation for additional research. The Department of Defense, Air Force Communications Agency (AFCA), Major Commands, Commanders, and individual service members will benefit from an increased understanding of BANs. Specifically, Air Force infrastructure architects and planners will benefit from this research.

The timing of this research is very significant. In the summer of 2004, the Air Force Communications Agency transitioned the SCOPE Network mission to SCOPE EDGE. The transition replaced a preventative maintenance and fine-tuning mission involving visits to every Air Force Base every 18 to 24 months with a new mission focused on achieving a consistent, sustainable, and cost-effective communications medium to support a seamless information grid (SCOPE EDGE, 2004). Does the new focus remove a critical helping hand for base-level maintainers? Will the new SCOPE EDGE mission be as successful as SCOPE Network? Will the mission change have detrimental consequences? Time will reveal the answers to these questions; this research provides a peek into BANs at this important juncture.

Research Questions

The research objectives are to increase existing knowledge on the phenomenon of disparate Air Force BANs and to determine if the Air Force should standardize BANs, if the results reflect that BANs are indeed disparate. This research provides insight and a foundation for leaders and managers to make BAN and AFEN related decisions. To satisfy the research objectives, Chapter IV presents an analysis and discussion of the following investigative questions:

1. Are BANs different throughout the Air Force? If so, how?
2. Why are a variety of BANs currently in use throughout the Air Force?
3. What problems are created by using a variety of BANs throughout the Air Force?
4. What are the advantages of using a variety of BANs throughout the Air Force?
5. How should the Air Force respond to the current state of BANs?

Research Propositions

This study addresses the following research propositions according to the research model illustrated in Figure 3:

1. Research will show BANs are different throughout the Air Force
2. Research will identify sources of disparate Air Force BANs.
3. Research will show advantages and disadvantages of disparate Air Force BANs.

Research Model

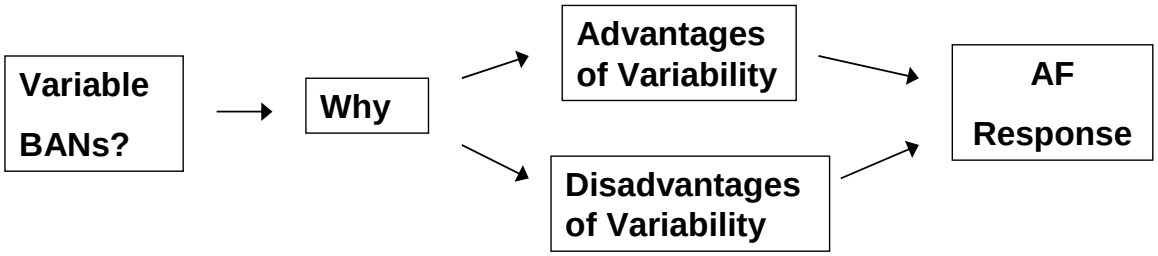

Figure 3. Research Model

Scope and Limitations

The focus of this research study is Air Force base area networks (BANs) and whether the Air Force should take action to standardize these networks. Deployable communications architectures are not covered. The research objectives are to increase understanding and to elevate the importance of BANs; the critical interfaces between warfighters, everyday users, and critical information required to accomplish the mission.

Specific equipment specifications and technologies are not explored, unless required to support the main research focus. This research does not explore other military branches because their command structures and methods of addressing information technology depart greatly from the Air Force. The other branches, commercial organizations, and government nonmilitary agencies present opportunities for additional research.

Thesis Overview

This thesis is presented in five chapters followed by appendices and references. The current chapter introduces the research topic, provides background information, identifies the significance of the research, and highlights the scope and limitations of the research. Chapter II provides and outline of the current Air Force information technology infrastructure and summarizes theoretical perspectives and previous research findings in a clearly defined literature review. Chapter II also reviews existing literature and presents an overview of the CITS program and guidance from the Department of Defense and the Air Force. Definitions, models, and research on related topics are included in the literature review. Chapter III outlines the methodology. This chapter describes how a multiple site comparative case study analysis with focused interviews is used in data collection and analysis. Next, the results are analyzed in Chapter IV. Finally, Chapter V features a discussion of the research results, itemizes the conclusions, promotes recommendations, and identifies areas for future research.

II. Literature Review

Overview

This literature review examines existing literature relevant to the scarcely researched topic of Air Force BANs. The paramount goal of this chapter is to expand understanding provide a common frame of reference for this exploratory inquiry into the Air Force BANs. Very little literature exists concerning base or installation level communications networks. Accordingly, this chapter presents literature pertaining to the larger Air Force Enterprise Network (AFEN) and the base level networks; changes to the AFEN also affect the BANs. To accomplish the chapter goal, this literature review is divided into four main sections. First, the AFEN network architecture is described. Second, the Clinger-Cohen Act of 1996, Strategic Visions 2010, and 2020 are reviewed. Third, organizations that influence the AFEN structure are presented. Fourth, other AFEN and BAN relevant topics, not fitting into the three previous sections, are covered.

Air Force Enterprise Network Architecture

Overview

This section describes the structure and management components of the Air Force Enterprise Network. First, a description of Air Force Base Area Networks (BANs) is presented. Next, trust relationships and Windows NT domain models are discussed. Then, the structure of the AFEN is outlined, followed by a discussion of the three management levels. Finally, the Air Force network operations command relationship is provided. The goal of this section is to inform and establish a common understanding of the Air Force Enterprise Network Architecture.

Air Force Base Area Networks

Deployed communications architectures are outside the scope of this study. However, it is important to note that fixed base communications networks provide critical home base support for deployed warfighters. Home base networks also provide the environment to train, organize and equip information technology professionals prior to deployments. Home networks if properly configured and maintained prepare our airman to successfully support warfighting operations in all arenas.

Over 95 percent of voice, video, and data capabilities used by the Air Force to make force management and deployment decisions rely on cable, wireless, and fiber systems for intra-base network connectivity and information transfer. However, the existing infostructure is insufficient to support the current and future requirements for integrated voice, data, video, imagery, and sensory information data transmission to operators, planners, and support personnel (USAF/XORI, 2004). Local communications networks; providing voice, data, video, etc.; for non-deployed locations throughout the Air Force are referred to by the following names: Base Information Transport System (BITS), Information Transport System (ITS), and Base Area Network (BAN). This research study primarily uses BAN to describe these installation-level networks. Regardless of the name used, it is important to understand what constitutes a BAN. Base area networks consist of the components, systems, and equipment that provide communications services for the local installation; it includes transmission systems, voice networks, data networks, building wiring, network interfaces, video services, and the base Network Control Center (NCC); the focal point for management of the local network, see Figure 4, Base Area Network. The illustration shows a typical configuration. The local

missions, environmental factors, and past history dictate configurations of BANs. An Air Force briefing for senior leaders in 2003, described BANs as independent architectures and a smorgasbord of hardware (AETC, 2003). Many of the systems that make up BANs are highly segregated preventing the desired level of interoperability. The rapid evolution of computing power and networks has contributed to current state of BANs. The updated version of Moore's Law, named after the co-founder of Intel and originally observed in 1965, states that computing power doubles every 18 months and will continue to do so for at least the next two decades (Intel, 2004). Individual BANs come together to form the Air Force Enterprise Network, an Air Force-wide information environment.

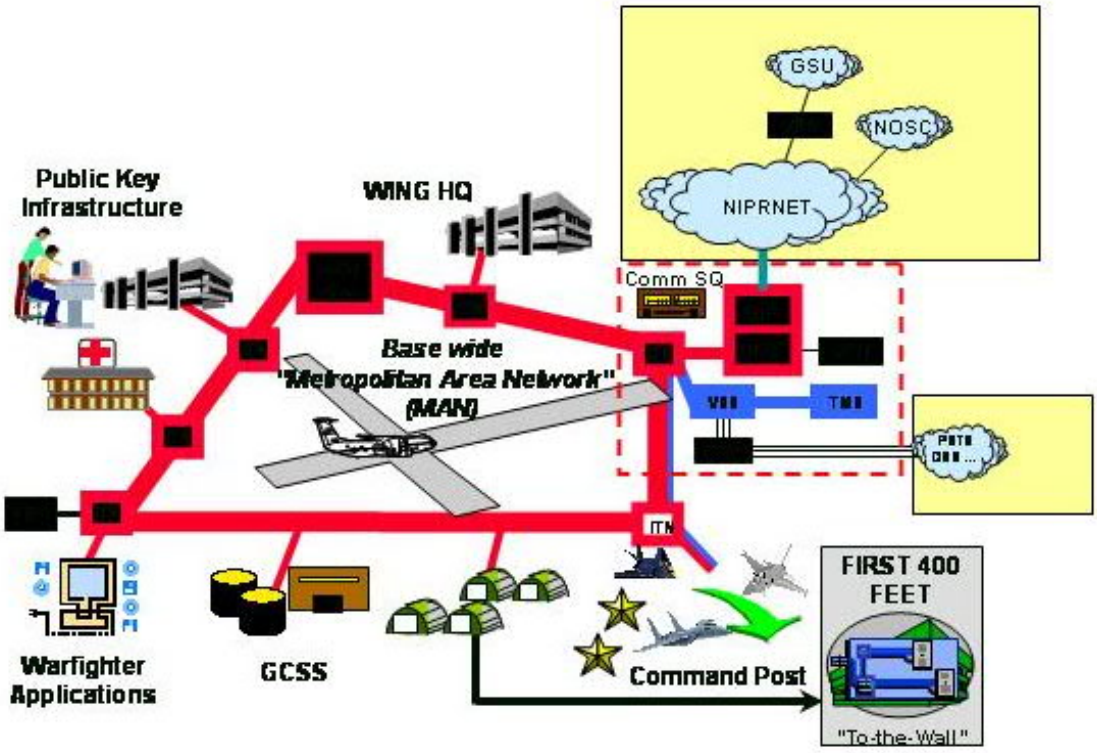

Figure 4, Base Area Network

Trust Relationships and Windows NT Domain Models

A Windows NT domain organizes the resources from one or more servers into a single administrative composition (Locher, 1999). Windows NT provides login privileges to the domain rather than to individual servers and Domain Administrators grant users access to a domain's resources (Locher, 1999). Organizations may choose to establish multiple domains because the number of users or workstations is too large, departments need to manage their own resources, or the number of servers on a single domain is too large and effecting performance (Locher, 1999). Trust relationships between domains allow administrators to manage multiple domains as a single administrative entity and only require users to login to a single domain (Locher, 1999). The next four sections outline the four existing Windows NT domain models: Single, Single Master, Multiple Master, and Complete Trust.

Single Domain Model

This model has a single domain with accounts and resources; provides advantages of centralized management of accounts and resources, does not involve any trust relationships and works best for small organizations (Windows, 2004). Disadvantages are performance problems as the domain grows, lack of internal security divisions for units or divisions to reflect segments of a growing enterprise, and maximum of 40,000 accounts (Windows, 2004).

Single Master Domain Model

This model has a single account domain and multiple resource domains; provides advantages of departmental resource control based on resource domains, centralized account management, global groups (to many multiple accounts) are defined centrally in

account domain, and provides good solution for moderately sized networks (Windows, 2004). The number of trust relationships is based on the number of resource domains. In order for this model to work well, account domain administrators must assign global groups to manage resource security; resource domain administrators should assign permissions to groups, not individuals; and number of accounts can not exceed 40,000 (Windows, 2004).

Multiple Master Domain Model

This model is an extension of the single master model; provides the following advantages: accommodates any number of accounts by adding additional account domains, resources are locally and logically grouped to provide departmental-focused management, any master domain is capable of managing accounts, and provides a good solution for very large organizations (Windows, 2004). The disadvantage is the complexity associated with the additional number of account domains and trust relationships (Windows, 2004).

Single Master Domain Model

This model is a decentralized, high overhead environment consisting of a set of single domains with trusts relationships between each domain; advantages are scaleable for any number of users, each entity has full control over accounts and resources located in the same domain, and very useful for organizations without a Management Information Systems department (Windows, 2004). The disadvantages are lack of centralized management, many trust relationships and associated complexity, and administrators must trust each other to manage accounts, resources, and privileges (Windows, 2004).

A single model described above or a combination of the models can be employed to manage networks (Locher, 1999). Table 1 provides a summary of the Window NT domain models.

Table 1, Domain Model Summary

Domain Model	Maximum Accounts	Account Management	Resource Management	Trusts
Single	40,000	Centralized	Centralized	No
Master	40,000	Centralized	Decentralized	Yes
Multiple Master	Unlimited	Centralized in Account Domains	Decentralized	Yes
Complete Trust	Unlimited	Decentralized	Decentralized	Yes

Fixed base BANs are the focus of this research study, deployable communications architectures are outside the scope of this study. The BANs provide fixed base communications services and represent a significant part of the Defense Information Infrastructure Common Operating Environment (DII COE), a plug and play, client server architecture that defines interfaces and how system components will interact. The DII COE is fully compliant with DOD standards and guidance (AFCA, 1996). Figure 5, Air Force's System Domains (AFCA, 1996), shows how the services BANs provide for fixed base communications relate to other domains of the DII COE.

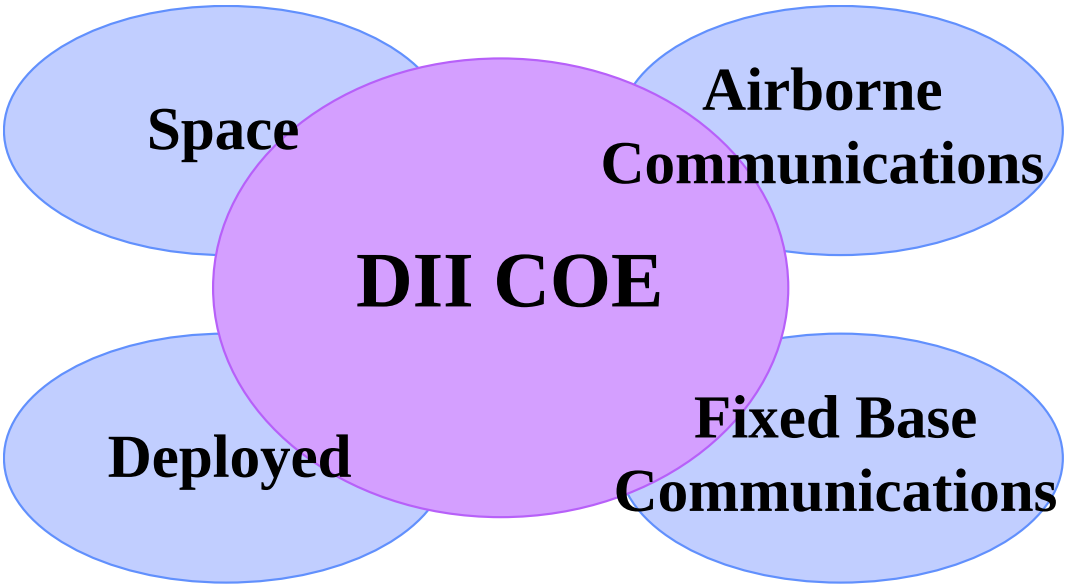

Figure 5, Air Force's System Domains (AFCA, 1996)

The purpose of the DII COE is to field systems with increasing interoperability and operational capability while reducing development time and life cycle cost. The DII COE was developed in late 1993 and designed to eliminate design incompatibility among DOD systems (Carnegie, 2004).

Air Force Enterprise Network

The Air Force Enterprise Network (AFEN) is the Air Force-wide information environment that operates in a global context and is comprised of interoperable computing and communicating components that provide processing; information storage, dissemination, assurance, and transport; human interaction; and network management. The AFEN consist of all owned and leased communications and computing systems, software, and services; data; and security services required to accomplish the Air Force mission. The AFEN encompasses 130 separate bases (Hoeft, 2004). Figure 6, depicts the target architecture for the AFEN and how it fits into the larger DoD architecture. As

mentioned in Chapter I, the Air Force has 108 connections to the DoD enterprise network (AFCA, 2004:10).

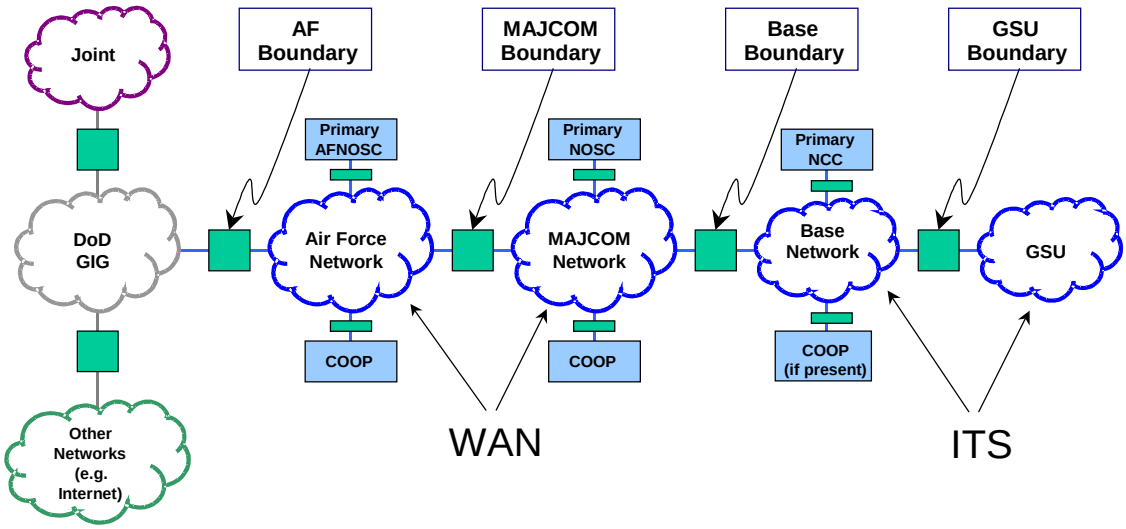

Figure 6, Target Architecture

The AFEN is a part of the Global Information Grid (GIG), an information environment supporting the DoD, national security organizations, and intelligence community. AFEN users, designers, and technicians must follow accepted standards whenever feasible to foster interoperability, assure mission success, commonality, and reduce cost of ownership (DoAF, 2000). The lowest level of the AFEN and the focus of this research study is the Air Force installation-level network architecture or BAN (DoAF, 2004:4).

