ATP 6-02.60
3 February 2016

TECHNIQUES FOR WARFIGHTER INFORMATION NETWORK-TACTICAL

DISTRIBUTION RESTRICTION. Approved for public release; distribution is unlimited.

This publication supersedes FMI 6-02.60, dated 5 September 2006, and FM 11-55, dated 22 June 1999.

HEADQUARTERS, DEPARTMENT OF THE ARMY

This publication is available at Army Knowledge Online
(https://armypubs.us.army.mil/doctrine/index.html).
To receive publishing updates, please subscribe at
http://www.apd.army.mil/AdminPubs/new_subscribe.asp

Army Techniques Publication
No. 6-02.60

Headquarters
Department of the Army
Washington, DC, 3 February 2016

TECHNIQUES FOR WARFIGHTER INFORMATION NETWORK - TACTICAL

Contents

Page

PREFACE ..... **iii**

INTRODUCTION ..... **iv**

Chapter 1 INTRODUCTION TO WARFIGHTER INFORMATION NETWORK-TACTICAL **1-1**
Overview 1-1
Increment 1 1-1
Increment 2 1-3
Network Transport 1-4
Tactical Internet 1-5

Chapter 2 SYSTEM DESCRIPTION AND EQUIPMENT **2-1**
System Description 2-1
Increment 1b Components 2-2
Increment 2 Components 2-4
Increment 2 System Allocation 2-13
Communications on-the-Move Capabilities 2-14

Chapter 3 MANAGING WARFIGHTER INFORMATION NETWORK-TACTICAL **3-1**
Department of Defense Information Network Operations 3-1
Distributed Node Management 3-14
Colorless Architecture 3-14
Network Quality of Service and Speed of Service 3-15
Configuration Management 3-17

Chapter 4 INTEROPERABILITY AND EMPLOYMENT **4-1**
Interoperability Between Increments 4-1
Employment of Increment 2 4-1
Employment of Increment 1b 4-4

Distribution Restriction: Approved for public release; distribution is unlimited.

*** This publication supersedes FMI 6-02.60, dated 8 May 2008 and FM 11-55, dated 22 June 1999.**

Training and Exercise 4-6
GLOSSARY Glossary-1
REFERENCES References-1
INDEX Index-1

Figures

Figure 1-1. Key advantages of satellite communications 1-5
Figure 2-1. Satellite Transportable Terminal 2-2
Figure 2-2. Tactical Communications Node 2-7
Figure 2-3. Tactical Relay-Tower 2-9
Figure 3-1. Sample link establishment priorities 3-6
Figure 3-2. Sample High Capacity Line of Sight outage report 3-11
Figure 3-3. Sample satellite communications transmission report 3-12
Figure 3-4. Sample battle drill 3-13
Figure 3-5. Colorless core routing 3-15
Figure 3-6. Sample quality of service table 3-16

Tables

Introductory Table-1. New Army terms iv
Introductory Table-2. Rescinded Army terms v
Table 2-1. Increment 1b system allocation 2-4
Table 2-2. Increment 2 system allocation 2-14
Table 2-3. Communications on-the-move capabilities 2-14

Preface

ATP 6-02.60, *Techniques for Warfighter Information Network–Tactical*, builds on the tactical communications information provided in FM 6-02, *Signal Support to Operations*. This manual establishes non-prescriptive ways to perform missions, functions, and tasks associated with Warfighter Information Network–Tactical (WIN-T) to provide the secure, tactical information network that enables mission command. It also addresses WIN-T increment 2's on-the-move networking and satellite communications capabilities, and introduces the combat net radio gateway that provides transport for the lower tier tactical internet. These capabilities support the commander's mission and intent from division to company.

The principal audience for ATP 6-02.60 is all Army professionals who plan, operate, maintain, and use the WIN-T network. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Trainers and educators throughout the Army will also use this manual.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable U.S., international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement (see FM 27-10).

ATP 6-02.60 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. Terms for which ATP 6-02.60 is the proponent publication (the authority) are marked with an asterisk (*) in the glossary. Definitions for which ATP 6-02.60 is the proponent publication are boldfaced in the text. For other definitions shown in the text, the term is italicized, and the number of the proponent publication follows the definition.

This publication applies to the Active Army, Army National Guard/Army National Guard of the United States, and United States Army Reserve unless otherwise stated.

The proponent for this publication is the U.S. Army Cyber Center of Excellence. The preparing agency is the Doctrine Branch, U.S. Army Cyber Center of Excellence. Send comments and recommendations on a DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, U.S. Army Cyber Center of Excellence and Fort Gordon, ATTN: ATZH-DT (ATP 6-02.60), 506 Chamberlain Avenue, Fort Gordon, GA 30905-5735, or via electronic mail (E-mail) to usarmy.gordon.sigcoe.mbx.gord-fg-doctrine@mail.mil.

Introduction

ATP 6-02.60, *Techniques for Warfighter Information Network-Tactical,* outlines doctrinal techniques for employing WIN-T to support unified land operations. WIN-T is the tactical implementation of the Army's enterprise network to provide warfighters seamless, highly reliable, mobile communications and connect them to the Department of Defense information network (DODIN). It also includes advanced network management tools to help align network resources with the commander's intent and priorities.

To apply the techniques contained in this ATP, readers should be familiar with the Army's capstone doctrine publications (ADP 1, ADP 3-0, ADRP 1, and ADRP 3-0) in order to understand how Army forces operate as part of a larger national effort characterized as unified action. Commanders and network planners should be familiar with, and apply, the military decisionmaking process in ADP 5-0, ADRP 5-0, and FM 6-0. WIN-T implements the tactical portion of the Army network to support the goals of the Army Campaign Plan and other Army and joint mandates. WIN-T establishes an integrated network for deployed Army forces, subject to unit commanders' intent and security policies.

ATP 6-02.60 supersedes FMI 6-02.60, *Tactics, Techniques, and Procedures for the Joint Network Node-Network* and FM 11-55, *Mobile Subscriber Equipment Operations*. The changes incorporate updated concepts, terminology, and DODIN operations techniques.

This publication contains four chapters—

Chapter 1 provides an overview of WIN-T. It begins with the background of WIN-T increment 1; the transition to increment 2; and the characteristics of WIN-T increment 2 that enable mission command on-the-move. Finally, it discusses line of sight and satellite communications network transport, and introduces the upper, mid, and lower tiers of the tactical internet

Chapter 2 discusses WIN-T systems and equipment. It provides a brief description of WIN-T, introduces the equipment and components that make up WIN-T increments 1b and 2, the allocation of WIN-T subsystems, and the communications on-the-move capabilities of the various WIN-T increment 2 node types.

Chapter 3 discusses WIN-T management, including DODIN operations and cybersecurity policies; network defense-in-depth; the network operations and security center (NOSC); network management functions and software; network planning; WIN-T network and node management; colorless core architecture; quality of service and speed of service management; and prioritizing information to align with the commander's intent.

Chapter 4 discusses interoperability between WIN-T increments and employment of WIN-T at each echelon. It introduces the regional hub node that provides global reach; describes WIN-T increment 2 employment at the division and brigade combat team (BCT), and increment 1b employment at the corps, expeditionary signal battalion, and support brigades; and individual, crew, and unit training.

Based on current doctrinal changes, certain terms for which ATP 6-02.60 is the proponent have been added, rescinded, or modified for purposes of this manual. The glossary contains acronyms and defined terms.

Introductory Table-1. New Army terms

Term	*Remarks*
regional hub node	New term and definition

Introductory Table-2. Rescinded Army terms

Term	*Remarks*
MSE Mobile Subscriber Equipment	Rescinded

This page intentionally left blank.

Chapter 1

Introduction to Warfighter Information Network-Tactical

WIN-T extends the Army enterprise network to tactical users. This high-speed, high-capacity network reaches from the sustaining base to company level. This chapter discusses the equipment and techniques of WIN-T increment 1, and the systems and techniques introduced with increment 2. It further discusses WIN-T's network transport using line of sight and satellite communications, and concludes with a discussion of the tiers of the tactical internet.

OVERVIEW

1-1. WIN-T provides commanders and staffs with secure, mobile communications in a deployed environment. It maintains connectivity to the DODIN to ensure situational understanding, enables mission command, and supports all other warfighting functions. WIN-T is an integrated collection of transportable communications equipment that interfaces networking hardware and software with line of sight and satellite communications transport. It provides robust network extension to deployed forces to support unified land operations. It accomplishes this using various subsystems performing specific functions. These systems at the corps, division, brigade, battalion, and company provide a secure, distributed network.

1-2. WIN-T Increment 1 provides high-speed, high-capacity voice, data, and video communications down to battalion level at-the-halt. Increment 2 introduces networking radios; enhances DODIN operations, network planning, and network monitoring; pushes some capabilities to the company level; and supports operation on-the-move as well as at-the halt.

INCREMENT 1

1-3. The WIN-T program restructure in 2007 incorporated the existing Joint Network Node-Network into the WIN-T program as WIN-T increment 1. Increment 1 provides SECRET Internet Protocol Router Network (SIPRNET), Nonsecure Internet Protocol Router Network (NIPRNET), secure Voice over Internet Protocol (VoIP), secure and nonsecure analog phones, Defense Red Switched Network phones, and battlefield video teleconferencing services to tactical users at-the-halt.

1-4. Increment 1 systems include the Joint Network Node, the Command Post Node, the Satellite Transportable Terminal, High Capacity Line of Sight, and the tactical hub node (division headquarters only). For more information about increment 1 systems, see paragraph 2-6, on page 2-2.

INCREMENT 1 EQUIPMENT UPGRADES

1-5. Increment 1 equipment upgrades took place in two steps. The upgraded equipment is either increment 1a (extended networking at-the-halt), or increment 1b (enhanced networking at-the-halt).

Increment 1a

1-6. Increment 1a includes upgrades to WIN-T's satellite communications capabilities. The upgrade added additional satellite communications components to utilize the Ka band capabilities of the Department of Defense (DOD) Wideband Global Satellite Communications satellites in addition to commercial Ku band satellites. This reduces WIN-T's reliance on costly commercial satellite communications bandwidth while allowing the flexibility to augment DOD satellite usage with commercial access when necessary.

Increment 1b

1-7. Increment 1b introduces two new technologies to the existing WIN-T network: the network centric waveform, and colorless core architecture. These upgrades provide communications interoperability with increment 2 systems.

Network Centric Waveform

1-8. The network centric waveform uses multi-frequency time division multiple access and demand-assigned multiple access for internet protocol (IP) over satellite. These techniques allow more efficient bandwidth and satellite use and effectively increase throughput. The network centric waveform modem provides a full mesh network, whether on-the-move or at-the-halt, while supporting terminals with different antenna, power, and transceiver characteristics. These terminals range from the large regional hub node terminals to smaller, tactical (Point of Presence, Soldier Network Extension, Satellite Transportable Terminal, and tactical hub node) terminals. The ***regional hub node*** **is a component of the network service center, which provides a transport connection between the Warfighter Information Network-Tactical and the wider Department of Defense information network.** The network centric waveform modem supports a mobile, distributed network by design. (For more information about the regional hub node, see paragraph 2-15.)

1-9. A multi-frequency time division multiple access satellite network depends on accurate master network timing from one network centric waveform modem acting as a network controller. In order for all terminals in the network to share the allotted satellite bandwidth, the network controller—

- Transmits timing information to each node.
- Controls network signaling and communications traffic between nodes.
- Manages, controls, and allocates those satellite resources (bandwidth and time) assigned in the satellite access authorization for all network signaling and communications traffic.

1-10. Although any network centric waveform modem can logically perform the function of network controller, the number of nodes a small aperture antenna with a single modem can properly manage is limited. The unit NOSC plans the configuration of the multi-frequency time division multiple access network, including the controlling terminal and alternates. All terminals in the network must operate within the power and bandwidth allocated in the satellite access authorization from the regional satellite communications support center. For more information about satellite access authorizations, see Army doctrine for satellite communications.

Colorless Core

1-11. Colorless core is a Defense Information Systems Agency-compliant cybersecurity architecture that offers more efficient IP network encryption and transport. *Cybersecurity* is prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DODI 8500.01) The key benefits of colorless core are data protection and more efficient bandwidth use. Increment 1b added the colorless core technique to existing WIN-T equipment for compatibility between increments 1 and 2. The colorless core architecture encrypts all data, regardless of classification, from end-to-end. This is different from legacy systems that encrypted only classified information.

1-12. The DOD uses color designations to indicate whether data is secure on various parts of the signal path in encrypted networks. The DOD refers to unencrypted (unsecure) data as red, and encrypted (secure) data as black. Legacy systems only encrypted classified data for transmission. With colorless core, both classified and unclassified data undergo encryption before passing over the network transport backbone (the wide-area network). Since all the encrypted information looks the same, an adversary cannot distinguish between the two. This makes the unclassified information just as hard to recover as classified information. It also makes it harder for adversaries to target classified networks for cryptanalysis.

1-13. In the colorless core architecture, data undergoes encryption twice, once at the network layer (communications security) and again at the link layer (transmission security). The data must also undergo

decryption twice. Link layer encryption isolates the network backbone from external networks. For more information on colorless core architecture, see chapter 3, paragraph 3-71.

INCREMENT 2

1-14. WIN-T increment 2 replaces increment 1 in the division and BCT. All other units, including corps, support brigades, and expeditionary signal battalions retain increment 1b (Joint Network Node and battalion Command Post Node).

1-15. WIN-T increment 2 builds on the increment 1b at-the-halt capabilities by adding on-the-move networking in addition to the at-the-halt capability. It also extends the division network down to company level. Increment 2 provides an on-the-move, high-rate network backbone to link warfighters with the DODIN. Increment 2 uses a combination of line of sight (highband networking waveform) and military or commercial satellite communications (frequency division multiple access and network centric waveform) network transport to replace increment 1's satellite communications transport from division to battalion.

HIGHBAND NETWORKING WAVEFORM

1-16. The highband networking waveform is a terrestrial waveform that operates both at-the-halt and on-the-move. It establishes line of sight connectivity down to battalion level. The Tactical Communications Node (TCN), Point of Presence, and Tactical Relay-Tower use the highband networking waveform.

SELF-FORMING, AD HOC NETWORK

1-17. For operational flexibility and reliability, node management software automatically configures individual WIN-T nodes. High-throughput line of sight communications combines with the longer range of satellite communications transport to make up the self-forming network. This self-forming network is an adaptable, moving communications grid that reduces the need for fixed communications infrastructure.

1-18. Ad hoc networks can rapidly deploy to provide communications in a variety of environments without needing pre-existing infrastructure. Communicators can establish the initial network and access Defense Information Systems Network services within minutes. Properly configured nodes can automatically join the network as they arrive or as needed. Each node participates in routing by forwarding data for other nodes. Routing paths are dynamic, based on network connectivity. If there is no predetermined routing path, the network forwards the data using a default route established during network planning. The highband networking radio automatically detects adjacent nodes with the same radio type. The radio maintains a list of active neighbors through which it can communicate, and can calculate the shortest path for transmission.

