

# Deployed Tactical Network Guidance

*Appendix D to Guidance for 'End State' Army Enterprise  
Network Architecture*



Version 1.0  
As of: 31 May 2012



*PAGE INTENTIONALLY BLANK*

---

### Revision History

Revision	Source	Date	Description of Change
V 0.1	SAIS-AOB	30 August 2010	Initial Staffing Draft
V 1.0	SAIS-AOB	31 May 2012	Final draft based on additional comments received from review process

*PAGE INTENTIONALLY BLANK*

---

## Table of Contents

1.	Introduction .....	1
1.1	Purpose .....	1
1.2	Background .....	1
1.3	Approach .....	3
1.4	Unity of Effort.....	3
1.4.1	Unity of Effort in Network Concept Development.....	3
1.4.2	Unity of Effort in Acquiring, Fielding and Managing Integrated Tactical Network Solutions.....	5
1.4.3	Unity of Effort in Operating and Managing the Army Networks.....	6
1.4.4	Unity of Effort in Developing the Army Deployed Tactical Network Architecture. ....	7
2.	Components of the Army Deployed Tactical Network Architecture.....	8
2.1	Tactical Network Transport.....	9
2.2	Services.....	10
2.2.1	Networks.....	10
2.2.2	Network Services .....	10
2.3	Applications .....	11
2.3.1	Business Applications .....	11
2.3.2	Intelligence Applications.....	12
2.3.3	Warfighting Applications.....	12
2.3.4	Network Operations (NetOps) .....	12
3.	Control Points .....	13
3.1	Forward Deployed Installation/Base Transport .....	14
3.2	Forward Deployed Installation/Base Services .....	16
3.3	Forward Deployed Installation/Base Applications .....	18
3.4	Forward Deployed Installation/Base NetOps.....	19
3.5	Forward Deployed Installation/Base Desired End State.....	21
3.6	Control Point ❶ – Enterprise to TOC/Command Post.....	22
3.6.1	Transport at Control Point 1 .....	22
3.6.2	Applications at Control Point 1 .....	23
3.6.3	IP Network Access and Enterprise Services at Control Point 1 .....	23
3.6.4	NetOps at Control Point 1 .....	23
3.6.5	Control Point 1 Summary .....	24
3.7	Control Point ❷ – Enterprise/Command Post to Platform/Soldier/ Sensor .....	26
3.7.1	Transport at Control Point 2 .....	27
3.7.2	Network Services at Control Point 2.....	27
3.7.3	Network Applications at Control Point 2 .....	28
3.7.4	Network Operations (NetOps) at Control Point 2.....	28
3.7.5	Summary of Control Point 2 .....	29
3.7.6	Control Point 2 – Desired End State.....	30
3.8	Control Point ❸ – Enterprise/Command Post to Soldier.....	31
3.8.1	Transport at Control Point 3 .....	32
3.8.2	Network Services at Control Point 3.....	32
3.8.3	Network Applications at Control Point 3 .....	32
3.8.4	NetOps at Control Point 3 .....	33
3.8.5	Control Point 3 Mounted and Dismounted Soldier Mobile Device Vignette ...	33

3.8.6	Control Point 3 Desired End State.....	34
3.9	Control Point ④ – Platform/Soldier to Sensor.....	35
3.9.1	Transport at Control Point 4 .....	35
3.9.2	Network Services at Control Point 4.....	35
3.9.3	Network Applications at Control Point 4 .....	35
3.9.4	Network Operations (NetOps) at Control Point 4.....	36
3.9.5	Control Point 4 Desired End State.....	36
4.	Summary and Way Ahead .....	36

### Figures

Figure D-1:	Army Enterprise Network (LandWarNet).....	3
Figure D-2:	Army Concepts Describe Integrated Network Requirement.....	4
Figure D-3:	Army Agile Acquisition Process .....	6
Figure D-4:	Notional Deployed Tactical Network Architecture Integration Construct.....	8
Figure D-5:	LandWarNet Capabilities (TRADOC Pamphlet 525-5-600).....	9
Figure D-6:	Control Point Concept .....	14
Figure D-7:	Control Point 1: Enterprise to TOC/Command Post.....	22
Figure D-8:	Control Point 2: Enterprise/Control Point to Platforms and Soldiers.....	27
Figure D-9:	Control Point 3: Enterprise/Command Post to Soldiers.....	32
Figure D-10:	Control Point 4: Platform/Soldier to Sensor .....	35

### Tables

Table D-1:	Transport.....	15
Table D-2:	Enterprise Services .....	17
Table D-3:	Applications.....	19
Table D-4:	NetOps .....	20

### Tabs

TAB A	'End State' Imperatives.....	37
TAB B	Acronyms .....	39
TAB C	References .....	41

## Executive Summary

On 28 December 2009, the Vice Chief of Staff of the Army (VCSA) directed Chief Information Officer (CIO)/G-6 to develop 'as is' and 'end state' network architectures to guide evolution of network procurements and enhancements. The Strategy for 'End State' Army Network Architecture – Tactical, Version 1.1 dated 06 April 2010 was written in response to the VCSA Memorandum with a focus on the Deployed Tactical Network environment. This appendix is revised to focus on the Deployed Tactical Network in the context of the Army Enterprise Network as described in the basic document Guidance for 'End State' Army Enterprise Network Architecture, Version 1.0.<sup>1</sup>

Appendix D standardizes a framework for describing and analyzing the deployed tactical network in order to guide future architecture capability development efforts. The document focuses on four (4) specific components for LandWarNet: Transport, Application, Services and Network Operations (NetOps). Appendix D builds on the discussion of Control Points introduced in Appendix C to address how the Mission Environment shapes the capabilities of network solutions delivered to command posts, platforms and Soldiers operating in that mission environment. The mission environments in which Soldiers operate are differentiated by varying network bandwidth requirements; latency, high bit-error rate, system size/weight/power, environmental factors, and location performance and have an impact on capabilities delivered.

This document will be reviewed annually, and updated based on: 1) enduring changes in the as-is tactical architecture; and 2) revisions in the Army Strategic guidance in regards to emerging technology for vision of the 'to-be' architecture. Follow on architecture documents will articulate the specific standards critical to ensuring the Army Deployed Tactical Network supports an integrated end-to-end network which supports the Army operational requirements for all echelons during every phase of joint operations.

Approved By:



Gary Blohm

Director, Army Architecture Integration Center

CIO/G6

<sup>1</sup> "As of October, 2011, the Army Enterprise Architecture (AEA) Network is now referred to as the Army Enterprise Network Architecture (AENA).

*PAGE INTENTIONALLY BLANK*

## 1. Introduction

On 28 December 2009, the VCSA directed the CIO/G 6 to develop 'as is' and 'end state' network architectures to guide future network procurements. The Strategy for 'End State' Army Network Architecture – Tactical, Version 1.1 dated 06 April 2010 was written to respond to the Army Memorandum: "Achieving Army Network and Battle Command Modernization Objectives." This appendix addresses the Tactical Network component of the Army Enterprise Network and is organized as Appendix D to the Guidance for 'End State' Army Enterprise Network Architecture.<sup>2</sup>

### 1.1 Purpose

This document provides guidance to the Army stakeholders and industry partners that are developing architecture solutions for the Army's Deployed Tactical Network. Appendix D describes the relationships and inter-dependencies of the computing environment described in Appendix C with network transport, applications, services and Network Operations (NetOps) and how these impact the mission environment's ability to provide secure, uniform and interoperable network access to command posts, mobile platforms, dismounted Soldiers and sensors. Appendix D also identifies desired end state goals for future network capabilities.

### 1.2 Background

The Army Deployed Tactical Network has undergone revolutionary changes over the past 10 years. However, it is not an integrated network. It is a composite of many different technologies and functional capabilities that are available to the commander at his command post, mobile platforms and dismounted soldiers and sensors. As commanders identified urgent operational needs, the Army purchased and rapidly deployed emerging research and development and COTS solutions directly to deployed forces in theater. Often, the fielding of these urgent material solutions took precedence over the other components of Doctrine, Organization, Training, Materiel, Leadership Development and Education, Personnel, and Facilities (DOTMLPF). Over time, as the Army delivered an increasing number of capabilities to commanders in the field, it became obvious the burden of integrating these technologies became the responsibility of the deployed commander. Much of this new technology had to remain in the theater for the next organizational rotation so many of the hard won DOTLMPF lessons learned as a result of the introduction of this new technology could not be re-deployed with the unit back to its home station.

The current corps and below command post is supported by a host of powerful but separate functional network systems that are funded, acquired, fielded, deployed, managed, sustained and operated as separate entities. Some of these capabilities include the Warfighter Information Network Tactical (WIN-T), Trojan Spirit, Combat Service Support Very Small Aperture Terminal (CSS VSAT), Global Broadcast System (GBS), Secure Mobile Anti-jam Reliable Terminal Tactical (SMART-T), Blue Force Tracker (BFT (Joint Capabilities Release (JCR)), Movement Tracking System (MTS (Joint Capabilities Release-Logistics (JCR-L)), and many others. Each of these rely on satellites (primarily commercial) to provide the primary network umbilical to subordinate in theater forces and to the Army and Joint network enterprise. In 2003, only corps and division headquarters had dedicated command and control satellite

---

<sup>2</sup>Memorandum, Achieving Army Network and Battle Command Modernization Objectives, dated December 28, 2009.

terminals and the wide area network (WAN) and local area network (LAN) technology to provide internet protocol (IP)-based Mission Command support networks to the command post staff. In the past ten years commanders can access satellite based, secure, IP-based network capabilities down to the company level and soon down to the platform level.

Inside the command post the commander and his staff must install, operate and maintain separate network access services of varying classification levels, such as: Non-Classified Internet Protocol Network (NIPRNET), Secure Internet Protocol Network (SIPRNET), Joint Worldwide Intelligence Communications System (JWICS), National Security Agency Network (NSANet), Combined Enterprise Regional Information Exchange System (CENTRIXS), and others. Each network requires separate clients, routers, servers, storage, network management support and all of the other elements that make up a LAN to support users in the command post.

Commanders must contend with hundreds of different applications that are hosted on servers in the command post and managed by the staff. Not only are Mission Command applications not fully interoperable with each other – and require separate hosting and management efforts - but any Microsoft Office instances must be replicated separately for each security level (unclassified, secret, top secret, ally only, coalition, etc.) adding to the complexity of the networks the commander and his staff must integrate. Commanders must also provide the resources to manage network services such as identify management, knowledge management, collaboration, and a host of others including help desk and NetOps functions.

The dynamics of change in the Army Deployed Tactical Network Architecture will continue to rapidly transform as technology and the global cyber threat evolve. Currently, the Army Deployed Tactical Network supports all echelons of the Army's deployable force, Army Service Component Commands, down to mobile platforms and dismounted Soldiers, and sensors. The network must support hundreds of separate deployed command posts, thousands of mobile ground and aerial platforms and tens of thousands of dismounted Soldiers and sensors all separated by time, distance, terrain, weather, constant movement and an enemy who is trying to deny them access to their own networks.

As an appendix to the Army Guidance for 'End State' Army Enterprise Network Architecture, Appendix D discusses components of the Army tactical network (transport, applications, services, and network operations), as they relate to each other and to the larger Army and Joint enterprise network as a way to set the stage for an architecture that will support a network end state. Training and Doctrine Command (TRADOC) Pamphlet (PAM) 525-5-600, "The U.S. Army's Concept of Operations, LandWarNet 2015" states:

*"LandWarNet, underpinned by integrated architectures enables, "one Army battle command system" as part of "one network" and facilitates a consistent alignment of joint capabilities across all layers of the network (platforms and sensors, applications, services, transport, and standards) to design and field an integrated system of systems (see Figure D-5; LandWarNet Capabilities). This network provides the link from Soldier to sustaining base, with tailored software applications that are optimized for conducting joint operations."<sup>3</sup>*

<sup>3</sup> TRADOC PAM 525-5-600, The United States Army's Concept of Operations (CONOPS) – LandWarNet, dated 11 February 2008

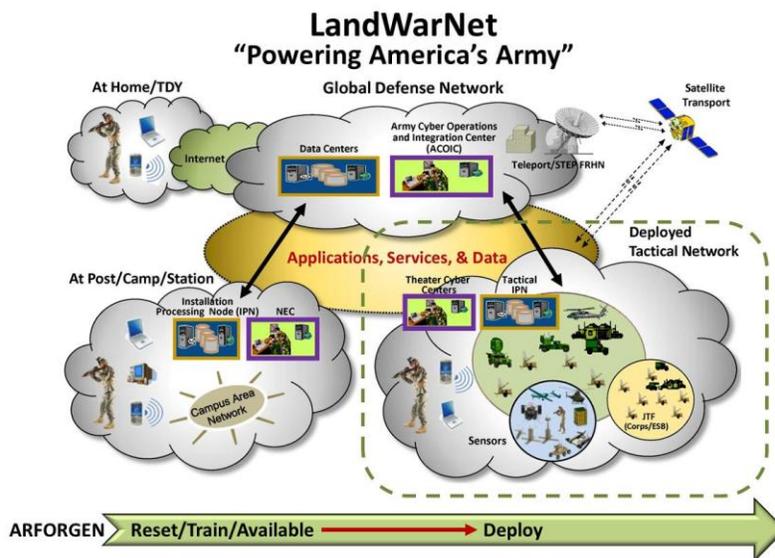


Figure D-1: Army Enterprise Network (LandWarNet)

### 1.3 Approach

This appendix standardizes a framework for describing and analyzing the deployed tactical network in order to guide future architecture capability development efforts. The focus is on four (4) specific components for LandWarNet: Transport, Application, Services and NetOps. Appendix D will use the concept of Control Points, introduced in Appendix C to address how the mission environment (ME) shapes the capabilities of network solutions delivered to command posts, platforms and Soldiers operating in that mission environment. Appendix D identifies the Deployed Tactical Network "End State" goals that best support current and future Army operations. Follow on architecture documents will articulate the specific standards critical to ensuring the Army Deployed Tactical Network supports an integrated end-to-end network which supports the Army operational requirements for all echelons during every phase of joint operations.