Successful Network Operations (NETOPS) provide effective, efficient, secure, and reliable information network services used in vital DOD and Air Force communications and information processes. The Air Force NETOPS hierarchy is used to

manage the AFEN; this hierarchy adheres to the Defense Information Infrastructure Control Concept, a three tier DoD NETOPS hierarchy. Within the Air Force NETOPS hierarchy, all three tiers are represented, as shown in Table 2. Air Force NETOPS Hierarchy. Within the DoD NETOPS hierarchy, the Air Force only has a presence at the regional and local tiers. The Defense Information Systems Agency, global tier of DoD NETOPS hierarchy, has overarching responsibility for the military services and other DoD components, as reflected in Table 3. DoD NETOPS Hierarchy. Successful management of the AFEN through NETOPS provides high quality service to customers and satisfies increasing warfighter demands. The paragraphs below Table 2 and Table 3 discuss the three levels of the Air Force NETOPS hierarchy.

Table 2. Air Force NETOPS Hierarchy

NETOPS Level	**Responsible Air Force Organization**
Global (Tier 1)	Air Force Network Operations and Security Center (AFNOSC)
Regional (Tier 2)	Major Command (MAJCOM) NOSC
Local (Tier 3)	Network Control Center

Table 3. DoD NETOPS Hierarchy

NETOPS Level	**Responsible Organization**
Global (Tier 1)	DISA Global NOSC (GNOSC)
Regional (Tier 2)	MAJCOM NOSC, AFNOSC, other service and component NOSCs
Local (Tier 3)	Network Control Center

Network Control Center

The Network Control Center (NCC) represents the local level of Network Operations management within the Air Force NETOPS hierarchy, tier 3. The NCC is the focal point for operation, maintenance, and management of all aspects of the BAN including Local Area Networks (LANs) and Metropolitan Area Networks (MANs) on a particular base. The NCC provides support 24 hours a day, 7 days a week. Personnel assigned to the NCC provide an on-site technical capability for network modifications and restorations of faulty equipment and circuits when directed by higher level Network Operations and Security Centers (NOSC).

Prior to 2004, management of the AFEN was centered on base NCCs because the majority of supported systems were independently installed and created fragmented lines communications (DoAF, 1999). NCCs provided the local network management expertise to offset the inherent obstacles associated with early networks. Today, to provide effective, efficient, secure, and reliable information network services, management of the AFEN has evolved to the three network operations management tiers reflected in table 1. The explosive growth and increasing interconnectivity of networks and information systems making up the AFEN resulted in the change in management focus.

Major Command Network Operations and Security Center

A Major Command (MAJCOM) is a major subdivision of the Air Force. Each MAJCOM has a specific portion of the Air Force mission and is directly subordinate to Headquarters United States Air Force. The Air Force is organized by MAJCOM functionally in the United States and geographically overseas (DoAF, 2003). MAJCOM Network Operations and Security Centers (NOSC) represent the regional or mid-level

organization in the Air Force NETOPS hierarchy, tier 2. The MAJCOM NOSC provides real-time network intrusion detection, perimeter defense capabilities, and fault resolution activities. Additionally, MAJCOM NOSC personnel monitor and support the daily operational issues of subordinate bases and units within their command.

If this study determines that BANs throughout the Air Force are disparate, NOSC personnel will be particularly interested because disparate networks could lead to extended outages and loss of service due to unfamiliarity with various base architectures. Changing the focus for network management and troubleshooting from the NCC to the NOSC creates gaps between troubleshooters and the location of the outage, potentially preventing outage resolution. Several independent studies report that over 80 percent of information technology system downtime is due to processes and people, not technology (Mossing, 2004). This presents a difficult challenge for NOSC personnel attempting to guide local NCC personnel during the resolution of an outage caused by people or processes. Geographic separation may hinder restoration efforts.

Air Force Network Operations and Security Center

The AFNOSC is the highest Air Force NETOPS level, tier 1 or global level. In the DoD NETOPS hierarchy the AFNOSC represents a region level, tier 2, see Table 3. The AFNOSC develops options and directs configuration and security posture changes in response to vulnerabilities and incidents, Joint Task Force direction, and outages that cross MAJCOMs, affect a majority of the AFEN or are time critical (DoA, 2004). The AFNOSC directs the actions of subordinate NOSCs and NCCs when necessary.

Air Force Network Operations Command Relationship

This section describes the command relationships established within the Air Force to accomplish effective management of the AFEN, Figure 7, Air Force NETOPS Command Relationships. Each entity plays a significant role in providing reliable, secure, and on-demand communications services. The relationships help ensure global systems interoperate without diminishing the authority of local commanders to direct and manage assets under their control (DoAF, 2004b).

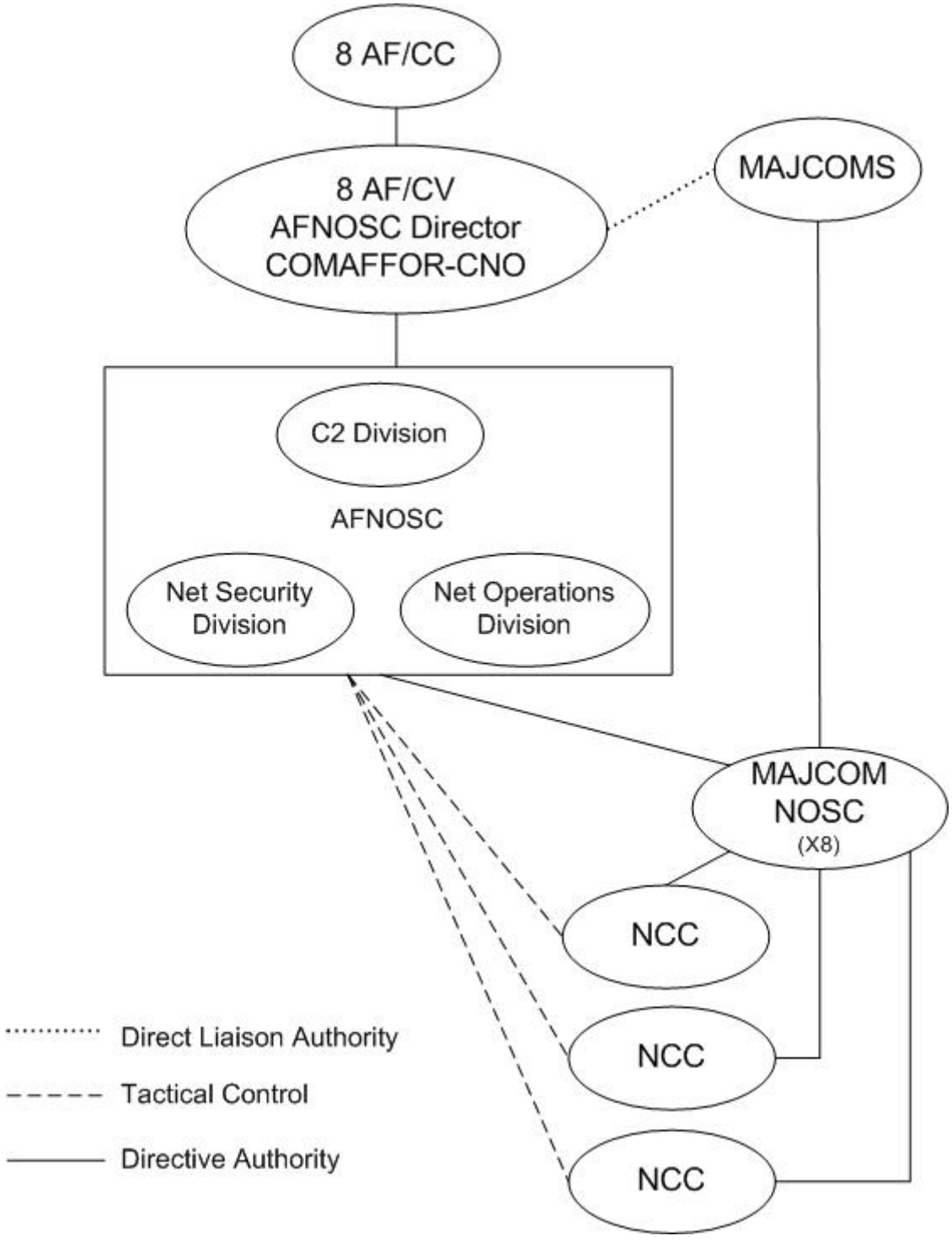

Figure 7, Air Force NETOPS Command Relationships

Eighth Air Force Commander

The Eighth Air Force Commander (8 AF/CC) is designated the NETOPS commander and is responsible for NETOPS across the Air Force. MAJCOMs are directly subordinate to Headquarters United States Air Force. However, the 8 AF/ CC enforces compliance and has directive authority over MAJCOM units and assets. Directive authority is delegated to the Eight Air Force Vice Commander, the AFNOSC director.

Eighth Air Force Vice Commander

The Eighth Air Force Vice Commander (8 AF/CV) is the Commander of Air Force Forces-Computer Network Operations and the director of the AFNOSC. The commander ensures missions are performed in support of joint objectives and integrates NETOPS and computer network defense functions across the AFEN. To ensure network availability and security, the commander directs configuration and security posture changes of NOSCs and NCCs in response to or in anticipation of events.

Air Force Network Operations and Security Center

The AFNOSC is the highest tier in the Air Force NETOPS hierarchy. The AFNOSC provides senior leaders with global visibility of AFEN resources, performs system and network management, disseminates information, works with external agencies to resolve Air Force network anomalies and directs AFEN operational, security, and configuration changes (DoAF, 2004b). Personnel assigned to the AFNOSC provide top-level technical assistance for IT professionals assigned to subordinate NOSC and base NCCs. The AFNOSC has the following three divisions: Command and Control (C2) division, Network Security division, and the Network operations division.

Major Commands

In order to accomplish their portion of the Air Force mission, MAJCOMs must maintain an effective and reliable network that provides communications services to assigned bases and resources. Each of the eight MAJCOMs develops network procedures, policies, and standards for subordinate units. Considerable coordination is required to ensure interoperability and compatibility between MAJCOMs and across the AFEN. Additionally, each MAJCOM maintains a NOSC to provide command and control and NETOPS of their network assets.

Major Command Network Operations and Security Centers

The mid-level organization in the three level Air NETOPS hierarchy is the MAJCOM NOSC. This organization is a critical link in the daily operation of the AFEN. Personnel assigned to the MAJCOIM NOSC provide the commander with front-line network intrusion defense and real-time visibility of assigned network resources throughout the command. MAJCOM NOSC personnel also provide NCCs with fault resolution support, engineering assistance, and visibility into NOSC managed devices. The NOSC also provides systems control, maintenance, and administration functions of the MAJCOM network (DoAF, 2004:22). For example, the Air Combat Command (ACC), a large MAJCOM, NOSC manages one of the largest enterprises in the Air Force. The ACC NOSC provides network services to more than 110,000 users located across the command's 15 Air Force bases (Mossing, 2004). The Air Force is currently transitioning the focus for management of the AFEN from NCCs to NOSC. How this transition is executed will determine if BANs are maintained to provide optimal performance, this study provides foundation research.

Network Control Centers

The NCC is the lowest level in the Air Force NETOPS hierarchy. They provide Wing commanders with visibility and command and control of the fixed base network. Personnel assigned to the NCC help achieve information assurance, oversee operation of the network, and perform maintenance and management of the base network. The NCC provides an on-site technical capability to make physical network changes, modifications, and restoration of defective network transmission equipment and circuits when directed by the MAJCOM NOSC or AFNOSC. Air Force NCCs are the heart of this research study because they provide the first level of management for BANs. Regional control and management of networks, the new Air Force position, seems well suited for information assurance, update dissemination, and command and control. However, fault resolution, quality of service, restoration of network transmission equipment may suffer if regional and global tier technicians aren't familiar with the BANs their responsible for administrating. This research study attempts to determine if variation is present in BANs throughout the Air Force and to explore the nature of any identified differences.

Clinger-Cohen Act and Strategic Visions that Shaped the Air Force Enterprise Network

Overview

This section provides background information concerning the laws and strategic visions that began the transformation of Air Force and DoD network architectures from an assortment of vertical systems to an eventually robust and integrated critical weapons system, see Table 4, Law/Vision Timeline. First, the Clinger-Cohen Act of 1996 is

discussed. Next, Joint Visions 2010 and 2020 are explored to provide a framework and common point of reference for this research study. Finally, the DoD construct for logically improving interoperability is introduced. This section highlights the importance of information and networks, identifies the joint interoperability mandate source, outlines the visions that initiated the DoD transformation, and provides a construct for improving interoperability.

Table 4, Law/Vision Timeline

CLINGER COHEN ACT	1996
Clinger Cohen Act, Amendment	1998
Joint Vision 2010	July 1996
Joint Vision 2020	May 2000

Clinger-Cohen Act 1996

The Clinger-Cohen Act of 1996 establishes and mandates the position of Chief Information Officer (CIO) for federal departments and agencies. The act also sets guidance for acquisition and management of information resources. An amendment to the Clinger Cohen Act requires the following:

- Establishment of IT standards throughout the Department of Defense
- Elimination of duplicate information technology systems within and between the military departments and Defense Agencies
- Interoperability of IT and national security systems throughout the Department of Defense

The amendment assigned additional responsibilities to the Department of Defense and Military Department CIOs (Public Law 105-261). The requirement to establish CIOs did not outline how to implement the new positions. The military departments and the Marine Corps, a division of the Navy, selected different avenues for establishing the position of CIO. The Army and Marine Corps have military officers. Conversely, the Navy and Air Force have civilians. Predictably, each service has distinct methods and procedures for installing, operating, and maintaining their respective networks.

Joint Vision 2010

Joint Vision 2010, released in July 1996, had a profound impact on the development of military capabilities by outlining an operational concept of joint warfighting (Brewin, 1997). The doctrine provided a guiding template for the future direction of warfare; standardization represents the heart of the Joint Vision 2010 (DoD, 2000a). The vision initiated the process of military transformation and established a process for conducting joint experimentation and training (DoD 2000). The document established a common framework and language for the services to develop and articulate their contributions to the joint force and placed emphasis on the ability to disseminate information quickly through networks (DoD, 2000). As a result, network-centric warfare, "employing Information Age concepts to increase combat power in war and mission effectiveness in operations other than war" (DoD, 2001:37), became a central focus of military strategy. Information technology managers in all three services believed in 1997 that the only way to transform network-centric warfare from a concept into reality is through the development of cohesive base-level and shipboard networks

rooted in commercial standards (Brewin, 1997). This research study will increase understanding and focus attention on critical foundation level Air Force networks.

Joint Vision 2020

Joint Vision 2020 builds on the foundation established by Joint Vision 2010 and provides the overarching strategic vision for the continued transformation of our military services. This document is essential to this research study because it defines a future information environment that fosters free and timely information sharing between all DoD components. Base area networks, the focus of this study, provide the critical link between local users and other MAJCOM, Air Force, and DoD assets. The updated vision calls for significantly improved interoperability to provide joint force capabilities beyond the simple combination of service capabilities. The document's primary focus is full spectrum dominance, the ability to operate alone or in combination with partners to defeat any adversary and control any situation, achieved through the interdependent application of dominant maneuver, precision engagement, focused logistics, and full dimensional protection (DoD, 2000, p. 6). Joint Vision 2020 identifies information superiority as a key enabler in the transformation of operational joint force capabilities, Figure 8, (Cohen, 1997).

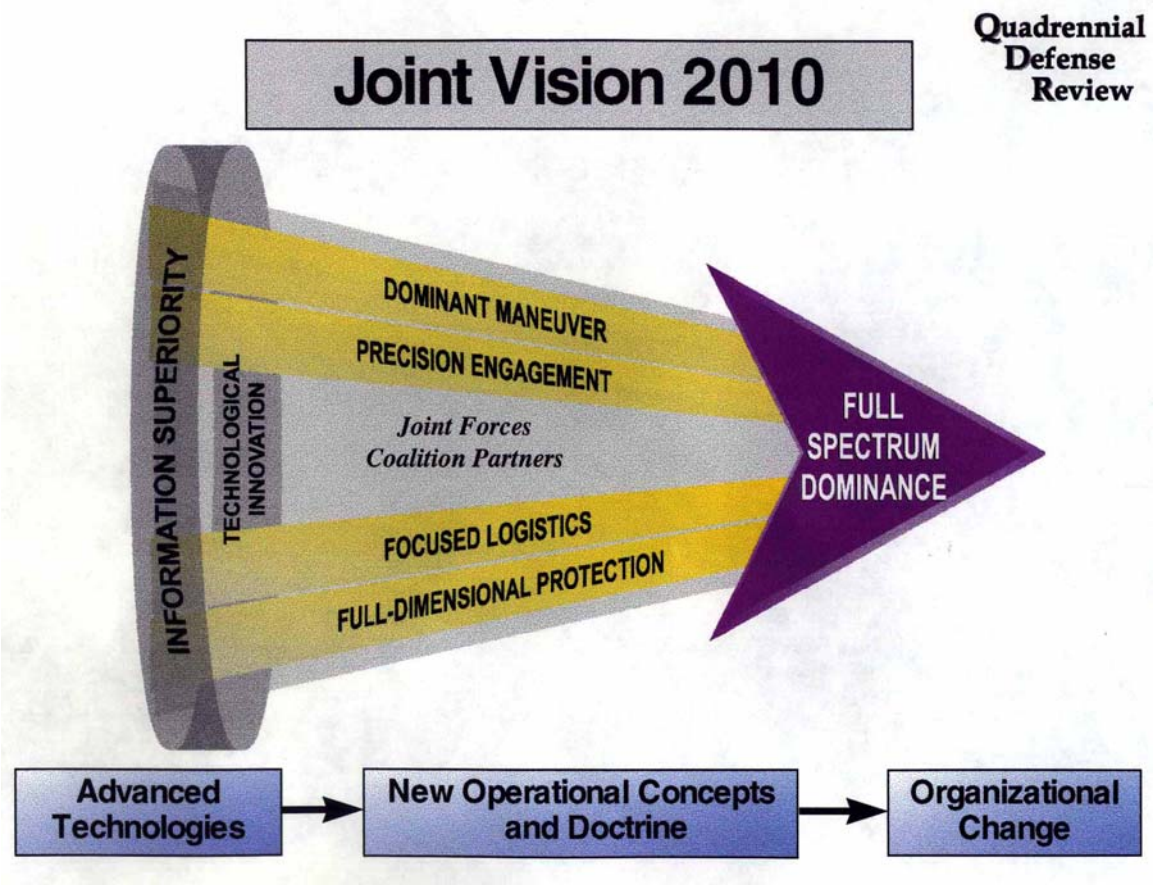

Figure 8, (Cohen, 1997)

Joint Vision 2020 also calls for the development of a Global Information Grid (GIG); a seamless, common user, information infrastructure; for a detailed definition, to provide the network-centric environment required to achieve information superiority (DoD, 2000). Although the GIG alone does not guarantee interoperable DoD information systems, the architecture makes significant progress by providing the missing enterprise roadmap required for enabling interoperability among DoD systems (Miller, 2001). Organizations, doctrine, and training must evolve to realize the full potential of Joint Vision 2020, (DoD, 2000).