SELF-HEALING NETWORK

1-19. A key goal of increment 2 is to maintain high-throughput communications transparently to the user, regardless of surroundings and conditions. With legacy technologies, maintaining line of sight communications while traveling over irregular terrain is difficult. Increment 2 nodes use a combination of node design and advanced communications techniques to reduce terrain considerations.

1-20. Networking software continually monitors signal quality over all transmission media. Increment 2 nodes can detect degrading signal quality and switch to an alternate link without operator intervention before losing the signal completely. If possible, the software reestablishes the link through a different Highband Networking Radio within range (except the Soldier Network Extension, which uses only satellite communications). If no Highband Networking Radio is available, the system establishes a satellite communications link.

1-21. Satellite bandwidth is costly, limited, and suffers inherent transmission delay. Because of this, the Highband Networking Radio is the preferred medium for network transport. Satellite-linked nodes continuously poll neighboring Highband Networking Radio nodes for available line of sight connectivity. When a satellite-linked node acquires a usable Highband Networking Radio signal, it automatically establishes a line of sight link and drops the satellite link. WIN-T continues to track the satellite to facilitate reconnection.

1-22. The network always searches for the shortest transmission path in order to pass traffic with the fewest hand-offs between nodes. If it would take too many line of sight links to accomplish timely transmission, the networking equipment may automatically switch to satellite transport as the better option.

1-23. Although the network transitions automatically between line of sight and satellite transmission, the transition is not always seamless. The changeover is relatively quick, but not instantaneous. A satellite communications connection introduces latency due to satellite transmission delay and has a much lower transmission rate, especially using network centric waveform. Changing transmission paths reduce quality of service on streaming tools (unmanned aerial vehicle video, video teleconferencing, VoIP, Ventrillo chat) due to network reconvergence. The network will not lose any data packets, but some streaming traffic may become garbled or suffer buffering delays due to the traffic backlog.

1-24. Because of the increment 2 network's self-healing characteristic, losing a single network node does not affect other nodes in the network. For example, if the battalion headquarters temporarily loses network connectivity, its assigned companies can continue to communicate with the rest of the network.

REACHBACK COMMUNICATIONS

1-25. Both WIN-T increment 1 and increment 2 connect to the DODIN via either the regional hub node or a tactical hub node. Hub node access provides reachback to higher headquarters and the sustaining base, and gateway access to Defense Information Systems Network services. *Reachback* is the process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed (JP 3-30).

NETWORK TRANSPORT

1-26. WIN-T systems' network transport combines line of sight and satellite communications for network reliability, and to best use of the advantages of each. The network backbone prioritizes line of sight (Highband Networking Radio) bandwidth as much as possible to minimize the demand for satellite transmission.

1-27. Satellite communications establishes the initial network connectivity and reachback to access Defense Information Systems Network services. It also provides alternate network transport for uninterrupted connection to critical services.

LINE OF SIGHT TRANSPORT

1-28. WIN-T increment 2 nodes employ line of sight communications both at-the-halt and on-the-move using the Highband Networking Radio. The Highband Networking Radio is WIN-T's implementation of the highband networking waveform to automatically establish ground-to-ground communication. When operating on-the-move, it uses the electronically-steered Highband Radio Frequency Unit antenna for connectivity. For operation at-the-halt, the TCN and Tactical Relay-Tower can use the higher gain Range and Throughput Extension kit to support much greater data rates.

1-29. Once forces establish themselves in theater, the major WIN-T nodes can connect using the High Capacity Line of Sight system to form a high-rate data backbone. The High Capacity Line of Sight system is capable of greater throughput than WIN-T's satellite communications systems (up to 16 megabits per second), but it is limited to line of sight distances (no more than 40 kilometers, or 25 miles, depending on terrain and man-made obstacles). High Capacity Line of Sight systems can only operate at-the-halt.

SATELLITE COMMUNICATIONS TRANSPORT

1-30. Satellite communications provide significant advantages for an expeditionary force. Some of the unique advantages of satellite communications (not specific to WIN-T systems) include—

- Global reach from the national command authority to deployed forces.
- Connection to Defense Information Systems Network services in austere environments with no existing communications infrastructure.
- Immediate access to the DODIN on initialization.
- Access for isolated special operations forces without terrain or distance limitations.

- Long-haul backbone data transport and reachback to the sustaining base.
- Communications that span beyond line of sight distances, terrain obstacles, or hostile forces.
- Mission command communications on-the-move to mobile command vehicles, combat vehicles, and dismounted Soldiers.

1-31. Connecting to the sustaining base via satellite communications transport provides full access to Defense Information Systems Network services as soon as the first nodes establish the network. Despite its advantages, satellite communications also has some drawbacks. Satellite bandwidth is costly, is susceptible to transmission delays, and availability may be limited, particularly in some remote or sparsely populated regions. It is also subject to degradation during severe weather. Figure 1-1 shows the key advantages satellite communications can provide. For more information about satellite communications, see JP 3-14, FM 3-14, and Army doctrine for satellite communications.

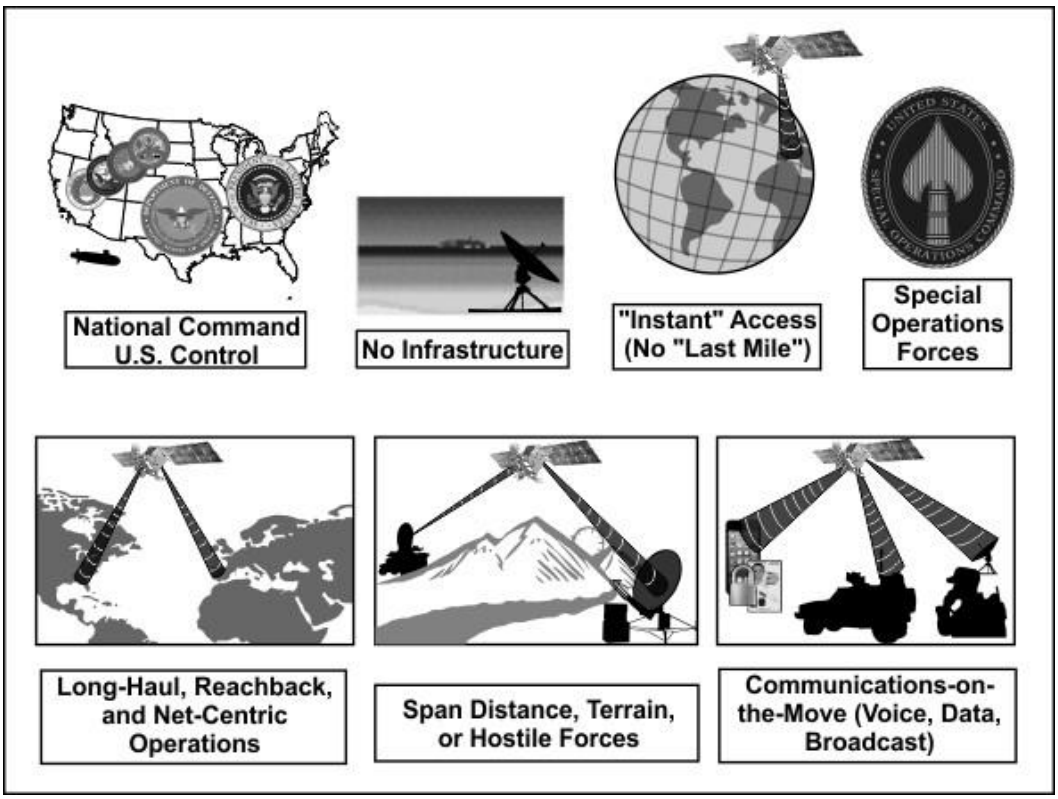

Figure 1-1. Key advantages of satellite communications

TACTICAL INTERNET

1-32. The tactical internet is the deployed communications network. The deployed tactical network is functionally similar to the commercial internet, because the communications infrastructure uses the same technologies. The tactical internet extends home station quality classified and unclassified Defense Information Systems Network services and mission command applications to deployed units.

1-33. At brigade and below, the tactical internet extends critical information services to Soldiers and weapons platforms. From a management standpoint, the tactical internet divides into three logical segments or tiers.

UPPER TIER

1-34. WIN-T provides the upper tier tactical internet, and connects the mid and lower tiers to the DODIN. At the division and BCT, the upper tier tactical internet consists of WIN-T increment 2 resources that provide

networking on-the-move and at-the-halt. The corps headquarters and support brigades use WIN-T increment 1b for networked services at-the-halt only.

1-35. Pooled theater WIN-T increment 1b resources in the expeditionary signal battalions extend network services at-the-halt only for supported units not equipped with WIN-T. DODIN operations personnel at brigade and above perform DODIN operations for the upper tier tactical internet.

MID TIER

1-36. The mid tier consists of organic networking and transmission resources that support battalions and companies. The mid tier provides battalion and company commanders a terrestrial network to process voice and data across their tactical formations.

1-37. The mid tier provides the gateway capability between the upper and lower tiers. It is an interoperability point for higher echelons, joint and aviation integration, and interoperability with joint, interorganizational, and multinational elements. The primary mid tier waveform is the advanced networking wideband waveform. (For more information about the mid tier tactical internet, see ATP 6-02.53).

LOWER TIER

1-38. The lower tier supports company and below formations down to the team leader. It consists primarily of secret radio networks at platoons and companies. The primary lower tier waveforms are the Soldier radio waveform and the single-channel ground and airborne radio system (see ATP 6-02.53).

1-39. The lower tier tactical internet provides transport for mission command information. Mobile applications enable visualization, operator interface with ancillary devices (such as Global Positioning System), targeting data, voice communications, and sensor capability. WIN-T's combat net radio gateway provides a bridge to connect combat net radio voice networks to the mid and upper tiers. Two-channel radios integrate Soldier radio waveform and single channel ground and airborne radio system networks.

Chapter 2

System Description and Equipment

Army and joint operations may require a large volume of data passed over great distances while maintaining flexibility and mobility. Much of the information exchanged is critical, and must be analyzed and used quickly. WIN-T provides voice, video, and data communication tools to meet these requirements at the corps, division, brigade, battalion, and company. This chapter provides an overview of the WIN-T system, introduces the equipment that comprises WIN-T increments 1 and 2, and the capabilities this equipment provides.

SYSTEM DESCRIPTION

2-1. WIN-T is an integrated collection of transportable communications equipment. This equipment establishes and controls communications links to form the upper tier of the tactical network, and connects the mid and lower tiers of the tactical network to the DODIN. WIN-T interfaces networking hardware and software with line of sight and satellite communications transport to provide a secure, distributed network supporting unified land operations.

2-2. WIN-T increment 2's line of sight and beyond line of sight (satellite communications) transport provide redundant transmission paths to enhance connectivity. The network integrates division, BCT, battalion, and company commanders so they can conduct operations while maintaining contact with their higher and adjacent headquarters.

2-3. WIN-T increment 2 provides voice, video and data exchange from Army divisions to BCTs, down to the company level. The network architecture supports the following objectives—

- **Network extension:** Allows division, brigade, battalion, and company leaders to access the Army's wide-area network. This includes beyond line of sight communications capability and links to the mid and lower tier tactical internet.
- **Network mobility:** Facilitates collaboration between division, BCT, battalion command and staff, and their companies in order to plan and conduct operations.
- **Network flexibility:** Provides network resources for each operational phase, and supports moving resources between commands based on time, phase-lines, location, and so forth.
- **Network integration:** Provides interoperability between legacy, current, and planned future networks.
- **Network survivability:** The network provides communications-in-depth using wired and wireless links, line of sight, and satellite communications. Network management software manages bandwidth and transmission paths automatically to bypass outages and congestion. Highband Networking Radios utilize frequency diversity and self-steering antennas. This technology provides self-healing for a more survivable network.

2-4. WIN-T increments 1b and 2 are integrated communications systems that provide network transport and information services and the SIPRNET and NIPRNET local area networks. WIN-T's networking, transport, and DODIN operations components enhance interoperability.

2-5. Increment 2 adds the significant advantage of communications on-the-move without sacrificing backward compatibility with increment 1b systems. Following is an overview of the subsystems that make up WIN-T increments 1 and 2.

INCREMENT 1B COMPONENTS

2-6. WIN-T increment 1b operates at-the-halt only. It provides services using the following major nodes:

JOINT NETWORK NODE

2-7. The Joint Network Node is a vehicle-mounted communications platform that extends network services and provides node management and prioritization. The Joint Network Node connects to either a regional hub node or tactical hub node for gateway access to the DODIN and Defense Information Systems Network services.

2-8. The Joint Network Node connects users to SIPRNET, NIPRNET, secure and nonsecure analog phones, secure VoIP phones, and battlefield video teleconferencing. The Joint Network Node uses either the Satellite Transportable Terminal or the High Capacity Line of Sight radio system for its primary network transport. It can also use a Phoenix satellite communications terminal or Secure Mobile Anti-Jam Reliable Tactical Terminal as alternate network transport.

2-9. The Joint Network Node's backbone connection to the regional hub node uses a dedicated frequency division multiple access satellite communications link. It shares bandwidth among its Command Post Nodes using network centric waveform.

SATELLITE TRANSPORTABLE TERMINAL

2-10. The Satellite Transportable Terminal is a trailer-mounted, 2.4-meter Ku and Ka band satellite communications terminal. It provides beyond line of sight network transport for the Joint Network Node and Command Post Node. The Satellite Transportable Terminal operates at-the-halt only.

2-11. There are two versions of the Satellite Transportable Terminal. One uses both frequency division multiple access and time division multiple access modems. This version supports the Joint Network Node shelter. The second version uses time division multiple access only, and supports Command Post Nodes. The Satellite Transportable Terminal can operate using a trailer-mounted generator. Units should not rely on the onboard generator for primary power, but should operate using an external 10-kilowatt generator whenever possible. Figure 2-1 shows the Satellite Transportable Terminal operating with an external generator.

Figure 2-1. Satellite Transportable Terminal

HIGH CAPACITY LINE OF SIGHT

2-12. The High Capacity Line of Sight terminal provides alternate network transport for the Joint Network Node and Command Post Nodes. The High Capacity Line of Sight radio is a terrestrial microwave radio system capable of up to 16 megabits per second data throughput, depending on the radio band selected. Each High Capacity Line of Sight system has either two (LOS V1) or four (LOS V3) line of sight radios. Its maximum range is 25 miles, depending on terrain. The High Capacity Line of Sight system interfaces with the Joint Network Node shelter via the flex multiplexer, fiber optic modem, or Tactical Fiber Optic Cable Assembly. The High Capacity Line of Sight terminal provides much greater throughput and lower operating cost than the Satellite Transportable Terminal, but it is limited to line of sight ranges (under 40 kilometers).