### 1.4 Unity of Effort

Section 1.2 Background describes the Deployed Tactical Network as a "composite of many different, non-integrated technologies and functional capabilities." It is necessary that the Army synchronize around a common approach for tactical network development and capability integration in order to move integration responsibilities to the enterprise and provide commanders with an integrated network capability. Tactical network architects from the enterprise to the solution level must adhere to central coordinating tenants to achieve Unity of Effort. Particular areas of emphasis are Unity of Effort in network concept development; acquiring, fielding and managing tactical network solutions; and developing the Army Deployed Tactical Network Architecture.

#### 1.4.1 Unity of Effort in Network Concept Development

The deployed tactical network requirements of the Army are derived from the underlying Warfighter conceptual framework developed by Training and Doctrine Command (TRADOC) (see Figure D-2). This conceptual framework traces a sequential focusing of network

requirements from strategic to functional concepts. The LandWarNet Concept of Operation (CONOPS) consolidates conceptual network requirements from functional concepts into a single network concept document. Concepts Plans such as Network Transport and Services are derived from the LandWarNet CONOPS. It is from this conceptual framework that specific Joint Capabilities Integration Development System (JCIDS) documents are developed to implement material solutions.

**Army Concepts.** TRADOC Pamphlets (PAMs) provide the documented requirements for the development and integration of solutions into a joint Warfighting environment, from concept to capability, for all aspects of the future force. TRADOC develops and integrates Joint and Army concepts, architectures DOTMLPF capabilities; validates science and technology priorities; and leads future-force experimentation. The framework for the Army Network architecture evolves from this guidance. See Figure D-2 for a depiction of how the guidance evolves into the network requirements.



Figure D-2: Army Concepts Describe Integrated Network Requirement

### Army Capstone Concept:

TRADOC PAM 525-3-0, The Army Capstone Concept, describes the broad capabilities the Army will require in 2016-2028. It provides details on how the Army will apply available resources to overcome adaptive enemies and accomplish challenging missions. Prioritized capabilities that emerge from this concept and subordinate more detailed concepts will guide changes in doctrine, organization, training, materiel, leader development and programs related to the human dimension for our Army. A central idea to this document is the integration of technology into formations and how the mindsets of leaders, as well as technological developments, must continuously evolve to meet new and unanticipated challenges.

### Army Operating Concept:

TRADOC PAM 525-3-1, The Army Operating Concept (AOC), describes how future Army forces conduct operations as part of the joint force to deter conflict, prevail in war, and succeed in a wide range of contingencies in the future operational environment. It describes the employment of Army forces in the 2016-2028 timeframe with emphasis on the operational and tactical levels of war.

---

### **Army Functional Concepts:**

The following TRADOC PAMs detail the Army concepts for Intelligence, Mission Command, Fires, Protection, Movement and Maneuver, and Sustainment.

- TRADOC PAM 525-2-1, The U.S. Army Functional Concept for Intelligence
- TRADOC PAM 525-3-3, The U.S. Army Functional Concept for Mission Command
- TRADOC PAM 525-3-4, The U.S. Army Functional Concept for Fires
- TRADOC PAM 525-3-5, The U.S. Army Functional Concept for Protection
- TRADOC PAM 525-3-6, The U.S. Army Functional Concept for Movement and Maneuver
- TRADOC PAM 525-4-1, The U.S. Army Functional Concept for Sustainment

**LandWarNet Concept of Operations (CONOPS):** TRADOC PAM 525-5-600, The LandWarNet CONOPS captures the network capabilities requirements identified in each of the functional concepts above, provides a singular network reference across the warfighting functions, and outlines Army network expectations for the future Modular Force of 2015. Most importantly, the LandWarNet CONOPS provides a comprehensive view of the capabilities the Army network must provide to enable the Warfighter. As the Army continues to provide capability enhancements to the LandWarNet, we must remain focused on enabling our Soldiers from the “first tactical mile” all the way back to the operational base.

**Army Concept Capability Plan for Network Transport and Services:** TRADOC PAM 525-7-17, The United States Army Concept Capability Plan for Network Transport and Services for the Future Modular Force 2015-2024 describes “how the future Modular Force will leverage the power of network transport and service capabilities on the future battlefield.” The document addresses network transport and services with a focus from the Soldier all the way through the enterprise to the operational base.

### **1.4.2 Unity of Effort in Acquiring, Fielding and Managing Integrated Tactical Network Solutions**

Using Capabilities Based Assessments (CBAs) or other studies the Army assesses capability requirements and associated capability gaps and risks. Any capability requirements which have significant capability gaps typically lead to an ICD which can then drive development of Capabilities Design Documents (CDDs) and Capabilities Production Documents (CPDs) which represent requirements documents tailored toward a particular materiel approach for a capability solution.

**Agile Acquisition Process:** The Army is transforming its traditional JCIDS approach to acquiring material solutions for the tactical network through the Agile Acquisition Process (See Figure D-3). The Agile Process focuses primarily on filling identified and prioritized capability gaps by integrating emerging technological materiel solutions in iterative, predefined, predictable windows for testing and insertion. These windows are aligned with Army Force Generation, the systematic process whereby brigades equip, train, and deploy. By employing the Agile Process, the Army can keep pace with industry and technological advances, accelerating network modernization to a rate unachievable using traditional acquisition strategies. This acquisition process will seek technology improvements from both large and small industry partners to fill hardware and software needs as determined by requirements analysis.

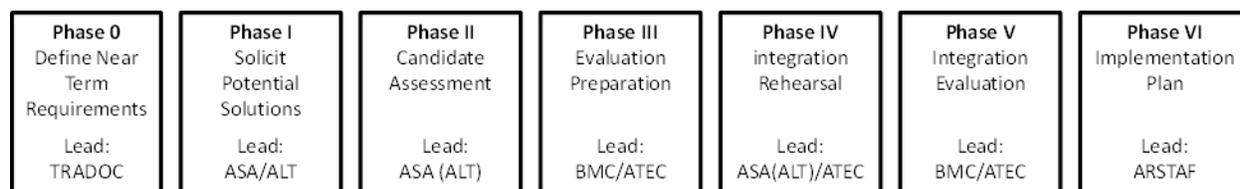


Figure D-3: Army Agile Acquisition Process

Agile acquisition allows the Army to keep pace with the technological development and advances of industry permitting the acceleration of network modernization at a cost and time savings previously unachievable. Most importantly, the process reduces the burden of integrating new individual network solutions from the shoulders of the unit commander by conducting robust integration evaluations in an operational context called a Network Integration Evaluation (NIE).

**Army Forces Generation (ARFORGEN) Process:** The ARFORGEN process offers a predictable model to support a wide variety of planning and decisional factors, to include budgeting and equipment fielding. As a result of this predictability, the Army has chosen to tie network testing, integration, and fielding to the Train/Ready and Deployment force pools of the ARFORGEN process. Aligning Capability Set Management (CSM) and the Agile Acquisition Process to ARFORGEN provides the Army the most logical, efficient, and cost effective method to ensure that those units identified for deployment are provided the latest, and most operationally effective solutions.<sup>4</sup>

**Network Integration Evaluations (NIE):** The NIE is integrated into the Agile Process. It is an adaptive and evolutionary approach to designing, integrating and maturing the Army tactical network through a systematic DOTMLPF approach to evaluating tactical network components. Soldiers, materiel developers (industry and government), research and development personnel, test and evaluation personnel, engineers and trainers all participate in the exercise and inform the recommendations that result. The Army intends for the NIE to facilitate a more integrated and operationally effective Capability Set strategy in support of Army Force Generation requirements. The fiscal year (FY) 13.1 Agile Process Evaluation will expand beyond the network to include other DOTLMPF evaluations beyond the network alone. At that time its name will change to Capability Integration Evaluation (CIE).

Integrated Network Technical Architecture Baseline Guides are developed for each NIE event.

### 1.4.3 Unity of Effort in Operating and Managing the Army Networks

**Joint Information Environment (JIE):** DOD initiative to collapse DOD network interface to the internet, reduce governance and NetOps redundancies and inefficiencies across the Joint and Service networks, increase access and to increase network efficiencies across all mission environments during all phases of joint operations.

<sup>4</sup> Army Regulation (AR) 525-29, Military Operations Army Force Generation, dated 14 March 2011.

---

**Army Network Initiatives:** Army network initiatives to reduce network infrastructure and services redundancies and inefficiencies to increase governance and NetOps across Army organizational and mission boundaries. Initiatives include;

- Modernization
- Visibility and Control of IT expenditures
- Streamline IT Governance
- Agile, Adaptive IT Capability Delivery
- IT Workforce Rebalancing

**Army Cyber Command/2nd Army:** Army Cyber Command/2nd Army plans, coordinates, integrates, synchronizes, directs, and conducts network operations and defense of all Army networks; when directed, conducts cyberspace operations in support of Unified Land Operations to ensure U.S./Allied freedom of action in cyberspace, and to deny the same to our adversaries. Army Cyber Command/2nd Army also serves as the Army's Cyber Proponent and conducts Information Operations. The Army is currently revising its General Orders guidance to incorporate Army Cyber Command's role and relationships and those of its subordinate organizations. Army Deployed Tactical Networks connect to the enterprise through network capabilities operated and managed by Army Cyber Command and other DOD, Intelligence Community (IC), Joint, Service and Commercial network providers.

#### **1.4.4 Unity of Effort in Developing the Army Deployed Tactical Network Architecture.**

The Army is developing 'End State' Enterprise Architecture Guidance for the LandWarNet. The 'End State' guidance will include seven appendices shown in Figure D-4. Figure D-4 is a notional construct to illustrate the relationships between Army 'End State' guidance, emerging agile acquisition process architecture products such as Capability Set Build Guides, NIE Baseline Guides and traditional Operational, Systems and Technical architectures supporting specific programs. At Phase VI of the Agile Acquisition process updates to Operational, Systems, and Technical architectures based on the results of integration evaluations, technology initiatives, Capability Set priorities and the ARFORGEN.

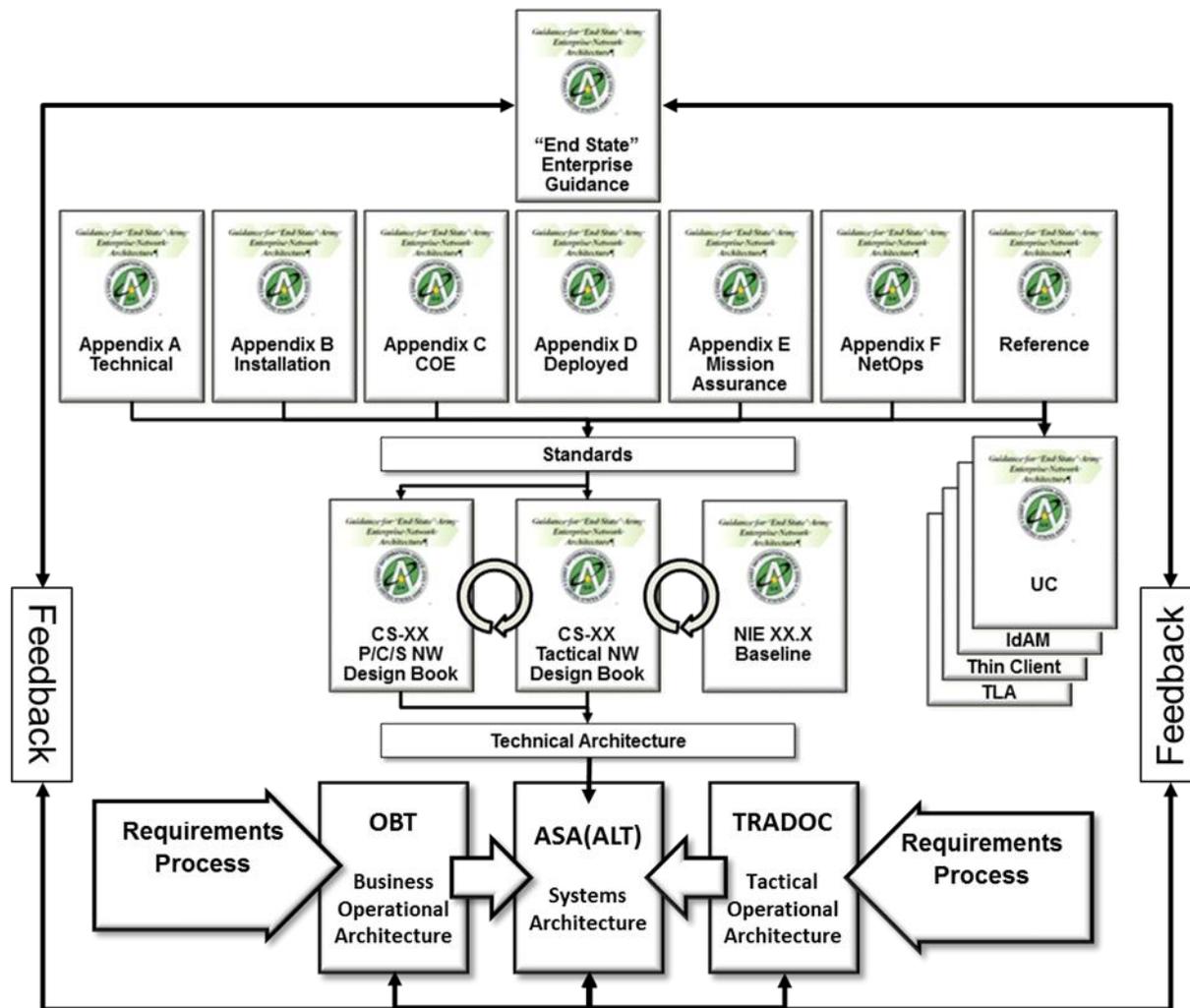


Figure D-4: Notional Deployed Tactical Network Architecture Integration Construct

## 2. Components of the Army Deployed Tactical Network Architecture

The major capabilities of LandWarNet are described as Sensors and Platforms, Transport, Services, Applications, Standards, NetOps and Information Management as depicted in Figure D-5. The Army develops Operational, Systems, and Technical architectures to standardize the development of material solutions to approved requirements for both enterprise and deployed networks. The following discussion describes key components of the Army Deployed Tactical Network Architecture. Appendix D focuses on the relationship of Transport, Services, Applications and NetOps to the computing environment at each mission environment control point to provide common framework for architecture and capability design. Following is a working definition and detailed discussion on each. Network standards are addressed in Appendix A.