Level of Information Systems Interoperability Model

Interoperability is a common theme found in the guidance provided by Clinger-Cohen, Joint Vision 2010, and Joint Vision 2020. The rapid evolution of information technology enables the commercial industry to field products faster then the policy bodies can prescribe standards (DoD, 1998). Ironically, the same advances that dramatically enhance the inherent capabilities of information systems also compound the challenge to field systems that are interoperable with each other at comparable levels of sophistication (DoD, 1998). The Level of Information Systems Interoperability (LISI) model, Figure 9, is used to increase integration and interoperability between DoD systems (Carney, 2004). The model provides a common basis for logical and incremental improvement (DOD, 1998: ES-4). The LISI model was developed by the C4ISR universal reference resources to define interoperability between information systems, provide a mechanism to measure the maturity of information systems, and outline a way to proceed from one level to the next (Clark, 1999). The LISI model complements other initiatives that support the improved use of information system within the DoD, such as the Defense Information Infrastructure (DII) Master Plan, DII Common Operating Environment, DoD Technical Reference Model, and the Joint Technical Architecture (replaced by the DoD Information technology Standards Register, DISR) (C4ISR, 1998).

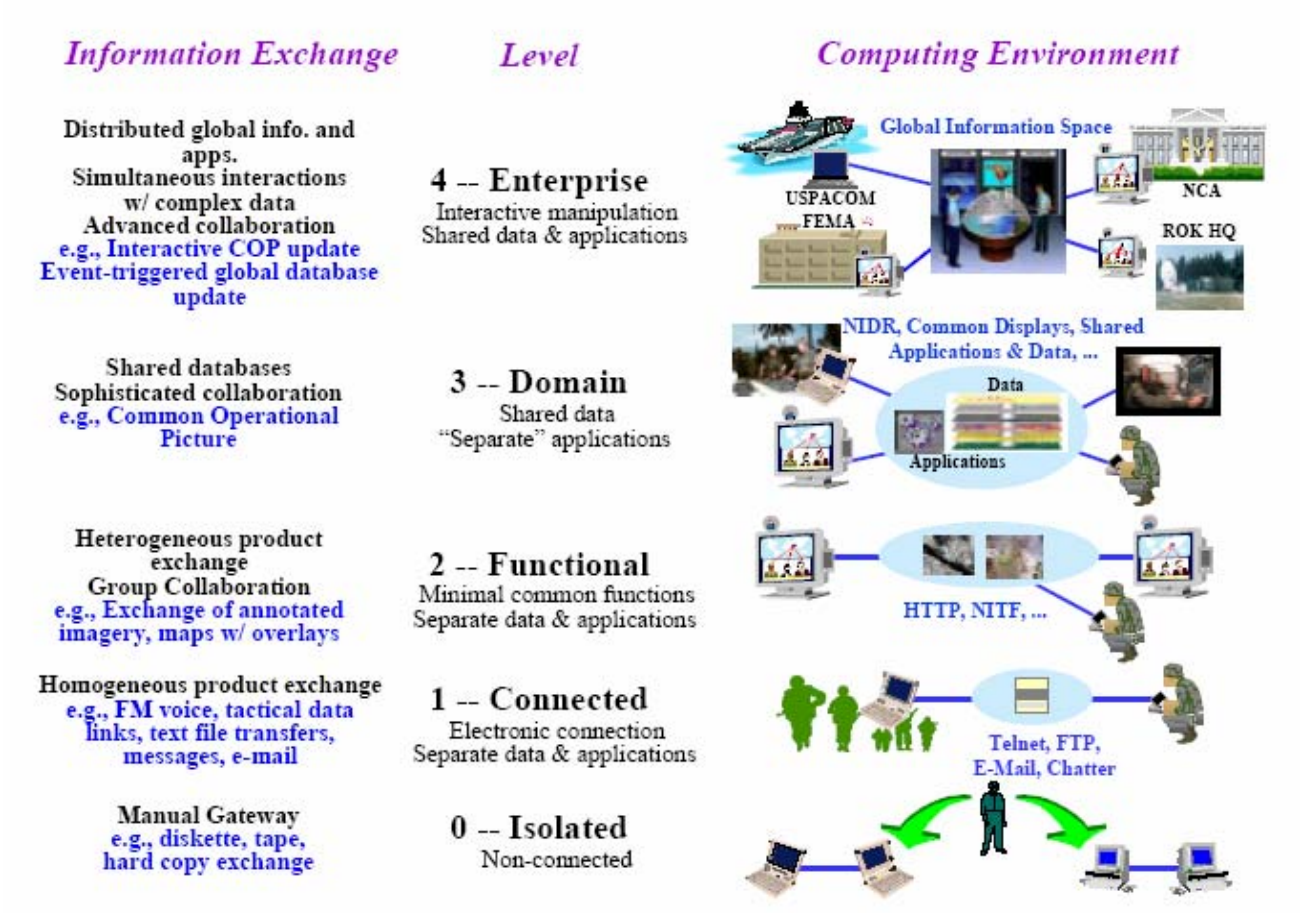

Figure 9, LISI model (DOD, 1998)

The model reflects five, zero thru four, increasing levels of sophistication regarding system interaction, the ability of the system to exchange and share information and services, and the associated computing environment; each higher level represents a progressive and demonstrable increase in capabilities (DOD, 1998).

LISI Procedures, Applications, Infrastructure, and Data Model

Within the levels of the LISI model, many additional factors influence the ability of information systems to interoperate. These factors are categorized into the following four attributes and illustrated in Figure 10: Procedures, Applications, Infrastructure, and Data (PAID) (DOD, 1998). Consideration and understanding the interrelationships

between all PAID attributes is required to improve interoperability beyond the simple connection of systems.

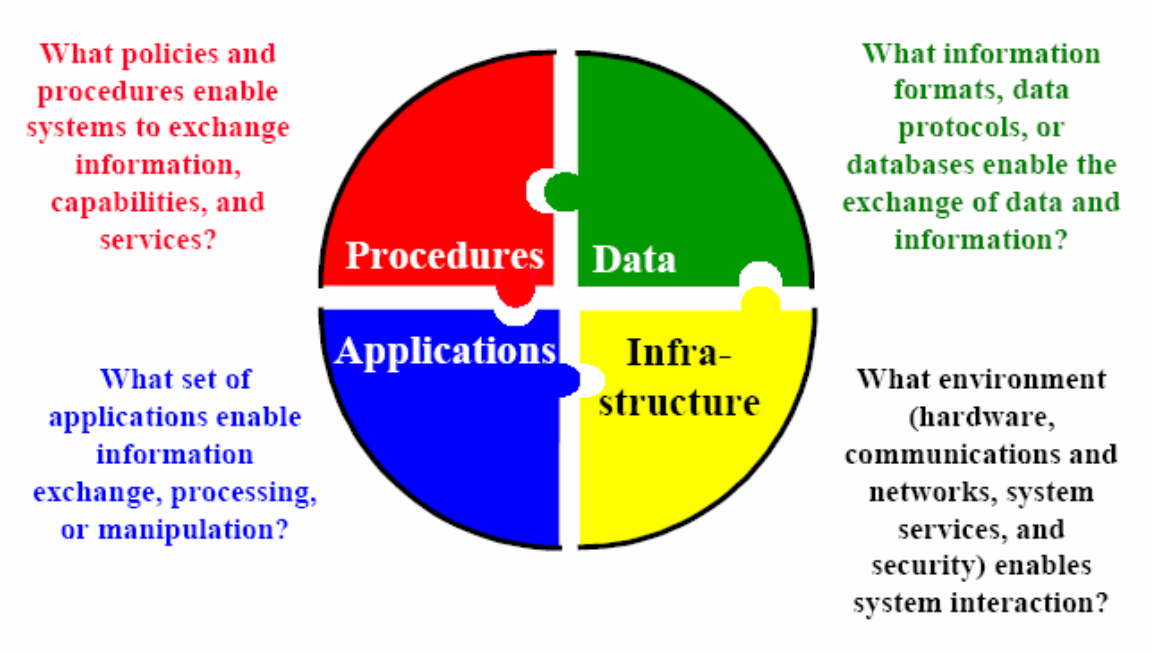

Figure 10, LISI PAID Model (DOD, 1998)

Alone, none of the PAID attributes sufficiently provides enough detail to complete a meaningful definition of interoperability, but each represents a critical, interdependent, and interlocking piece of the overall interoperability puzzle (DOD, 1998). Figure 11 demonstrates how the PAID attributes are used to describe and assess levels of interoperability (DOD, 1998).

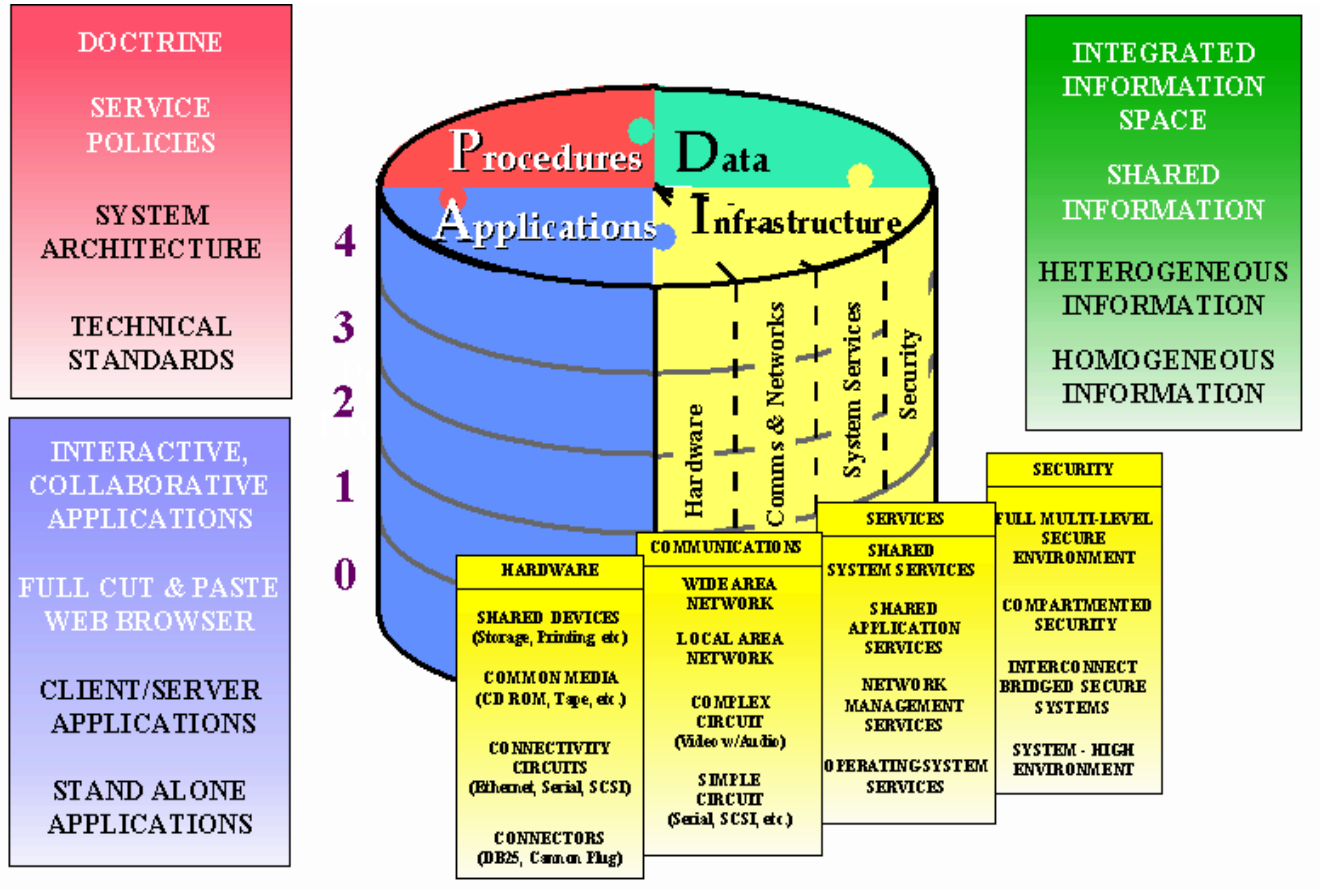

Figure 11, PAID Attributes and Levels of Interoperability (C4ISR, 1998)

At each level of the LISI model, a word highlights the most import aspect of the attributes. The significance and relative impact of each attribute will vary by level (Clark, 1999). One attribute serves as the primary enabler for achieving the different levels of interoperability (Clark, 1999). Table 5 illustrates the primary enabling attribute for each level of the LISI model and provides a description of information exchange taking place at each level.

Table 5, LISI Primary Enabling Attributes (Clark, 1999)

Level	LISI Description	Procedures	Applications	Infra-structure	Data
4	Enterprise/Universal	✓			
3	Domain/Integrated				✓
2	Functional/Distributed		✓		
1	Connected/Peer-to-peer			✓	
0	Isolated/Manual	✓			

This study focuses on the infrastructure portion of the PAID model. Accordingly, hardware, communications, and services are compared to determine if BANs are different. Security is excluded because the CITS program effectively standardized a major portion of security through boundary protection initiatives.

Organizations Affecting the Air Force Enterprise Network Structure

Overview

This section covers key positions or organizations that have an affect on the AFEN, but were not previously covered in the preceding sections concerning the AFEN network Architecture and Laws and Strategic Visions. Table 6 provides an overview of the areas covered in this section.

Table 6, Section Overview

Department of Defense Chief Information Officer
Air Force Communications Agency
Deputy Chief of Staff/Warfighting Integration
Deputy Chief of Staff/Installations and Logistics (HQ USAF/IL)
Defense Information Systems Agency

Department of Defense Chief Information Officer

The Department of Defense (DoD) Chief Information Officer (CIO) implements policies to advance interoperability and supportability of IT and National Security Systems (NSS) throughout the DoD. This position highlights the importance on IT within the DoD and facilitates conflict resolution by providing a higher level authority for subordinate CIOs. The DoD CIO is responsible for the development, implementation, and maintenance of the GIG as a sound integrated information technology architecture and ensuring that the Defense Information Systems Agency works with other DoD components to verify the interoperability and supportability of IT and NSS, (DoD, 2004).

Defense Information Systems Agency

The Defense Information Systems Agency (DISA) is the DoD executive agent for information standards; conducts interoperability assessment, test, and evaluations; and the single integrator for joint, coalition, and combined command and control. The agency ensures a link is maintained between published standards and the acquisition system. The executive agent for information standards reduces redundancy by providing systems engineering, planning, program guidance and interoperability testing for DoD components. DISA provides the DoD with global classified and unclassified voice, data, video, and transport services in manner that ensures US forces have access to information, geography, and space (DISA, 2004). DISA also maintains the Defense Information Technology Systems Registry (DISR) consisting of approved IT standards and profiles to help acquisition and field interoperable and network-centric enabled systems and products. The DISR provides mandatory standards and guidelines for the management, development, and acquisition of new or improved IT systems; guidance is

stable, technically mature, and publicly available. The DISR replaced the Joint Technical Architecture and provides a basis for seamless interoperability (DoD, 2004a). The DISR is also covered later in this chapter under the DOD guidance section.

Deputy Chief of Staff/Warfighting Integration

The Deputy Chief of Staff, Warfighting Integration, Director of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Infostructure (HQ USAF/XIC) provides oversight of requirements, plans, schedules, budgets, and performance criteria for Air Force communications and information modernization efforts (USAF, 2004). This organization leads the development and implementation of communications and information architectures and represents the Air Force position for the development of joint architectures.

Deputy Chief of Staff/Installations and Logistics (HQ USAF/IL)

The Deputy Chief of Staff for Installation and Logistics, Directorate of Communications Operations (HQ USAF/ILC) is responsible for communications and information readiness and oversees the daily execution of Air Force communications and information programs and processes. The directorate establishes course requirements and planning guidance for the professional development, education, and training of the communications and information workforce (USAF, 2004).

Air Force Communications Agency

The Air Force Communications Agency (AFCA) serves as the technical arm of Headquarters United States Air Force (HQ USAF); ensures integration and interoperability among command, control, communications and computer (C4) systems (AFCA, 2004a). The agency acts as the policy and standards adjunct of HQ USAF and

the Air Force CIO and develops service level agreements with external organizations (USAF, 2004). AFCA administers the Air Force Operationalizing and Professionalizing The Network (OPTN) program.

Operationalizing recognizes the network as a mission critical system with operations that are fully integrated with mainstream Air Force processes. Operationalizing requires applying operational rigor to establish an environment that fosters mission readiness. Warfighting needs drive the core requirements for operationalizing the network. Operationalizing involves the following five key elements: readiness, inspections and evaluations, graduated response, operational reporting, and rules of engagement (AFCA, 2004c).

Professionalizing the network is an operating approach that changes the way we train, organize, and equip to match the disciplined approach used with weapons systems that are more traditional. Protected and rigorously engineered interoperable networks staffed by certified professionals can only satisfy the information requirements of Air Force leaders. Standardizing Air Force network operations and management to align with Joint network operations and management efforts will enable Air Force forces to train as we fight (AFCA, 2004c). This is perspective succinctly describes the importance of exploring the nature of Air Force BANs.