COMMAND POST NODE

2-13. The Command Post Node provides SIPRNET, NIPRNET, secure and nonsecure VoIP, battlefield video teleconferencing, and analog telephone services. It supports static battalion command posts. It accesses the DODIN through either satellite communications or High Capacity Line of Sight link to the Joint Network Node, or satellite communications to the hub node.

2-14. The supported battalion's communications staff officer (S-6) controls network services from the command post. The supported unit supplies its own Army Battle Command Systems and information technology equipment. Therefore, the supported unit sets up and operates this equipment with technical oversight from their S-6.

REGIONAL HUB NODE

2-15. The regional hub node's network transport extends Defense Information Systems Network services to deployed WIN-T enabled units. Regional hub nodes provide the primary communications connection between operational forces and the sustaining base. Major WIN-T nodes can connect to the regional hub node using either military (X or Ka band) or commercial (Ku band) satellites.

2-16. A typical regional hub node can support up to 3 Army divisions and 12 separate enclaves (such as BCTs, support brigades, or joint users), or 56 discrete missions simultaneously. Distributed geographically, the regional hub nodes are collocated with selected DOD gateways. They operate in sanctuary (outside the combat zone) for access to Defense Information Systems Network services. Regional hub nodes' strategic positioning provides global coverage to give Soldiers immediate access to secure and nonsecure data and voice communications. This allows them to do their jobs wherever their mission takes them. These missions may be close to home station or in austere environments where communications infrastructure often does not exist. Regional hub node access allows forces to mobilize without having to develop their own network access solutions. The regional hub node's full-time operation allows deploying units to establish reachback communications much quicker. A unit may be able to establish their initial communications capabilities within minutes, rather than hours or days as with legacy systems.

2-17. A regional hub node permanently connects to a tier 1 network. Its Ka (military) and Ku (commercial) band satellite communications capabilities extend access to the Defense Switched Network, mission partner environment, SIPRNET, NIPRNET, secure VoIP, data, and video teleconferencing. The regional hub node's frequency division multiple access, time division multiple access (Linkway), and network centric waveform satellite communications capabilities are compatible with all increment 1a, 1b, and 2 node types. The regional hub node provides master reference timing for time division multiple access and network centric waveform networks. Regional hub nodes provide enclave boundary protection (tier1 to tier2; SIPRNET to NIPRNET). The regional hub node's equipment also includes colorless core routers and type 1 encryption devices. The regional hub node's network centric waveform modems and colorless core routers support increment 1b and increment 2 satellite communications links. (For more information about tiers 1 and 2, see Army doctrine for communications security.)

2-18. In addition to WIN-T increment 1b and 2, regional hub nodes can also provide Defense Information Systems Network access to U.S. Marine Corps units operating their Support Wide Area Network. The Support Wide Area Network provides WIN-T like capabilities to deployed Marine units.

TACTICAL HUB NODE

2-19. Division headquarters also have a mobile version of the hub node. The tactical hub node is the central element of the increment 1 network. In increment 1, the tactical hub node links deployed Joint Network Nodes and battalion Command Post Nodes via satellite communications transport, while providing communication interfaces to other fixed and deployed networks. The tactical hub node can extend Defense Information Systems Network and mission command services to subordinate BCTs where regional hub node service is not available. It may also augment a regional hub node.

2-20. The tactical hub node supports the organic WIN-T systems of one division. It merges the time division multiple access and frequency division multiple access satellite network architectures. It provides end-to-end network transport to extend Defense Information Systems Network services to the deployed tactical network. The tactical hub node consists of three major subsystems—one baseband shelter and two time division multiple access and frequency division multiple access capable satellite communications shelters. The satellite communications shelters provide master network timing for time division multiple access networks. In order to extend Defense Information Systems Network services, it normally deploys to a DOD Gateway site. When not located at a DOD Gateway site, the tactical hub node connects via a satellite communications link to the DOD gateway for access to Defense Information Systems Network services.

INCREMENT 1 SYSTEM ALLOCATION

2-21. WIN-T uses standardized system configurations, according to the function and echelon of the unit. Table 2-1 shows WIN-T increment 1b system allocation within the corps, division, expeditionary signal company, and joint/area signal company.

Table 2-1. Increment 1b system allocation

Increment 1 Nodes	*Corps Signal Company*	*Division Signal Company*	*Expeditionary Signal Company*	*Joint/Area Signal Company*
Tactical Hub Node	—	1	—	—
Joint Network Node	3	3	2	—
Command Post Node	—	—	10	4
STT	3	3	12	6
High Capacity Line of Sight	3	3	8	3
Single Shelter Switch	—	—	—	2
Legend: STT Satellite Transportable Terminal				

INCREMENT 2 COMPONENTS

2-22. Most of the components and subsystems of WIN-T increment 2 are completely different from those of increment 1. The increment 1 subsystems were designed from the outset for operation at-the-halt. The newer increment 2 nodes enable mission command on-the-move.

TACTICAL HUB NODE

2-23. Divisions equipped with WIN-T increment 2 retain the upgraded tactical hub node, which can provide alternate reachback capability in case regional hub node service is not available. However, increment 2 divisions' tables of organization and equipment no longer include designated personnel to support the tactical hub node. The unit is responsible for operating their hub node within their existing personnel authorizations.

TACTICAL COMMUNICATIONS NODE

2-24. The TCN is the core of the increment 2 network. It provides network services using line of sight and satellite communications transport, both on-the-move and at-the-halt. It interfaces with the High Capacity Line of Sight terminal and Satellite Transportable Terminal with upgrade kit (STT+) to provide higher data

rate network transport at-the-halt only. The TCN provides the greatest capabilities of any increment 2 node. The following unit types have TCNs—

- Division headquarters.
- BCT headquarters.
- Maneuver battalions.

2-25. TCNs may be paired with a Tactical Relay-Tower and/or a NOSC. A Vehicle Wireless Package and an STT+ always accompany the TCN. A TCN can also interface with a Secure Mobile Anti-Jam Reliable Tactical Terminal or High Capacity Line of Sight terminal.

2-26. The TCN's capabilities include—

- **Unified Communications Manager**. Performs SIPRNET and NIPRNET VoIP call control. It also acts as an IP private branch exchange to provide call forwarding, call transfer, redial, and conference bridging.
- **Combat net radio gateway**. Connects combat net radios to a VoIP network.
  - Provides a half-duplex connection between the combat net radio and the WIN-T IP infrastructure.
  - Capable of interfacing two different combat radio networks through the WIN-T network.
  - Provides telephone signaling and conversion from analog to digital.
  - Extends combat net radio ranges beyond line of sight using WIN-T's satellite communications transport.
- **Ethernet switches**. Interface the SIPRNET and NIPRNET local area networks to the wide-area network. The Ethernet switches also provide power over Ethernet for IP phones. Power over Ethernet eliminates the need for power adapters when connecting IP phones to the switches. Both the switch and the telephone equipment must be power over Ethernet capable.
- **Flex multiplexer**. A multi-channel, synchronous time division digital multiplexer and fiber optic modem with Tactical Fiber Optic Cable Assembly connections for line of sight interface.
- **Global Positioning System input/output block**. Provides positioning data and system timing.
- **Highband Networking Radio**. Delivers high rate data throughput on-the-move and at-the-halt. It enables automatic connection to other Highband Networking Radio-equipped nodes.
  - Highband Radio Frequency Unit is a directive-beam, C band antenna that supports high rate data, both on-the-move and at-the-halt.
  - The Range and Throughput Extension Kit is a fixed-beam, higher-gain antenna, which operates at-the-halt only.
- **Inertial navigation unit**. Provides continuous, accurate vehicle position, velocity, and attitude reporting to improve the Highband Radio Frequency Unit antenna's pointing accuracy. This allows on-the-move antennas to react to vehicle motion and maintain accurate pointing.
- **Local access waveform radio system**. Provides 802.16-compliant (WiMAX) wireless access on-the-move.
  - Point-to-multipoint local access waveform radio extends the local area network to the Vehicle Wireless Package.
  - Local access waveform base station can support two Vehicle Wireless Packages simultaneously.
  - Maximum range is 4 kilometers (2.5 miles) at-the-halt, and 800 meters on-the-move.
- **Network centric waveform modem**. Uses spread spectrum, multi-channel modulation and demodulation, advanced turbo coding, and advanced encryption standard for satellite communications interface.
- **Routers—**
  - **Colorless (wide-area network)**. Cryptographically isolated from the SIPRNET and NIPRNET local area network routers. It serves as cybersecurity perimeter protection. The colorless router includes embedded firewalls and intrusion detection system.
  - **SIPRNET and NIPRNET (local area network)**. Routers include embedded intrusion detection system modules.

- **Secure wireless local area network**.
  - The secure wireless bridge access point allows a unit to set up its command post without running cables for each workstation. It combines the functions of a wireless access point, wireless bridge, Ethernet switch, and security gateway. Its design allows operation in harsh environments.
  - 2.4 gigahertz mast amplifier.
  - 2.4 gigahertz omnidirectional antenna.
- **TACLANEs**. Encrypt and decrypt SIPRNET and NIPRNET traffic for transmission over the wide-area network. The plain text side connects to SIPRNET and NIPRNET switches; the cipher text side connects to the colorless router.
- **Enhanced Position Location Reporting System**. The TCN can interface with user-provided Enhanced Position Location Reporting System equipment.
- **Satellite communications antenna**. This antenna is mounted on the roof of the shelter. It uses Global Positioning System data and the inertial navigation system to track geostationary Ku or Ka band communications satellites while on-the-move.
- **Prime Power**.
  - An on-board 15-kilowatt diesel generator supports operation while on-the-move.
  - Either the towed, 30-kilowatt generator or utility power provides prime power while at-the-halt.
- **User access cases**. Two user access cases (SIPRNET and NIPRNET) with uninterruptible power supplies. The user access cases provide digital and analog voice, and digital data subscriber access ports for users at static command posts. Each user access case provides 48 Ethernet ports and 24 2-wire analog telephone ports. The user access cases have no transmission capabilities, so the TCN provides their network transport. Figure 2-2, on page 2-7, shows the TCN operating at-the-halt.

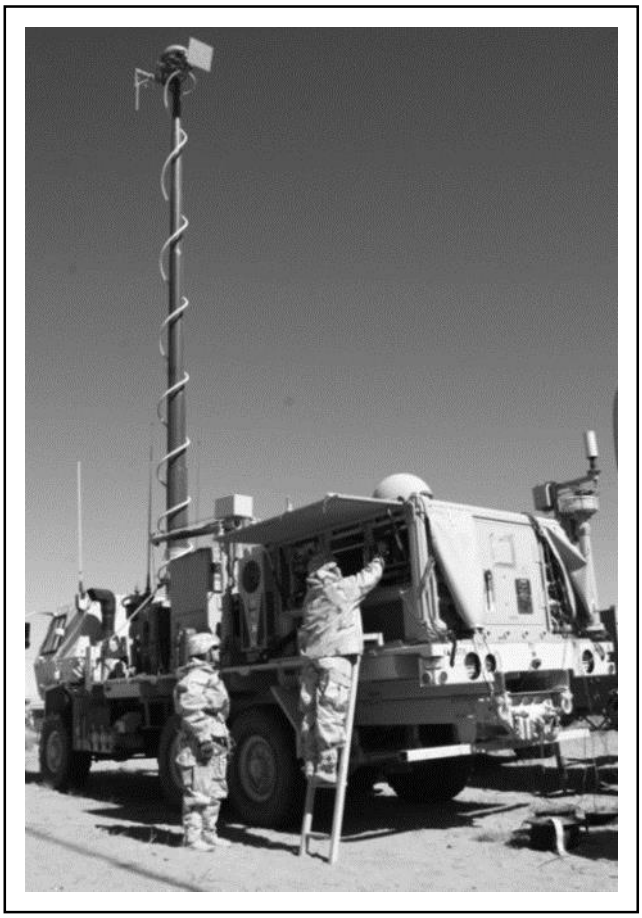

Figure 2-2. Tactical Communications Node

SATELLITE TRANSPORTABLE TERMINAL WITH UPGRADE KIT

2-27. The division, brigade, and battalion usually employ the STT+ in conjunction with a TCN. The larger antenna of the STT+ supports greater data throughput for operation at-the-halt than the built-in mobile antennas on the TCN, Point of Presence, and Soldier Network Extension.

2-28. The STT+ provides network transport for the colorless router. There are no direct user access ports at the STT+, so it has no SIPRNET or NIPRNET enclave connections.

2-29. The distributed computing element server with the STT+ uses a laptop computer for local node management. The distributed computing element manages local devices, and monitors and manages the transmission medium.

2-30. The STT+ is capable of frequency division multiple access, time division multiple access (Linkway), and network centric waveform operation. Even though the STT+ associated with the battalion TCN has the same capabilities, using frequency division multiple access at each battalion would exceed the regional hub node's support capabilities. For this reason, the battalion STT+ normally uses only network centric waveform.

2-31. Two additional versions of the satellite transportable terminal are fielded to some units. They are the satellite transportable terminal high power, generation 1 and 2. These higher-powered terminals use 400-watt power amplifiers and differ only in the size of the equipment cabinets mounted on their associated trailers. Since their method of employment is the same as the STT+, further references to the STT+ in this publication may apply to any of these three versions.

NETWORK OPERATIONS AND SECURITY CENTER

2-32. The NOSC uses a TCN for network connectivity. The TCN routes data between network devices, network links, and the NOSC. This allows the NOSC to monitor network status. DODIN operations personnel analyze status information so they can effectively mitigate adverse events on network devices or links.

2-33. The WIN-T NOSCs include subsystems for network planning, administration, monitoring, and response in the SIPRNET, NIPRNET, and colorless enclaves. The NOSCs include external modular command post facilities to support the S-6 and assistant chief of staff for communications (G-6) staffs. WIN-T increment 2 includes two versions of the NOSC: the NOSC-Division, and the NOSC-Brigade. Each NOSC conducts DODIN operations in its corresponding portion of the network. The NOSC provides these monitoring and operations capabilities in the colorless, SIPRNET, and NIPRNET enclaves—

- Colorless—
  - Wide-area network management.
  - Network management.
  - Virtual machine management.
- SIPRNET—
  - Cybersecurity device management.
  - Wide-area network management.
  - WIN-T network management.
  - Key management.
  - Virtual machine management.
  - Inline network encryptor management.
  - Service desk management.
  - Desktop configuration management.
  - Spectrum management (see Army doctrine for spectrum management).
  - Network management.
- NIPRNET—
  - Cybersecurity device management.
  - Wide-area network management.
  - Operations management which includes, event monitoring, performance tracking, security policy enforcement, and an auditing capability.
  - WIN-T network management.
  - Inline network encryptor management.
  - Service desk management.
  - Desktop configuration management.
  - Network client management.