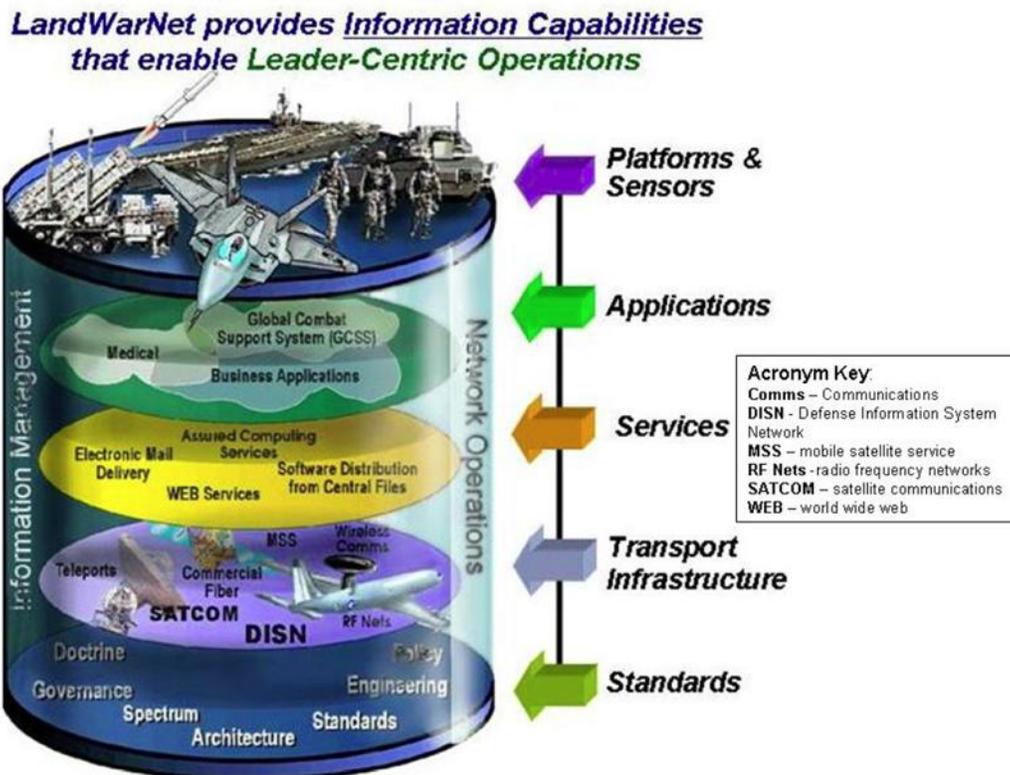


Figure D-5: LandWarNet Capabilities (TRADOC Pamphlet 525-5-600)

## 2.1 Tactical Network Transport

Transport is best described as the system solutions which connect Soldiers, data systems, platforms, and sensors. The transport layer supporting the Deployed Tactical Network is diverse. It includes:

**Satellite:** The satellite transport layer includes military and commercial satellite platforms supporting an equally wide variety of electromagnetic spectrum bands providing Extremely High Frequency (EHF) (Ka band), Super High Frequency (SHF) (K Ku, X, C, and S bands), and Ultra High Frequency (UHF) (S & L bands) spectrum coverage. In the currently deployed force, satellites are the most common connection to enterprise services and applications. Multiple satellite transport systems are found at the command post. Some support mobile leader platforms and provide access to a few dismounted leaders as well. The satellite transport layer offers the most flexibility in supporting the Army goal of extending enterprise network services and capabilities down to the tactical edge.

**Terrestrial:** The terrestrial transport layer includes commercial and host nation global cable and fiber networks, military and commercial microwave line of sight (LOS) relay networks, commercial cellular telephone networks, commercial Wi-Fi networks, broadcast radio, and others. The Deployed Tactical Network terrestrial transport layer is primarily LOS and operates normally in the HF, VHF, and UHF, and SHF Microwave segments, are usually low to medium bandwidth, and found primarily on mobile platforms or carried by dismounted leaders. Primarily due to their relatively low bandwidth and short operational range and the fact they support thousands of users mounted on highly mobile platforms or operating dismounted in a wide

variety of difficult terrain and operational environments, terrestrial transport layers present a problematic technical challenge to the Army goal of extending enterprise network services and capabilities down to the tactical edge. Except for a few Tropospheric Scatter (SHF) beyond LOS (BLOS) systems at the theater level, the Army forces at corps and below are no longer organized, manned or equipped to deploy, sustain and protect remote hill top terrestrial LOS microwave relay sites.

**Aerial:** The aerial transport layer is not a standard transport layer that is factored into day to day network planning. For the near term, the aerial layer is a low density special purpose transport capability that is deployed and managed for specific operational missions. It includes manned and unmanned fixed and rotary winged commercial and military platforms, as well as tethered low altitude and untethered medium and high altitude platforms. Except for short duration, unit owned and operated Unmanned Aerial Vehicles (UAVs); aerial layer platforms are not normally organic to tactical units at the corps and below.

## 2.2 Services

The Deployed Force Network also relies on Joint enterprise services which are extended from the enterprise through transport systems to command posts, platforms, and in some cases to individual dismounted leaders. Services will be described as those enterprise and organic network capabilities which allow deployed tactical users to access enterprise or theater IP and non-IP networks which provide specific network user services.

### 2.2.1 Networks

**IP Networks.** Most IP networks available to the Deployed Tactical Network are enterprise IP networks managed by the DOD (NIPRNET, SIPRNET), Intelligence Community (JWICS and NSANet) to support user communities of interest or levels of classification. These Joint and Joint, Interagency, Intergovernmental, and Multinational (JIIM) IP Networks (sometimes called IP network enclaves) are provided as a service and are extended into Army tactical networks from the enterprise to allow deployed tactical users (with the appropriate permissions) to “access” enterprise, IP based services and collaboration resources. Other IP Networks may be extended to the Deployed Tactical Network based on specific mission or functional requirements. Mission Command networks such as CENTRIX and Allied Networks such as NATO Secret are examples. Certain intelligence functions or even unclassified commercial networks may also require the establishment of separate IP Network enclaves at forward deployed installations, command posts or, under some circumstances platforms.

**Non-IP Networks.** In certain cases, network services can via non-IP or circuit based services. Many of these non-IP network services are residual capabilities or are required by special missions or functions. Deployed commanders must have, or be provided with the required equipment to support the use of these capabilities. Examples include dedicated teleconferencing, circuit based telephony, and others. The Army’s goal is to transition all network access to Internet Protocol over time.

### 2.2.2 Network Services

**Computing.** Appendix C describes the Army computing Common Operating Environment. The computing environment hosts applications and provides the user with the physical devices which allow access to network services and capabilities at every operational echelon during all operational phases.

---

**IP Services.** Voice, data and video collaboration, imagery, geospatial, directory services, content discovery, content delivery, storage, help desk, and others which are delivered by accessing the appropriate IP network.

**Non IP-Based Services.** The Army end state goal is to transition enterprise services to a totally IP based architecture. However, there are some residual services still employed by some Deployed Tactical Network elements.

## 2.3 Applications

In Appendix D, applications are those capabilities developed to satisfy approved Army functional or general purpose information exchange requirements. The underlying software of these general purpose or functional applications should be hardware agnostic and comply with guidance contained in Appendix C and other network standards guidance directives. Applications are hosted on hardware solutions defined in one of the computing environments described in Appendix C. Applications are accessed by users in a number of ways including applications hosted on the user's own computing environment (CE), applications accessed remotely through a virtual network connection, applications accessed through a web or applet interface.

In the current Army Deployed Tactical Network, most Mission Command applications reside on servers and clients organic to the corps, division, brigade or battalion command post. The number of individual applications hosted by the command post network infrastructure has increased significantly in the past ten years. Additionally, the security requirements to host unclassified, secret, top secret and coalition client server networks physically on separate hardware require the commander to replicate the supporting internal command post infrastructure for each level of classification. As a result, command posts have grown larger, are more complex to establish, sustain and are significantly less mobile.

The Army is pursuing a strategy to host business, intelligence and warfighting applications in the enterprise. Striking the right balance between relying completely on enterprise applications and the need for the commander to continue operations when disconnected from the enterprise network will continue to be a challenge for requirements developers, network architects and solution developers. Solution developers will determine the appropriate approach for user access to applications.

The following applications categories are generic and not intended to represent specific application portfolios or doctrinal alignments.

### 2.3.1 Business Applications

This category includes but is not limited to: Enterprise business applications (financial, personnel, logistics, medical); General purpose office applications (document development, spreadsheet, database management); Special Purpose Applications (music, graphics, modeling and simulation, photography, gaming, video); Collaboration and Data Sharing (Voice, email, video teleconferencing, white boarding, imagery).

### 2.3.2 Intelligence Applications

This category includes strategic intelligence capabilities and functions provided by national and joint assets and provided as a service to national and Department of Defense (DOD) forces through classified network access services. Deployed tactical forces access these capabilities and applications through JWICS or other Intelligence Community (IC) networks or they are delivered to deployed commanders via organic networks.<sup>5</sup>

### 2.3.3 Warfighting Applications

This category includes Army, Joint, allied and coalition applications that support Mission Command, Maneuver, Intelligence, Fires, Protection, and Sustainment. Many Army Mission Command and functional warfighting applications are not available through the enterprise as they reside only in the command post. The Army "End State" network goals include transitioning converged OPS-Intel applications to the enterprise to support home station, ARFORGEN and Phase 0 - 5 operations, while retaining the right balance of capabilities at the command post to allow the commander to continue operations when temporarily disconnected from the network.

Note: On 8 March 2012 the Army G-3/5/7 published a memorandum - Subject: Directed Requirement for Operations-Intelligence (OPS-Intel) Convergence for the Common Operating Environment (COE) Computing Environments (CEs).

The overall objective of this directive is the achievement of a common, scalable, and integrated Mission Command (MC) architecture and infrastructure (hardware, services, and applications)

### 2.3.4 Network Operations (NetOps)

Army Deployed Tactical Networks do not operate in a vacuum. The Army depends on NetOps control and support from numerous DOD, IC, Service, Theater, Joint Task Force (JTF) and commercial facilities and organizations. The Army has organized regional Theater Network Operations and Security Centers (TNOCS) under the control of Army Cyber Command/2nd Army and Army Service Component Commands (ASCC) as the Army's primary regional NetOps centers. These TNOCS not only support the generating force networks but also the Army's deployed tactical networks as they enter the enterprise through regional hub nodes. However, there is no guarantee that deployed forces will always be directly under the NetOps management of these Army TNOCS. A more likely scenario is that Army deployed tactical networks will be under the simultaneous direction of several tactical, theater, regional, joint, allied or coalition and commercial NetOps organizations - each controlling their own functional segment of the overall network construct. The DOD is revising its global network strategy under the Joint Infrastructure Environment (JIE) concept. The JIE seeks to place all DOD networks under Joint NetOps control. As this initiative matures the Army will review and adapt its NetOps concepts, doctrine, architecture and supporting infrastructure and organizations to adapt to new guidance and operating models. The desired 'End State' for NetOps includes, reduction in the number of organizations and commands currently implementing NetOps management over elements of the Army networks; consolidation of the plethora of NetOps tools currently employed in managing the Army networks; an integrated network situational awareness of all echelons from dismounted soldier to the enterprise enablers, a robust cyberspace capability with indicators and warning, critical infrastructure protection, and theater security cooperation. The Army Deployed Tactical Network relies almost exclusively on wireless transport systems (space, aerial, terrestrial) therefore effective access to and management of the electromagnetic

<sup>5</sup> Department of the Army Memorandum for Assistant Secretary of the Army (Acquisition, Logistics and Technology), dated 8 March 2012

spectrum is vital. Without the ability to manage wireless network devices and emitters and predict or mitigate electromagnetic interference, commanders can suffer degradation transport system performance and subsequent negative impact on services and applications.

This appendix discusses current NetOps challenges and 'End State' goals for the Deployed Tactical Network. Appendix D NetOps includes all elements of network operations (not just those that support the IP based computing environment) and includes Network: Management, Defense, Content Management, Electromagnetic Spectrum Management, and Situational Awareness. The Deployed Tactical Network Guidance Appendix F (NetOps Architecture) to Guidance for 'End State' Army Enterprise Network Architecture will address NetOps in detail.

**NetOps Staffing.** The deployed commander has only a small network operations staff to coordinate internal support and to interface with theater and enterprise NetOps tiers as part of an integrated end to end network operations capability. It is unlikely that future force design updates will include increased NetOps personnel at the brigade level and below. Therefore, as advances in transport technology allow more access to enterprise network services and applications down to thousands of mobile platforms, dismounted soldiers and sensors, it will become even more important to ensure commanders are provided the NetOps tools and processes to support complex mobile networks that do not require more diversion of already limited resources to support increased NetOps demands.

### 3. Control Points

Control Points are information exchange interface points between two or more CE that enable operational data exchange between ME. Appendix D will use the same Control Point Concept construct defined in Appendix C, Common Operating Environment (See Figure D-6). These Control Points are:

- Control Point (1) – Enterprise to Deployed TOC/Command Post
- Control Point (2) – Enterprise/Command Post to Platform/Leader/Sensor
- Control Point (3) – Enterprise/Command Post to Leader
- Control Point (4) – Platform/Soldier to Sensor

The Control Points represented in Figure D-6 are conceptual in nature but describe CE boundaries that often require different transport, computing, application, services and network operations technological solutions (based on terrain, weather, geographical dispersion, distance, and thread) to support information exchange between the command post, mobile platforms and dismounted soldiers in each of the mission environments. It is understood that adaptations to this initial control point conceptual framework will be required as architectural guidance is implemented over time in the delivery of materiel solutions to requirements. For example, at Control Point 2 in Figure D-6, it is implied that the command post will have unique CE interface requirements with specific (as recently identified by the ASA(ALT) Mounted, Mobile / Hand Held, Sensor, and the Real Time / Safety Critical computing environments on the right side of the first Control Point 2 entry. These environments are depicted by the platform icons in the figure. Likewise, it is implied that the other CE (mounted, mobile, sensor, real time) will have similar complex interface requirements. Figure D-6 also implies that the Command Post will have unique CE interface requirements with the forward deployed installation as well as with enterprise CE and Data Centers in the GIG.