The agency ensures information infrastructure optimization by deploying strike teams globally for assured Air Force network combat power. Strike teams either augment base or NOSC personnel to reconstitute failed or falling networks and provide targeted networking engineering expertise. Additionally, base assistance teams assess compliance to standards and provide technical and optimization assistance. During the

summer of 2004, AFCA changed the name and focus of their base assistance teams, from SCOPE Network to SCOPE EDGE; both build on the Scope Creek concept employed much earlier in Air Force history.

Scope Creek

In 1968, Project Scope Creek was the first large-scale, precise system analysis conducted by highly skilled, specially trained engineers and Airmen (SCOPE EDGE, 2004). The exceptional success of Scope Creek led to its application in evaluating DoD worldwide communications and a substantial growth in the Scope Creek workforce. By the end of 1975, the workforce grew to 40 teams with a total of 231 personnel positions (SCOPE EDGE, 2004). Eventually, the term "Scope Creek" became an Air Force figure of speech meaning the systematic evaluation of a communications network (SCOPE EDGE, 2004). The Scope Creek provided precision system analysis by expert technicians. In 1997, AFCA resurrected the concept and applied it to modern technology in a preventive maintenance and fine-tuning capacity under term SCOPE Network (SCOPE EDGE, 2004).

SCOPE Network

From 1997 to the summer of 2004, AFCA SCOPE Network teams focused on optimizing and securing existing network work equipment at Air Force installations to achieve peak performance. Ten five-person SCOPE Network teams traveled to every base in the Air Force every 18 to 24 months to perform the following tasks:

- Tune base network for optimal performance
- Enhance network security
- Improve operations management
- Train and mentor local information technology professionals
- Identify and share best practices

- Respond to emergency situations, as required

SCOPE Network teams provided a valuable tool for that produced immediate results. In worst-case scenarios, team members discovered and restored base networks operating at one-tenth of capacity due to unnecessary software (Barry, 2001). The very rapid deployment of Air Force networks through the 1980s and 1990s created the need for SCOPE Network (SCOPE EDGE, 2004). Visiting locations on a yearly basis fostered the development of sound local operating procedures and continued the Scope Creek tradition of providing precision system analysis by expert technicians.

SCOPE EDGE

After several SCOPE Network visits, many bases improved to the point that additional visits provided diminishing returns (SCOPE EDGE, 2004). Diminishing returns and the reorganization AFCA resulted in a fundamental shift in the SCOPE Network mission to support Air Force needs. In 2004, SCOPE Network evolved to SCOPE EDGE in preparation for one of the largest overhauls of all Air Force networks in decades (SCOPE EDGE, 2004). After the change, the network is viewed as an enterprise instead of a collection of 130 separate bases (Hoeft, 2004). The EDGE in SCOPE EDGE stands for Enterprise, Design, Guidance and Evaluation. SCOPE EDGE Teams continue the tradition of providing a valuable service by focusing on the following four mission areas: base compliance assessments, NOSC network optimization, fielding Strike Forces to provide targeted network engineering expertise, and base optimization; a team is assigned to visit each MAJCOM (Hoeft, 2004). Since evolving from SCOPE Network, base assistance visits have been cut back from 120 visits in a 18 month period to 30 visits in a 12 month period (SCOPE EDGE, 2004). Teams perform a detailed remote analysis

before the actual visit to increase the value of time spent at the site. An authoritative checklist is used to evaluate compliance with accepted architectures and standards. The SCOPE EDGE capability ensures the AFEN is run with rigor and discipline, through compliance assessment, while also addressing issues not covered by standards or policy, through optimization visits (NOSC, 2004). Instead of mainly focusing on precision system analysis like its predecessor, SCOPE EDGE focuses more on "standardizing Air Force networks towards achieving a consistent, sustainable, and cost-effective communications medium to support a seamless information grid", (SCOPE EDGE, 2004).

Air Force Enterprise Network and Base Area Network Relevant Topics

Overview

This section covers areas relevant to the AFEN and BANs. Topics in this section do not fit neatly into any of the proceeding sections; however, the topics provide essential information covering the following: Combat Information Transport System, Defense Information Technology Systems Registry, Global Information Grid, Air Force Instructions, Open Systems Strategy, and the Defense Standardization Program.

Combat Information Transport System

The Combat Information Transport Systems is a $4.7 billion HQ USAF level program for the acquisition, sustainment, implementation, and upgrade of high speed, broadband, and digital information transport assets that provide inter-base connectivity linking in-garrison command and control and combat support systems to the DoD Information Systems Network (Horn, 2004). The centers of gravity for the CITS program are network connectivity, information assurance, asset management,

interoperability, and standard interfaces to joint service networks. The program identifies BANs as a key enabler of the development of a DoD global communications network and a vital link between home base resources and warfighters deployed abroad (CITS, 2004). The Air Force Communications Agency administers the CITS program.

The CITS program is charged with ensuring every active duty and reserve base has a BAN, referred to as Information Transport System by CITS, which links existing and future voice, data, video, imagery, and sensory systems. The program provides full network interconnection to core buildings and backbone capacity capable of handling future, non-core building requirements. The CITS program fields new capabilities using a block numbering system. Specifically, an odd numbered block signifies a NOSC focused capability and an even numbered block signifies an NCC focused capability. Block 30 of the CITS program is designed to replace the aging network equipment on bases, standardize architectures, and move security boundaries from bases to NOSC (Horn, 2004). Additionally, Block 30 will allow for commonality of architecture, equipment, and training (GD, 2003). The CITS program management office provides specific, technical installation and implementation direction for BANs at each base. These directions are divided into the following three parts: network, distribution systems, and internal wiring from the communications closet to the end user equipment (CITS, 2004).

Defense Information Technology Systems Registry (DISR)

Department of Defense Directive 4630.5 and DoD Instruction 4630.8 establish responsibilities of CIOs and other components. The documents define a capability-focused, effects-based approach to information technology and national security system

interoperability and supportability across the DoD. These directives mandate the joint technology leveraged foresight of Joint Visions 2010 and 2020. This guidance requires the leaders of DoD components to ensure use and implementation of approved standards contained in a consolidated standards repository, the DISR, previously covered in this chapter under the DISA section. The DISR replaced the Joint Technical Architecture; a document that defined the service areas, interfaces, and standards applicable to all DoD systems. The instruction requires the Director, Defense Information Systems Agency to maintain the DISR, provide online access to the registry, and ensure the standards registry is linked to the acquisition system (DoD, 2004). Information previously found in the Joint Technical Architecture makes up the backend database for web-based DISR applications (DISRonline, 2004). The guidelines and standards found in the DISR are technically mature, stable, and publicly available at http://disronlin.disa.mil/ (DISRonline, 2004).

Global Information Grid

The Global Information Grid (GIG) called for in Joint Vision 2020 is the foundation for achieving information superiority by providing enterprise wide information services for DoD command and control, communications computers, intelligence, surveillance, and reconnaissance, and e-business systems. To provide interoperability, the GIG construct requires the integration of systems adhering to open systems standards. When fully implemented the GIG provides a net-centric, globally focused information environment that facilitates information sharing among people, sensors, and weapon platforms (DoD, 2003). The GiG provides capabilities from all

operating locations (bases, posts, camps, stations, facilities, and mobile platforms) and provides interfaces to coalition allied, and non-DoD users and systems (DoD, 2003:7).

Air Force Instructions

Air Force Instruction (AFI) 33-133, Joint Technical Architecture-Air Force (JTA-AF), tailors and refines core standards defined in the DoD Joint Technical Architecture. This instruction provides additional standards, standard profiles, recommended products, information technology architectures, and guidance not included in the DoD JTA (DoAF, 2000). An updated AFI referencing the DISR, replaced the DoD JTA needs to be published.

Air Force Instruction 33-115, Volume 3, implements Air Force Network Operating Instructions (AFNOI), directive guidance network managers use during daily operations to maintain network software and equipment. The AFNOIs provide detailed procedures and checklist for operating network components and responding to specific events (DoAF, 2004). These instructions provide a flexible vehicle for providing standardized directive guidance to practitioners in the field.

Air Force Instruction 33-115, Volume 1, Network Operations, provides the policy, direction, and structure of the AFEN. The instruction implements the AFNOSC reporting structure and provides the guidance necessary to manage the increasingly complex network environment to provide a cohesive Air Force network. This AFI assigns responsibilities from the AF CIO down to the local base units.

Open Systems Approach to Weapon System Acquisition

The open systems strategy employs modular design tenets and uses widely supported and consensus based standards for key interfaces to develop an affordable and

adaptable information system (DAG, 2004). Under the open systems initiative, equipment is not standardized, but a standard information architecture and standard cable attachments are required to permit interfacing with existing equipment (DoD, 2000a:22). The open systems strategy offers tremendous flexibility by providing a standardized "plug and play" capability among physical and electronic interfaces, while allowing equipment upgrades to keep pace with technological advances (DoD, 2000a). This approach supports achieving the following four benefits: 1) reduced acquisition cycle time and overall life-cycle cost, 2) ability to insert cutting edge technology as it evolves, 3) commonality and reuse of components among systems, 4) increased ability to leverage commercial investment (DoD, 2000a).

The Open System Joint Task Force (OSJTF) was chartered as a cooperative effort of the Army, Navy, Air Force, and the Office of the Under Secretary of Defense with the purpose to sponsor and accelerate the adoption of an open system approach for new systems and system upgrades (DLA, 2004). The OSJTF does not attempt to dictate the use of common hardware everywhere; the task force seeks to standardize to each unique need while retaining the advantages of common architecture and major interfaces (DLA, 2004).

Defense Standardization Program

The Defense Standardization Program (DSP) is conducted under the statutory provisions requiring the Secretary of Defense to maintain a standardization program for the following areas of focus (DoD, 2000a):

1. Standardizing like procedures and technologies
2. Using a common set of specifications and standards

3. Cooperating with industry in the development of standards
4. Assigning standardization responsibilities in the DoD
5. Resolving disputes between the Military Departments and Defense Agencies
6. Making final decisions in all DSP-related matters

This research is primarily concerned with areas 1 and 2 above. Standardization is an enabling strategy for achieving the Joint Vision goals to provide the warfighter with interoperable, reliable, and technologically superior equipment (DoD, 2000a:10). Interoperability, information superiority, and the rapid application of new technology represent key areas of the Joint Vision doctrine and depend on standardization to be successful (DoD, 2000a). The goals of the DSP are (DoD, 2000a):

1. Improve military operational readiness by achieving interoperability, improving logistical support, improving reliability, and modernizing existing systems.
2. Reduce costs by reducing number of nonstandard parts, facilitating competition, promoting use of common process and open systems, promoting standard commercial processes and practices, reducing training costs, and reaching a consensus on requirements to optimize systems engineering.
3. Reduce replenishment cycle time by using standard items and identifying interchangeability and interoperability requirements to facilitate the rapid introduction of new technologies.

The DSP concedes that standardization is not always desirable. It may not be practical or desirable to standardize when the technology involved is rapidly evolving and acquiring the desirable state-of-the-art solution or items go out of production after a short period of time (DoD, 2000a). This describes the nature of BANs and information

technology components. In these instances, it may be beneficial to standardize interfaces or protocols by pursuing an open systems strategy (DoD, 2000a).

Chapter Summary

Chapter II presented a literature review of topics related and important to whether the Air Force should standardize BANs at installations across the service, the topic of this research project. The literature review established a framework and common perspective for this research project.

III. Methodology

Chapter Overview

This chapter presents the process used to answer the research and investigative questions, presented in chapter I of this research study. This chapter discusses the qualitative research approach, role of the researcher, rationale for selecting the case study methodology, case study research design, quality of the research design, data collection, data analysis, and research limitations. This research project uses a multiple site case study methodology to examine Air Force BANs. Documented base assistance team visits and focused interviews provide the data for analysis.

Qualitative Approach

The qualitative study is an inquiry process of understanding a social or human problem conducted in a natural setting (Creswell, 1994). The following three factors determine the appropriate research approach: research problem, personal experiences of the researcher, and the audience (Creswell, 2003:22). The qualitative approach is appropriate to investigate exploratory research problems by researchers with experience in literary writing and intending to present their results to practitioners (Creswell, 2003). In this study, the research problem is exploratory, the researcher has experience in literary writing, and the target audience is practitioners in the field of information technology.

In addition to the guidance provided by Creswell, other researchers provide parameters for selecting the qualitative approach. According to Leedy, a case study is a type of qualitative research in which information is gathered about a single or multiple

cases to learn more about an unknown or poorly understood state of affairs (Leedy, 2001). Yin offers, case studies investigate contemporary problems within real-life context to account for pertinent influences on the research topic (Yin, 1994). This study examines the little understood topic of Air Force BANs, a contemporary problem, in a natural environment. According to "Moores Law"; named after Gordon Moore, a co-founder of the computer chip maker Intel; available computing power doubles every 18 months, (Intel, 2004). Rapid changes in technology, AFEN size, and decentralized growth across the Air Force contribute to the current lack of understanding BANs. The goal of this research is to add to the body of knowledge concerning Air Force BANs by examining existing literature and documented visits to three separate locations and interviewing information technology professionals.

Role of the Researcher

The qualitative researcher's sustained involvement with participants introduces a range of strategic, ethical, and personal issues into the research process. Researchers should explicitly identify their biases, values, and personal interests about their research topic, including past experiences that enable the audience to better understand the topic, setting, or participants (Creswell, 2003:184). To improve quality, use your own prior expert knowledge in your case study (Yin, 2003:137). The researcher has twelve years experience working in various base level communications positions at four different locations. He managed the infrastructure element of a base NCC on an installation visited by an Air Force Communications Agency base assistance team; the team provided significant technical support and guidance for future enhancements. The researcher does not have a direct connection or previous experience with any of the three documented trip

report locations examined in this study. The researcher is believes the current move towards regional control and network management of Air Force networks lacks adequate attention on local level support. Failing to address this concern may lead to extended outages, derogated service, interrupted information sharing, and ultimately prevent mission accomplishment.

Case Study Rationale

This study uses the case study strategy and focused interviews. The case study is especially suitable for learning more about a poorly understood situation (Leedy, 2001). Use the case study strategy when the research satisfies the following three conditions: the research questions must be in the form of how or why, the researcher must not have any control over events, and the study must focus on a contemporary event or problem (Yin, 1994). This study fulfills all three conditions. The investigative questions are in the required form, the research investigates an exploratory question about a contemporary problem, and the researcher has no control over the events. The documented base assistance team visits were conducted prior to the start of this research. The following three sections detail how this research study satisfies the conditions cited in this paragraph and listed in Table 7.

Strategy	Form of Research Question	Requires Control of Behavioral Events?	Focuses on Contemporary Events
Experiment	How, why?	Yes	Yes
Survey	Who, what, where, how many, how much?	No	Yes
Archival analysis	Who, what, where, how many, how much?	No	Yes/No
History	How, why?	No	No
Case Study	How, why?	No	Yes

Table 7, Strategy for Research Design (Yin, 1994)

Form of Research Question

Research questions take one of the five following basic forms: how, why, what, who, and where (Yin, 1994). The first three forms apply to this research and support the case study strategy. Research questions taking the form of how and why are explanatory and support using the case study, historical and experimental research strategies (Yin, 1994). Research questions in the form of what are either exploratory or prevalence and support all of the strategies or surveys and archival analysis, respectively (Yin, 1994). Whom and where research questions support strategies other than case study, as reflected in Table 7. The investigative questions used to address the main research question in this study are in the form of how, why, and the exploratory what.

Extent of Control

Lack of researcher control over events is an important characteristic of case study research; see Table 7, (Yin, 1994). This study uses previously completed base assistance team reports, focused interview transcripts, and a review of existing literature. Therefore, the study satisfies the case study extent of control guidelines. Additionally, interviewees reviewed transcripts for accuracy and correct interpretation.

Focus

Case study is the preferred research strategy when asking how and why questions, the researcher has little control over events, and the focus is on a contemporary rather than a historical issue (Yin, 1994:1). Case study data collection methods include the following: interviews, documentation, and observations (Leedy, 2001:157). In this research study; the research questions are in a favorable format, the focuses is on a contemporary Air Force problem, and the data collection methods include documentation and interviews.

Research Design

The research design is the logical sequence that ties the research data to the initial research questions and, eventually, to the conclusions of the study (Yin, 1994:19). The design determines what questions to study, what information is relevant, what to collect, and how to analyze the research results (Yin, 1994:20). An exploratory case study should define what is explored, the purpose of the exploration, and the criteria used to determine if the exploration is successful (Yin, 1994:29). This study explores BANs on established Air Force bases. The purpose of this exploration is to provide leaders and managers with sound information for making current and future BAN related decisions. This exploration is successful if it addresses the research propositions, facilitates greater understanding, and generates interest for additional research. The following five research design components are particularly important to the case study research strategy: research questions, research propositions, units of analysis, logic linking between data and research propositions, and criteria for interpreting the results (Yin, 1994:20). Sections below reflect how this study addresses each component.

Research Questions

This section outlines the main research question, investigative questions, and research propositions, originally introduced in Chapter I. A latter section of this chapter, the Data Collection section, contains the interview questions.

Main Research Question

Should the Air Force Standardize Base Area Networks?

Investigative Questions

6. Are BANs different throughout the Air Force? If so, how?
7. Why are a variety of BANs currently in use throughout the Air Force?
8. What problems are created by using a variety of BANs throughout the Air Force?
9. What are the advantages of using a variety of BANs throughout the Air Force?
10. How should the Air Force respond to the current state of BANs?

Research Propositions and Model

4. Research will show BANs are different throughout the Air Force
5. Research will identify sources of disparate Air Force BANs.
6. Research will show advantages and disadvantages of disparate Air Force BANs.
7. Research will identify an appropriate AF response to current state of BANs.