2-34. The NOSC is also equipped with three access cases (SIPRNET, NIPRNET, and colorless) with uninterruptible power supplies for use while at-the-halt. The SIPRNET and NIPRNET user access cases provide digital and analog voice, and digital data subscriber access ports for users at static command posts. Each user access case provides 48 Ethernet ports and 24 2-wire analog telephone ports. User access cases have no transmission capabilities, so the TCN provides network transport.

TACTICAL RELAY-TOWER

2-35. The division and brigade headquarters each have a Tactical Relay-Tower. It operates either as a standalone unit, or in conjunction with a collocated TCN. It extends the range of a Highband Networking Radio network to as much as 30 kilometers with an unobstructed line of sight. The Tactical Relay-Tower operates at-the-halt only. The Tactical Relay-Tower sends and receives backbone data over the colorless enclave. The Tactical Relay-Tower provides no network capabilities or user services for either SIPRNET or NIPRNET.

2-36. The Tactical Relay-Tower's transmission subsystem consists of a Highband Networking Radio for high-capacity ground-to-ground communications with other Highband Networking Radios. It operates as part of a mobile, ad hoc, wireless wide-area network. The radio uses time division duplex/time division multiple access highband networking to provide bandwidth-on-demand. It uses two receive and transmit antennas – the Highband Radio Frequency Unit-C band antenna, and the directional Range and Throughput Extension Kit.

2-37. The trailer-mounted Global Positioning System input/output block and the inertial navigation unit at the top of the antenna mast provide positioning information. The antennas and Network Management System use the positioning information. Figure 2-3 shows the Tactical Relay-Tower with the antenna stowed for transport.

Figure 2-3. Tactical Relay-Tower

Site Selection

2-38. The Tactical Relay-Tower requires a line of sight path to the other end of the intended link. Pre-planned mission scenarios, used in conjunction with maps, reports, and other information, assist in site selection. These scenarios take obstructions such as terrain, foliage, and buildings into consideration.

2-39. Planners and installers should set up the Tactical Relay-Tower away from aircraft runways and heliports. Planners need to coordinate with the installation airfield/airspace officer or, in a combat zone, the senior airfield authority. Operators should install, operate, and use the mast's aircraft warning beacons if the mission permits.

HIGH CAPACITY LINE OF SIGHT

2-40. The High Capacity Line of Sight terminal provides alternate network transport for the division and brigade TCNs at-the-halt to support fixed command posts. The High Capacity Line of Sight system interfaces with the TCN via the flex multiplexer, fiber optic modem, or Tactical Fiber Optic Cable Assembly.

VEHICLE WIRELESS PACKAGE

2-41. The Vehicle Wireless Package is a general-purpose user operated communications package for command vehicles at divisions, BCTs, maneuver battalions, and support battalions. The Vehicle Wireless

Package's design allows installation in multiple vehicle types. The local access waveform radio provides the node-to-node connection between a Vehicle Wireless Package and a nearby TCN, either at-the-halt or on-the-move. Unit maintenance personnel maintain the Vehicle Wireless Package.

2-42. The local access waveform radio uses the 802.16 (WiMAX) wireless communications standard. Its range can vary during operation, depending on terrain and other obstructions. The Vehicle Wireless Package normally operates within 4 kilometers (2.5 miles) of the TCN at-the-halt. The maximum range is limited to 800 meters when operating on-the-move, depending on local conditions. The radio operates in a military (4500-4700 megahertz) band as well as an unlicensed commercial (5725-5850 megahertz) band, allowing use in other countries without interfering with local transmissions. Both the antenna and the radio frequency unit require changing in order to switch between bands. A TCN can support two Vehicle Wireless Packages in a point-to-multipoint topology. When sharing bandwidth, individual throughputs drop.

2-43. The local access waveform radio uses 256-bit advanced encryption standard. The local access waveform radio in the vehicle wireless package uses a TACLANE type 1 encryption device. (For additional information on TACLANEs, see Army doctrine for communications security.) The base station and associated subscribers in the same group must use the same channel and frequency to maintain a link. Other groups in the area of operations require separate frequencies if interference degrades performance.

2-44. When operating at-the-halt, the embedded switch provides 16 wired access ports for SIPRNET data terminals or VoIP phones. The Vehicle Wireless Package has no local call management capability. All IP phones register with the TCN's Unified Communications Manager.

POINT OF PRESENCE

2-45. A Point of Presence allows collaboration and access to the DODIN at the battalion, brigade, or division. The Point of Presence supports high-throughput line of sight and satellite communications network transport. The Point of Presence is general-purpose user operated; it does not require dedicated manning by signal personnel. It operates either at-the-halt or on-the-move, but is mainly used on-the-move.

2-46. The Point of Presence can integrate into a variety of mission command vehicles. The Point of Presence provides data and voice network access for reach between BCTs, and reachback communications to division.

2-47. When operating at-the-halt, the Point of Presence can provide access for wired IP data terminals or SIPRNET VoIP phones. When on-the-move, it provides the same capabilities to users on-board the vehicle.

2-48. Network planners configure Point of Presence components before deployment. The network management subsystem can dynamically update subsequent configurations.

Point of Presence Services

2-49. Point of Presence network services include—

- **Quality of Service:** The Point of Presence provides quality of service assurance for the SIPRNET local area network using differentiated services code point marking. Differentiated services provide low latency for traffic that cannot handle delayed transmission, such as VoIP. A quality of service edge device provides measurement-based admission control and network preemption to ensure the amount of traffic does not exceed the network's ability to support.
- **Information Services:** Domain Name System, Dynamic Host Configuration Protocol, and Active Directory on the SIPRNET local area network.
- **Cybersecurity:** The Point of Presence provides multiple layers of cybersecurity protection. Encrypting the SIPRNET data for transmission over the Highband Networking Radio or satellite communications system provides communications security protection. The colorless and SIPRNET routers provide enclave-level transmission security protection. The distributed computing element and Soldier Kiosk employ cybersecurity software for additional layers of defense-in-depth. They also include common access card readers for user authentication.
- **Node Management:** Operators perform basic fault isolation based on power on self-test results and other diagnostics.

- The Node Management Subsystem monitors, and manages local SIPRNET services, devices, and interfaces.
- The Local Area Network Management Subsystem monitors, and manages external SIPRNET local area network hosts, devices, and interfaces.

- **Call Control:** The Point of Presence uses Skinny Client Control Protocol for SIPRNET voice call control. Besides normal call processing, the call management software provides call forwarding, call transfer, and redial for IP users.
- **Conference Bridging:** The Point of Presence provides a nonsecure conference bridge for multi-party voice calls and progressive conferencing.

Transmission Technologies Supported

2-50. The Point of Presence supports both ground-to-ground and satellite communications while on-the-move and at-the-halt. Both the terrestrial Highband Networking Radio and satellite communications network centric waveform require position information to operate, whether at-the-halt or on-the-move. The inertial navigation unit and the Global Positioning System receiver provide this position data. The Point of Presence also forwards this position data for the map-based monitoring function of the NOSC's Network Management System.

Ground-to-Ground Communications

2-51. The Highband Networking Radio provides bandwidth-on-demand for the Point of Presence. It uses a C band antenna to transmit and receive the highband networking waveform at-the-halt and on-the-move.

2-52. The Highband Networking Radio continuously scans for other Highband Networking Radios within range. When one radio detects another, it establishes a connection, or relationship. This creates a network to forward data from the source to the intended destination.

2-53. Neighboring radios forward calls to provide alternate communication paths. A neighbor in this case is another platform using a Highband Networking Radio. This forms a mesh network. The Highband Networking Radio functions in peer-to-peer and point-to-multipoint modes.

Satellite Communications

2-54. The Point of Presence also employs either Ku or Ka band satellite communications. The Network Management System automatically switches between line of sight and satellite communications transport as needed to provide uninterrupted service using the better connection.

Employment

2-55. Points of Presence at the division, brigade, and battalion levels provide wide-area network connections to enable collaboration and mission command both on-the-move and at-the-halt. Points of Presence can also provide high data rate user connections for wired IP data terminals or VoIP phones at the quick halt and at-the-halt to support command post operations.

2-56. The commander's Point of Presence hosts mission command applications and services to facilitate situational understanding and enable mission command on-the-move. Commanders can use the Point of Presence to monitor activities in their operational area via Command Post of the Future or chat applications while traveling or during command post displacement.

2-57. The brigade operations section Point of Presence enables continuous staff coordination and planning while on-the-move, at the quick halt, and during command post displacement.

SOLDIER NETWORK EXTENSION

2-58. One of the lessons learned from Iraq and Afghanistan was the need for robust beyond line of sight communications among Army echelons from squad to battalion. These lower echelons relied mostly on single channel radios, which are constrained to line of sight distances. Even with improved radios, line of sight

communications can still limit range. For this reason, the Soldier Network Extension uses satellite communications transport to provide a beyond line-of-sight network connection.

2-59. The Soldier Network Extension can operate installed in a variety of command vehicles at battalion and company levels. It provides either Ku or Ka band satellite communications on-the-move. The Soldier Network Extension provides reach between BCTs, and reachback communications to the division. It supports company commanders and selected platoon leaders in maneuver battalions. The communications traffic served includes mission command messages, voice calls, and situational awareness information. The Soldier Network Extension can serve as an access port to extend the range of legacy combat net radios. This makes these networks more robust. The combat net radio gateway connects the combat net radio to the WIN-T IP infrastructure. It can connect two different radio networks through the WIN-T network. This leverages WIN-T's satellite communications capabilities to extend the effective range of the radio network beyond line of sight. The combat net radio gateway provides telephone signaling and converts analog to digital data. The Soldier Network Extension is a general-purpose user operated system not supported by dedicated signal personnel manning.

2-60. Antenna position information from the Global Positioning System receiver helps maintain antenna pointing. The position information also supports the map-based monitoring function of the NOSC's Network Management System.

SIPRNET and Colorless Enclaves

2-61. The Soldier Network Extension supports the colorless and one additional security enclave. All wide-area network traffic to and from a Soldier Network Extension passes through the colorless enclave. Users operate in the SIPRNET enclave. There are no user connections directly to the colorless core. The Soldier Network Extension uses software call management for local call control, as opposed to the TCN's Unified Communications Manager device.

Soldier Network Extension Services

2-62. Soldier Network Extension network services include—

- **Quality of Service:** The Soldier Network Extension provides quality of service assurance for the SIPRNET local area network using differentiated services code point marking. Differentiated services provide low latency for traffic that cannot handle delayed transmission, such as VoIP. A quality of service edge device provides measurement-based admission control and network preemption to ensure the amount of traffic does not exceed the network's ability to support.
- **Information Services:** Domain Name System, Dynamic Host Configuration Protocol, and Active Directory on the SIPRNET local area network.
- **Cybersecurity:** The Soldier Network Extension provides multiple layers of cybersecurity protection. Encrypting SIPRNET data for transmission over the satellite communications system provides communications security protection. The colorless and SIPRNET routers provide enclave-level transmission security protection. The distributed computing element and Soldier Kiosk employ cybersecurity software for additional layers of defense-in-depth. They also include common access card readers for user authentication.
- **Node Management:** Operators perform basic fault isolation based on power on self-test results and other diagnostics.
  - The Node Management Subsystem monitors and manages local SIPRNET services, devices, and interfaces.
  - The local area network management subsystem monitors and manages external SIPRNET local area network hosts, devices, and interfaces.
- **Call Control:** The Soldier Network Extension uses Skinny Client Control Protocol for SIPRNET voice call control. Besides normal call processing, the call management software provides call forwarding, call transfer, and redial for IP users. The Soldier Network Extension also provides a nonsecure conference bridge for multi-party voice calls and progressive conferencing.

Transmission Technologies Supported

2-63. The Soldier Network Extension provides either Ku or Ka band satellite communications on-the-move and at-the-halt. It also provides a combat net radio gateway to connect single-channel ground and airborne radio system voice networks to the IP network.

Employment

2-64. The Soldier Network Extension serves several different roles within the formation. It is fielded to company level and in wireless network extension teams and battalion operations section in the BCT.

2-65. The Soldier Network Extension at maneuver and forward support companies primarily provides mission command capabilities for key company leaders on-the-move and at the quick halt, as well as providing a combat net radio gateway to connect the lower tier tactical internet to the wide-area network.

2-66. The Soldier Network Extension at the battalion operations section enables continuous staff coordination on-the-move and at the quick halt.

2-67. The field artillery battalion fire direction center Soldier Network Extension enables fires coordination and maintains awareness and system connectivity while fire direction centers displace. The system allows positioning of firing batteries and fire direction centers wherever the commander needs without the constraints of fixed line of sight transmission. This allows faster displacement of fire direction centers following counterfires.

2-68. The brigade and battalion wireless network extension teams' Soldier Network Extensions enable the S-6 to meet the commander's priorities to extend or expand network connectivity and capacity. The combat net radio gateway can extend one organic combat net radio voice network over the wide-area network to extend mission command capabilities across a non-contiguous or extended operational area.

MODULAR COMMUNICATIONS NODE-BASIC

2-69. The Modular Communications Node-Basic operates only at-the-halt. It consists of two user access cases (SIPRNET and NIPRNET) with uninterruptible power supplies. The user access cases provide voice and digital data subscriber access ports for users at static command posts. Each user access case provides 48 Ethernet ports. Some versions also provide 24 2-wire analog telephone ports. The Modular Communications Node-Basic user access cases have no transmission capabilities, so a TCN provides their network transport. The Modular Communications Node-Basic functions as a stand-alone pooled asset.

SECURE WIRELESS LOCAL AREA NETWORK

2-70. The secure wireless local area network is part of the TCN. It provides 802.11-compliant (Wi-Fi) wireless SIPRNET access between remote laptop computers and a base station at-the-halt. The secure wireless connection requires a type 1 network encryptor on both the laptop and the router. The secure wireless local area network provides an alternative to wired Ethernet in a NOSC or command post when wired connections are either unavailable or inconvenient. The wireless connection is available as soon as the client laptop is powered on.

2-71. The secure wireless local area network system has three major components—

- Secure wireless bridge access point.
- 2.4 gigahertz mast amplifier.
- 2.4 gigahertz, omnidirectional antenna.

2-72. The secure wireless local area network operates over a range up to 100 meters, depending on conditions.

INCREMENT 2 SYSTEM ALLOCATION

2-73. Table 2-2, on page 2-14, shows the WIN-T increment 2 system allocation plan.

Table 2-2. Increment 2 system allocation

Increment 2 Nodes	*Division*	*BCT*	*Battalion*	*Company*
MCN-B	X	X		
NOSC–Brigade		X		
NOSC–Division	X			
Point of Presence	X	X	X	
Soldier Network Extension		X	X	X
STT+	X	X	X	
TCN	X	X	X	
tactical hub node	X			
Tactical Relay–Tower	X	X		
Vehicle Wireless Package	X	X	X	
High Capacity Line of Sight	X	X		

Legend:
BCT brigade combat team
MCN-B Modular Communications Node-Basic
NOSC network operations and security center
STT+ Satellite Transportable Terminal with upgrade kit
TCN Tactical Communications Node

COMMUNICATIONS ON-THE-MOVE CAPABILITIES

2-74. The various WIN-T increment 2 node types provide on-the-move capabilities using line of sight, satellite communications, and mobile broadband technology. Table 2-3 provides a summary of increment 2 nodes' on-the-move communications and node management capabilities.