This Appendix focuses on control point interfaces of deployed forces (including forward deployed installations) and does not directly address the control point interface requirements between the command post and the Home Station installation or training environments. That

discussion will be integrated into **Installation Networks**, Appendix B to Guidance for 'End State' Army Enterprise Network Architecture.

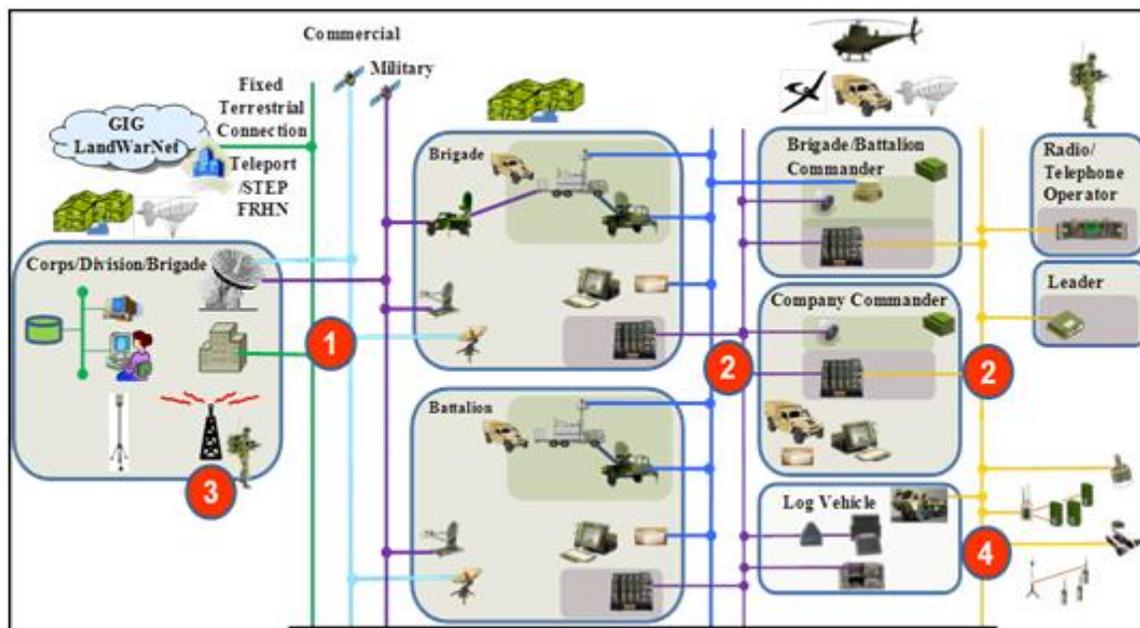


Figure D-6: Control Point Concept

### 3.1 Forward Deployed Installation/Base Transport

In Figure D-3 above the enterprise network capabilities of the Army are represented by the GIG and LandWarNet cloud icon. Enterprise capabilities are also represented in the forward deployed installation or forward operating base represented by the graphic with the radio tower and fixed satellite terminal icon. The employment of forward operating bases (FOB) and combat operating posts (COP) in Iraq and Afghanistan provided a hybrid fixed operational platform supported with a robust mix of commercial off the shelf and tactical network systems. This combination allows commanders and their subordinate forces to enjoy a network environment as close to an Army or Joint permanent installation as possible. Depending on size and geographic location, these forward deployed installations can emulate the capabilities and sometimes the performance of networks at permanent Army installations. Most are managed as a theater asset and are supported by theater capabilities based on local conditions and mission requirements. The senior commander at these installations is, more often than not, a modular force commander (corps, division, brigade, or battalion) who assumes the additional roles and functions of an installation commander to include all of the facilities, life support, force protection, and morale and welfare needs of residents on an installation. The commander relies on his staff to support these additional installation duties. For example, a modular force G/S6 often assumes the role of installation signal officer Network Enterprise

Note: In all of the tables that follow in this paragraph an X indicates a capability available today. An E indicates a desired 'End State' capability.

It is not the intent of this Appendix to represent current acquisition priorities, Basis of Issue (BOE), Tables of Equipment (TOE) for any timeframe, specific echelon or unit. For example, if the term Soldier is used in a table it represents a dismounted Soldier and is not intended to imply either "all" Soldiers or "only" leaders, nor is it intended to refer to a Soldier operating in a specific echelon or radio network.

Center/Directorate of Information Manager (NEC/DOIM) or even the joint task force J6 with all the additional duties and responsibilities that go along with that role. This includes providing network support to installation tenants that are not part of the unit. Sometimes these additional duties and support requirements are augmented by other Army, Joint or commercial contract resources - but not always. Regardless, the planning, management and integration of all network components on the forward deployed installation/base belong to the senior commander's signal support staff. The employment of a forward deployed installation is the base case for the following Control Point discussions. However, the availability of a forward deployed installation or operating base cannot always be assumed in every operational scenario. Forward Deployed Base Transport

Transport solutions employed at the deployed base can vary widely and include, but are not limited to, embedded modular force satellite and LOS systems, theater signal battalion provided satellite and LOS capabilities, joint or other Service satellite terminals, BLOS (Tropospheric Scatter) and LOS (Microwave) capabilities provided by the theater commander as well as contracted commercial satellite and LOS systems. Allies and coalition partners may also provide transport support under certain mission situations. Where possible, local national or commercial wire, cable and fiber optic transport connections may sometimes be available. Commercial mobile telephone, Wi-Fi and other wireless capabilities are employed to provide additional support to the forward deployed base. The use of tethered balloons, radio towers, and other theater unique systems help the forward installation/base network extend the reach of installation/base LOS networks to distances beyond the physical boundaries of the facility. Table D-1 is a generic depiction of transport capabilities by echelon.

Table D-1: Transport

Provider	Capability	Purpose	Command Post					Mobile Platform	Soldier	Sensor
			ASCC	Corps & Div	Brigade	Battalion	Company			
<b>Space Layer</b>										
Commercial	EHF (Ka)	Control Point Support	E							
	SHF(C, X, Ku)	Control Point Support & Mobile C2	X		X	X	X	X		
	UHF (L, S)	Mobile C2	X	X	X	X	X	X	X	
	Broadcast	Control Point Support	X	X	X	E	E			
DOD	EHF (Ka)	Control Point Support	X	E	E	E	E	E		
	SHF (C, X, Ku)	Control Point Support	X	E	E	E	E			
	UHF (UHF, L, S)	Mobile C2	X	X	X	X	X	E	X	
	Broadcast	Control Point Support	X	X	X	E	E	E	E	
<b>Ground Layer (LOS/BLOS)</b>										
Commercial	EHF millimeter wave	Control Point Support	E	E	E					
	SHF Microwave	Control Point Support	X	E	E					
	UHF Microwave	Control Point Support	X	E	E					
	UHF/VHF/HF	Mobile C2	X	X	X	X	X	X	X	
	WiFi	Mobile Computing	X	E	E	E	E	E		
	Wireless Mobile	Mobile Voice/Data	X	E	E	E	E	E	E	

Provider	Capability	Purpose	Command Post					Mobile Platform	Soldier	Sensor
			ASCC	Corps & Div	Brigade	Battalion	Company			
Military	SHF Microwave	Control Point Support	X	X	E	E				
	UHF - Directional	Control Point Support	X	X	E	E	E			
	UHF, VHF, HF	Mobile C2	X	X	X	X	X	X	X	
	WiFi	Control Point Support	X	E	E	E	E	E		
	Wireless Mobile	Mobile Voice/Data	E	E	E	E	E	E	E	
<b>Aerial Layer (LOS)</b>										
Commercial	EHF	Extend the Network								
	SHF	Extend the Network	E	E	E	E	E	E	E	
	UHF	Extend the Network	E	E	E	E	E	E	E	
DOD/Army	EHF	Extend the Network								
	SHF	Extend the Network	E	E	E	E	E	E	E	
	VHF/UHF	Extend the Network	E	E	E	E	E	E	E	
<b>Fiber/Wire/Cable</b>										
Enterprise Commercial	Fiber	Global Access	X							
	Wire/Cable	Global Access	X							
Enterprise DOD	Fiber	Global Access	X							
	Wire/Cable	Global Access	X							
Internal to Command Post or Platform	Fiber	Internal Connect	X	X	X	X	X	X		
	Wire/Cable	Internal Connect	X	X	X	X	X	X		
<b>Legend: X = Current E = End State</b>										

### 3.2 Forward Deployed Installation/Base Services

In the forward deployed installation/base environment Joint and Coalition network services normally include enterprise IP network services such as NIPRNET, SIPRNET, JWICS, NSA Net and theater mission command coalition networks such as CENTRIXS. Enterprise Services such as voice, imagery, collaboration, and messaging and a variety of other IP based services and capabilities are also usually available at forward deployed installations. Table D-2 is a generic example of Enterprise Services available by echelon.

Table D-2: Enterprise Services

Service	Classification	Echelon							
		ASCC	Corps & Div	Brigade	Battalion	Company	Mobile Platform	Soldier	Sensor
<b>IP Network Services</b>									
NIPRNET	Unclassified	X	X	X	X	E			
SIPRNET	Secret	X	X	X	X	E	E		
JWICS	Top Secret	X	X	X	X				
Coalition	Theater Classified	X	X	X	E	E	E		
NSA Net	Top Secret	X	X	X	X				
Internet	Commercial Unclassified	X							
<b>Computing Services</b>									
Application Hosting	Unclassified	X	X	X	X	E			
	Secret	X	X	X	X	E			
	TS/SCI	X	X	X	X	E			
Storage	Unclassified	X	X	X	X	E			
	Secret	X	X	X	X	E			
	TS/SCI	X	X	X	X	E			
Distribution	Unclassified	X	X	X	X	E			
	Secret	X	X	X	X	E			
	TS/SCI	X	X	X	E	E			
Web Access	Unclassified	X	X	X	X	E	E	E	
	Secret	X	X	X	X	E	E	E	
	TS/SCI	X	X	X	E	E	E		
<b>Voice Services</b>									
NON-IP Telephony	Unclassified	X							
	Secret	X							
	TS/SCI	X							
IP Telephony	Unclassified	X	X	X	X				
	Secret	X	X	X	X	E	E	E	
	TS/SCI	X	X	X	E	E			
	Coalition Classified	X	X	X	E	E			
Combat Net Radio	Secret		X	X	X	X	X	X	X
<b>Video</b>									
Broadcast Video	Commercial Unclassified	X	X	E	E				
	DOD Classified	X	X	E	E				
Streaming Video	Secret	X	X	E	E	E			
	TS/SCI	X	X						
	Coalition Classified	X	X						
Dial Video	Unclassified	X							
	Secret	X							
	TS/SCI	X							

Service	Classification	Echelon							
		ASCC	Corps & Div	Brigade	Battalion	Company	Mobile Platform	Soldier	Sensor
Circuit Video	Unclassified	X							
	Secret	X	X						
	TS/SCI	X	X						
IP Video	Unclassified	X	X	X	X	E			
	Secret	X	X	X	X	X			
	TS/SCI	X	X	X	X				
<b>Messaging</b>									
Chat	Unclassified	X	X	X	E				
	Secret	X	X	X	E	E	E	E	
	TS/SCI	X	X	X	E				
White Board	Unclassified	X	X	X					
	Secret	X	X	X	E	E	E		
	TS/SCI	X	X	X	E	E			
DMS	Unclassified	X	X						
	Secret	X	X						
	TS/SCI	X	X						
<b>Imagery</b>									
Intelligence	Unclassified	X	X	X	X				
	Secret	X	X	X	X	E	E		
	TS/SCI	X	X	X	X				
Geospatial	Unclassified	X	X	X	X				
	Secret	X	X	X	X	E	E		
	TS/SCI	X	X	X	E				
Real Time	Unclassified	X	X	X	E				
	Secret	X	X	X	E	E	E		
	TS/SCI	X	X	X	E				
<b>Legend: X = Current E = End State</b>									

### 3.3 Forward Deployed Installation/Base Applications

Users within the forward deployed installation/base footprint have access to (depending on the maturity of the supporting network infrastructure) Enterprise Applications. Other applications are hosted on unit owned and theater provided servers. Users at the forward deployed installation/base are usually able to access Army and Joint enterprise business, intelligence and Warfighter applications with almost the same level of reliability as at home station. Table D-3 is a generic example of applications available by echelon.

Table D-3: Applications

Application	Function	Purpose	Echelon							
			ASCC	Corps & Div	Brigade	Battalion	Company	Platform	Soldier	Sensor
Business	Finance	Force Management	X	X	X	X	E			
	Personnel	Force Management	X	X	X	X	E			
	Medical	Force Management	X	X	X	X	E			
	Word Processing	Office Support	X	X	X	X	E			
	Spread Sheet	Office Support	X	X	X	X	E			
	Database Management	Office Support	X	X	X	X	E			
	Briefing Graphics	Office Support	X	X	X	X	E			
	eMail/Messaging	Mission Command	X	X	X	X	E			
	Training	Force Management	X	X	X	X	E			
Warfighting	Mission Command	Command and Control	X	X	X	X	E	E	E	
	Fires	Indirect Fires Management	X	X	X	X	E	E	E	
		Indirect Fires Forward Observer	X	X	X	X	E	E	E	
		Air Defense	X	X	X	X	E	E	E	
	Maneuver	Position Location	X	X	X	X	E	E		
		Air Space Management	X	X	X	X	E	E		
		Situation Awareness	X	X	X	X	E	E		
	Sustainment	Ammunition	X	X	X	X	E	E		
		Maintenance	X	X	X	X	E	E		
		Supply Management	X	X	X	X	E	E		
		Property Book	X	X	X	X	E	E		
	Intelligence	HUMINT	X	X	X	X	E	E	E	
		Imagery	X	X	X	X	E	E	E	
		SIGINT	X	X	X	X	E	E		
		ELINT	X	X	X	X	E	E		
Protection	Protection	X	X	X	X	E	E	E		
Intelligence	Intelligence	X	X	X	E	E	E			
	Geospatial	X	X	X	E	E	E			
<b>Legend: X = Current E = End State</b> <b>Note:</b> Solution Developer will determine the appropriate approach to user accesses to applications (web enabled, locally hosted, applets, etc.)										