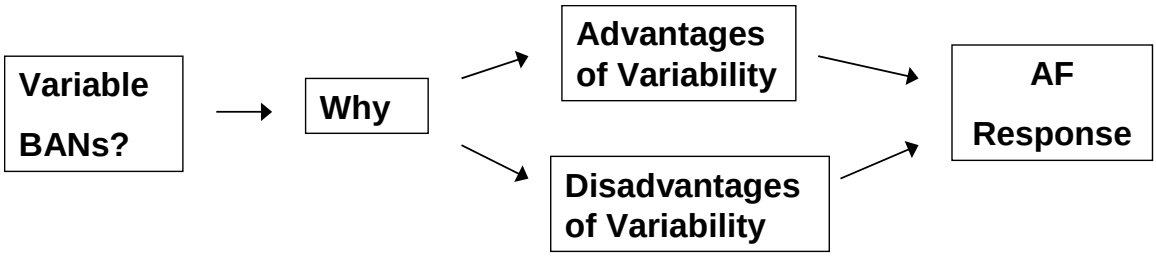

Figure 12, Research Model

Research Procedures

This section illustrates the procedures used to answer each research question. The answer to the main research question is inferred by reviewing answers to each of the investigative questions. The first investigative question is the linchpin of the study. In order to answer this key question, documentation in the Base Assistance Team site report for each location and information obtained during interviews are compared base on the infrastructure attribute of the LISI model, introduced in chapter II. The table below identifies how each investigative research question is addressed. Interview questions are listed later in this chapter under the Data Collection section.

Table 8, Research Procedures

Investigate Question	Method of address
1	AFCA Base Assistance Team (BAT) Trip Report, Interview Question 1, Cross Case Analysis, and Literature Review.
2	Interview Questions 3 and 4, Cross Case Analysis, and Literature Review
3	Interview Question 6 and Cross Case Analysis
4	Interview Question 5 and Cross Case Analysis
5	Interview Question 7, Cross Case Analysis, and Literature Review

Unit of Analysis

Accurately specifying the primary research questions facilitates selecting the appropriate unit of analysis (Yin, 1994:23). The unit of analysis determines what the "case" is (Yin, 1994:21). Fixed BANs at established Air Force installations are the units of analysis for this study, not deployable or contingency networks. Key participants include personnel assigned to the local Network Control Center on each installation.

Logic Linking of Data to Propositions

Interpreting data in terms of common themes and synthesizing data into an overall portrait of the cases are methods of processing case study information (Leedy, 2001:157). "Pattern-matching", linking information from cases to propositions, is a promising method of linking case study data to the research propositions (Yin, 1994:25). This study examines information from each case to identify support or lack of support for each research proposition. Cross-case analysis is used to identify any similarities, differences and common themes.

Criteria for Interpreting Results

Analyzing case study evidence is one of the least developed and most difficult aspects of conducting case study research (Yin, 2003). The following three general analytic strategies and five specific techniques can be used to process case study evidence (Yin, 2003):

General Analytic Strategies

- Relying on theoretical propositions
- Setting up a framework based on rival explanations
- Developing case Descriptions

Specific Analytic Techniques

- Pattern matching

- Explanation building
- Time-series analysis
- Logic models
- Cross-case synthesis

The analytic strategy sets the priority for what to analyze and why (Yin, 2003). This study relies on theoretic propositions, pattern matching, and cross-case synthesis to analyze evidence. The theoretic propositions; Air Force BANs are disparate, sources of disparity, and advantages and disadvantages of disparity; form the general analytic strategy. The specific analytic techniques used are pattern matching and cross-case synthesis. Theoretic propositions and the Level of Information System Interoperability (LISI) model provided data collection parameters. Specifically, locations are compared for variability based on the range of considerations associated with the infrastructure attribute of the LISI model, see the LISI sub-section of Ch II for a detailed explanation.

Quality of Research Design

The following four tests determine the quality of any case study research effort: construct validity, internal validity, external validity, and reliability (Yin, 1994:33). Table 9, summarizes the tests and tactics used to satisfy research design requirements during various phases. The four subsequent sections address how each test is satisfied in this research study.

Table 9. Case Study Tactics for Four Design Tests (Yin, 1994:33)

Tests	Case Study Tactic	Phase of research in which tactic occurs
Construct validity	• **Use multiple sources of evidence** • **Establish chain of evidence** • **Have key informants review draft case study report**	**data collection** **data collection**
Internal validity	• **Do pattern-matching** • **Do explanation-building** • **Address rival explanations** • **Use logic models**	**data analysis** **data analysis** **data analysis** **data analysis**
External validity	• **Use theory in single-case studies** • **Use replication logic in multiple-case studies**	**research design** **research design**
Reliability	• **Use case study protocol** • **Develop case study database**	**data collection** **data collection**

Construct Validity

The first test, construct validity, consists of establishing the correct operational measures for the investigated concepts and is especially problematic in case study research. Case study critics point to the fact that investigators fail to sufficiently develop an operational set of measures and that subjective judgments are used to collect data (Yin, 1994:34). Table 9 lists the following three tactics for increasing construct validity: multiple sources of evidence, establish a chain of evidence, and key informant review (Yin, 2003:34). This study employs all three tactics. Multiple cases and focused interview transcripts provide multiple sources of evidence. The researcher received documentation, trip reports, directly from the Air Force Communications Agency and documented interview transcripts to establish a chain of evidence. Key informants, practitioners working in base level communications positions, reviewed the case study report and interviewees reviewed interview transcripts for accuracy and correct interpretation.

Internal Validity

The second test, internal validity, involves establishing causal relationships, certain conditions lead to other conditions. This type of logic is inapplicable to descriptive or exploratory studies (Yin, 1994:35). Internal validity for case study research extends to the bigger problem of making inferences; is the evidence convergent and are the inferences correct (Yin, 1994)? Table 9 identifies the following four tactics for increasing internal validity: pattern matching, explanation building, address rival explanations, and logic models. This research study uses pattern matching.

External Validity

The third test, external validity, deals with knowing whether a study's findings are applicable beyond the immediate case study, replication (Yin, 1994). Table 9 identifies theory in single case studies and replication logic in multiple-case studies as tactics for increasing external validity. This research examines multiple cases by exploring BANs at five locations, three with documented trip reports and two where key informants are currently stationed. Accordingly, replication logic is used to increase external validity. Key informant interviews, outside the three select trip report locations, were conducted to improve the overall applicability of results.

Reliability

The forth and final test, reliability, deals with demonstrating the operations of a study are repeatable and will provide the same results and conclusions if a subsequent investigator follows the same procedures in conducting the same case study (Yin, 1994:36). The goal of reliability is to minimize the biases and errors in a research study (Yin, 1994:36). Table 9 reflects the following two tactics for increasing reliability: use

of a case study protocol and development of case study database. In this study, documenting research procedures is used to increase reliability.

Data Collection

In qualitative research, purposeful selection of participants or sites provides the best opportunity for the researcher to address the research questions (Creswell, 2003:185). This logic is in contrast to random sampling or the selection of a large number of participants typically found in quantitative research (Creswell, 2003). This exploratory inquiry uses documentation specifically focused on BANs and focused interviews of personnel with practical experience in base level communications.

Qualitative data collection steps include setting the boundaries of the study, collecting information through unstructured (or semi-structured) observations and interviews, documents, and visual materials (Creswell, 2003). This study uses documentation and focused interviews for data collection. Five personnel at each of the documented trip report locations are interviewed as well as key informants at two other locations. Only personnel with networking experience at more than one location will be interviewed. Air Force Communications Agency, base assistance team, final trip reports are the form of documentation used. The following semi-structured interview questions address the research questions and propositions:

1. Are base area networks throughout the Air Force the same or different? Support for your reply?

2. The Air Force CIO, Mr. John Gilligan, created the Standards Council to help reduce the variability found in base area network architectures throughout the Air Force. Do you think base area networks should look the same or similar? Why or why not?

3. What do you feel are the primary reasons base area networks across the Air Force are configured, arranged, and equipped differently?

4. Why is there so much variation concerning base area networks throughout the Air Force?

5. What are the advantages of employing a variety of network architectures at bases throughout the Air Force?

6. What problems are created by employing a variety of network architectures at bases throughout the Air Force?

7. How do you think the Air Force should respond to the current state of base area networks?

Pilot interviews resulted in the creation of interview question one to directly addresses whether BAN architectures are different throughout the Air Force. Previously, the researcher assumed they were different based on personal experience. In contrast, some pilot interviewees believed BANs are relatively the same or didn't know.

Question Development

The main research question, investigative questions, and the research propositions were used to develop the interview questions. Interview questions were developed to ensure collected data adequately covered the research objectives. Table 10, identifies how each interview question is related to a research question or proposition.

Table 10, Interview Question Development

Interview Question	Supported Investigative Question(s)	Supported Proposition(s)
1	Investigative 1	1
2 and 7	Investigative 5	4
3 and 4	Investigative 2	2
5	Investigative 4	3
6	Investigative 3	3

Interview question number 1 supports the first investigative question and the first research proposition by revealing the interviewee's view on the whether BANs throughout the Air Force are disparate, or not. This question was not included in the initial interview questions; it was added after several test interviews.

Interview questions 2 and 7 solicit input concerning what should be done about disparate Air Force BANs to address the fifth investigative question and the fourth research proposition. These questions were developed based on input from test interviews. Interview question 2 establishes the interviewee's position on the desirability of standard networks. Question 7 asks what should be done about the current state of BANs, regardless of whether the interviewee believes them to be disparate or not.

Interview questions 3 and 4 support the second investigative question and the second research proposition by attempting to identify sources of BAN variation. Question 3 constrains the inquiry to configuration, arrangement, and equipment. Question 4 employs no limitation and is designed to capture a broader range of responses.

Interview question five addresses the fourth investigative question and the third research proposition by identifying the advantages of variety. This question is the polar opposite of interview question 6.

Interview question 6 supports the third investigative question and the third research proposition by identifying problems encountered due to variation in BANs throughout the Air Force. Interviewees were encouraged to include any experiences prior to their current duty assignment.

Key informant feedback led to the development of interview question 1, 4, and 7. Question 1 and 7 help address the fifth investigative question more directly and question 4 provides an additional opportunity to capture data for investigative question 2 and proposition number 2. Practitioners assigned to an NCC not included in this research study reviewed the interview questions and provided input for restructuring questions. Responses to the interview questions reflect the views of seasoned professionals responsible for maintaining Air Force BANs during at least two assignments.

Pre-interview Procedures

The nature of the topic restricted the pool of potential interviewees to individuals having knowledge of BANs. Accordingly, the researcher interviewed personnel working at base NCCs. To reduce any bias, interviewees were not told the nature or goal of the study. Participation in this study is voluntary and anonymous. Interview questions were provided to participants at least 24 hours in advance. Each participant signed the informed consent letter prior to the start of the interview and provided an email address to facilitate review and approval of their responses. Any requested modifications received via the email feedback loop were accomplished before any answers were analyzed. Participants were offered a copy of the final report.

Data Analysis

Data analysis involves examining, categorizing, tabulating, or otherwise processing the evidence to address the initial research propositions of the study (Yin, 1994:102). The following two general strategies help investigators choose among different techniques and to complete the analytic research phase successfully: relying on theoretical propositions and developing a case description (Yin, 1994:103). Within the

general strategy, the following four analytic techniques should be used: pattern matching, explanation building, time series analysis, and program logic (Yin, 1994:102). A fifth technique, cross-case synthesis, applies specifically to analyzing multiple cases; having more than two cases strengthens the findings much more than if produced by one case (Yin, 2004:133). This research study relies on theoretical propositions for the general analytic strategy and pattern matching and cross-case synthesis as the specific techniques.

Theoretical Propositions

Theoretical propositions help to focus attention on certain information and to ignore other information (Yin, 1994:104). The propositions introduced in Chapter 1 and earlier in this chapter shaped the data collection and analysis of this research project. The purpose of this study is to increase existing knowledge concerning BANs. The theoretical propositions directed the exploration of BANs with a focus on key areas.

Pattern Matching

Pattern matching, comparing a empirically based pattern with a predicted pattern, is one of the most desirable case study analysis strategies (Yin, 1994:106). This study compares patterns from multiple cases and focused interviews. The details of the comparison are included in chapter IV.

Key Informant Review

Interviewees reviewed transcripts prior to data analysis. Key informants reviewed the case study for validity and logic. The key informant review increased the internal validity and reliability of this research effort.

Cross-case Synthesis

Five sites are compared during this research study. Three cases have documented trip reports and two locations where selected because they are the current duty stations of key informants. Locations are compared based on the range of considerations associated with the infrastructure attribute of the LISI model. Additionally, interview responses are compared across locations.

Research Limitations

There are several limiting factors for this research study. First, the size of the AFEN is a limiting factor. The Air Force has at least a semi-permanent communications presence at over 120 locations worldwide. This study examines BANs at five locations in detail to find indicators that apply to the larger AFEN. Sites were selected with diversity in mind and include the following: Air National Guard Base, Oversea installation, and continental United States bases. Second, little research exists on the specific area of BANs. As a result, there is not much to build upon. Third, the fluid nature of information technology poses a significant hurdle for conducting research; the information technology environment changes rapidly. Fourth, this study will not produce results comparing similar locations; this is an opportunity for additional research. Fifth, Time represents the final major limitation of this study. The importance and complexity of this study demand more time than this effort can provide. Despite these limitations, this research makes a contribution to current understanding. This study aims to establish grounds for additional research.

Chapter Summary

This chapter presented the process used to answer the research questions presented in Chapter I of this research study. This chapter discussed the qualitative research approach, role of the researcher, rationale for selecting the case study methodology, case study research design, quality of the research design, data collection, data analysis, and research limitations.

IV. Analysis

Chapter Overview

This chapter provides the results of the exploratory research methodology outlined in Chapter III. The research model, figure 13, represents the logical map followed in attaining the results; convergent sources of information were used. The results are based on documented AFCA SCOPE Network Reports, focused interviews of network professionals, and a detailed literature review. This chapter is presented in five primary sections. First, support for conducting this research effort is presented. Second, the case study report section describes the sites included in this study. Third, an overview of the interview data is presented. Fourth, each investigative question is answered and summarized. Fifth, the main research question is addressed. A total of five sites are used in this study to address five investigative questions and answer the main research question; documented trip reports were available for three locations and focused interviews were completed at four locations.

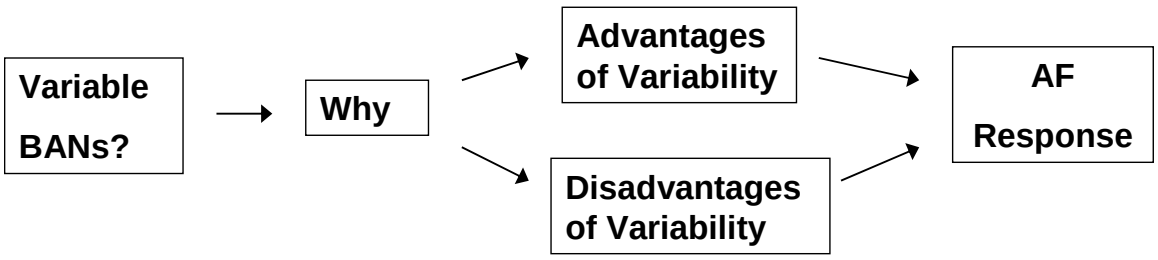

Figure 13, Research Model

Support for Conducting Current Research

As an initial step in the interview process, question two was asked and analyzed. Responses were split pretty evenly regarding whether interviewees BANs should be the same or similar across the Air Force; results indicate a lack of a clear consensus among practitioners.

Interview Question 2

- The Air Force CIO, Mr. John Gilligan, created the Standards Council to help reduce the variability found in base area network architectures throughout the Air Force. Do you think BANs should look the same or similar? Why or why not?

Fifty seven percent of the interviewees spread over three locations stated BANs should be the same, four out of seven. Forty-three percent, three of seven, all from site two said BANs should be similar but not the same. Even though clear preference didn't emerge from the raw results, all three very experienced key informants and the most experienced non-key informant think BANs should look the same. The personnel interviewed at site two, reported BANs should be similar, are the least experienced in the pool of interviewed personnel, see Table 13 Interview Demographics. Table 11 provides a complete summary of interview question two responses. Some thoughts from the majority that think BANs should be the same are listed below:

- Need a common NCC solution for core services
- Common baseline infrastructure solution that is developed, funded, and implemented from the highest level
    - This concept allows knowledge gained at one base to be directly applicable to other bases
- AF should franchise the process of providing communications and network services. Would easily provide NOSC with site specific base configurations
- Approval for exceptions should be centrally managed

The minority who feel BANs should look similar shared a rationale centered on the concept of security through diversity. They feel that disparate BANs increase security by making it more difficult for intruders to gain unauthorized access. After completing this initial step, further research is clearly justified.

Table 11, Interview Question 2 Response Summary

Response Summary Questions 2	Interviewee(s)	# of Individuals	% of Individuals	# of Sites
Same	3, K1, K2, K3	4	57	3
Similar	2A, 2B, 2C	3	43	1

Site Descriptions

This section provides a description of the five sites selected for this exploratory research project. Purposeful selection of participants or sites provides the best opportunity for the researcher to address the research questions (Creswell, 2003:185). A desire to better understand BANs, a very scarcely researched topic, influenced site selection. Sites 1 through 3 were selected for this study because the sponsoring agency provided documented trip reports and the sites provide good examples of current installations according to network size; small, medium, and slightly large. Two additional trip reports were provided by the sponsoring agency for locations with small networks; these sites were not selected for this study because the researcher did not want to over influence the results with small network characteristics. Sites 4 and 5 were selected because the three key informants used in this study are currently stationed at either Site 4 or Site 5. The sites used in this study include four locations in the continental United States and one overseas location; at least one Air National Guard base is included. Information reflected in this section is based on SCOPE Network trip reports

to Sites 1 thru 3 in calendar year 2003 and focused interviews of personnel at four of the five locations, Site 1 personnel were not interviewed. The BANs at the sites are maintained by military, government civilians, and contract personnel.

Site 1

Site 1 has approximately 2,000 user accounts and a vendor A provided Asynchronous Transfer Mode (ATM) backbone with vendor B distribution switches. Servers running Window NT 4.0 provide network services, with two DNS Windows 2K servers. The NT architecture is a multiple master domain model. The NCC controlled domain has a two-way trust with an external agency. This relationship allows the external agency to control accounts and access to the network. This is not a desirable configuration and the NCC is working to remove the external domain. Personnel from Site 1 were not interviewed.