Table 2-3. Communications on-the-move capabilities

Mobile Configuration Item	*Network Centric Waveform (SATCOM)*	*Highband Networking Radio (line of sight)*	*Combat Net Radio Gateway*	*Local Access Waveform*	*Node Management*	*Multi-Domain Atlas*	*Soldier Kiosk*
TCN	X	X	X	X	X	X	
Point of Presence	X	X			X		X
Soldier Network Extension	X		X		X		X
Vehicle Wireless Package				X			

Legend:
SATCOM satellite communications
TCN Tactical Communications Node

Chapter 3

Managing Warfighter Information Network-Tactical

This chapter introduces WIN-T management. It discusses DODIN operations (including cybersecurity), NOSCs, and node management functions and tools. It also addresses planning, configuring, and setting data priorities for quality of service and speed of service assurance so the network can support the commander's intent.

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS

3-1. DODIN operations capabilities enable the signal staffs at each echelon to execute commanders' priorities throughout the enterprise. DODIN operations allow commanders to utilize automated information systems to effectively communicate, collaborate, share, manage, and disseminate information. DODIN operations consist of three critical tasks—DODIN enterprise management, cybersecurity, and DODIN content management.

3-2. Shared network situational understanding, along with coordination between stakeholders on network events, ensures commanders are aware of network actions taking place in their areas of responsibility and enables them to manage their networks as they would other combat systems. The division and brigade NOSCs perform DODIN operations for the upper tier tactical internet (for more detailed information on the DODIN operations critical tasks, see Army doctrine for DODIN operations). DODIN operations for the lower tier tactical internet are distributed to the battalion level (for more information about DODIN operations in the lower tier tactical internet, see ATP 6-02.53).

3-3. WIN-T uses commercial firewalls, network planning and management tools, and cybersecurity techniques as a framework for network defense-in-depth. Increment 2 extends the defense-in-depth approach and further integrates network management into the architecture.

CYBERSECURITY

3-4. Network devices, computer servers, information databases, and the information passing to and from these devices are increasingly at risk from external and internal threats. Some possible threat sources are—

- Foreign intelligence entities.
- Terrorist groups.
- Disgruntled users.
- Unsophisticated users whose naive actions might have unintended consequences.
- Criminal organizations.

3-5. Multi-layer cybersecurity protection maintains the integrity of both the network and the information passing through it. WIN-T provides network defense consistent with the classification of information passed over the network. The cybersecurity architecture allows G-6 and S-6 network leaders to make informed risk decisions; fulfill mandatory incident notification requirements to U.S. Army Cyber Command, law enforcement, and counterintelligence; and effectively secure network resources. For more information about cybersecurity risk management and reporting, see DODI 8510.01 and AR 25-2.

Network Defense-in-Depth

3-6. WIN-T's cybersecurity protection integrates network defense-in-depth, starting at the Defense Information Systems Network and extending to the local area networks and individual user devices. In addition to the encrypted IP backbone, the WIN-T defense-in-depth strategy implements robust cybersecurity

schemes throughout the network. This layers protection at the outer perimeter and further downstream at the local area networks. The laptops and servers provide an additional layer of protection. These protection mechanisms use commercial off-the-shelf cybersecurity hardware and software for firewall, anti-virus detection and blocking, intrusion detection, malicious mobile code detection, and access control.

Administering Cybersecurity Policies

3-7. The NOSCs implement and administer cybersecurity policies in order to ensure the availability, integrity and confidentiality of the WIN-T network. These policies apply measures to defend against threats to networks and infrastructure, network boundaries, and computing environments. For more information about cybersecurity, see Army doctrine for DODIN operations.

NETWORK OPERATIONS AND SECURITY CENTERS

3-8. The division and brigade NOSCs perform network planning, monitoring, administration, and reporting. Network planners, operators, maintainers, and technicians in the NOSCs—

- Plan for networks and devices—develop and maintain both high-level and in-depth layouts and plans for DODIN operations, including detailed configuration files for most devices.
- Adjust plans as needed—relay changes and updates where required.
- Monitor networks—collect and report the status of the implemented network. The interpretation of the status prompts anomaly response. Either the NOSC or a managed element (such as a TCN) may initiate this response.
- Manage user profiles—control user profiles to ensure all users share a common network configuration. This reduces the number of network environment-related problems.
- Perform network management activities—monitor the performance of network assets, including media. This includes updating software versions and virus definitions, and troubleshooting to mitigate network and device problems. The goal is continuous, effective network performance.

Network Operations and Security Center Equipment

3-9. The NOSC shelters contain computer servers, Ethernet switches, and network appliances dedicated to planning and managing the SIPRNET, NIPRNET, and colorless enclaves. During operation, shelter-mounted assets remain in the truck. The SIPRNET, NIPRNET, and colorless user access cases may operate in a unit-provided command post while at-the-halt. The remote laptops communicate with the shelter-mounted servers and other networking assets.

3-10. The Ethernet switches in both the shelter and the user access cases have twin Gigabit Ethernet ports. At the shelter Ethernet switch, one port provides a high-throughput link between the NOSC assets and the user access cases supporting the remote management laptops in the command post. The second port provides a high-throughput connection to the TCN. This link allows the NOSC to access extended network assets, providing both a path for status reporting and the ability to remotely manage configurations and operating policies. The Tactical Fiber Optic Cable Assembly provides the Gigabit Ethernet connections to the TCN and the command post.

3-11. The brigade NOSC is subordinate to the division NOSC in operations, and performs DODIN operations for the brigade portions of the network. The brigade NOSC is scaled to the brigade's DODIN operations mission, and lacks certain traffic analysis and network diagnostics capabilities. The division NOSC performs these additional functions.

NETWORK MANAGEMENT FUNCTIONS

3-12. Typical management functions include—

- Monitoring the network, including map-based monitoring of at-the-halt and on-the-move nodes.
- Implementing distributed node management.
- Managing cryptographic keys and public key infrastructure.
- Managing quality of service.

- Correlating network and device events and predicting trends to avoid problems.
- Managing network topology and administering cybersecurity policies.
- Planning spectrum use for all known emitters and managing friendly network emitters (see Army doctrine for spectrum management).
- Coordinating satellite access requests with the applicable regional satellite communications support center and ensuring all satellite terminals in the network operate in accordance with their assigned satellite access authorization.

3-13. DODIN operations personnel oversee device configurations and network architecture for multiple types of communications equipment. They manage constantly changing networks and maintain gateways to external networks. Transmission distances may be great, and might involve multiple line of sight and satellite communications links. The NOSC provides the tools to monitor and manage all of these networking variables.

3-14. The NOSC provides updated information to the networking components, including—

- Configuration files.
- Virus definition updates.
- Cybersecurity updates.
- Communications goals.
- Network policies.

3-15. Network nodes collect local device and network link status. They provide it to the NOSC via the TCN.

Network Management Software

3-16. Various software applications support the NOSC's functions. These applications fall into one of three categories, operating system, network management, or network operations.

Operating System Software

3-17. An operating system is a collection of software that manages computer hardware resources and provides common services to execute application software. All servers and laptops have underlying operating systems to manage their internal resources. Networking appliances, such as routers and switches, also require operating systems to manage their hardware.

Network Management System Software

3-18. This category includes software applications developed specifically to support WIN-T, including—

- Network planning software.
- Wide-area network monitoring software.
- Node management software.
- Key management software.
- Encryptor management software.

Commercial Off-the-Shelf Network Operations Software

3-19. WIN-T uses commercial off-the-shelf software applications for network management. These are the same types of applications used to manage mid-sized to large networks in commercial and business settings. Popular software applications in this group include—

- Application and server management software.
- Network monitoring applications.
- Anti-virus and spyware applications.
- Centralized security management applications.

Government Off-the-Shelf Network Operations Software

3-20. These are preexisting, government-owned applications developed to fulfill specific requirements for one or more government agencies. Software in this group includes—

- Automated Communications Engineering Software.
- Spectrum XXI spectrum management software.
- Common access card middleware.
- Radiant Mercury (cross-domain solution software).

PLANNING WIN-T NETWORKS

3-21. At a NOSC, senior networking personnel typically develop network plans from strategic concept to tactical implementation, including the resources, device and network configurations, and operational policies to develop and maintain networks and services. Their efforts support division and attached or subordinate BCT operations.

3-22. A network planner can graphically model, plan, define, and configure network assets for both at-the-halt and on-the-move employment. The graphical planning applications support configuring nodes, units, antennas, satellite communications bandwidth, and radios. Planning also includes—

- On-the-move node planning.
- Frequency and coverage planning for secure wireless local area networks.
- Local access waveform radios.
- Highband Networking Radios.
- Network centric waveform modems.
- High Capacity Line of Sight Radios.
- Frequency division multiple access satellite communications planning.
- Combat net radio planning (single-channel ground and airborne radio system and Enhanced Position Location Reporting System) See ATP 6-02.53 for additional information.
- Quality of service planning.
- IP and router planning.
- Voice service planning.
- Spectrum planning for all known emitters and management of network emitters (see Army doctrine for spectrum management).
- Cybersecurity planning.
- Mission command address book planning.

3-23. Establishing routing tables with appropriate path costing and establishing stable, reliable line of sight links reduces reliance on satellite communications as a backup and prevents network reconvergence issues due to continuously switching between line of sight and satellite communications.

WIN-T Satellite Communications Planning

3-24. WIN-T relies heavily on satellite communications transport. Network planning must begin early enough to route satellite access requests or commercial satellite service requests through the regional satellite communications support center in time for approval. Planners identify all satellite communications emitters (by satellite communications database number), throughput requirements, and the geographic area the systems will operate in.

3-25. Planners generate a satellite access request for each frequency division multiple access, time division multiple access, or network centric waveform network. The satellite access request should include all terminals and satellite connections required for the network. For increment 2, planners submit satellite access requests for—

- Division main command post.
  - STT+—frequency division multiple access and network centric waveform.
  - TCN—network centric waveform.

  - Tactical hub node (if used).
  - Secure Mobile Anti-Jam Reliable Tactical Terminal (to higher headquarters).
- Division tactical command post.
  - STT+—frequency division multiple access and network centric waveform.
  - TCN—network centric waveform.
- Brigade main command post.
  - STT+—frequency division multiple access and network centric waveform.
  - TCN—network centric waveform.
  - Secure Mobile Anti-Jam Reliable Tactical Terminal (to higher headquarters).
- Brigade tactical command post.
  - STT+—frequency division multiple access and network centric waveform.
  - TCN—network centric waveform.
- Battalion command post.
  - STT+—network centric waveform.
  - TCN—network centric waveform.
- Point of presence: network centric waveform.
- Soldier network extension: network centric waveform.

3-26. The network management technician normally oversees submission of satellite access requests. The satellite communications planner compiles the required information and provides it to the spectrum manager for entry into the Army Centralized Army Service Request System or the Joint Integrated Satellite Communications Tool (SIPRNET). For more information on satellite access requests, see Army doctrine for satellite communications.

Regional Hub Node Coordination

3-27. The regional hub node provides the unit's primary access to the DODIN and Defense Information Systems Network services when deployed. For this reason, communications planners should conduct several coordination calls leading up to each exercise or mission. This ensures the regional hub node can adequately support mission intent. Significant training events should include regional hub node leadership for proper command emphasis. This leads to increased technical and field service representative support at the regional hub nodes during the training event.

3-28. The United States Army Communications-Electronics Command provides regional hub node playbooks as technical guides to support installation and troubleshooting. The regional hub node playbooks are available at the Army Centralized Army Service Request System website.

ESTABLISHING WIN-T NETWORKS

3-29. Though the WIN-T network is largely self-forming, after the initialization of the equipment, network planners and operators must accomplish certain tasks to establish and secure the network.

Priorities of Work

3-30. Leaders should establish clear priorities of work for all operators and all systems. Maintaining clear priorities increases a team's efficiency in accomplishing assigned tasks, reduces Soldier idle time and maintains focus on mission requirements and link establishment.

3-31. Priorities of work should always support the next higher echelon. That is, an individual team's priorities support the section or platoon. The platoon's priorities support the company. The S-6 or G-6 priorities must support the battalion or brigade operations staff officer (S-3) or assistant chief of staff, operations and commander's priorities. Figure 3-1, on page 3-6, shows a sample table for link establishment priorities.

CODE

LINK CODE	
SX	Satellite
FL	Fiber
L	LOS
CX	Cable

SF=FDMA, ST=TMDA, SM=SMART-T
FT=TFOCA, FS=Single Mode, FM=Multimode
LH=HCLOS, LI=IPLOS
CC=CatV, CX=CX11230

Nodes	
Hub	00
JNN 7747	47
JNN 7748	48
CPN 77472	72
CPN 77473	73
CPN 77474	74
CPN 77475	75
CPN 77476	76
CPN 77477	77
Node 78	78
Node 79	79

ESTABLISHMENT PRIORITY

Priority	Link	Adjacent Nodes	In Time	Remarks:
1	ST47	00, 48, 72, 73, 74, 75, 76, 77		TDMA mesh established allowing all 2BCT nodes to connect to each other and hub.
1	ST48	00, 47, 72, 73, 74, 75, 76, 77		
1	ST72	00, 47, 48, 73, 74, 75, 76, 77		
1	ST73	00, 47, 48, 72, 74, 75, 76, 77		
1	ST74	00, 47, 48, 72, 72, 75, 76, 77		
1	ST75	00, 47, 48, 72, 72, 75, 76, 77		
1	ST76	00, 47, 48, 72, 72, 75, 75, 77		
1	ST77	00, 47, 48, 72, 73, 74, 75, 76		
2	SF4700	0		JNN FDMA connectivity to hub.
2	SF4800	0		
3	LH4748	48		JNN HCLOS backbone.
3	LH4847	47		
4	FT4775	75		CPN 7745 fiber link to 7747.
4	FT7547	47		JNN SMART-T reduddant links to each other.
5	SS4748	48		
5	SS4847	47		

LEGEND

BCT	bridge combat team
CPN	command post node
FDMA	frequency division multiple access
HCLOS	high capacity line of sight
IPLOS	internet protocol line of sight
JNN	Joint Network Node
LOS	line of sight
SMART-T	Secure Mobile Anti-Jam Reliable tactical Terminal
TDMA	time division multiple access
TFOCA	tactical fiber optic cable assembly

Figure 3-1. Sample link establishment priorities

Port Security

3-32. Port security is one of the fundamental methods to prevent unauthorized access to the network. Using Dynamic Host Configuration Protocol simplifies and speeds command post initialization, since automation personnel do not need to manually configure and add each user to the switch. However, using Dynamic Host Configuration Protocol during normal operation creates an opportunity for unknown users to connect to the

network. For this reason, network managers should disable Dynamic Host Configuration Protocol and implement port security as soon as they establish the digital command post footprint and primary users. Unused switch ports should be disabled or configured in a parking (un-routable) virtual local area network. Network administrators will need to add any new users manually.