### 3.4 Forward Deployed Installation/Base NetOps

Today, there is no single integrated NetOps system, organization, capability or process at the forward deployed installation/base to support all missions, organizations, or network capabilities and systems. In many cases the senior Army commander's G6 or S6 staff assumes overall NetOps responsibility for the installation which is integrated into a larger theater or regional Joint or Combined Task Force network structure. The forward deployed installation could include a mixture of regional, theater and modular force network systems managed by a separate NetOps staff either located on the installation or at a remote site. Theater provided network support to the forward installation is not always integrated with modular force network management

structures. Contractor provided network support may or may not be integrated with other forward installation network management systems. As a result, NetOps relationships at forward deployed installations are often ad hoc and unique to the theater and the mission and it is not always possible for the unit NetOps team, the Theater Commander's Network Operations and Security Center (NOSC), the theater Defense Information Systems Agency (DISA) Network Operations Support Center (NOSC), or the Army Cyber Command TNOSCS are not always able to deliver an integrated NetOps situational awareness to commanders. As stated earlier the DOD recently initiated the JIE to address this NetOps challenge.

Even at Army command posts functional network systems are not integrated into a single NetOps common operational picture for the commander, his supporting NetOps staff or other NetOps managers at theater, regional and enterprise levels. WIN-T, Trojan Spirit and CSS VSAT, GBS, BFT(JCR), MTS (JCR-L), and others are transport system examples but the problem extends to IP Networks (NIPR, SIPR, JWICS, etc.), applications and services. The ASA(ALT) has initiated several efforts to consolidate transport, mission command, and other systems to provide increased efficiency, operational effectiveness and to achieve an integrated network common operational picture. Table D-4 is a generic depiction of NetOps capabilities by echelon with current and 'End State' capabilities identified.

Table D-4: NetOps

NetOps	Purpose	Command Post							
		ASCC	Corps & Div	Brigade	Battalion	Company	Platform	Soldier	Sensor
<b>Management</b>									
<b>Electro-magnetic Spectrum</b>	Host Nation Coordination	X	X	X					
	Spectrum Planning	X	X	X	E				
	Spectrum Management	X	X	X	E				
	Interference Identification, Reporting & Resolution	E							
<b>Network Management</b>	Network Planning	X	X	X	E				
	Network Engineering	X	X	X	E				
	Network Performance/Fault Management	X	X	X	E				
	Help Desk Support	X	X	X	E				
	Asset Management	E	E	E	E				
	Transport System Management	E	E	E	E				
	Computing Management	X	E	E	E				
	Applications Management	X	X	X	E				
	Services Management	X	X	X	E				
	Identity Management								
Configuration Management	X	X	X	E					
<b>Content Management</b>	Store Information	X	X	X	E				
	Discover Information	X	X	X	E				
	Share Information	X	X	X	E				

NetOps	Purpose	Command Post							
		ASCC	Corps & Div	Brigade	Battalion	Company	Platform	Soldier	Sensor
Computer Network Defense	Policy and Governance	E							
	Host Device Management	X	X	X	X				
	Data Protection Management	X	X	E	E				
	Network Access Management	X	X	X	X				
	Network Intrusion Prevention	X	X	X	E				
	Network Intrusion Detection	X	X	E	E				
Crypto Management	Key Management	X	X	X	X				
	Crypto Planning	X	X	X	X				
Legend: X = Current E = End State									

### 3.5 Forward Deployed Installation/Base Desired End State

Each forward deployed installation/base is unique and the network solutions employed to support the installation are based on mission requirements and available resources. Army Cyber Command/2nd Army and its subordinate NETCOM Theater Signal Commands and Theater Signal Support Brigades (TSSBs) are responsible, when directed, to coordinate the Army's portion of the theater commander's forward deployed installation network augmentation strategy with the Theater or Joint Task Force (JTF) J6. Army Theater Tactical Signal Brigades (TTSBs) (organized under Forces Command (FORSCOM)) and their subordinate Expeditionary Signal Battalions (ESB) are also deployed to augment Army network requirements for Corps, Divisions, JTF Headquarters and those deployed forces who do not have embedded network capabilities. Commercial network augmentation is employed to build out required system processes to ensure the forward installation/base can support tenant network needs and access enterprise network services.

The desired end state for the forward deployed installation is an integrated forward deployed installation/base support network that provides all tenants and operational commanders with:

- The same level of Joint and Army enterprise services as a permanent installation in Continental United States (CONUS).
- Access to host nation or contract provided commercial wireless voice and data services.
- Extended LOS network connectivity to platforms, dismounted Soldiers and sensors operating in the operational vicinity of the installation/base.
- Maximize the use of enterprise capabilities and reduce the burden of routine day to day network management on the local forward deployed installation commander.
- Provide the responsible commander with the ability to shape the installation support and tactical networks to meet local mission requirements.

### 3.6 Control Point 1 – Enterprise to TOC/Command Post

Control Point 1 represents an Army brigade or battalion command post connecting to home station or a forward deployed installation/base from an operational environment well beyond LOS or extended LOS. At Control Point 1 the command post can normally rely only on those network capabilities which are embedded in the organization's force structure or issued specifically for the duration of the mission by the theater commander. Figure D-7 depicts Deployed Tactical Network Control Point 1.

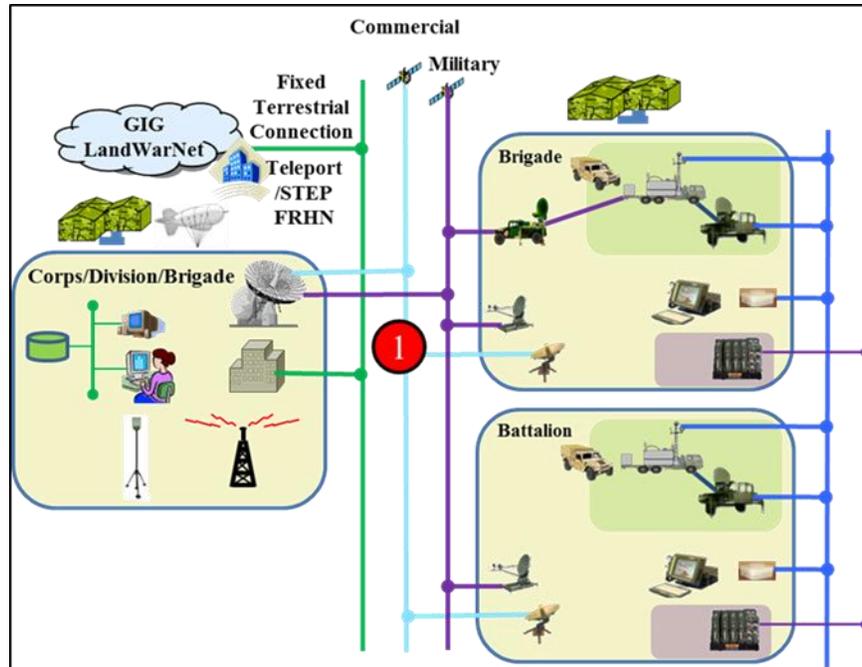


Figure D-7: Control Point 1: Enterprise to TOC/Command Post

#### 3.6.1 Transport at Control Point 1

The brigade or battalion 'at-the-halt' relies on a variety of internal or embedded network transport capabilities to support the commander's information requirements. WIN-T Increment 1, Trojan Spirit, Phoenix Terminal, SMART-T, GBS, CSS VSAT and UHF Tactical Satellite (TACSAT), are some of the key transport systems that support command post connectivity to theater and enterprise capabilities. Many Army brigade and battalion formations do not have embedded network systems that can provide enterprise network connectivity. These units rely on prioritized "pooled" command post network support from theater controlled signal teams provided by the Enterprise Signal Battalion. Blue Force Tracker, Movement Tracking System, UHF TACSAT, Enhanced Position Location and Reporting System (EPLRS), Single Channel Ground to Air Radio System (SINCGARS) and COTS radios such as the Harris PRC-117G are some of the transport systems that provide satellite or LOS command and control connectivity to subordinate formations. In the near future WIN-T Increment 2, the Mobile User Objective System (MUOS), the Joint Tactical Radio System (JTRS) and emerging aerial tier relays will be available to support command post to subordinate unit connectivity. Under some scenarios commercial satellite based systems such as Iridium and International Marine/Maritime Satellite / Broadband Global Area Network (INMARSAT/BGAN) can also be employed to support operational requirements.

---

### 3.6.2 Applications at Control Point 1

Network users at the brigade command post normally have access to enterprise as well as mission command applications. These applications are usually hosted in an Installation Processing Node (IPN). A tactical IPN (T-IPN) is a forward deployed provisioned instance of the high performance computing, storage, or enterprise service in order to meet mission specific performance requirements (T-IPNs might not be high performance computing). However, depending on the robustness of the command post's transport systems, access to enterprise business, intelligence, or logistics applications may compete with Mission Command applications for prioritization of available bandwidth. The ability of any given command post to host mission command applications, general purpose business support applications or other functional applications will depend on the unit's LAN capabilities to support application hosting and internal command post network distribution capabilities. The issue of internal LAN infrastructure is complicated by the number of times the same applications must be hosted and managed in the different classification environments (NIPRNET, SIPRNET, JWICS, CENTRIXS, and others). The Brigade S6 shares application management duties with other key staff sections (intelligence, logistics, fires, maneuver, protect, and others) who are responsible for managing functional applications within the command post. In most cases brigades, battalions and now company commanders have increased their internal application hosting capabilities beyond those outlined in existing Table of Equipment/Modified Table of Equipment (TOE/MTOE) authorization documents through the purchase of additional COTS hardware and software to support requirements. Direct information sharing between applications in the command post is not guaranteed based on current network solutions. The majority of Mission Command (MC) applications were developed as stove piped functional systems. They are not integrated into a system of systems capability to support cross functional or cross security domain information sharing. Cross security domain information sharing is also not guaranteed by existing capabilities. Mobile users (platform and dismounted Soldiers) are not usually able to connect seamlessly to command post network capabilities.

The Army end state goal is to deliver applications that are hardware agnostic and have the capability to increase or decrease functionality as required to conform to the supporting network infrastructure.

### 3.6.3 IP Network Access and Enterprise Services at Control Point 1

At the forward deployed corps, division and brigade command post, most DOD enterprise network services (NIPRNET, SIPRNET, JWICS, etc.) will be available to the command post users equipped with the proper network systems supported by satellite based transport connections. Access to commercial capabilities provided at the forward deployed installation will not always be available. Access to enterprise services (collaboration, etc.) will depend on the availability and capability of the supporting enterprise network service.

### 3.6.4 NetOps at Control Point 1

Network Operations at Control Point 1 is a cooperative effort between the brigade commander and those higher echelon corps, division, theater and enterprise NetOps tiers to which the brigade is connected via available transport systems.

**Brigade.** Today, Army NetOps tools are delivered to the unit based primarily on specific network transport systems because these systems (and the services and applications they support) are provided by different functional staff sections such as the Operations (S3), Intelligence (S2) and Sustainment and Logistics (S4). These staff sections access a variety of

supporting NetOps organizations and supporting entities that are not always part of the theater NetOps infrastructure. An example is Trojan Spirit - a functional intelligence system that provides TS/SCI network capability for a variety of mission critical applications. It has a separate NetOps infrastructure that is not integrated with the Army Theater NOSC, COCOM Regional TNOSC or Defense Information Systems Network (DISN) NOSCS because of its TS/SCI classification. It is managed entirely as a private TS/SCI intelligence network. Another example, CSS VSAT, is managed by a support contractor and is also not an integrated component of the theater network management structure. Today, neither the brigade commander nor his signal officer (S6), his primary NetOps responsible officer, have integrated NetOps situational awareness or control of Trojan Spirit or CSS VSAT systems or the applications and services they bring to the command post. This is also true for BFT (JCR), MTS (JCR-L), GBS and other private functional networks that provide theater or enterprise network support to the brigade and battalion command post. The Maneuver Brigade S6 has a dedicated NetOps team that manages internal NetOps (including network defense) support to the command post and to subordinate battalions and (when equipped) companies. Most multifunctional and support brigades do not have this dedicated NETOPs cell. The Maneuver Brigade S6 has only limited influence over enterprise or theater NetOps and is subject to the directions and restrictions of the higher controlling headquarters. The brigade commander's primary influence is over those systems for which he has direct control (subordinate battalions and companies and attached units) but his influence is always subject to the network operations directions of the higher controlling headquarters. The brigade S6 is also responsible for oversight and management of all non-IP systems and networks that operate within the unit's area of responsibility to include spectrum management, cryptography and software configuration planning and management.

**Battalion.** The battalion S6 does not have a dedicated network operations cell. The battalion S6 follows the network operations direction of the brigade, higher headquarters and of those managers who directly control network assets delivered directly from the theater or enterprise to the battalion (MTS (JCR-L), BFT (JCR), CSS VSAT, Trojan Spirit, UHF tactical satellite (TACSAT) systems, or commercial capabilities such as Iridium). Most non-maneuver battalions do not have satellite enabled IP based networks supporting SIPRNET or NIPRNET access. The battalion S6 is also responsible for oversight and management of all non-IP systems and networks that operate within the unit's area of responsibility to include spectrum management, cryptography, software configuration planning and management.

**Company.** There are currently no requirements supporting network management personnel or NetOps tools at the company level.