Site 2

Site 2 has approximately 4,000 user accounts. The ATM backbone network consists of vendor C switches with two primary vendor C switch routers. The access layer, first 400 feet to the user, is primarily comprised of vendor C routers. Network services are provided by a Windows NT, Hybrid Single Master Domain architecture with five trusting resource domains. Three personnel from Site 2 were interviewed for this research project.

Site 3

Site 3 has approximately 300 user accounts and the base backbone is a large flat network with all users, servers, and infrastructure equipment in the same broadcast domain. The backbone consists of vendor C switches. Distribution layer switches also

serve as access layer switches. Network services are provided by a Single Master Windows NT domain with a one-way trust with an external entity. One person from Site 3 was interviewed for this research project.

Site 4

Site 4 has approximately 5,500 users, uses a Gigabit Ethernet backbone, and operates primarily vendor C equipment. Unlike the first three sites, documented trip reports to this location were not available. Site 4 is included in this study because two key informants are currently stationed at this location. Site specific information was obtained during interviews.

Site 5

Site 5 has approximately 6,000 users, has a Gigabit Ethernet backbone, and operates all vendor C equipment. A documented trip report was not available for this location. This site is included because it is the current duty station of the most experienced key informant. Site specific information was obtained from the interviewed informant.

The comparison matrix below compares the five sites used in this study. The matrix identifies differences in the type of network backbone, type of hardware, and method of providing network services via the type of Windows NT architecture employed. All of the sites, except Site 1, use vendor C equipment.

Table 12, Site Comparison Matrix

Location	Approximate Number of Users	Network Type	Hardware	Network Services	Trip Report	Interviews (Number)
Site 1	2,000	ATM	Vendor A and B	Multiple Master Windows NT Architecture	Yes	No
Site 2	4,000	ATM	Vendor C	Hybrid Single Master Windows NT Architecture	Yes	Yes (3)
Site 3	280	Flat	Vendor C	Single Master Windows NT Architecture	Yes	Yes (1)
Site 4	5,500	Gig E	Vendor C	unknown	No	Yes (2)
Site 5	6,000	Gig E	Vendor C	unknown	No	Yes (1)

Interview Data

Network Control Center leadership at Sites 2 and 3 identified personnel with enough knowledge concerning the base network and the larger AFEN to make a contribution to this study. Additionally, each interviewee was asked to refer someone they thought could contribute. The goal established in Chapter III to interview at least five people at each of the locations was not met do to one of the following reasons: not enough people working in the NCC processed knowledge beyond their assigned task (bigger picture perspective), individuals weren't willing to participate, or NCC leadership did not approve interview request. Despite these obstacles, personnel from four of the five locations were interviewed. A total of seven interviews were conducted for this study. Four interviews were conducted at locations with documented trip reports, three at Site 2 and one at Site 3. Network Control Center management at Site 1 did not approve

the request to interview personnel. Three key informant interviews were conducted, two at Site 4 and one at a Site 5, see the Interview Demographics table below.

Table 13, Interview Demographics

Location	Interviewee	Networking Experience (Yrs)	Multiple Locations	Employee Grade
Site 2	2A	4.5	No	SrA
Site 2	2B	3	Yes	SrA
Site 2	2C	4	Yes	SSgt
Site 3	3	9	No	Contractor
Site 4	K1	8	Yes	SSgt
Site 4	K2	11	Yes	MSgt
Site 5	K3	17	Yes	MSgt

The attempt to only interview personnel with at least network management experience at two different Air Force locations was not successful. At each location, the majority of personnel working in the NCCs only had experience with their current network. However, some had several years experience and were informed of other networks through conversations and interactions with other network professionals assigned to other bases. Key informant interviews from two locations increase the external validity and construct validity of the study.

All key informants possessed experience with multiple networks at multiple locations and at least eight years of networking experience. Although the target interview pool of 15 personnel at the first three locations did not materialize, the interview results are insightful and add value to the current body of knowledge. It was very difficult to locate personnel with enough networking experience, were willing to participate, had the time to be interviewed, and management granted access to, despite only having seven interview questions.

Investigative Questions

This section addresses each of the five investigative questions in separate subsections. In each subsection, the evidence is presented in the following sections, if applicable: document trip report information, interview data with select excerpts, and a summary of convergent information.

Investigative Question One

- Are BANs different throughout the Air Force? If so, how?

The results of this study indicate BANs are different throughout the Air Force based on comparing documented trip reports, analyzing interview results, and reviewing existing literature. In this study, sites are compared according to the range of considerations under the infrastructure attribute of the LISI model, see Figure 14. The infrastructure attribute defines the range of components that enable interactions between systems including hardware, communications and networks, system services, and security (C4ISR, 1998). This range of considerations minus security is used to determine if BANs at the five locations included in this study are different. Security is excluded because the CITS program has effectively standardized a major portion of this area.

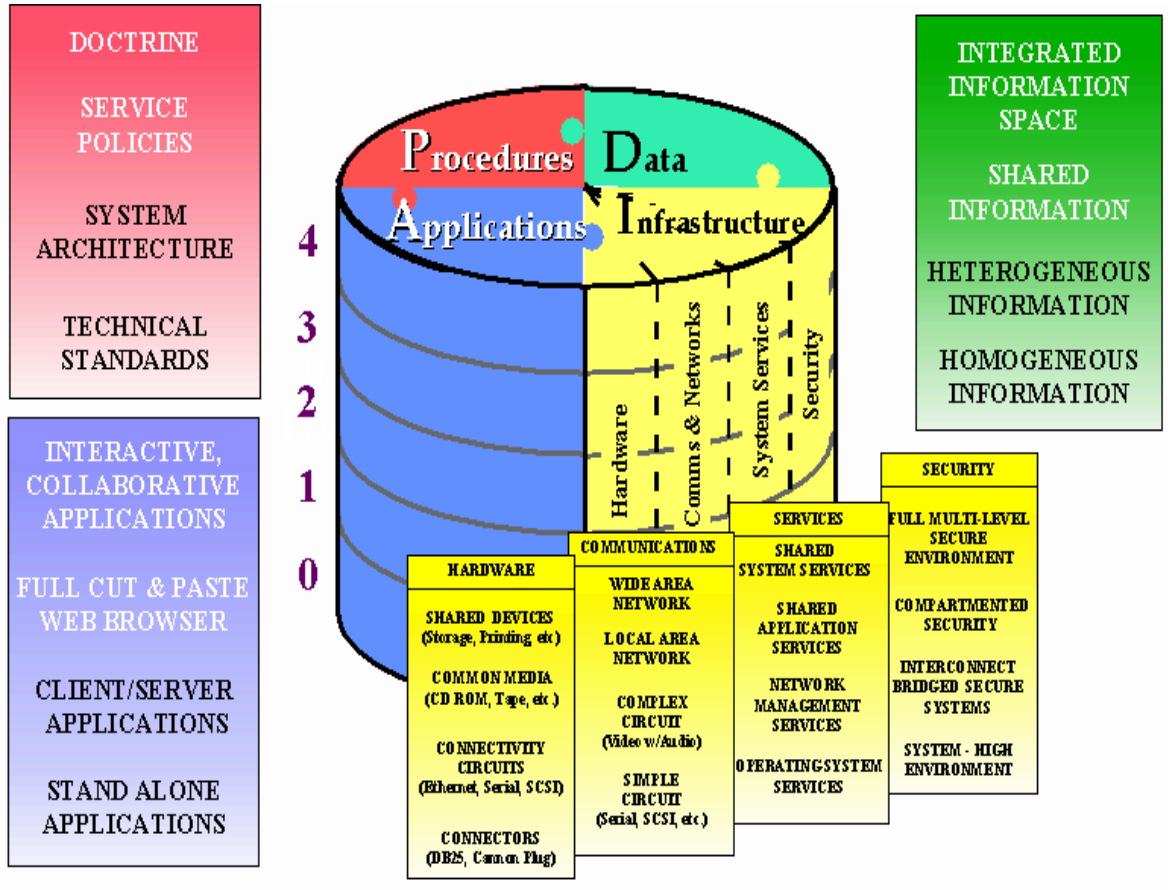

Figure 14, Paid Paradigm Reflecting Range of Considerations for Each Attribute

Trip Report

The comparison matrix, Table 12, developed from documented Base Assistance Team (BAT) trip reports and focused interviews reflect differences in the three areas of interest: network type, hardware employed, and method for providing network services. The hardware area reflects the least amount of difference; four of five sites use vendor C equipment.

Interview Question 1

- Are base area networks throughout the Air Force the same or different? Support for your reply?

Responses to this question substantially supported the thought that BANs are different. Six out of seven interviewees stated that BANs are different, 86 percent, and one individual didn't know if they were different or not because he has only worked at one base, 14 percent. Interviewees at each of the four possible locations believe BANs are different, see Table 14 for a summary of responses by location. Two individuals mention similarities and differences present among some BANs. After discussing their responses further, they made it clear they believe the network architectures are different. Not one individual reported that BANs are the same. The following statements were taken from interviews:

- "Due mostly to working topologies and network saturation varying from base to base. Also if they were the same the AF wouldn't be sending out teams to standardize"
- Too much freedom is given at each base for the local commander to determine what can and can't be done on the network. "When the risks are explained to them, the response is one of indifference, as long as they get what they want".
- Different bases stood up campus networks at different times
- Funding has been haphazard at times; sometimes from the base, MAJCOM, AF, DOD, etc
- Design decision making has been managed very differently at times by the AF engineers out of Tinker AFB
- "Home grown solutions, implemented "on the cheap" at times, developed by local "experts". I myself have been the guilty party of more than one of these local incarnations"

Table 14, Interview Question 1 Response Summary

Response Summary Questions 1	Interviewee(s)	# of Individuals	% of Individuals	# of Sites
Different	2B, 2C, 3, K1, K2,K3	6	86	4
Don't Know	2A	1	14	1

Literature Review

An Air Force Education and Training Command briefing, for senior leaders, describes BANs as independent networks and a smorgasbord of hardware (AETC, 2003).

The briefing clearly articulates the problem and level of attention the situation has grasped. Additionally, Block 30 of the CITS program provides an opportunity to establish common architectures, equipment, and training for BANs (Horn, 2004). These sources provide further evidence that BANs are different.

Investigative Question One Results Summary

Convergent evidence is provided to support the believe that BANs are different throughout the Air Force. First, the comparison matrix identified differences in three of the four areas identified in the PAID paradigm of the LISI model in Figure 14. Second, the responses to interview question one align with the documentation in providing support that BANs are different. Third, information from the literature provides additional support that BANs are different; specifically, a briefing for senior Air Force leaders and goals of Block 30 of the CITS program.

Investigative Question Two

- Why are a variety of BANs currently in use throughout the Air Force?

Nine different reasons for variety were found during the course of this research. Interview questions three and four, cross case analysis, and existing literature were used to answer investigative question two. Interview question three was designed to solicit the primary reason for differences and question four was designed to gather additional reasons for variation. However, only two additional responses were given to question four, the other responses were excluded because they duplicated responses provided for question three, see Table 15.

Interview Questions 3 and 4

- What do you feel are the primary reasons base area networks across the Air Force are configured, arranged, and equipped differently?

- Why is there so much variation concerning base area networks throughout the Air Force?

Decentralized decision authorities is the primary reason interviewees gave for BANs being configured, arranged, and equipped differently across the Air Force. Three interviewees at two different locations gave this response, including two very knowledgeable key informants; 43 percent of all interviewees.

The next significantly contributing factor is different funding avenues available for different bases. Two very knowledgeable key informants located at different bases reported this response, 29 percent. Different missions and security by being different was also reported by 29 percent of the interviewed pool. However, these two responses were reported by two individuals at the same locations, see Table 15. The following statements were taken from interview transcripts:

- "Since there is no single focal point setting the rules, local commanders are free to do what they want at each base. They are allowed to spend base funds upgrading infrastructure, hardware and software, as well as determining what they will and won't allow on an AF network". What was acceptable locally before may not be acceptable for the larger enterprise.
- Different channels available for funding IT at each base and different support contracts
- Timing, MAJCOM program management office (PMO) focus at the times of implementation created different technological pursuits
- Inconsistent solutions coming from the engineers at Tinker AFB and the CITS PMO

Table 15, Interview Question 3 and 4 Response Summary

Primary Reason for Difference, Q3	**Interviewee(s)**	**# of Individuals**	**% of Individuals**	**# of Sites**
Decentralized decision authorities	3,K1,K2	3	43%	2
Different funding avenues	K1,K3	2	29%	2
Different Missions	2A,2B	2	29%	1
Security by being different	2B,2C,	2	29%	1
Networks evolved at various times	K3	1	14%	1
Implementing locally developed technical solutions	K3	1	14%	1
MAJCOMs not on the same page	K3	1	14%	1
Inconsistent solutions from levels above base	K3	1	14%	1
Why is there so much variation, Q4	**Interviewee**	**# of Individuals**	**% of Individuals**	**# of Sites**
Base level decision authorities lack knowledge	K2	1	14%	1
No idea	2C	1	14%	1

Literature Review

Existing literature supports the top interview responses. The Air Force network operations hierarchy was designed to provide command relationships that ensured global systems interoperate without diminishing the authority of the local commanders to direct and manage the information technology assets under their control (DoAF, 2004). However, these relationships generated often conflicting and incompatible guidance. The recent consolidation of three Air Force headquarters directorates into a single directorate responsible for networks and warfighter integration acknowledges the need for change and provides a solution (SAF, 2004). This move should streamline policy development and enforcement. Additionally, new DoD instructions require DISA to be involved in the development and operational testing of information technology assets (DoD, 2004b). Some of the replies to this question were reported at only one site or by one individual, but existing literature provides another source of support; see Table 16, Triangulated Response Summary. Triangulation is a major strength of the case study methodology;

most importantly it establishes converging lines of inquiry (Yin, 2003:98). First, each BAN is made up of existing and new components configured as a consolidated network (CITS, 2004). As such, each is tailored to provide for the various mission of each installation. Second, the combination of BANs that make up the AFEN evolved over time with explosive growth (DoAF, 2004). During the 80s and 90s technology grew faster than regulatory guidance could be published. As a result, locally developed solutions were common. The responses listed in the Triangulated response table below provide convincing evidence because they are corroborated by multiple sources of data.

Table 16, Triangulated Response Summary

Primary Reason for Difference, Q3	Interviewee(s)	# of Individuals	% of Individuals	# of Sites	Lit Review
Decentralized decision authorities	3,K1,K2	3	43%	2	Yes
Different funding avenues	K1,K3	2	29%	2	Yes
Different Missions	2A,2B	2	29%	1	Yes
Networks evolved at various times	K3	1	14%	1	Yes
Implementing locally developed tech solutions	K3	1	14%	1	Yes

Investigative Question Two Results Summary

In summary of the results for investigative question two, not one particular reason received was reported by a majority of interviewees. However, the triangulated responses, identified in the table above, provide the most convincing evidence for why a variety of BANs are currently in use throughout the Air Force. The top reported reason for variation is decentralized decision authorities with different funding avenues and different missions placing second and third, respectively. The responses that are not triangulated provide good insight and should also be investigated further, see Table 17.

Table 17, Single Source Response Summary

Primary Reason for Difference, Q3	**Interviewee**	**# of Individuals**	**% of Individuals**	**# of Sites**	**Lit Review**
Security by being different	2B,2C,	2	29%	1	No
MAJCOMs not on the same page	K3	1	14%	1	No
Inconsistent solutions from levels above base	K3	1	14%	1	No
Why is there so much variation, Q4	**Interviewee**	**# of Individuals**	**% of Individuals**	**# of Sites**	**Lit Review**
Base level Decision authorities lack knowledge	K2	1	14%	1	No

Investigative Question Three

- What problems are created by using a variety of BANs throughout the Air Force?

A range of nine problems were identified, from training to preventing standardization. The third investigative question is answered by responses to interview question six and a cross case analysis of these responses.

Interview Question 6

- Interview question six is identical to investigative question three.

Training difficulties was significantly reported as a problem created by using a variety of BANs throughout the Air Force. Five out of a possible seven interviewees sited training as a problem, 71 percent. All of the very experienced key informants reported training as a problem. Interviews from each of the four locations used in this study reported training as a problem. Difficulty in troubleshooting problems is the second most significantly reported problem created by employing a variety of BANs throughout the Air Force. Three individuals at three separate locations reported

troubleshooting as a problem, 43 percent. Difficulty in this area can lead to denial of service for users and adversely affect mission accomplishment, the third most significantly reported problem. Adverse impact on mission accomplishment is the third most significantly reported problem, but is the most important of the reported problems because training and troubleshooting problems have a direct impact on mission accomplishment. This problem is reported by three people covering two different locations, 43 percent. Adding to the significant of this problem is the fact that it is reported by all three of the experienced key informants. The rest of the reported problems are identified in Table 18 below and provide important insight from practitioners that maintain and support BANs on a daily basis. Examples of training problems reported during interviews are listed below:

- “Every time a technician moves to a new base they not only have to learn the new network layout, there is a high probability that the will have to learn a completely new vendor's equipment”
- “When I get a new technician from Tech School, I pretty much know what level of experience I will be getting. But when I get an "experienced" NCO inbound, I really have no idea what equipment that they will be familiar with”.
- An experienced technician recently arrived to an installation that uses vendor B equipment with a Gigabit Ethernet backbone with network switches. The technician is trained on vendor B equipment routers using an ATM backbone. He has a skill that will never be use at his current base.