3-33. Port security could entail using persistent media access control (MAC) address learning (sticky MAC) and MAC limiting. With sticky MAC and MAC limiting enabled, switch interfaces can learn the MAC addresses of trusted workstations, phones, and servers until they reach their limits for MAC addresses. Once a device reaches its MAC address limit, it will not allow new devices on the switch, even after a switch restart.

Wide-Area Network and Local Area Network Diagrams

3-34. Wide-area network and local area network diagrams visually represent network topology on both the wide-area network and local area network. Accurate network diagrams simplify network troubleshooting and aid in planning for potential network growth. Network diagrams are also effective briefing tools, since they make the network topology much easier to visualize.

3-35. DODIN operations personnel should produce wide-area network and local area network diagrams for each training event. DODIN operations personnel update local and wide-area network diagrams continually to reflect network changes.

3-36. Wide-area network diagrams should depict—

- Each node (with node identification number).
- Node location.
- Assemblages.
- Each wide-area network link (satellite communications, line of sight, or cabled).
- Non-organic elements.

3-37. Local area network diagrams should identify—

- All access cases.
- Separate switches.
- Port count.
- Loopback IP addresses.
- Physical locations inside command post tents or buildings.
- Supported users.

MAINTAINING WIN-T NETWORKS

3-38. The two complementary functions in maintaining a network are network management and network monitoring. Network management implies active responses to known issues. Network monitoring gauges the health of network assets based on the status information they report to the NOSC. Network monitoring supports the network management function.

Simple Network Management Protocol Management

3-39. Simple Network Management Protocol is an internet standard for managing devices (including routers, switches, servers, workstations, and printers) on IP networks.

3-40. The primary network management software used in WIN-T increment 1 is SNMPc. SNMPc is a secure, distributed network management system that monitors the network infrastructure in near real-time. Network managers should configure SNMPc maps to monitor network devices, links, and services.

3-41. In increment 2, the Network Management System is the primary Simple Network Management Protocol management tool.

3-42. Network managers should configure their management console to poll networking devices using loopback IP addresses, and links using the open shortest path first neighbor relationship to the adjacent router.

The console should also poll servers periodically to ensure services are still available (for example, domain name system server port 53, Exchange port 25, Command Post of the Future Ventrillo port 3784).

3-43. SNMPc OnLine provides the signal company commander, S-3, S-6, or G-6, and command post a read-only view of the network. This allows remote viewing of Simple Network Management Protocol maps using a web browser to provide near real-time network status. This allows the commander and S-3, S-6, or G-6 to monitor the network, and facilitates status briefings.

3-44. Simple Network Management Protocol manager-to-manager communication allows battalions to remotely view the brigade network, and the brigade to view the division or an adjacent brigade network. This creates an icon on each management console that provides a read-only view when selected. Using manager-to-manager communication reduces network management overhead by providing the current network status without polling each network device.

3-45. Asynchronous monitoring, using Simple Network Management Protocol traps, alerts DODIN operations personnel to critical events. Monitoring the router's central processing unit and memory utilization with traps can identify potential network or hardware problems (bad routing, network convergence, or multicast broadcast storms that increase central processing unit and memory utilization). Environmental (fan and temperature) traps provide alerts if network devices overheat, or are in danger of overheating.

3-46. The Simple Network Management Protocol community string on routers, switches, and firewalls transmits in clear text. Network managers should change the default community string as they would a password so attackers cannot exploit it to gain network access.

Internet Protocol Management

3-47. IP management is essential to planning, managing, and tracking assigned IP addresses. During planning, it is critical to identify where specific systems are located logically and identify specific subnets associated with devices in the planned network architecture. The Lightweight Directory Access Protocol Data Interchange Format is the sourcing document for all assigned unit organic IP Space. Army Battle Command Systems use their assigned IP space as identified in the Lightweight Directory Access Protocol Data Interchange Format.

3-48. IP address planning entails forecasting IP address capacity requirements. This ensures IP addresses are available to those who need them and provides room for growth. During planning, coordinate IP address advertisement and de-advertisement with the local installation (when using installation as a docking station) and the regional or tactical hub node to avoid dual advertisement.

3-49. An IP address database tracks used, reserved, allocated, and free IP addresses. This presents a clear picture of IP address usage within the organization. An accurate database prevents fragmented IP address usage and allows network planners to take necessary actions before allocations run out. Comparing the inventory database with the established network identifies network discrepancies and helps track allocated IP space. DODIN operations personnel should periodically compare the established network with the IP database. Automated IP discovery tools speed the process and keep inventories accurate.

3-50. IP management tracking associates computers and network devices with their physical locations and users. This helps rapidly identify, locate, and remediate compromised systems and assists in identifying cybersecurity events or violations.

Password Management

3-51. Proper password management is a key to network security, since compromised or easily guessed passwords can grant unauthorized users unfettered network access. Units should use centrally managed password management systems (for example, RADIUS or Terminal Access Controller Access Control System). Users require individual logins for each system and role, using strong passwords according to Army password standards. User accounts with system-level privileges require a separate password from all other accounts held by that user.

3-52. Using default passwords on networking devices or consoles presents a significant network vulnerability. Army password standards require changing the passwords on routers and system consoles from

the factory default. This includes changing from the default passwords provided by the program manager during equipment fielding. Since these default passwords are widely known, they will certainly be tried by adversaries or opposing forces in their attempts to infiltrate the network.

3-53. All system or system-level privileged-level accounts (root, enable, administration accounts) require at least a 15-character case-sensitive password, changed every 60 days. For additional password requirements, see Army Information Assurance Best Business Practices Document 04-IA-O-0001.

Firewall Management

3-54. Effective firewall management requires understanding of the Lightweight Directory Access Protocol Data Interchange Format; effective IP management; and a system for ports, protocols, and services management. DODIN operations personnel need to know where their organic IPs are located, both physically and logically in the network, and which IPs to allow access from outside the local area network. They also need to configure ports, protocols, and services for Army Battle Command Systems and other automated information systems and authorized software.

3-55. The default firewall configuration uses a block by exception rule set. This default setting allows the vast majority of outside traffic to access the network. Managers should always change from the default setting to allow by exception.

Ports, Protocols, and Services Management

3-56. The DODIN operations section uses ports, protocols, and services management system to manage non-Army Battle Command Systems software on the network. This system may require unique ports, protocols, or services outside the baseline WIN-T configuration. Any non-mission command system software requires a Network Enterprise Technology Command-approved Certificate of Networthiness, and must be on the approved software list.

3-57. The ports, protocols, and services management system should be able to capture and track who the user is, what the software is for, and the duration a specific port should be open. DODIN operations personnel monitor firewall logs to detect malicious use of opened ports.

Event Reporting and Network Monitoring

3-58. Network monitoring is a supporting function to network management, which more junior personnel can perform. Network monitoring can—

- Detect slow or failing components and links.
- Send notifications of device and network activity to a central location.

3-59. The local node's node management function collects operational event status from managed devices and forwards the status information to the NOSC. NOSCs compile the status information for storage, analysis, and/or display.

3-60. When monitoring is active, the wide-area network monitoring function polls the status database continually. Some events are for information only, while others require action to mitigate the event. Either the NOSC or an individual network node may perform mitigating actions. Monitoring functions at a NOSC can become specialized. For example, one operator may exclusively monitor communications security functions while another operator performs spectrum management.

3-61. In addition to network planning, network monitoring, and node management, a NOSC provides—

- A topology generator that automatically generates a detailed network topology diagram.
- Map-based monitoring for at-the-halt and on-the-move nodes.
- Recording and playback of monitoring data.

3-62. The NOSC gathers network status and performance data through synchronous (status) and asynchronous (alert) reporting—

- Synchronous reporting uses Simple Network Management Protocol. There are two scenarios—
  - Simple Network Management Protocol-based commercial off the shelf software gathers and reports status.
  - The local node's operating environment messenger server performs Simple Network Management Protocol polling and forwards status updates to the NOSC's operating environment server for reporting within the Network Management System.
- Asynchronous reporting includes—
  - Simple Network Management Protocol traps and system logs, which are sent locally to the operating environment and/or commercial off-the-shelf applications, and by exception, across the network to the NOSC.
  - Network traffic analysis data.
  - Collecting network discovery and call detail (configuration, Simple Network Management Protocol, event, and VoIP) records.

Network Performance Reports

3-63. Network managers monitor all wide-area network links (satellite communications, line of sight, and cable) independently for bandwidth utilization. Network planners and managers use bandwidth utilization reports for link analysis and trend development to identify peak and minimum utilization periods. This drives command decisions to allocate or reallocate resources to support disadvantaged locations.

3-64. For example, if a remote site has a high bandwidth requirement and is only equipped for satellite communications connectivity, they may experience problems with network congestion and latency. Moving a High Capacity Line of Sight terminal to support that site increases available throughput, reduces costly satellite communications bandwidth requirements, decreases latency, and provides redundant network transport.

Transmission Reports

3-65. Transmission reports identify degradation in transmission systems or link quality before they cause link outages. A transmission report includes signal strength, energy per bit to noise power spectral density ratio (Eb/N0), bit error rate, error count, and alarms over a specified period. Transmission reports should include all transmission systems (Satellite Transportable Terminal, High Capacity Line of Sight, Highband Networking Radio). Figure 3-2, on page 3-11, shows a sample High Capacity Line of Sight outage report.

HCLOS OUTAGE

TRAINED		VERIFIED		
DATE	INITIALS	DATE	INITIALS	TASK
				1. Identify link with packet loss. - through SNMPc - ping test
				2. Loops - local patch panel loopback - local flex-mux loopback - local HVA loopback - local cable loopback - RF loopback - distant end flex-mux loopback
				3. Tests - data cable TQM test - VSWR test - radio loop test - input loop test - spectrum scan test

Verified by: _____ Soldier: _____

LEGEND

HCLOS	high-capacity
HVA	high voltage amplifier
mux	radio frequency
RF	technical quality
TQM	technical quality measures
VSWR	vertical standing wave ratio

Figure 3-2. Sample High Capacity Line of Sight outage report

3-66. Figure 3-3 shows a sample satellite communications transmission report.

8-HOUR SATCOM REPORT				
		0000	0800	1600
ASSEMBLAGE				
LINK TO				
RSL				
Eb/N0				
TPO				
WEATHER				
TRACKING				
INITIALS				

LEGEND

Eb/N0 energy per bit to noise power spectral density ratio
RSL receive signal level
SATCOM satellite communications
TPO total power out

Figure 3-3. Sample satellite communications transmission report

Communications Status Report

3-67. The communications status report is a consolidated daily report of all network nodes' status. This provides an accurate view of the network to facilitate shift change and to brief the S-6 or G-6. The communications status report should encompass all battalion nodes and attached enablers. The report includes planned network changes and authorized service interruptions.

Shift Changes

3-68. Structured shift changes facilitate effective information exchange between incoming and outgoing personnel. Operators enter shift change information in the team's master station log for historical reference. At a minimum, the shift change briefing should capture significant events over the previous shift (including outages or equipment failures), planned events for the next shift, and any pertinent administrative information.

Digital Battle Drills

3-69. Battle drills provide operators and DODIN operations teams structured, pre-planned responses to network, communications security, cybersecurity, power outage or server-related events. Established standards are easy to enforce, and help manage expectations inside the command. All echelons should formulate and actively rehearse battle drills for a variety of anticipated events to ensure timely and appropriate responses. Unit leaders should provide attached enabling elements copies of the unit's battle drills and include them in rehearsals. Figure 3-4, on page 3-13, shows a sample battle drill for malicious software found on the network.

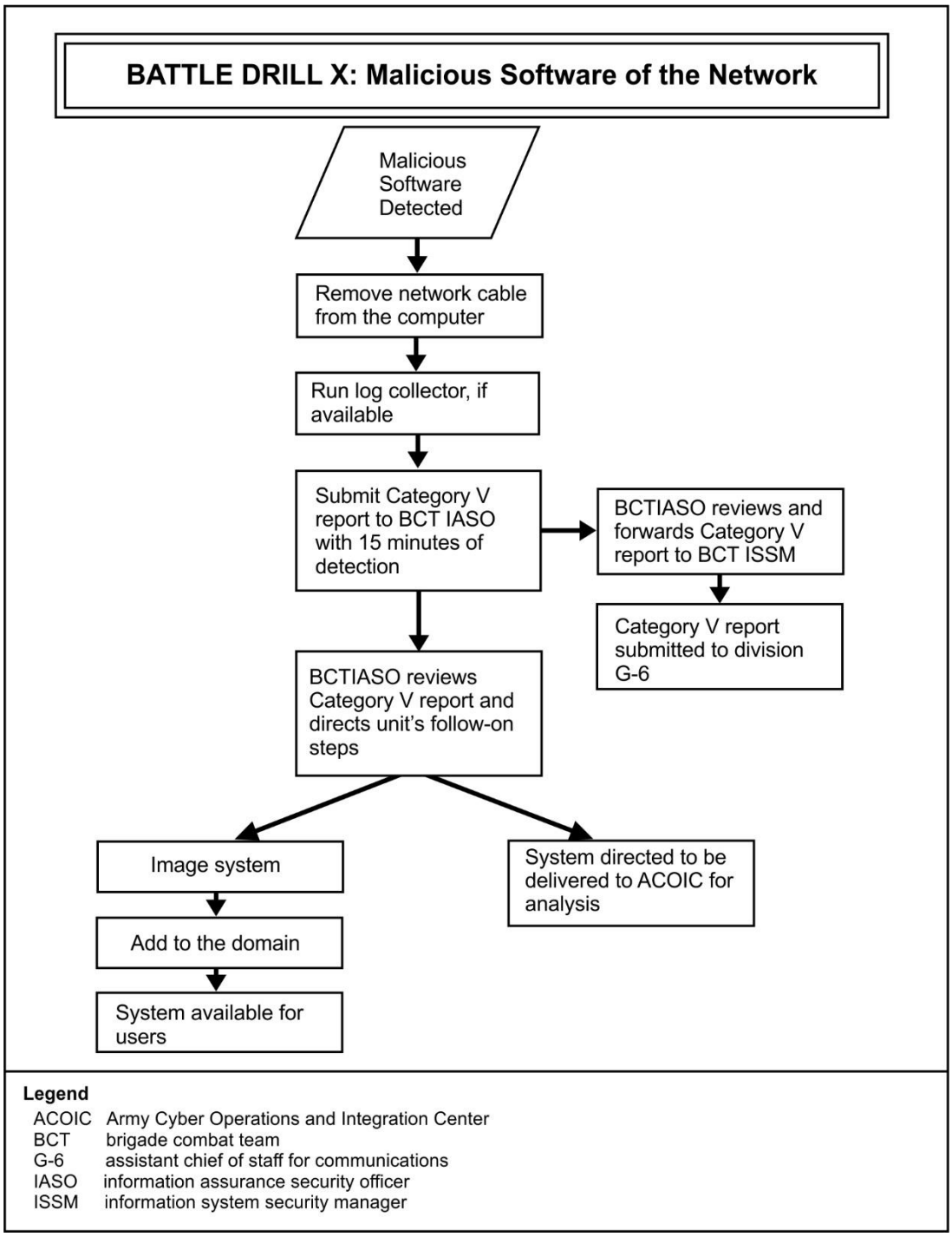

Figure 3-4. Sample battle drill

Unclassified Communications Blackout

3-70. The unit requires a plan to block unofficial communications between the time a casualty occurs and official notification of the next of kin. This prevents unofficial disclosure by well-meaning individuals in the unit. The unit may also implement an unclassified communications blackout (NIPRNET blackout) if a Soldier is in duty status – whereabouts unknown.