### 3.6.5 Control Point 1 Summary

Control Point 1 represents a mission environment in which the command post is connected to the enterprise using only organic network systems. The brigade command post and the battalion command post, for the most part, have access to the capabilities of the enterprise network. This access is directly tied to the ability of the unit's internal network systems to connect to and interact with the enterprise. As mentioned earlier, many tactical brigades and battalions (Multi-Functional and Support) do not possess the internal assets necessary to connect the unit to the enterprise and must be supported by pooled theater assets provided by an Expeditionary Signal Battalion when available. The Army plans to reduce the complexity of supporting transport, applications, internal infrastructure and network management systems and capabilities at the brigade and battalion to help improve the mobility of the command post. The

Army intent is to shift the burden of disparate network systems integration from the commander at his command post to the ASA(ALT) as part of the acquisition process.

The desired end state for the forward deployed Command Posts at Control Point 1 is an integrated network that:

### **Transport**

- Reduce dependence on commercial satellites.
- Integrate satellite transport systems into a single integrated capability that increases mobility, enterprise access and quality of service.
- Integrate LOS systems into a single capability.
- Reduce transport system size and weight and complexity and increase improves sustainability and mobility.
- Provide improved connectivity to subordinate command posts, mobile platforms and Soldiers and sensors that facilitates the seamless sharing of information at all echelons across all mission environments.
- Provide wireless network access to command post local area network.

### **Services**

#### **Computing.**

- Integrate command post computing environment to: reduce redundant systems, improve operational flexibility, increase reliability, reduce size, weight, power requirements and management complexity, improve sustainability and facilitate command post mobility.
- Allow computers from any mission environment to access command post local area networks.

#### **IP Services.**

- Integrate DOD, Intelligence Community, unclassified, secret, top secret, and coalition IP-based networks into an integrated capability that reduces hardware redundancy, improves improve operational flexibility and mobility, increases reliability, reduces size, weight, and power requirements, reduces management complexity, improves sustainability and facilitates command post mobility.
- Extend enterprise services and Unified Collaboration capacities to the brigade, battalion and company command post.

**Non-IP Based Services.** Phase out residual Non-IP based enterprise services.

### **Applications**

- Extend enterprise applications access to the battalion and company command post using most appropriate technology.
- Transition current command-post centric Mission Command applications to the enterprise to support home station training and operations during any phase of joint operations while retaining the ability of commanders to continue operations when disconnected from the enterprise and separated from the command post.
- Provide commanders and staff with one integrated Operations-Intelligence (Ops-Intel) application suite at the command post that can share information directly with mission command applications hosted in a variety of computing devices found at every environment and mission environment.

- Extend converged Ops-Intel and enterprise application access to the battalion and company command posts and mobile platforms.
- Provide applications that are hardware agnostic and adapt to the computing and mission environment network limitations at each echelon.

### NetOps

- Provide the commander with real time network situational awareness for his supporting network whether he controls the assets or not.
- Transition NetOps tools and processes to an end-to-end enterprise capability that simplifies network management functions for all network components at the command post.
- Maximize the commander's ability to shape supporting network to meet changing mission requirements during all phases of joint operations.
- Retain the ability of commanders to continue internal network operations when disconnected from the enterprise network.

### 3.7 Control Point ② – Enterprise/Command Post to Platform/Leader/Sensor

As shown in Figure D-8, at Control Point 2 information is flowing between an at-the-halt command post and individual platforms, leaders or sensors, typically over disadvantaged network links. Here, deployed forces must rely upon embedded network capabilities where system bandwidth limitations become a critical concern for the commander and seriously impact access to enterprise capabilities. At Control Point 2 computing power is not always an issue. Access to enterprise applications and services at Control by the mobile platform and by dismounted leaders and sensors is more than likely limited based on the capabilities of supporting transport solutions based on DOTLMPF and technical limitations. Transport, applications, services and network operations solutions found at Control Point 2 must adapt to the mission realities and adopt those standards and protocols that can most easily facilitate highly mobile operations by aerial and ground platforms and dismounted leaders. The Army goal is to adopt COTS and IP technology at all network echelons whenever possible. Replicating a commercial-like (transport, and NetOps) infrastructure to support these COTS solutions in a highly mobile and potentially hostile activity is problematic because platforms, Soldiers, and sensors are separated by time, distance, weather, and topography. Unlike commercial mobile networks where the supporting infrastructure is fixed and users move within that fixed infrastructure at Control Point 2 the supporting network infrastructure (installed on platforms and carried by leaders) is co-located with and as highly mobile as its users. At Control Point 2, the commander is responsible (except for theater provided capacities such as BFT (JCR) and WIN-T) for installing, operating, maintaining and defending his own network.

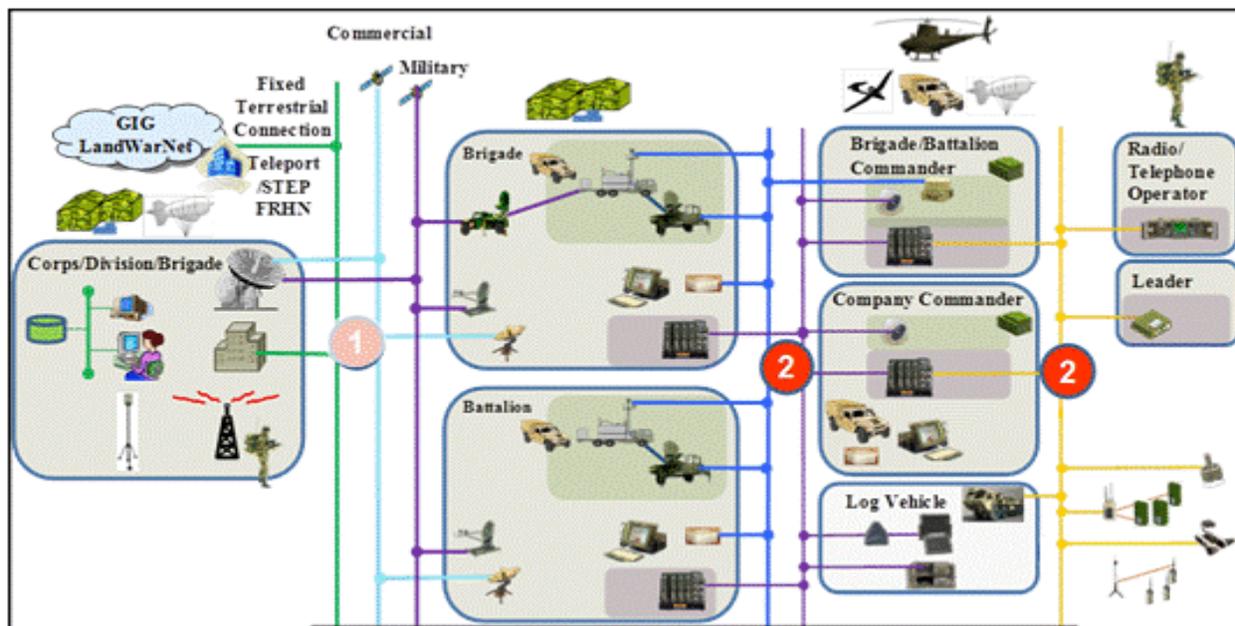


Figure D-8: Control Point 2: Enterprise/Control Point to Platforms and Soldiers

### 3.7.1 Transport at Control Point 2

In the mission environment at Control Point 2 Commanders exercise command and control and users share information using a combination of tactical satellite systems (UHF, BFT (JCR), MTS (JCR-L), WIN-T Increment 2, etc.) and tactical LOS systems primarily WIN T Increment 2, SINCGARS, JTRS or a commercially compatible COTS radio and, in some units, EPLRS. Internal capabilities are available in some organizations that allow retransmission of combat network radio traffic (SINCGARS, etc.) over minor terrain obstacles. Under certain operational conditions, rotary wing and UAV platforms are made available to support network access for ground mobile platforms and leaders. However, aerial platforms have limited flight times, fixed power output and are grounded in adverse weather conditions. The Army is no longer organized, manned or equipped to deploy, sustain and protect remote hill top terrestrial LOS microwave relay sites. Expeditionary Signal Battalions, the only deployable signal battalions that remain in the Army's force structure, are organized to provide command post support to those modular organizations that do not have their own internal network capabilities. ESBs are not equipped to support mobile networks at Control Point 2.

### 3.7.2 Network Services at Control Point 2

Access to enterprise services is limited after Control Point 2. It is unlikely that access to NIPRNET, SIPRNET, JWICS, CENTRIX or enterprise services such as email, identity management, or collaboration capabilities will be available to mobile platforms not equipped with WIN-T Increment 2/3 and perhaps some Intelligence, Surveillance, and Reconnaissance (ISR) network users who will be supported by ISR unique intelligence systems.

---

### 3.7.3 Network Applications at Control Point 2

Commanders and key subordinates leaders at Control Point 2 have very limited access to enterprise applications. Force XXI Battle Command Brigade and Below (FBCB2) is the primary maneuver application available at this Control Point. However, improved tactical computing devices will be capable of hosting more applications at lower echelons than supporting network infrastructure may be able support. The issue for the network architect however, is not the capability of the computing device, which continues to provide more computing power in smaller packages, but the need to rely on LOS and low capacity satellite based transport networks (BFT (JCR), MTS (JCR-L), and MUOS) to support information exchange with enterprise applications. Some platforms equipped with WIN-T Increment 2 and 3 will have a more reliable connection (albeit low bandwidth) to enterprise capabilities. Generally, applications supporting tactical operations at Control Point 2 must conform to the limitations of the capabilities of the supporting network transport systems available to the platform and dismounted Soldier.

Example: A computing device that hosts operating systems and applications to connect to tactical network transport at Control Point 2 could also host the ability to access commercial mobile network capabilities as well. When a dismounted Soldier moves from Control Point 2 to a forward deployed installation/base his computing device should be able to activate the OS that supports access to commercial mobile networks once that network is recognized. An application on that same device that operates at a reduced functionality in a low bandwidth environment at Control Point 2 should be able to adapt to the larger available bandwidth at the installation and deliver increased functionality without significant actions required by the operator. To accomplish this all network components, transport, applications, services and the computing environment must be fully integrated and the NetOps managers and tools at each control point must be able to recognize and support mobile computing devices that transit between control points.

### 3.7.4 Network Operations (NetOps) at Control Point 2

**Brigade** - The maneuver brigade S6 exercises network management for those mobile platform network systems over which he has direct control. However, the maneuver brigade S6 does not operate in a NetOps vacuum. Corps, division, theater and regional Army and Joint network managers all share responsibility for disparate elements of the network.

**IP Networks** - In the future, Control Point 2 will involve thousands of mobile platforms and dismounted soldiers equipped with satellite and LOS transport systems that are capable of supporting routed IP information exchange. Control Point 2 presents the most demanding NetOps challenge for the Army. Today there are very few mobile platforms in the brigade and subordinate battalions and companies that have IP based network systems. In the future WIN-T, JTRS, and commercial network systems that support IP based information exchange will be proliferated in maneuver brigades. Whether the brigade has direct control over the management of these systems will depend on how these mobile platform network systems are employed. Those mobile platforms that are a component of the brigade's network will be managed by the brigade. However, it is possible that mobile platforms operating within the brigade's area of operation will be components of networks not under the direct control of the brigade (MTS (JCR-L), BFT (JCR), some WIN-T, and others).

**Non IP Based Networks** - Significant portions of the Army will continue to be supported by netted LOS radios systems such as SINCGARS with limited data non-IP capabilities.

---

**LOS Supported Networks** - Networks at Control Point 2 will remain primarily Line of Sight (LOS) and as such information exchange between mobile platforms and dismounted soldiers and sensors will be horizontal through numerous interconnected LOS nodes until the data reaches a node that will provide vertical distribution to higher networks via mobile or fixed satellite transport system or where available and aerial relay node. Today most LOS networks in the brigade do not support routed IP networks. In the future, LOS radios (both programs of record and COTS) will be deployed with mobile platforms and dismounted soldiers that will support LOS routed IP information exchange.

**Satellite Supported Networks** - A limited number of key leader platforms in maneuver and some multi-functional and support battalions will be supported by satellite based transport systems (WIN-T, etc.) that will also support routed IP information exchange. At this point routed IP information exchange from LOS systems will transit vertically via IP capable satellite transport equipped nodes to theater networks or even directly to enterprise networks. The brigade S6 will be responsible for overall management of those systems over which he has direct control. He will coordinate with those network managers who control network nodes operating in the brigade area of operation.

**Battalion** - The battalion signal officer (S6) is the primary NetOps manager for organic LOS systems at Control Point 2. The S6 must be capable of planning and providing network operations for all organic network systems in the battalion including satellite transport systems, tactical LOS radio systems, computing environment both in the control point and those used by mobile users, networked applications and sensors. The battalion must be able to remotely load software based radio configurations, system specific frequency assignments, and crypto keys. The battalion must be able to see the supporting radio network and dynamically adapt network topography based on mission requirements

**Company** - There are currently no network management personnel or NetOps tools at the company level. The company commander is responsible for oversight and management of all non-IP based systems and networks that operate within the unit's area of responsibility to include spectrum management, cryptography, software configuration planning and management tools at the company. The network management burden on the company commander will increase significantly as routed IP based network systems are proliferated to mobile platforms and dismounted soldiers and sensors. The company must be able to remotely load software based radio configurations, system specific frequency assignments, and crypto keys, see the supporting radio network and dynamically adapt network topography based on mission requirements.