Table 18, Interview Question 6 Response Summary

Problems caused by variety of BANS, Q6	Interviewee(s)	# of Individuals	% of Individuals	# of Sites
Training Difficulties	2C, 3, K1, K2, K3	5	71	4
Difficulty troubleshooting problems	2A, 3, K1,	3	43	3
Adverse impact on mission accomplishment	K1, K2, K3	3	43	2
Continuity	2C, K1	2	29	2
Interoperability	K1, K2	2	29	1
Complicates planning for future	K2	1	14	1
Lost hours due to class attendance	K3	1	14	1
Multiple approval levels	K2	1	14	1
Prevents standardization	2B	1	14	1

Investigative Question Three Results Summary

In summary of the answers to investigative question three, training was the most significantly reported problem, followed by, troubleshooting difficulty and adverse impact on mission accomplishment. Adverse impact on mission accomplishment is the most critical of the reported problems because problems with training and difficulty in troubleshooting will adversely impact mission accomplishment. The actions of the key informants is noteworthy in this section. The key informants all reported training difficulties and adverse impact on mission accomplishment. Surprisingly, only one key informant reported difficulty in troubleshooting. Difficulties with training were reported by personnel at all of the interviewed sites, Site 1 personnel were not interviewed. Troubleshooting difficulty was reported by personnel from three sites and adverse impact on mission accomplishment was reported by personnel at two of the four locations including all three key informants.

Investigative Question Four

- What are the advantages of using a variety of BANs throughout the Air Force?

The following four replies were identified by interviewees: security through diversity, variety of training opportunities, tailoring to specific needs, and no advantage. Investigative question four is answered by responses to interview question five and a cross case analysis of the responses.

Interview Question 5

Interview question five is the same as investigative question four. Security through diversity was the most significantly reported advantage of using a variety of BANs. This advantage was reported by four out of seven people, 57 percent, covering all four locations used in this study. Reporting individuals believe a variety of network architectures increases the difficulty in hacking into Air Force systems and limits the impact of equipment specific vulnerabilities or design flaws. They fear that standard networks would be less secure because once a hacker gained access to one network it may be possible to gain access to other networks using similar techniques. Diversity also protects against vulnerabilities designed for a particular vendor's line of equipment or software. Providing a variety of training opportunities is the second most significantly reported advantage. Three out of seven reported it, 43 percent, covering two of the four sites used in this study. Table 19, located below, provides a complete summary of the advantages reported. None of the reported advantages was reported by more than one of the experienced key informants. The following statements are excerpts from the interviews:

- Need to understand that some standardization is needed, but for major security issues such as viruses not all bases can be the same; too much standardization makes it easier for hackers break into multiple networks
- If a network incident takes down one network, it may not affect all networks

- "A single vendor supplying all of the equipment for the AF going out of business would be catastrophic"
- A common vulnerability and/or failure prone to a particular piece of equipment would only affect locations that use the equipment
- Helps to see different network architectures, in regards to troubleshooting and just basic network knowledge; the more variety the better your technicians are going to be
- "Broad training opportunities and cost savings by just buying what is needed instead of purchasing a standard package that provides more capability than required"
- None, - UPS has a standard architecture across the globe, why can't we emulate their process?

Table 19, Interview Question 5 Response Summary

Advantages created by a variety of BANs, Q5	**Interviewee(s)**	**# of Individuals**	**% of Individuals**	**# of Sites**
Security through diversity	2B, 2C, 3, K3	4	57	4
Variety of training opportunities	2B, 2C, K1	3	43	2
Tailoring to specific needs	2A, K1	2	29	2
No advantage	K2	1	14	1

Investigative Question Four Results Summary

The results of investigative question four identified three advantages. Security through diversity was the top reported advantage, reported by 57 percent. Variety of training opportunities was reported by 43 percent of the interviewees and tailoring to specific needs was reported by 29 percent.

Investigative Question Five

- How should the Air Force respond to the current state of BANs?

Investigative question five identifies potential responses to the current state of BANs. This investigative question is answered by interview question seven, cross case analysis of responses, and a review of existing literature. The interview results show a slight majority in support of developing standard baseline architectures and implementation plans to correct disparate BANs throughout the Air Force. Existing

literature compliments the interview data by promoting the open systems strategy over attempting to standardize equipment everywhere, especially when the in question is rapidly evolving.

Interview Question 7

- How do you think the Air Force should respond to the current state of base area networks?

Fifty-seven percent of interviewed personnel believe developing standard baseline architectures and a prioritized implementation plan is the best way to deal with the current state of BANs. This slight majority consists of four out of seven people from three of the four interviewed locations. The three experienced key informants are in agreement. Responses below the top response were not reported by more than one interviewee, no agreement is reached on any other response; each response below the top response represents fourteen percent of interviewed personnel. Table 20 provides a complete summary of responses to interview question seven. The following comments were reported during interviews:

- "Develop model and strategic plan for standardizing to 1 AF network with central approval (remove lower levels from approval process)"
- "Institute baseline architectures, regardless of MAJCOM and put the horse before the cart and implement Tech School and follow on classes to support the new baselines, BEFORE THEY ARE IMPLEMENTED."
- Secure data by responding to weaknesses first, backdoors and vulnerabilities. Work gradually towards a standard network AF wide
- Top down implementation plan, based on the number of users at a base. Much like CITS has done with its NO/IA equipment. Each base gets x number of servers to support users, a couple of file servers, anti-virus servers, email, domain controllers, and a network backup solution that will handle a tape backup of critical systems. "The base would not be allowed to add to or change this setup without justification and approval from the top." Publish directives stating how much email space, and server space each user is allotted, and have consequences for commanders that try to change things without approval.

Table 20, Interview Question 7 Response Summary

Response Summary Question 7, Response to Disparate BANs	Interviewee(s)	# of Individuals	% of Individuals	# of Sites
Develop standard baseline architectures and a prioritized implementation plan (secure vulnerabilities first, other areas through attrition)	3,K1,K2,K3	4	57	3
NOSC and Base Technicians work better together	2b	1	14	1
Standardize from lowest level up	2c	1	14	1
Standardize from top down	3	1	14	1
Publish required standards	3	1	14	1
Don't Know	2a	1	14	1

Literature Review

Existing literature under the standardization body of knowledge supports caution in attempting to standardize volatile technology. In attempting to improve standardization, the Defense Standardization Program (DSP) guidance acknowledges that it may not be practical or desirable to standardize when technology is rapidly evolving or the desired solution or items go out of production after a short period (DoD, 2000a). This is extremely applicable to Air Force BANs. According to the updated version of Moore's Law, computing power doubles every 18 months and is expected to maintain this course for at least two more decades (Intel, 2004). Before 130 locations could be equipped and installed with the same suite of equipment, replacement technology for locations receiving the initial install would be required. In these instances, the DSP suggest employing standard interfaces or protocols provided under the open systems strategy (DoD, 2000a).

The open systems strategy promotes modular design tenets and widely supported and consensus based standards for key interfaces to develop affordable and adaptable information systems (DAG, 2004). Under this strategy, tremendous flexibility is offered

by providing a standardized "plug and play" capability among physical and electronic interfaces, while allowing equipment upgrades to keep pace with technological advances (DoD, 2000a). The Open System Joint Task Force (OSJTF), a chartered and cooperative effort of the Army, Navy, Air Force, and the Office of the Under Secretary of Defense, seeks to sponsor and accelerate the adoption of an open system approach for new systems and system upgrades within DoD (DLA, 2004). Instead of attempting to dictate the use of common hardware everywhere, the task force seeks to standardize according to each unique need while retaining the advantages of common architecture and compatible major interfaces (DLA, 2004).

The Defense Information System Agency maintains the DISR, a consolidated standards registry that replaced the Joint Technical Architecture (JTA). This registry is available on-line and identifies interfaces and standards that are technically mature and stable (DoD 2004). Although DoD guidance requires all components to use and implement the standards identified in the registry, Air Force level guidance is not available. Air Force guidance does exist on the Air Force JTA, but the DoD JTA has been replaced by the DISR.

Investigative Question Five Results Summary

Investigative question five results consist of a range of six different responses recorded during focused interviews and information retrieved from existing literature. Of the six recorded interview responses, developing and implementing standard baseline architectures was reported by fifty-seven percent of interviewed personnel; no other response was reported by more than one individual; interview data is supported by literature. Existing literature finds standardization in the technology arena is not always

beneficial especially when the technology is rapidly evolving or items remain in production for short periods of time, as is the case with networking equipment. The literature also supports modular design tenets and the use of consensus based standards for key interfaces instead of attempting to standardize equipment everywhere. Additionally, Air Force guidance on concerning the DoD consolidated registry, DISR, is needed.

Main Research Question

- Should the Air Force Standardize Base Area Networks?

Yes, the results of five investigative questions support the development and funding of standard baseline architectures from a high level in the department of the Air Force; reducing lower levels removes opportunities to deviate from accepted standards. Existing literature reveals the existence of a DoD composite repository of standards and a Joint Task Force for accelerating the adoption of open systems practices. However, Air Force guidance is not currently available.

The main research question is answered by the results of the five investigative questions. To address investigative question one, documented trip reports, interview data and existing literature established that BANs are different throughout the Air Force.

To address investigative question two, interview data and existing literature identified the following nine reasons for variation in Air Force BANs: decentralized decision authorities, different funding avenues for bases, different missions, networks evolved at different times, implementing locally developed technical solutions, security by being different, MAJCOMs not being on the same page, inconsistent solutions from levels above the base, and base-level decision authorities lacking knowledge to make

network architecture decisions. The first five are supported by multiple sources of information and are the most significant sources of variation.

To address investigative question three, interview data identified the following nine problems created by employing a variety of BANs throughout the Air Froce: training difficulties, troubleshooting problems, adverse impact on mission accomplishment, continuity problems, interoperability concerns, planning for the future, lost hours, multiple approval levels, and prevent standardization. The first four were reported by multiple individuals at more than on location and represent the most significant problems caused by using a variety of BANs.

To address investigative question number four, interview data identified the following three advantages of using a variety of BANs throughout the Air Force: security through diversity, variety of training opportunities, and tailoring to specific needs. Each response was reported by multiple individuals at more than one location.

To address investigative question number five, interview data and existing literature to identify how the Air Force should respond to the current state of BANs. Interview data supports the development of standard baseline architectures to address varying situations at different locations. Existing literature supports adhering to the open systems strategy of concentrating on major interfaces and consensus based standards. A mechanism, the DISR, to support this line of action is established and reinforced by the creation of the Joint Force Task Force to help accelerate the adoption of open systems practices; however, Air Force guidance is not available at this time. Table 21 illustrates how the research model presented in the overview section of this chapter, Figure 13, is followed to answer the main research question.

Table 21, Main Research Question Evidence Summary

Research Stage	Research Results
Are BANs different	Trip reports, interview results, and existing literature provide evidence that BANs are different
Reasons for Differences	Interview data and existing research identified the following nine reasons for variation: - Decentralized decision authorities - Different funding avenues - Different missions - Networks evolved at various times - Implementing locally developed tech solutions - Security by being different - MAJCOMs not on the same page - Inconsistent solutions from levels above base - Base level decision makers lack knowledge
Disadvantages of Variability	Interview data identified the following nine problems created by using a variety of BANs: - Training difficulties - Difficulty troubleshooting problems - Adverse impact on mission accomplishment - Continuity - Interoperability - Complicates planning for future - Lost hours due to class attendance - Multiple approval levels - Prevents standardization
Advantages of Variability	Interview data identified the following three advantages of using a variety of BANs: - Security through diversity - Variety of training opportunities - Tailoring to specific needs
How Should AF Respond to current BANs	Interview data promoted establishing baseline architectures to address different situations at bases Existing literature supported following the open systems strategy to ensure the compatibility of key interfaces instead of attempting to standardize equipment everywhere
Should AF standardize BANS	Investigative question results indicate YES, by adhering to the open systems strategy to provide baseline architectures for BANs

Chapter Summary

This chapter presented the results of the exploratory research methodology outlined in Chapter III. Documented AFCA SCOPE Network trip reports, focused

interviews, and a detailed literature review were used to provide convergent sources of information for reaching the presented results. A total of five sites were used in this study to address five investigative questions and ultimately answer the main research question; documented trip reports were available for three locations and focused interviews were completed at four locations.

V. Discussion, Conclusions and Recommendations

Overview

The purpose of this exploratory research of Air Force BANs was to increase understanding and establish points of interest for further investigation. Documented trip reports, interview transcripts, and existing literature provided evidence that BANs are different throughout the Air Force, identified nine reasons for variation, identified nine disadvantages and three advantages of employing a variety of BANs, and recommended an Air Force response to the current state of disparate BANs. A comparison of interview data and documented trip reports covering five locations provided these results. This chapter discusses the interviewees; research results, implications, and recommendation; suggestions for future research; and a conclusion. In parallel to this research, Lieutenant Jamie Sharkey conducted a thesis on the key issues pertaining to Air Force enterprise architecture management.

Discussion of Interviewees

Research participants were purposefully selected based on their knowledge and experience in BANs. Accordingly, even the responses reported from only one individual at one location provide key insight. Comparing responses from several sites increases the external validity by identifying repeated responses; however, all responses, repeated or not, provide valuable insight. Participants in this study urged their support for any effort to reduce the amount of variation that currently exists in our BANs across the Air Force. Members firmly believe there must be a better way to operate. Frustrations stem from investing energy into developing technical capabilities only to have those capabilities

relegated to a hobby upon reassignment to a new location. Training new personnel provides an additional source of frustration. New NCC personnel face a steep learning curve; this isn't peculiar to information technology career fields. However, rapidly changing technology, a salient characteristic of these career fields, results in a shortage of experienced trainers in the field and attendance at off-site classes reduces the available workforce and compounds the problem of providing quality base level communications support. Experienced personnel declined to participate because they simply did not have time.

Discussion of Research Results

The research results provide a unique and rich perspective by documenting input from informed practitioners tasked to maintain and support BANs on a daily basis and coupling these insights with information provided by existing literature. Increased information demands, mandates for interoperability, rapidly changing technology, and guidance from multiple sources continue to complicate the daily challenge of providing reliable and effective communications to the right person, at the right time, and in the right format. The results provide signposts for improving our current capabilities and identifying potential pitfalls. Developing solutions for issues identified in this section is not enough; perception changing strategies are required.

Procedures, an attribute of the LISI model, emerged as a common theme in the research results. This attribute is the primary enabler for the highest level of interoperability in the LISI model, the enterprise level or level four. This highest level of

interoperability is needed to fully implement the GIG. The levels and their associated primary enablers are reflected in Table 22.

Table 22, LISI Primary Enabling Attributes (Clark, 1999)

Level	LISI Description	Procedures	Applications	Infra-structure	Data
4	Enterprise/Universal	✓			
3	Domain/Integrated				✓
2	Functional/Distributed		✓		
1	Connected/Peer-to-peer			✓	
0	Isolated/Manual	✓			

As networks and computer systems evolve and mature up through the levels, different attributes act as key enablers. Ironically, infrastructure, used in this research as a comparison construct, is the primary enabler at the very low level of peer-to-peer interoperability and procedures is at the top level of interoperability. According to the LISI model, effective management and coordination of information technology related procedures and practices across the Air Force would enable interoperability at the Enterprise level. However, networks must mature through the lower levels first by fostering and developing the key enablers for each level; applications, data, and procedures, respectively.

Should BANs look the same or different?

Initial inspection of the interview results shows an even split, no consensus, between the choice of same or different. Upon further review, a clear demarcation exists between practitioners with over eight years experience and those with less than five years experience; more experienced practitioners believe networks should look the same. The researcher believes the primary reason for the distribution of the results is experienced

personnel have a better understanding of the obstacles encountered when attempting to maintain, support, and connect disparate systems and networks.

The implications of these findings indicate a lack of consensus, either way, on this issue and provide evidence that additional research, education, and information dissemination is needed to help personnel work effectively towards a common goal of leveraging information and technology to increase interoperability and integration, as outlined in Joint Vision 2020. Recommend implementing information sharing initiatives through NOSCs or adding education sessions to AFCA base assistance visits to share policy, best practices, and disseminate information concerning the road ahead.

Are BANs different throughout the Air Force?

This study used an established construct, infrastructure element of the LISI model, to compare sites; the results strongly indicate BANs are different. This finding does not ignore the similarities that are present; instead it highlights the presence of major differences. The U.S. Code Title 10 provides a structured and disciplined approach to mission accomplishment by requiring the Armed Forces to organize, train, and equip their respective forces. Air Force disparate networks severely degrade the service's ability to satisfy the fundamental Title 10 requirements. As a direct result, mission effectiveness is decreased. Disparate networks make it more difficult to achieve information superiority and integration. In order to provide reliable access to needed information; the cables, systems, and networks must be effectively organized, controlled, and managed. Standardized architectures for unclassified and classified networks are a top level requirement of the CITS Block 30 initiative; however, this initiative is still in development.

Inherent differences in bases due to missions, terrain, or other environmental factors present a formidable challenge; however, a better job must be done in providing standardized base level communications. Capitalizing on the similarities is essential; standard networks can be developed for the finite categories all bases fall into. Implementing standard processes, procedures, and best practices for common tasks would greatly simplify BAN management and network operations.

Implications of these findings indicate BANs are different and work is required to ensure information technology assets are used more effectively to achieve the vision outlined in Joint Vision 2020. Recommend enforcing standard processes, procedures, and best practices for common task across the Air Force to reduce redundancy and site-specific solutions for functions performed at multiple locations.

Why are a variety of BANs currently in use throughout the Air Force?

All of the results for this investigative question stem from the previous Air Force focus for managing networks; centered on the NCC at each location. This arrangement worked well in the initial stages of network development during the 1980s and 1990s because mature enterprise guidance was not available. The importance of information and the role of the networks have evolved along with the DoD doctrine that now requires interoperability, integration, and global access to achieve decision superiority. Mature enterprise guidance is now available and the focus for managing networks has moved from individual NCCs to NOSCs; a more centralized approach. The recent announcement of plans to consolidate three headquarters organizations into a single directorate responsible for networks and warfighting integration is a clear sign Air Force

leadership acknowledges the need for a fundamental change in managing information technology assets; consolidation plans will change the Air Force CIO from a civilian position to a three star general (SECAF, 2004).