3-71. The DODIN operations section may implement an unclassified communications blackout using an access control list to block IP traffic, allowing by exception according to command guidance. In order to be effective, the unofficial communications blackout plan should also address the use of personal communications devices, such as cell phones and personal computers using commercial internet service.

DISTRIBUTED NODE MANAGEMENT

3-72. Legacy networks were managed from central locations. Regarding WIN-T increment 2, such locations correspond with the division or brigade NOSC. Operators monitored devices and network links for problems and responded accordingly. WIN-T still uses a hierarchy with the NOSC at the top, but node management is no longer strictly centralized. The NOSC need not actively monitor each device in a remote node. Distributed management delivers more flexibility, decentralizes certain node management tasks, and reduces network management overhead bandwidth.

3-73. Soldiers at certain nodes monitor both local and adjacent (hard-wired or directly connected through radio) network nodes, and perform defined local management functions. Distributed node management improves network response times by shifting some decisionmaking closer to the action. This provides more responsive network management.

COLORLESS ARCHITECTURE

3-74. Increment 1b and increment 2 implement a converged, colorless IP backbone where the system encrypts all user data for transport over the wide-area network. This encryption isolates the wide-area network from all external networks. This helps maintain network integrity. User data decryption takes place after the data leaves the wide-area network at its destination. Colorless core protects over-the-air broadcast, and limits insider threats to the overall WIN-T network. The colorless core backbone conforms to the Defense Information Systems Agency's cybersecurity architecture, though it is not part of the Defense Information Security Agency network.

3-75. The TACLANE provides encryption to isolate the backbone. The TACLANE is a National Security Agency-approved type-1 communications security device. Colorless architecture extends the secure deployed network to the DODIN through the regional hub node, and to the mid and lower tier tactical internet and BCTs through the Points of Presence, Soldier Network Extensions, and TCNs.

3-76. On the SIPRNET and NIPRNET local area networks, routers and switches provide local area network extension, services for local user access into WIN-T, and enclave protection. On the wide-area network, the TACLANE cryptographically isolates all user traffic from the wide-area network while the colorless routers provide a meshed transport network between WIN-T nodes.

3-77. The routing design consists of three areas—

- Local area network routers at the edge of the network host multiple IP subnets. The local area network router uplink connects to a TACLANE.
- The TACLANE encrypts and tunnels all the data before sending it to the core of the network (the wide-area network). The TACLANE uplink interface connects to the wide-area network router.
- The cluster of wide-area network routers forms the (colorless) core of the WIN-T network.

3-78. The SIPRNET and NIPRNET local area network data undergoes separate user data encryption (communications security) before passing through the TACLANE for link encryption (transmission security) at the local area network side of the wide-area network router. Only the encrypted colorless core data passes through the wide-area network. Figure 3-5, on page 3-15, illustrates the colorless core network architecture.

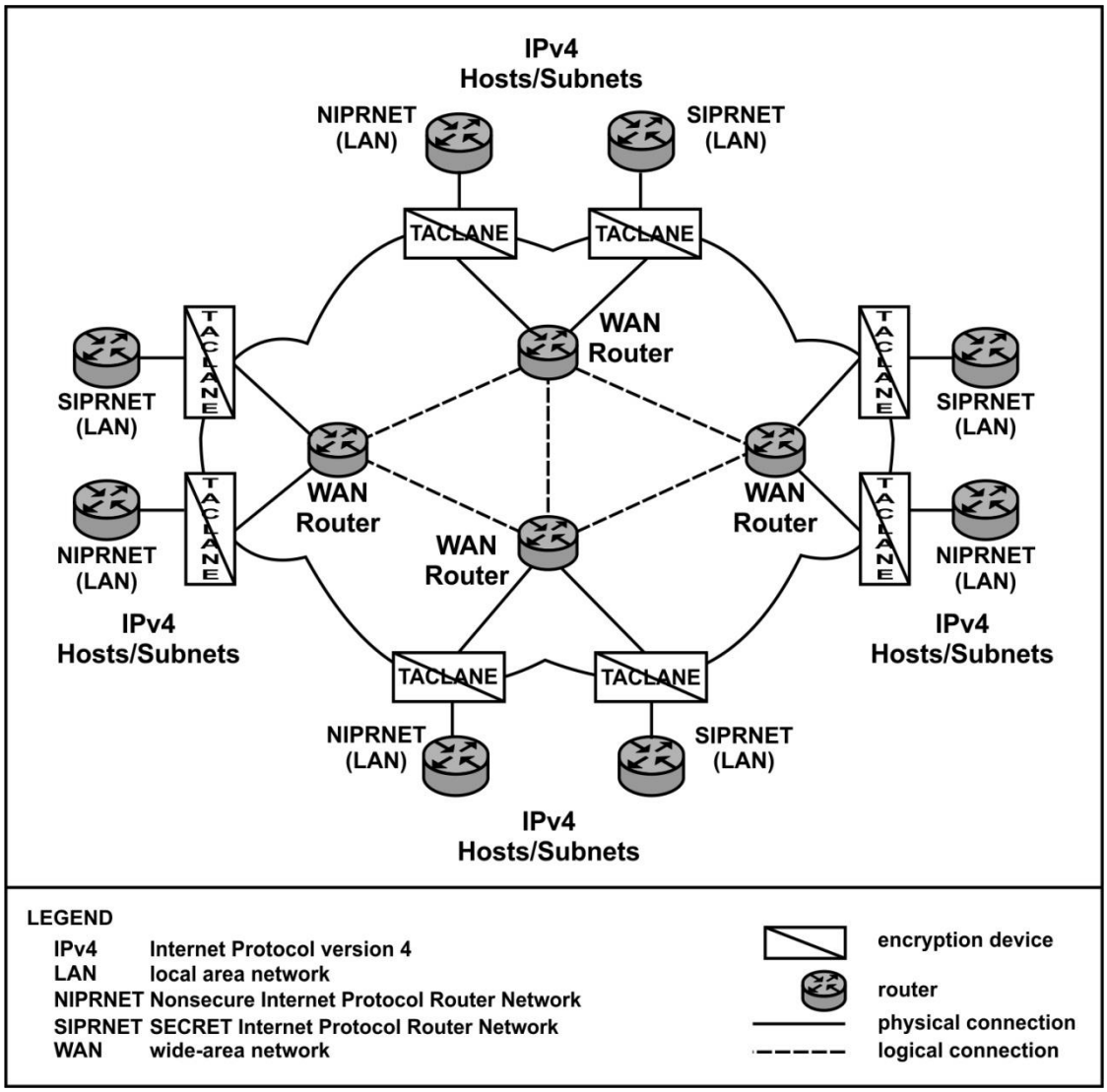

Figure 3-5. Colorless core routing

NETWORK QUALITY OF SERVICE AND SPEED OF SERVICE

3-79. When available network bandwidth is relatively fixed, it is important to allocate it wisely. WIN-T handles several different types of data of varying importance and transmission requirements. The various information types have different transmission requirements. For example, in an IP network, voice and video become digital packets during transmission similar to E-mail. Unlike E-mail though, if some of the voice or video packets suffer transport delays, the results at the receiving station may be unacceptable. Video can become choppy and un-viewable, and voice calls can become garbled. Packets comprising an E-mail, on the other hand, eventually arrive intact with no recognizable consequence of time delays.

3-80. Some types of data are more time-critical. Quality of service is a networking approach that helps optimize available bandwidth. It gauges user demand to maintain effective throughput. Quality of service edge devices provide the means to manage bandwidth-constrained traffic, taking into account both time criticality and information importance. Quality of service mechanisms help manage resources to avoid network bottlenecks, and ensure both quality and speed of service meet user requirements.

PLANNING AND CONFIGURATION

3-81. Quality of service edge device applications reside on a server between a local area network router and the colorless backbone. The network uses multiple quality of service edge devices. Configuring and implementing these devices are part of network planning. The quality of service edge device web client allows planners to remotely distribute and activate a selected plan to any or all of the edge devices. It also allows planners to verify which plan the edge devices are running.

PRIORITIZING INFORMATION

3-82. WIN-T baseline configurations as fielded include a quality of service framework, but units need to identify critical systems and services and create transmission rules for them. These rules determine how transmission services and resources handle the data. Networking rules for prioritized information can modify how and when information is sent and received. The division G-6 and BCT S-6 establish these rules, based on the commander's requirements.

3-83. If the access control lists are blank, the network treats all traffic as default priority. If the access control list contains the entire server range, all server traffic carries equal priority. Both options are valid, but the second one can potentially have adverse effects on the network. Tailoring transmission to a commander's priorities and polices can provide a tactical advantage. As an example, the S-6 may establish the quality threshold for transferring routine, non-time-sensitive information as delivery within 15 minutes, with the threshold for top priority survival information as less than 0.5 seconds. Tailored transmission thresholds improve commanders' situational understanding and ability to control their units.

QUALITY OF SERVICE MANAGEMENT

3-84. Determining which class of services each automated information system or service requires, based on the commander's priorities, is both complex and mission-dependent. Quality of service settings should be consistent across the wide-area network to work effectively. For example, an attached enabling unit may need to change their settings to match the supported brigade's quality of service plan. Figure 3-6 is a sample baseline quality of service model for a brigade with a normal distribution of mission command enabling systems.

	Video	Streaming	Low Latency Data	High Throughput Data	Short Message
Flash Override					JABBER, Ventrillo Chat, Tranverse, CPOF Ventrillo (All chat applications)
Flash			DNS, Domain Controller		
Immediate			CPOF, Mid Tier, Adobe Connect		
Priority			TIGR		
Routine	BVTC	UAV	Portal Page, TAIS, AFATDS, DCGS-A, CIDNE, C2PC		
Legacy					

Legend

AFATDS Advance Field Artillery Tactical Data System
BVTC battlefield video teleconferencing
C2PC Command and Control Personal Computer
CIDNE Combined Information Data Network Exchange
CPOF Command Post of the Future
DCGS-A Distributed Command Ground System-Army
DNS Domain Name System
TAIS Tactical Airspace Integration System
TIGR Tactical Ground Reporting System
UAV unmanned aerial vehicle

Figure 3-6. Sample quality of service table

CONFIGURATION MANAGEMENT

3-85. DODIN operations personnel establish baseline configurations for all network devices. Device configurations may evolve over time as missions change. DODIN operations personnel should avoid restoring WIN-T to its pre-validation exercise configuration. Network managers should restore the system to the established baseline before each new mission to remove previous mission-specific configurations.

3-86. The Defense Information Systems Agency's security technical implementation guides provide DOD-wide configuration standards for cybersecurity and cybersecurity-enabled devices and systems. Default WIN-T configurations are inherently unsecure and fail several critical security technical implementation guide requirements. Units should periodically download the current applicable security technical implementation guides to ensure their configurations meet these requirements or mitigate them properly. The security technical implementation guides are available on the Information Assurance Support Environment website.

3-87. The brigade NOSC manages the configuration for the entire BCT network, including attached support elements. Brigade DODIN operations personnel prepare the configurations necessary to integrate support elements into the network and allow themselves to access, monitor, and manage these systems. The brigade NOSC does not need permission to change support elements' configurations. The attached node maintains a backup copy of their pre-mission configuration so they can easily revert to baseline upon mission completion.

3-88. Scheduled, periodic backups of all network devices should be part of the operator and DODIN operations section battle rhythms. Operators should also create a backup after any configuration change. Network managers should compare and contrast backup configurations periodically to identify unplanned network changes. DODIN operations personnel should archive backup configurations to provide historical records and reference material for future missions.

3-89. Network managers should post procedures to restore configurations at each network node. This facilitates restoring network connectivity after a device failure. Managers should integrate restoration procedures into the section's cross-training plan.

This page intentionally left blank.

Chapter 4
Interoperability and Employment

WIN-T supports all tactical echelons and connects tactical forces with the operational force and sustaining base. The network is scalable to support command posts ranging from company command vehicles (increment 2 only) to larger and more complex command posts at the battalion, brigade, division, and corps. This chapter discusses WIN-T interoperability and system employment. It discusses the regional hub node that provides access to the DODIN and interoperability between increments 1 and 2. It explains increment 2 employment of at the division, brigade, battalion, and company, and increment 1b employment at the corps, support brigade, and expeditionary signal battalion.

INTEROPERABILITY BETWEEN INCREMENTS

4-1. WIN-T increments 1a, 1b, and 2 provide many of the same services, but they use different types of equipment. The regional hub node provides reachback and Defense Information Systems Network services for both increment 1 and 2, and serves as a bridge to provide communications interoperability between units operating different equipment.

4-2. The regional hub node provides Defense Information Systems Network and DOD gateway access (secure and nonsecure voice, video, and data) for deployed WIN-T systems. The regional hub node is not necessarily in the same theater of operations as the deployed WIN-T systems, but is located within range of a single-hop satellite communications link using either Ku band on a commercial satellite or military Ka band on the DOD Wideband Global Satellite Communications satellite.

4-3. Because increment 1b and increment 2 both use colorless core and network centric waveform, they can interface directly. Increment 1b systems can use their Linkway TDMA modems to operate in increment 1a networks, but increment 1a systems cannot operate in increment 1b or increment 2 networks. The regional hub node provides interface between increment 1a and either 1b or 2, since it is compatible with all three. Communicating between increment 1a and either increment 1b or 2 through the regional hub node may introduce network latency issues due to the satellite double-hop (increment 1a-to-regional hub node; regional hub node to increment 1b or 2). Excessive latency can interfere with some network and Army Battle Command System services (especially command post of the future). To mitigate these disruptions, increment 1b or 2 command posts can interface directly to increment 1a through High Capacity Line of Sight when operating at–the-halt.

EMPLOYMENT OF INCREMENT 2

4-4. WIN-T increment 2 provides network transport for mission command information and applications, both at-the-halt and on-the-move. These capabilities meet the unique requirements of divisions and BCTs.