### 3.7.5 Summary of Control Point 2

Control Point 2 represents the operational environment where leaders and platforms are operating at a distance from the deployed command post (brigade, battalion, company). Transport capabilities are limited to either LOS radio systems (the preponderance of transport systems in the tactical network) or satellite transponder based systems (usually on leader platforms in combat formations). Generally speaking, these systems are constrained by size, weight, and power limitations so that they can be carried by individual Soldiers or can be integrated into already crowded operational platforms. As a result, they may have significantly less bandwidth than transport systems found at the command post. Soldiers and platforms in Control Point 2 are routinely separated from each other by distance, terrain, weather, and continuous movement. This movement and separation complicates network management, further limits bandwidth and can place technical and operational limitations on the ability of

business or warfighting applications (regardless of the computing power of the device hosting the application) to efficiently exchange information across a complex and mobile network. For these and other reasons, Control Point 2 represents the greatest challenge to providing enterprise network capabilities and services to the tactical edge. Because of these mission environment design limitations network systems supporting Control Point 2 may not be as capable as network systems employed at Control Point 1 or at a forward deployed installation/base. At Control Point 2 Network operations depend by and large on LOS which, based on design limitations or physics, have limitations on available bandwidth. Limitations on bandwidth impact the ability of applications to exchange information across extended distances and for mobile or dismounted users to routinely access enterprise services. Although devices with significant computing power will be placed into the hands of Soldiers at Control Point 2 in the near future, these devices cannot overcome the inherent limitations of the supporting network infrastructure. As users move from Control Point 2 to Control Point 1 or to forward deployed installations future computing hosts and supported applications must be capable of adapting (either increasing or decreasing functionality) to the capabilities of supporting mission environment and supporting network infrastructure in which the user is operating.

### **3.7.6 Control Point 2 – Desired End State**

The desired end state for the forward deployed mobile platforms at Control Point 2 is an integrated network that:

#### **Transport**

- Increase mobile platform and dismounted leader access to enterprise network services in all formations and echelons.
- Integrate satellite transport and LOS systems into a single routed IP network that will provide: increased bandwidth, improved network flexibility, increased network reliability, reduced size and weight and management complexity, improved sustainability and facilitate on the move operations.

#### **Services**

##### **Computing.**

- A single integrated computing environment to the platform and dismounted soldier that will support users in all mission environments and control points.
- Host classified and unclassified enterprise, Mission Command and commercial applications.
- Improve operational flexibility, increase reliability, reduce size and weight and management complexity, improve sustainability and facilitate sustained on the move operations.
- Portable outside of the mobile platform.

##### **IP Services.**

- Provide access to unclassified, secret, and coalition IP-based enterprise networks.
- Provide access to enterprise services to the mobile platform and dismounted leaders on the same computing device.

## Applications

- Deliver Mission Command access to the platform and dismounted leader.
- Provide applications that are hardware agnostic.
- Provide applications that recognize and adapt to the mission environment and network limitations at each control point.

## NetOps

- Simplify integrated platform and dismounted soldier network management by providing the battalion and company the ability to simultaneously manage routed IP and non-IP management capabilities.
- Provide the ability to remotely load software enabled radio re-configurations, system specific frequency assignment, and crypto keys.
- Provide the ability to see all components of the network (IP and non-IP).
- Support rapid and seamless hand-off of mobile platform and dismounted soldier network management responsibilities from company and battalion to other organizations as mobile platforms and dismounted soldiers transition between mission environments and control points.
- Maximize the ability of the battalion and company commander to continue network management of large and complex mobile platform networks when disconnected from the brigade, theater or enterprise network.

### 3.8 Control Point ③ – Enterprise/Command Post to Leader

Control Point 3 is unique in that it describes individual Soldiers and platforms operating at a distance from a fixed, stable installation-like environment that is supported by or has access to enterprise DOD and/or commercial networks. These forward deployed installations are often reinforced with network extenders such as tethered aerial balloons, transmission towers, or other technologies that allow platforms or dismounted leaders to maintain connectivity to the forward deployed installation and its network capabilities during operations beyond normal LOS of the installation. Control Point 3 is substantively different from Control Point 2 in that these platforms and Soldiers operating under Control Point 3 conditions retain connectivity to an installation (which may also include a command post) that has enterprise, or at least theater level network capabilities, and potentially have access to network support not available to platforms and Soldiers operating in Control Point 2. Control Point 3 also supports the use of installation self-defense, ground and air command and control, and targeting sensors that are not normally available in Control Points 1, 2 and 4. Figure D-9 depicts Control Point 3 – as the environment where a platform or leader is operating from the vicinity of a forward deployed installation/base.

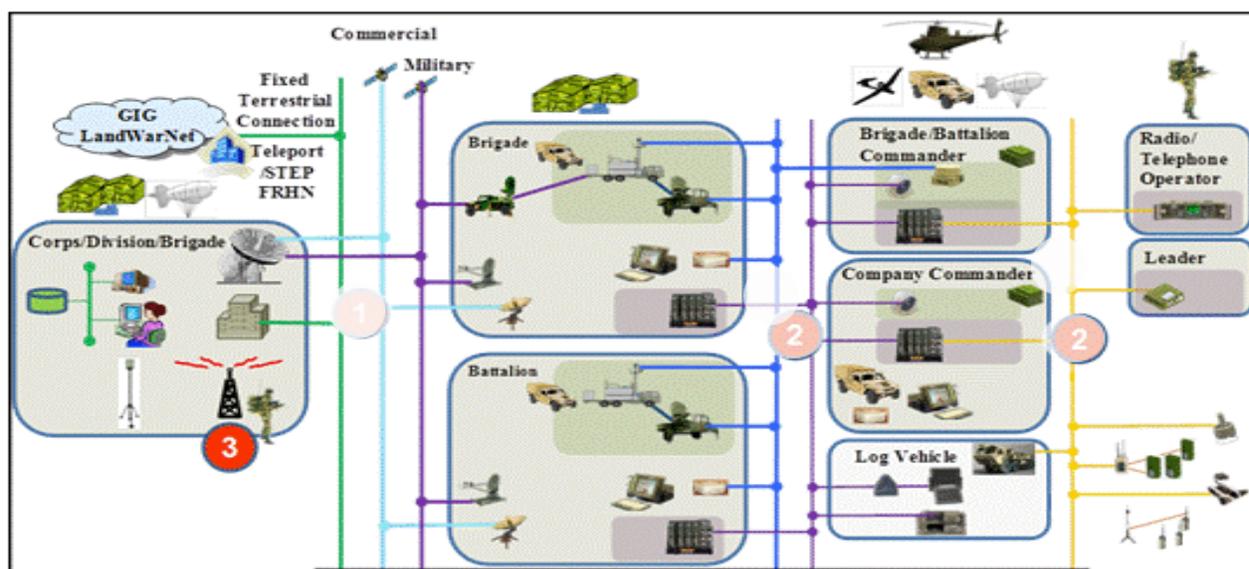


Figure D-9: Control Point 3: Enterprise/Command Post to Soldiers

### 3.8.1 Transport at Control Point 3

At Control Point 3 operations are conducted within a LOS or extended LOS distance from the forward deployed installation/base. Because forward deployed installation/base network capabilities are usually permanent or require increased force protection measures, they are rarely located beyond Control Point 1. Improved transport connectivity provided by the forward deployed installation/base allow commanders to connect mobile platform and dismounted leaders with a wider diversity of network capabilities (applications, services, network operations) and technologies (COTS and commercial) than can be employed by commanders beyond Control Point 1 or Control Point 2.

### 3.8.2 Network Services at Control Point 3

Enterprise services are limited at Control Point 2 because operations are normally conducted from mobile platforms or by dismounted troops. However, if mobile platforms or dismounted Soldiers are operating at Control Point 3 they may have access to improved capabilities supported by forward deployed installation/base network to extend transport and theater provided user devices to mobile users. Mobile users at Control Point 3 may have greater access to enterprise network services such as NIPRNET and SIPRNET and enterprise services (email, identity management, or collaboration capabilities) than when they are operating beyond the installation's boundaries at Control Point 1 or Control Point 2.

### 3.8.3 Network Applications at Control Point 3

At Control Point 2 commanders and key subordinate leaders operating from mobile platforms or conducting dismounted operations do not have routine access to enterprise applications unless that capability is provided by on-board network systems such as WIN T Increment 2. However, at Control Point 3 mobile users can gain greater access to the enterprise if theater provided capabilities, are available. The Army end state goals include applications that adapt to the supporting network and allow mobile platforms and dismounted soldiers to connect to the network seamlessly.

### **3.8.4 NetOps at Control Point 3**

NetOps responsibilities are shared between the responsible installation network provider and the unit signal officer if they are not the same person. For forces operating beyond the gates of the forward deployed installation/base NetOps is likely to be a combination of technologies and processes based on the mix of unit owned and theater provided network support.

### **3.8.5 Control Point 3 Mounted and Dismounted Soldier Mobile Device Vignette**

The Army is currently pursuing the development of a mobile hand held computing device that has the computing power and available software to allow it to adapt to the specifications and operational constraints of a wide variety of Joint, Army and commercial networks. Industry is more than capable of putting significant computing power into the hands of its mobile users. Armed with this computing power users can access a prodigious number of services and applications over current commercially provided wireless networks. However, that user's commercial mobile device is backed up by a highly engineered global wireless transport network that is operated and managed by an equally powerful network operations capability and connected by a robust fiber optic terrestrial infrastructure. It is actually this powerful, fixed, robust network infrastructure that is the key to the availability of today's commercial mobile voice and data computing services. The commercial infrastructure that supports mobile users is fixed, highly engineered and completely stable; it is only the user that is mobile.

Attempting to replicate a commercial-like transport and management infrastructure in an operational environment to deliver enterprise applications and services to thousands of Army mobile platforms and dismounted leaders is a daunting challenge. Of particular concern is that the infrastructure itself – the platforms and leaders themselves - are highly mobile and therefore inherently unstable requiring continuous reengineering as the components of the transport network move through terrain, weather, distance and enemy activity. This is something no commercial network has to deal with. So the greatest design challenge for mobile computing to the tactical edge is not mobile computing technology itself but:

- How to support a network composed of thousands of highly mobile individual users operating in restricted terrain under combat conditions;
- How to enable the computing device and hosted applications to “sense” the capabilities of the network environment in which they are operating and automatically “adapt” to the strengths or limitations of that environment;
- How to deliver network services and support network applications through such a network to empower the applications hosted on mobile computing device;
- How to manage the network in real time with minimal loss of capability; and
- How to accommodate the DOTMLPF impact of this new technology and operational doctrine on the Soldier and the organization's primary operational mission.

### 3.8.6 Control Point 3 Desired End State

Control Point 3 represents the operational environment where mobile platforms and leaders are operating within the LOS or extended LOS distance from a forward deployed installation or base. In this mission environment these mobile users may have access to more enterprise capabilities than they would when operating at Control Point 1 or Control Point 2. The desired end state for Control Point 3 is an integrated network that:

#### Transport

- Increase mobile platform and dismounted leader access to enterprise network services when operating in the vicinity of a forward deployed installation/base.
- Integrate satellite transport and LOS systems into a single routed IP network that will provide: increased bandwidth, improved network flexibility, increased network reliability, reduced size and weight and management complexity, improved sustainability and facilitate on the move operations.

#### Services

##### Computing.

- A single integrated computing environment to the platform and dismounted leader that will support users operating within the vicinity of a forward deployed installation/base.
- Host classified and unclassified enterprise, Mission Command and commercial applications.
- Improve operational flexibility, increase reliability, reduce size and weight and management complexity, improve sustainability and facilitate sustained on the move operations.
- Portable outside of the mobile platform.

**IP Services.** Provide access to unclassified, secret, and coalition IP-based enterprise networks and enterprise services on the same device.

#### Applications

- Deliver Mission Command applications access to the platform and dismounted leader.
- Allow the user to access commercial network applications and websites.
- Provide applications that are hardware agnostic.
- Provide applications that recognize and adapt to the mission environment and network limitations at each control point.

#### NetOps

- Simplify integrated platform and dismounted soldier network management by allowing the network manager at the forward deployed installation/base to seamlessly integrate mobile platform and dismounted routed IP and non-IP users (both internal and external to the parent organization).
- Support rapid and seamless hand-off of mobile platform and dismounted soldier network management responsibilities to other organizations as mobile platforms and dismounted soldiers transition from Control Point 3 to other mission environments.
- Maximize the ability of the network manager to continue network management when disconnected from the theater or enterprise network.

### 3.9 Control Point 4 – Platform/Leader to Sensor

At Control Point 4, individual mobile platforms and dismounted leaders can be connected to and control the activities of a variety of LOS (LOS) aerial and ground mobile or stationary sensors. This mission environment is typically described as Disconnected, Disadvantaged, Intermittent, or Low-bandwidth environment. Information flowing from these sensors is received by the leader or platform and is either consumed by the user at that point or forwarded to other data consumers. Network capabilities (transport, services, applications and NetOps) at Control Point 4 are significantly less capable than at any other point in the network primarily due to limitations of terrain, geographical separation, weather, spectrum, size, weight, and power.

Figure D-10 depicts Control Point 4 where dismounted leaders and mobile platforms control and exchange information with deployed sensors.