Implications of the research results reflect a major milestone in the development of BANs. The structure and focus for managing these critical assets is in transition. Centralized management and control are definitely a step in the right direction. Base level networks are no longer just base assets. Operating globally deployed unmanned aerial vehicles from stateside locations, warfighters accessing home station technical or support data from austere locations, and providing video conferencing between family and deployed military members are just a few examples of current reachback applications; the future holds additional applications. Base are networks play a pivotal role in the defense of our nation and should be managed at higher levels commensurate with their overall contribution to the fight; previous paradigms and delineation points are not useful. Policy should originate at the highest levels and get implemented across traditional barriers of commands and bases to achieve maximum benefit for the Air Force as a whole. Shortening the kill chain, introduced in the Research Significance section of Chapter I, requires all phases of the AFEN and GIG; including BANs, to achieve the optimal effects needed to defeat future adversaries and challenges. In spite of policy originated at a macro level and a big picture mission focus, support and quality of service for users at the lowest level must remain top priorities. Service to base level users represents the critical link between warfighters and technology and has a direct impact on mission accomplishment. Diligence is required to minimize the effects of any negative unintended consequences. Recommend the development of transition strategies for

initial stages and initiatives to foster very close relationships between NOSC and NCC personnel to overcome barriers associated with fault isolation and repair from a distance. Additionally, recommend monitoring the quality of service and amount of down time following the transition to SCOPE EDGE to determine if the reduction in base assistance team visits from 120 visits in 18 months to 30 visits in 12 months will have a detrimental effect.

What problems are created by using various BANs throughout the Air Force?

The results identified by this investigative question are related to maintaining BANs and the consequences of failing to maintain them. Problems satisfying two of the Title 10 responsibilities, training and equipping, were addressed by the results of this investigative question. Differences in network equipment, processes, and systems require a unique and complex training program to provide instruction over a wide range of diverse situations. The differences also reduce the size and composition of the knowledge base for developing experts. As a result of increased variation, many small and specialized groups form instead of fewer but larger groups of experts that improve capabilities through increased opportunities to share information and lessons learned. Administering such a training program is very difficult and time consuming; equipping largely diversified networks is equally difficult.

Implications of these results suggestion widespread problems in training exist and acquisition reform is needed to provide common equipment for practitioners. The $5 billion dollars in required network upgrades, estimated by the Air Force, to implement Joint Vision 2020 are wasted if personnel are not trained to maintain the developed

networks. Providing common equipment will positively impact current training problems. Block 30 of the CITS program incorporates vendor selection and will help reduce some variation. Recommend modifying the technical school training curriculums to reflect the use of commercial off the self products. For information technology related career fields, the bulk the technical instruction should come from commercial agencies. Attempting to maintain current lesson plans in Air Force operated classrooms providing technical instruction is a futile attempt to hold on a obsolete paradigm. Reducing variation reduces the amount of different items required to perform the similar functions, significantly reduces the logistics footprint required to support these items, and will aid the development of effective training programs. Additionally, disparate networks make it more difficult to find or use spare parts when needed.

What are the advantages of using a variety of BANs throughout the Air Force?

The results of this investigative question reveal security through diversity and the variety of training opportunities as the most advantageous benefits; only three benefits were identified compared to nine reported problems or disadvantages from the results of the previous investigative question. Training is identified as a problem and a benefit. Security through diversity is seen as a benefit because current security practices are ineffective; conveys a lack of confidence. Attempting to develop and implement effective security patches and procedures for the vast equipment configurations comprising our networks is very complex; however, the diversity does eliminate single points of failure concerning specific equipment or software.

Implications of these research results indicate a need to determine if the benefits of security through diversity are stronger than the potentially improved security that can be achieved by quickly monitoring and updating a less diverse suite of equipment and software; the researcher strongly believes greater security benefits are provided by effectively managing less diversity. The benefits obtained through security by diversity are minimized by the other problems identified by the previous investigative question. Recommend promoting security successes or capabilities to increase confidence and promoting opportunities to fine tune networking skills by concentrating on a reduced number of equipment and applications; quality over quantity.

How should the Air Force respond to the current state of BANs?

Results of this investigative question dismiss the idea of attempting to standardize equipment everywhere throughout the Air Force. Instead, the results promote the development of baseline architectures to exploit the benefits of the opens systems strategy for interoperability and following the guidelines of the Defense Standardization program. Additionally, results identified a gap in Air Force guidance concerning the DoD consolidated standards registry, DISR.

Implications of these results show practitioners are in tune with current strategies for improving standardization and identify a need to publish Air Force guidance concerning linking Air Force initiatives with DoD efforts and guidance, specifically the DISR. Recommend publishing guidance and promoting the use of the registry in developing and obtaining future networks, systems, and equipment.

Suggested Future Research

This section outlines opportunities for future research. First, duplicate this study using locations with similar sized BANS to determine if the results are complimentary. Comparing similar sized BANs will determine if identified variation and results are unique to this study. Second, repeat this study using observations instead of documented reports or interviews to eliminate any bias introduce by the authors of the documented trip reports. Third, investigate how many practitioners develop skills that are applicable at one location, but not used at subsequent duty assignments. Research will determine if selective assignment procedures are needed for technicians with specialized skill sets. Fourth, conduct surveys using this studies research results to explore support for sources of variation, problems and advantages of variation, and proposed the Air Force response to the current state of BANs. Fifth, perform similar study using commercial or government agencies to determine if similar results are achieved; the banking industry has security requirements similar to the military and could provide useful information.

Conclusion

This study concludes that the Air Force should standardize BANs in accordance with principles of the open systems approach to weapons systems acquisition and fund implementation from the highest level. In coming to this conclusion several important issues were uncovered. First, additional research is required concerning BANs and to tap the knowledge of current practitioners; virtually nothing has been published in this area. Second, the shift to a more centralized approach to managing Air Force networks is a significant development that should be monitored closely for unintended consequences.

Fourth, coordinating Air Force information technology procedures and practices are key enablers for achieving the enterprise level interoperability required to implement the GIG; considerable attention should be applied to controlling practices in order to fully exploit advantages provided by technology. Implementing more standardization will make it possible to manage BANs and the AFEN more effectively, improve training, reduce the length of outages, enhance interoperability, aid integration efforts, significantly increase operational capability, and leverage technology to help implement Joint Vision 2020.

This research provides leaders and managers with insightful information concerning BANs and successfully contributes to the existing body of knowledge by identifying differences in Air Force BANs, discovering sources of differences, revealing advantages and disadvantages of variety, providing a recommended response to the current state of BANs, and pinpointing additional areas for study.

Bibliography

Air Education and Training Command. *Scope Eagle 2003D Strategic Thought Session.* Briefing. 25 July 2003. Retrieved from https://private.afca.af.mil.

Air Force Communications Agency. *About AFCA: Communications and Information.* Retrieved 28 September 04a, from http://public.afca.af.mil/.

Air Force Communications Agency. *Infostructure Enterprise Architecture*, Overview and Summary Information (AV)-1. Version 1.2, Draft, 28 November 2003.

Air Force Communications Agency. *Integrated Network Operations and Security Center Enabling Concept.* Version 2.4, Draft, 11 July 2004b. Retrieved 20 November 2004 from, https://private.afca.af.mil/infostructure/main.html.

Air Force Communications Agency. *Joint Technical Architecture-Air Force.* Version 0.6 (Working Draft). Scott AFB, IL, 21 October 1996.

Air Force Communications Agency. *Operationalizing & Professionalizing the Network.* OPTN homepage. Retrieved 2 October 04c, from https://private.afca.af.mil/optn/.

Air Force Communications Agency. *U.S. Air Force Base Area Network (BAN) Platform Profile,* Ver 0.8 (Draft). Scott AFB, IL, 27 November 2002.

Air Force Communications Flight Plan Briefing. Discussion panel brief between Air Force Institute of Technology Students and Senior Communications Officers. Air Force Institute of Technology, Wright-Patterson AFB OH. 7 October 2004.

Barry, L., *Scope Net Teams Reinforce Effective Base Network Operations.* Intercom magazine article., Vol 42, No 3. Air Force Communications Agency, Scott AFB, IL, Mar 2001.

Brewin, B. *DOD Lays Groundwork For Network-Centric Warfare*, Federal Computer Week, 1 November 1997.

Bruns, J., *Network Centric Operations: Disciplining Development through Architecture.* Briefing provided to senior leaders. Retrieved 25 September 2004 from, https://private.afca.af.mil/infostructure/iac_council/meetings/.

Carnegie Mellon. *Defense Information Infrastructure Common Operating Environment: Software Technology Roadmap.* Retrieved 20 September, 2004, from http://www.sei.cmu.edu/str/descriptions/diicoe.

Carney, D. & Oberndorf, P., *Integration and Interoperability Models For Systems of Systems.* Carnegie Mellon briefing presented during the Systems and Software Technology Conference. 21 April 2004.

Clark, T. & Jones, R. Organisational Interoperability Maturity Model for C2. Paper presented at the International Command and Control Research and Technology Symposium 1999. Retrieved 14 November 04 from, www.dodccrp.org/events/1999/1999crts/pdf_files/track_5/049clark.pdf.

Cohen W. S., & Shalikashvil J., *Joint Vision 2010.* Briefing slides presented at the Pentagon on 19 May 1997. Retrieved 24 September, 2004, from http://www.defenselink.mil/photos/May1997/.

Combat Information Transport System. CITS Lead Command Home Page. Retrieved 30 August 2004 from, https://private.afca.af.mil/cits/its.htm.

Combat Information Transport System. *Information Transport System Baseline Program Directive,* Version 4., 8 January 2004. Retrieved 24 September 2004, from https://private.afca.af.mil/cits/bdp.

Creswell, J. W., *Research Design*. Thousand Oaks: Sage Publications, 1994.

Creswell, J. W., *Research Design* (2nd Edition). Thousand Oaks: Sage Publications, 2003.

Defense Acquisition Guidebook. Retrieved 20 December 2004, from http://akss.dau.mil/dag/Guidebook/.

Defense Information Systems Agency. (2004). "Communication: Today's Capabilities". Excerpt from core mission area website. n. pag. http://www.disa.mil/main/about/communications.html

Defense Information Systems Agency. *GIG ES Homepage*. Retrieved 20 November 2004 from, https://ges.dod.mil/.

Defense Logistics Agency. *Interoperability.* Article on interoperability. Retrieved 27 December 2004, from https://www.dsp.dla.mil/interop.htm.

Department of Defense. *Defense Standardization Program.* DoD Manual 4120.24. Washington: GPO, March 2000a.

Department of Defense. *Levels of Information Systems Interoperability (LISI).* C4ISR Architecture Working Group report. Washington: GPO, 30 March 1998.

Department of Defense. *Interoperability and Supportability of Information Technology and National Security Systems.* DOD Directive 4630.5. Washington: GPO, 5 May 2004.

Department of Defense. *Procedures for Interoperability and Supportability of Information Technology and National Security Systems.* DOD Directive 4630.8. Washington: GPO, 30 June 2004b.

Department of Defense. Joint Technical Architecture, Vol I., Version 6.0, 3 October 2003.

Department of Defense. *Joint Vision 2020.* Washington: GPO, June 2000.

Department of Defense. *Network Centric Warfare.* Report to Congress. Washington: GPO, 27 July 2001.

Department of Defense. *Procedures for Interoperability and Supportability of Information Technology and National Security Systems.* DOD Directive 4630.8. Washington: GPO, 30 June 2004a.

Department of the Air Force. *Air Force Network Operating Instructions.* AFI 33-115, Vol 3. Washington: HQ USAF, 15 April 2004.

Department of the Air Force. *Integrated Network Operations and Security Center Enabling Concept*, Draft, Version 2.4, 11 July 2004. Retrieved 20 November 2004 from, https://www.infostructure.hq.af.mil/infostructure/main.html.

Department of the Air Force. *Joint Technical Architecture-Air Force.* AFI 33-133. Washington: HQ USAF, 1 July 2000.

Department of the Air Force. *Network Management.* AFI 33-115, Vol 1. Washington: HQ USAF, 2 July 1999.

Department of the Air Force. *Network Operations.* AFI 33-115, Vol 1. Washington: HQ USAF, 3 May 2004b.

Department of the Air Force. *Promotion Fitness Examination Study Guide.* AFI 36-2241, Vol 1. Washington: HQ USAF, 1 July 2003.

DISRonline. *DOD IT Standards Regestry*. Homepage for DOD standards registry. Retrieved from 29 November 2004, from http://disronline.disa.mil/.

General Dynamics. *General Dynamics Awarded $5 Million to Redesign Air Force Networks.* Press release, dated 17 December 2003. Retrieved from, www.gd-ns.com/news/03-12-17-AirforceNetworkds.htm.

Horn, M. *Block 30 Update.* Powerpoint briefing for Colonels. Retrieved 26 August 2004, from https://private.afca.af.mil/

Intel Corporation. *Moore Optimistic on Moore's Law.* Article posted on Intel's Technology and Research web page. Retrieved 23 December 2004 from, www.intel.com/technology/silicon/mooreslaw/eml02031.htm.

Intel Corporation. *Silicon: Moore's Law.* Retrieved 20 November, 2004, from http://www.intel.com/research/silicon/mooreslaw.htm.

Leedy, P.D., & Ormrod, J.E. *Practical Research: Planning and Design* (7th Edition). Upper Saddle River, New Jersey: Prentice-Hall, 2001.

Locher, L. J. *Trusted and Trusting Domains in NT 4.0.* Article retrieved 26 December 2004, from http://www.winnetmag.com/windows/article/articleID/7588/7588.

McCarter, M. *Milestones for Air Force Modernization.* Military Information Technology article, Volume 7, Issue 10, 31 December 2003.

Miller, A., Jefferson, M., and Rogers, J. *Global Information Grid Architecture.* The Edge Magazine, July 2001. Retrieved from www.mitre.org/news/the_edge/july-01/miller.html.

Mossing, N. *ACC shares transformation success stories.* Intercom. Scott AFB, IL: Air Force Communications Agency, 5 Nov 2004.

Network Operations and Security Center/Network Control Center Worldwide Operationalize and Professionalize the Network Conference. Meeting Minutes. Retrieved 20 September 2004, from https://private.afca.af.mil/optn/.

Secretary of the Air Force. *Air Force to consolidate information technology directorates.* Press release Number 12-07-04.

SCOPE EDGE. *Our History.* Excerpt from SCOPE EDGE web page. Retrieved 26 August 2004, from https://private.afca.af.mil/scopeedge. 26 August 2004.

Thomas, R. C. *Managing Change: Through Workforce Transformation.* Intercom Article, Volume 45, Number 7, July 2004.

United States Congress. *Information Technology Management reform Act of 1996* (Clinger-Cohen Act). Public Law No. 105-261, Division E, Sec 5125(b)(2), 10. Washington: GPO, 1996.

United States Congress. Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (Clinger-Cohen Act Amendment). Public Law No. 105-261, Subsection (a), Section 2223, title 10. Washington: GPO, 1998.

United States Strategic Command. *Joint Concept of Operations for Global Information Grid NetOps*. Offutt AFB, Omaha, NE. 11 March 2004.

USAF/XORI. C*apability Development Document for Combat Information Transport System (CITS)*. Washington: GPO, 2004.

WindowsNetworking. *Windows NT 4 Domain Models.* Tips provided from administration knowledge base web page. Retrieved 26 December 2004 from, www.windowsnetworking.com/kbase/windowstips/windowsnt/admintips/network/windowsnt4domainmodles.html.

Williams, D. *New Frontier: Kill Chain Shortened by New Weapons Systems.* Intercom Article, Volume 45, Number 9, September 2004.

Yin, R. K., *Case Study Research* (2nd Edition). Thousand Oaks: Sage Publications, 1994.

Yin, R. K., *Case Study Research* (3rd Edition). Thousand Oaks: Sage Publications, 2003.

Vita

First Lieutenant Boyd graduated from Howard Career Center in Wilmington, Delaware. He enlisted in the Air Force in October 1985 as an inventory management specialist and cross trained into the communications – computer systems control specialty in 1992. In his 16-years prior to becoming an officer, Lieutenant Boyd achieved the rank of Master Sergeant and developed extensive experience in fixed and tactical communications. His first duty station was McGuire AFB, New Jersey followed by assignments to Spangdahlem AB, Germany; the Pentagon, Virginia; Offutt AFB, Nebraska; Izmir, Turkey; and Shaw AFB, South Carolina. Lieutenant Boyd earned his commission through the Officer Training School at Maxwell AFB, Alabama in June 2001.

After receiving his commission he was assigned to the Robins AFB, Georgia where he served as a combat communications squadron assistant engineer and a group executive officer. In August of 2003, he entered the Graduate School of Engineering and Management, Air Force Institute of Technology. Upon Graduation, Lieutenant Boyd will be assigned to Headquarters, Pacific Air Forces, Hickam AFB, Hawaii.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
21-03-2005	**Master's Thesis**	Aug 2003 – Mar 2005

4. TITLE AND SUBTITLE

Exploratory Inquiry: Disparate Air Force Base Area Network Architectures

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Boyd, Charlie, W. Jr., First Lieutenant, USAF

5d. PROJECT NUMBER
If funded, enter ENR #

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 641
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/05M-01

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFCA/SCOPE EDGE
Attn: Maj Sally Williams
203 W. Losey Street
Scott AFB, IL 62225

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Joint Vision 2020, the Department of Defense (DoD) blueprint for development and transformation, identifies information and technology as critical enablers for our nation's military and calls for the development of a joint force capable of integrated information sharing to provide decision superiority, the ability to make and implement better decisions before enemies can react (DoD, 2000). Networks have been identified as the single most important element for transforming our current military forces. Ironically, Air Force base-level communications networks have been identified as a weakness.

This research follows the qualitative approach to increases the current understanding of base level communications networks by conducting a multiple site comparative case study that includes practitioner interviews at four locations and the examination of existing literature and documented trip reports. This study determines if base- level networks are disparate, isolates sources of disparity, identifies advantages and disadvantages of disparity, and recommends an appropriate course of action.

This research is significant for members of the Air Force, DoD, and private citizens. Air Force networks support close to three-quarters of a million users, including active duty service members, Air Force Reserves, Air National Guard, civilians, and embedded contract employees (McCarter, 2003). In addition to potentially affecting many people and the larger DoD network, base-level networks provide support to deployed warfighters and provide the environment to train, organize and equip our forces. Additionally, these networks provide critical information to key decision makers.

15. SUBJECT TERMS
Case study; information systems network; network architecture; qualitative; interoperability; and standardization

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			Dr. Kevin L. Elder (ENV)
U	**U**	**U**	**UU**	122	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, ext 4600; email: Kevin.Elder@afit.edu