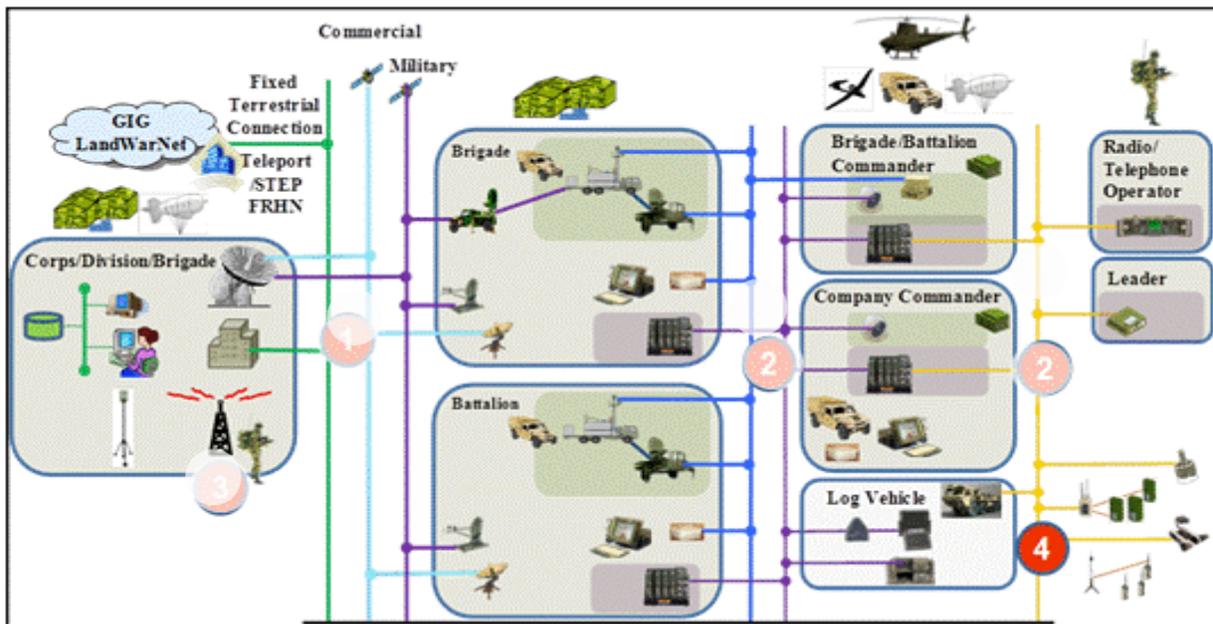


Figure D-10: Control Point 4: Platform/Soldier to Sensor

#### 3.9.1 Transport at Control Point 4

Unit controlled Line of Sight tactical network radios are the primary means of transport at Control Point 4. Special purpose control devices are employed by dismounted Soldiers to operate or monitor aerial or ground sensors. Unattended sensors may have other means of connectivity to other mission environments (i.e. satellite transport) based on special mission requirements.

#### 3.9.2 Network Services at Control Point 4

Network services are generally not available at Control Point 4.

#### 3.9.3 Network Applications at Control Point 4

Applications used at Control Point 4 are unique to the sensor mission.

---

### 3.9.4 Network Operations (NetOps) at Control Point 4

NetOps in Control Point 4 are generally operator managed.

### 3.9.5 Control Point 4 Desired End State

The desired end state for the forward deployed mobile platforms at Control Point 4 is an integrated network that:

**Transport.** Provide integrated network connectivity between sensors and mobile and dismounted users.

#### Services

- Computing. Integrate sensor and mobile and dismounted user computing environment.
- IP Services. None.

#### Applications

- Provide sensor applications that are seamlessly interoperable with mobile and dismounted user applications.
- When possible provide sensor applications that are hardware agnostic.

#### NetOps

- Integrate sensor systems management with other network components at company, battalion and brigade.
- Allow remote sensor management when supported by appropriate transport capabilities.

## 4. Summary and Way Ahead

After more than a decade of expeditionary combat operations, the technological boundaries between the Army enterprise network and its tactical network are becoming increasingly blurred. Today's tactical network is a composite of enterprise and tactical systems and capabilities that are totally interdependent, but not necessarily interoperable. The Army LandWarNet goal is to provide one integrated network that is interoperable across all mission environments and allows commanders at every echelon to shape the network to support operations during all phases of joint operations. Appendix D describes the relationships and inter-dependencies of the computing environment described in Appendix C with network transport, applications, services and NetOps components of the network and to articulate the impact of mission environment on the network hardware and software solutions that provides secure, uniform and interoperable network access to command posts, mobile platforms, dismounted Soldiers and sensors.

---

## TAB A 'End State' Imperatives

### Transport

- Reduce dependence on commercial satellites.
- Integrate satellite transport systems into a single integrated capability that increases mobility, enterprise access and quality of service.
- Integrate LOS systems into a single capability.
- Reduce transport system size and weight and operational complexity and improve sustainability and mobility.
- Provide improved connectivity to subordinate command posts, mobile platforms and leaders and sensors that facilitates the seamless sharing of information at all echelons across all mission environments.
- Provide wireless network access to command post local area network.
- Increase mobile platform and dismounted leader access to enterprise network services in all formations and echelons.
- Integrate satellite transport and LOS systems into a single routed IP network that will provide: increased bandwidth, improved network flexibility, increased network reliability, reduced size and weight and management complexity, improved sustainability and facilitate on the move operations.

### Services

#### Computing.

- Integrate command post computing environment to: reduce redundant systems, improve operational flexibility, increase reliability, reduce size, weight, power requirements and management complexity, improve sustainability and facilitate command post mobility.
- Allow computers from any mission environment to access command post local area networks.
- Deliver a single integrated computing environment to the platform and dismounted soldier that will support users in all mission environments.
- Host classified and unclassified enterprise, Mission Command and commercial applications on the same device.
- Improve operational flexibility, increase reliability, reduce size and weight and management complexity, improve sustainability and facilitate sustained on the move operations.
- Deliver computing devices that are portable outside of the mobile platform.

#### IP Services.

- Integrate DOD, Intelligence Community, unclassified, secret, top secret, and coalition IP-based networks into an integrated capability that reduces hardware redundancy, improves improve operational flexibility and mobility, increases reliability, reduces size, weight, and power requirements, reduces management complexity, improves sustainability and facilitates command post mobility.
- Provide access to unclassified, secret, and coalition IP-based enterprise networks and enterprise services on the same device.
- Extend enterprise services and Unified Collaboration capacities to the brigade, battalion and company command post.

**Non-IP Based Services.** Eliminate residual Non-IP based enterprise services.

---

## Applications

- Extend enterprise applications to the battalion and company command post.
- Transition current command-post centric Mission Command applications to the enterprise to support home station training and operations during any phase of joint operations while retaining the ability of commanders to continue operations when disconnected from the enterprise and separated from the command post.
- Provide commanders and staff with one integrated Operations-Intelligence (Ops-Intel) application suite at the command post that can share information directly with mission command applications hosted in a variety of computing devices found at every environment and mission environment.
- Extend converged Ops-Intel and enterprise application access to the battalion and company command posts and mobile platforms.
- Provide applications that are hardware agnostic and adapt to the computing and mission environment network limitations at each echelon.
- Delivers Mission Command access to the platform and dismounted leader.
- Provide applications that are hardware agnostic.
- Provide applications that recognize and adapt to the mission environment and network limitations at each control point.
- Applications available regardless of ARFORGEN cycle or Joint Operational Phase

## NetOps

- Provide the commander with real time network situational awareness for his supporting network whether he controls the assets or not.
- Transition NetOps tools and processes to an end-to-end enterprise capability that simplifies network management functions for all network components at the command post.
- Maximize the commander's ability to shape supporting network to meet changing mission requirements during all phases of joint operations.
- Retain the ability of commanders to continue internal network operations when disconnected from the enterprise network.
- Simplify integrated platform and dismounted soldier network management by providing the battalion and company the ability to simultaneously manage routed IP and non-IP management capabilities.
- Support rapid and seamless hand-off of mobile platform and dismounted soldier network management responsibilities from company and battalion to other organizations as mobile platforms and dismounted soldiers transition between mission environments and control points.
- Maximize the ability of the battalion and company commander to continue network management of large and complex mobile platform networks when disconnected from the brigade, theater or enterprise network.
- Provide remote software based network asset configuration management, system specific frequency assignments, crypto key and network situation awareness to the battalion and company commander.

## TAB B Acronyms

The acronyms found in this document are presented below:

<b>Acronym</b>	<b>Description</b>
AR	Army Regulation
ARFORGEN	Army Forces Generation
AOC	Army Operating Concept
AOR	Area of Responsibility
BLOS	Beyond Line of Sight
C2	Command and Control
CDD	Capabilities Design Document
CE	Computing Environment
CENTRIXS	Combined Enterprise Regional Information Exchange System
CIO	Chief Information Officer
COE	Common Operating Environment
CONUS	Continental United States
CONOPS	Concept of Operations
COP	Common Operating Picture
COTS	Commercial Off-The-Shelf
CPD	Capabilities Production Document
CPOF	Command Post of the Future
CSM	Capability Set Management
CSS	Combat Service Support
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DOD	Department of Defense
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership Development and Education, Personnel, and Facilities
EHF	Extremely High Frequency
EPLRS	Enhanced Position Location and Reporting System
ESB	Expeditionary Signal Battalions
FBCB2	Force XXI Battle Command Brigade and Below
FOB	Forward Operating Base
FORSCOM	Forces Command
FY	Fiscal Year
GIG	Global Information Grid
IC	Intelligence Community
ICD	Initial Capabilities Document
INMARSAT/BGAN	International Marine/Maritime Satellite / Broadband Global Area Network
IP	Internet Protocol
IPN	Installation Processing Node
ISR	Intelligence, Surveillance, and Reconnaissance
JIE	Joint Information Environment
JIIM	Joint, Interagency, Intergovernmental, and Multinational
JCIDS	Joint Capabilities Integration Development System
JCR	Joint Capabilities Release
JCR-L	Joint Capabilities Release-Logistics
JTF	Joint Task Force

---

<b>Acronym</b>	<b>Description</b>
JTRS	Joint Tactical Radio System
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
LOS	Line of Sight
MC	Mission Command
ME	Mission Environment
MTS (JCR-L)	Movement Tracking System
MUOS	Mobile User Objective System
NEC/DIOM	Network Enterprise Center
NetOps	Network Operations
NIE	Network Integration Exercise
NIPRNET	Unclassified but Sensitive Internet Protocol Network (formerly the Non-Classified Internet Protocol Network)
NOSC	Network Operations Security Center
OPS-Intel	Operations Intelligence
PAM	Pamphlet
SHF	Super High Frequency
SINGARS	Single Channel Ground to Air Radio System
SIPRNET	Secure Internet Protocol Network (Classified)
SMART-T	Secure Mobile Anti-Jam Reliable Terminal Tactical
STEP	Standardized Tactical Entry Point
T-IPN	Tactical-Installation Processing Node
TACSAT	Tactical Satellite
TNOSC	Theater Network Operations Security Center
TOC	Tactical Operations Center
TOE/MTOE	Table Of Equipment/Modified Table Of Equipment
TRADOC	Training & Doctrine Command
TSSBs	Theater Signal Support Brigades
TTSBs	Theater Tactical Signal Brigades
UAV	Unmanned Aerial Vehicle
UHF	Ultra High Frequency
VCSA	Vice Chief of Staff of the United States Army
WAN	Wide Area Network
WIN-T	Warfighter Information Network-Tactical

---

## TAB C References

- [1] Army Posture Statement 2012
- [2] Army Regulation 525-29, Army Force Generation
- [3] Common Operating Environment Architecture, Appendix C, Guidance for 'End State' Army Enterprise Network Architecture, 1 OCT 2011
- [4] Army Campaign Plan 2012 (DRAFT, 14 DEC 2011)
- [5] Army Weapons Systems 2012
- [6] U.S. Army Modernization Plan 2012
- [7] TRADOC PAM 525-5-600, The United States Army's Concept of Operations (CONOPS) - LandWarNet 2015, 11 Feb 2008
- [8] TRADOC PAM 525-3-0, The Army Capstone Concept
- [9] TRADOC PAM 525-3-1, The Army Operating Concept
- [10] TRADOC PAM 525-3-3, The US Army Functional Concept for Mission Command
- [11] TRADOC PAM 525-7-16, The U.S. Army Concept Capability Plan for Electromagnetic Spectrum Operations for the Future Modular Force 2015-2024
- [12] TRADOC PAM 525-7-17, The U.S. Army Concept Capability Plan for Network Transport and Services for the Future Modular Force.
- [13] 2011 Annual Report to the Stakeholders PEOC3T
- [14] Department of the Army Memorandum Achieving Army Network and Battle Command Modernization Objectives, dated December 28, 2009.
- [15] Army Regulation (AR) 525-29, Military Operations Army Force Generation, 14 March 2011
- [16] Department of the Army Memorandum for Assistant Secretary of the Army (Acquisition, Logistics and Technology), dated 8 March 2012.
- [17] Initial Capabilities Document for Network-enabled Mission Command, December 2011.

### Websites Used

<http://architecture.army.mil/>

<http://ciog6.army.mil/ArmyEnterpriseNetworkVision/tabid/79/Default.aspx>

<http://www.cecom.army.mil/armyteamc4isr.html>

[https://secureweb2.hqda.pentagon.mil/VDAS\\_ArmyPostureStatement/2011/aps\\_pages/strategic\\_context.asp](https://secureweb2.hqda.pentagon.mil/VDAS_ArmyPostureStatement/2011/aps_pages/strategic_context.asp)

<http://www.bctmod.army.mil/SoSI/sosi.html>

[https://secureweb2.hqda.pentagon.mil/VDAS\\_ArmyPostureStatement/2011/information\\_papers/PostedDocument.asp?id=353](https://secureweb2.hqda.pentagon.mil/VDAS_ArmyPostureStatement/2011/information_papers/PostedDocument.asp?id=353)

[https://secureweb2.hqda.pentagon.mil/VDAS\\_ArmyPostureStatement/2011/addenda/Addendum\\_L-Network.asp](https://secureweb2.hqda.pentagon.mil/VDAS_ArmyPostureStatement/2011/addenda/Addendum_L-Network.asp)

---

<http://www.bctmod.army.mil/>

[http://www.bctmod.army.mil/development\\_focus/apSlides.html?s=opportunity&mode=form&id=5827cd32f1391ec8b85ae71bcbfe4e6c&tab=core&\\_cview=0](http://www.bctmod.army.mil/development_focus/apSlides.html?s=opportunity&mode=form&id=5827cd32f1391ec8b85ae71bcbfe4e6c&tab=core&_cview=0)

[https://secureweb2.hqda.pentagon.mil/VDAS\\_ArmyPostureStatement/2011/information\\_papers/PostedDocument.asp?id=260](https://secureweb2.hqda.pentagon.mil/VDAS_ArmyPostureStatement/2011/information_papers/PostedDocument.asp?id=260)

[https://secureweb2.hqda.pentagon.mil/VDAS\\_ArmyPostureStatement/2011/addenda/Addendum\\_F-Army%20Force%20Generation%20\(ARFORGEN\).asp](https://secureweb2.hqda.pentagon.mil/VDAS_ArmyPostureStatement/2011/addenda/Addendum_F-Army%20Force%20Generation%20(ARFORGEN).asp)