4-5. Each unit has an equipment complement tailored to their echelon and unit type. These configurations ensure the unit's organic communications equipment supports its mission command on-the-move requirements.

DIVISION

4-6. WIN-T increment 2 provides DODIN operations for a division headquarters in order to enable connectivity to the DODIN. It also provides joint and Army interoperability so warfighters can access information services using line of sight and military or commercial satellite communications transport.

WIN-T-enabled commanders can dynamically tailor their assigned forces to conduct the full range of military operations.

4-7. WIN-T allows division commanders to tailor their network to mission, task, and purpose. Increment 2 allows the division headquarters to receive and share mission command data both at-the-halt and on-the-move. This allows warfighters to visualize and selectively control their area of operations while planning and conducting operations.

4-8. Personnel from the division signal company install, operate, and maintain the division headquarters' WIN-T assets, other than the user-operated vehicle wireless package. The division's organic WIN-T assets support the division main and tactical command posts.

Division Main Command Post

4-9. The main command post is the division's primary command post and the heart of the division's operation. The main command post is usually located out of the range of the enemy's medium artillery. Though the division main command post is mobile, it operates mainly at-the-halt supported by—

- TCN (x2).
- Tactical Relay-Tower.
- STT+ (x2).
- NOSC-Division.
- Modular Communications Node-Basic.
- Point of Presence (x2).
- Secure Mobile Anti-Jam Reliable Tactical Terminal.

Division Tactical Command Post

4-10. When fully active, the division tactical command post controls the close operation. The division tactical command post is a small, highly mobile, and survivable command post normally located close to the forward brigades. The division tactical command post operates at-the-halt or on-the-move using—

- TCN.
- STT+.
- Point of Presence
- Vehicle Wireless Package (x2).
- Secure Mobile Anti-Jam Reliable Tactical Terminal.

BRIGADE COMBAT TEAM

4-11. The BCT is a modular organization that provides the division, land component commander, or joint task force commander with close combat capabilities. WIN-T increment 2 allows BCT commanders and their command posts to receive and share near real-time, tactically relevant information without range, terrain, or vegetation limitations. Increment 2's on-the-move capability allows this without restricting them to traditional static command posts.

4-12. Personnel from the brigade signal company install, operate, and maintain the BCT's WIN-T equipment, other than the user-operated Vehicle Wireless Packages. Increment 2 allows the BCT S-6 to allocate communications capacity according to the commander's priorities, as well as controlling, monitoring, and maintaining the network. Increment 2 does not replace intelligence or sustainment-specific networks, but it can provide alternate network transport for them. BCTs usually conduct operations from two command posts, the brigade main command post, and the brigade tactical command post.

Brigade Main Command Post

4-13. The main command post is the unit's principal command post for mission command. It includes representatives of all staff sections and a full suite of information systems to plan, prepare, execute, and assess operations. It has a larger footprint and staff, and is less mobile than the tactical command post. The

brigade main command post operates mainly at-the-halt, though it can operate with reduced capacity on-the-move supported by—

- TCN.
- Tactical Relay-Tower.
- STT+.
- NOSC-Brigade.
- Point of Presence.
- Modular Communications Node-Basic.
- Vehicle Wireless Package (x2).
- Secure Mobile Anti-Jam Reliable Tactical Terminal.

Brigade Tactical Command Post

4-14. The tactical command post is fully mobile and usually is located near the decisive point of the operation. The brigade tactical command post operates on-the-move or at-the-halt using—

- TCN.
- STT+.
- Point of Presence.
- Vehicle Wireless Package (x2).
- Secure Mobile Anti-Jam Reliable Tactical Terminal.

MANEUVER BATTALION (BRIGADE COMBAT TEAM)

4-15. The BCT maneuver battalion receives its WIN-T support from organic assets. Battalion S-6 personnel install, operate, and maintain the battalion's WIN-T equipment, other than the user-operated Vehicle Wireless Packages. The battalion S-6 identifies the battalion's communications requirements. The brigade NOSC performs DODIN operations for the battalion's upper tier tactical internet. For information about DODIN operations on the lower tier tactical internet, see ATP 6-02.53.

4-16. The maneuver battalion operates on-the-move and at-the halt using—

- TCN.
- STT+.
- Point of Presence.
- Soldier Network Extension.
- Vehicle Wireless Package (x2).

MANEUVER COMPANY (BRIGADE COMBAT TEAM)

4-17. WIN-T increment 2 extends networked services to deployed maneuver companies for the first time. The Soldier Network Extension provides vehicle-mounted mission command services and applications to company commanders and selected platoon leaders.

4-18. The Soldier Network Extension extends data networks (for example Enhanced Position Location Reporting System and single-channel ground and airborne radio system networks). The Soldier Network Extension provides communications either at-the-halt or on-the-move whether traveling on improved roads or cross-country.

SUPPORT BATTALION (BRIGADE COMBAT TEAM)

4-19. BCTs also have various organic support battalions. The support battalions receive their WIN-T support from organic assets. Battalion S-6 personnel install, operate, and maintain the support battalions' WIN-T equipment. The brigade NOSC performs DODIN operations for the support battalions.

4-20. The support battalions' WIN-T support consists of—

- TCN.

- STT+.
- Point of Presence.
- Soldier Network Extension.

EMPLOYMENT OF INCREMENT 1B

4-21. Most non-divisional units operate mostly from static locations (such as forward operating bases or logistics support areas). For this reason, they do not require the mission command on-the-move capabilities of increment 2.

4-22. The corps headquarters and support brigades use organic increment 1b equipment to provide their mission command applications and services. The expeditionary signal battalion is a theater-pooled resource that supports those units not equipped with WIN-T.

CORPS

4-23. The corps is the operational headquarters for decisive land combat and includes enhanced capabilities for unified land operations. The corps defines the fight, ensures coherency, conducts operational maneuver, and serves as the bridge to translate strategic guidance into tactical tasks. The corps staff divides into two command posts. This expands the commander's ability to exercise mission command, and makes the mission command system more survivable. A deployed corps headquarters remains relatively static, so it does not require WIN-T increment 2's on-the-move capabilities. The corps' organic increment 1b equipment provides its WIN-T support, operated by elements of the corps signal company.

Corps Main Command Post

4-24. The corps main command post synchronizes the conduct of current operations and allocates available resources. Under the general supervision of the corps chief of staff, it also oversees the conduct of future planning, analysis for current and future operations, sustainment coordination, and other staff functions. The main command post's WIN-T support consists of—

- Joint Network Node (x2).
- STT+ (x2).
- High Capacity Line of Sight (x2).
- Secure Mobile Anti-Jam Reliable Tactical Terminal.

Corps Tactical Command Post

4-25. The corps tactical command post functions as an additional current operations cell. This command post can control corps operations for a limited time and can form the nucleus of an early-entry command post. It normally collocates with the main command post, but remains fully operational as a current operations cell so it can function independently. The tactical command post's WIN-T support consists of—

- Joint Network Node.
- STT+.
- High Capacity Line of Sight.
- Secure Mobile Anti-Jam Reliable Tactical Terminal.

SUPPORT BRIGADE

4-26. The support brigades (combat aviation, fires, battlefield surveillance, sustainment, and maneuver enhancement) receive their reachback and mission command applications and services using organic WIN-T increment 1b systems. Personnel from the brigade signal company install, operate, and maintain these systems to meet the commander's requirements. The brigade S-6 identifies these requirements.

4-27. Unlike the division and BCT, support brigades maintain just one command post. It operates at-the-halt using—

- Joint Network Node.

- STT+.
- High Capacity Line of Sight (x3).
- Network Management System.

SUPPORT BATTALION (SUPPORT BRIGADE)

4-28. The support battalion receives its WIN-T support using personnel and equipment organic to the brigade signal company. The battalion S-6 identifies communications requirements. The brigade performs DODIN operations for the support battalion's WIN-T equipment.

4-29. The battalion's WIN-T support consists of—

- Command Post Node.
- STT+.

EXPEDITIONARY SIGNAL BATTALION

4-30. Certain units do not have organic signal assets. However, they still need the same services and applications as maneuver units when deployed. The pooled theater assets of an expeditionary signal battalion are available to provide them WIN-T support. The expeditionary signal battalions provide modular support. They employ Joint Network Node and Command Post Node teams as needed to meet specifically tailored support requirements.

4-31. The expeditionary signal battalion provides nodal and extension communications for deployed Army and joint units. Supported headquarters may include a combatant command, Army Service component command, joint task force headquarters, or joint force land component command with no organic communications assets or insufficient assets.

4-32. The on-the-move communications capabilities of WIN-T increment 2 meet the unique needs of BCTs and divisions by design. Since support units do not require the same capability, the expeditionary signal battalion's WIN-T systems are increment 1b. They provide network centric waveform satellite communications to interface with the regional hub node and increment 2 equipped units, but not the increment 2 on-the-move capabilities. For more information about obtaining communications support from an expeditionary signal battalion, see Army doctrine for signal support.

4-33. The expeditionary signal battalion provides—

- Mission command for its assigned expeditionary and joint/area signal companies.
- Staff planning and network management for the battalion's communications assets.
- Communications-electronics support maintenance for network restoration.
- Continuous voice and data communications for supported units in austere environments.
- Connectivity to units within the theater network sensor grid.

Expeditionary Signal Company

4-34. The expeditionary signal company provides communications support to small and medium command posts. This includes line of sight and beyond line of sight network transport and cable and wire systems. The expeditionary signal company provides tailored communications packages consisting of one or more of the following—

- Joint Network Node.
- Command Post Node.
- STT+.
- High Capacity Line of Sight.
- Phoenix satellite communications terminal.
- Cable and wire team.

Joint/Area Signal Company

4-35. The joint/area signal company provides home station-quality Defense Information Systems Network and mission command enabling services to large and medium command posts and command post clusters. This includes line of sight and beyond line of sight network transport, network management, and cable and wire systems.

4-36. The joint/area signal company provides tailored communications packages consisting of one or more of the following—

- Single Shelter Switch.
- Command Post Node.
- STT+.
- High Capacity Line of Sight.
- Phoenix satellite communications terminal.
- Secure Mobile Anti-Jam Reliable Tactical Terminal.
- Digital troposcatter radio system.
- Cable and wire team.

TRAINING AND EXERCISE

UNIT TRAINING

4-37. There are currently no Army drill standards for installation and operation of WIN-T equipment. This leads to a lack of standardization of key tasks. It is up to the unit to develop its own standard operating procedure for the installation and operation of this equipment. This standard operating procedure should cover such key tasks as team time and training standards, certification, and priorities of work.

4-38. Units frequently only make time for WIN-T operator training when the unit goes to the field. This is not an acceptable practice, since network disruptions interfere with the larger exercise. Proper command emphasis can ensure operators and teams are proficient on their systems before field exercises. This training may take place in the unit's motor pool or a garrison training area, with or without the need for satellite time.

4-39. The unit's collective training plan should address the full range of likely tactical conditions under which users will operate in order to understand how the mission variables (mission, enemy, terrain and weather, troops and support available, time available, and civil considerations) affect equipment operation, and how users can maximize their systems' effectiveness under various conditions.

4-40. Units training at their home station or preparing for deployment to support significant training events utilize either installation as a docking station or their tactical hub node for Defense Information Systems Network access. Whenever possible, they should limit regional hub node access to significant training events (such as combat training center rotations) and real world missions, unless bridging increment 1b and increment 2 networks.

INDIVIDUAL TRAINING AND CERTIFICATION

4-41. Soldiers are assigned to meet units' specific military occupational specialty and grade requirements. Units establish unit-specific supervised on-the-job training plans and operator certification standards to ensure their Soldiers are proficient in the required critical tasks. WIN-T refresher training is available online at the Project Manager WIN-T Information and Support Exchange website.

CROSS-TRAINING

4-42. Developing and implementing a cross-training plan ensures personnel can perform basic tasks on most WIN-T equipment, regardless of their military occupational specialty. An effective cross-training plan enables signal teams to establish, sustain, and displace WIN-T systems more quickly and efficiently, and to a higher standard. Cross-training WIN-T operators to perform basic tasks outside of their military

occupational specialties develops signal Soldiers with greater depth and experience, and increased confidence. This is especially important during times of reduced manning and during 24-hour operations.

4-43. Each member of a team should be familiar with the basic tasks every member of that team. They cannot be expected to be experts on areas outside their military operational specialties, but they should be able to help install systems, identify when the systems are operating correctly, and get assistance when something goes wrong.

4-44. The cross-training plan should include the most commonly performed, basic operator tasks. This reduces reliance on key team members. The plan should be flexible enough to adapt to changing mission and manning requirements. Some examples of cross-training for WIN-T operators are—

- Training Joint Network Node team operators to perform DODIN operations in the brigade NOSC. This provides flexibility in manning the NOSC and gives the Joint Network Node team operators experience in more advanced network troubleshooting and management.
- Training all operators to add a VoIP phone to the Unified Communications Manager, and change display names and caller identification information.
- Training all operators on a Command Post Node team to verify the Satellite Transportable Terminal is tracking the satellite, and the satellite communications modem is in synchronization with the network controller.
- Training all WIN-T operators to check signal strength and errors on High Capacity Line of Sight systems.

4-45. Crew drills are an effective mechanism to validate and sustain team training. Teams should train and conduct crew drills according to the unit's combined arms training strategy or standard operating procedure.

4-46. The unit should implement team and crew certification standards to support the unit's mission, and incorporate these standards into their operational planning considerations.

This page intentionally left blank.

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

BCT	brigade combat team
DOD	Department of Defense
DODIN	Department of Defense information network
E-mail	electronic mail
G-6	(Army) assistant chief of staff for communications; (joint) Army or Marine Corps component command, control, communications, and computer systems staff officer.
IP	internet protocol
MAC	media access control
NIPRNET	Nonsecure Internet Protocol Router Network
NOSC	network operations and security center
S-3	battalion or brigade operations staff officer
S-6	(Army) battalion or brigade communications staff officer
SIPRNET	SECRET Internet Protocol Router Network
STT+	Satellite Transportable Terminal with upgrade kit
TCN	Tactical Communications Node
VoIP	Voice over Internet Protocol
WIN-T	Warfighter Information Network-Tactical

SECTION II – TERMS

cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DODI 8500.01)

local area network

A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. Note 1: Local area networks are usually restricted to relatively small areas, such as rooms, buildings, ships, and aircraft. Note 2: An interconnection of local area networks within a limited geographical area, such as a military base, is commonly referred to as a campus area network. An interconnection of local area networks over a city-wide geographical area is commonly called a metropolitan area network. An interconnection of local area networks over large geographical areas, such as nationwide, is commonly called a wide-area network. Note 3: Local area networks are not subject to public telecommunications regulations. Also called LAN. (American National Standard T1.523.2011)

reachback

The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed. (JP 3-30)

***regional hub node**

A component of the network service center, which provides a transport connection between the Warfighter Information Network-Tactical and the wider Department of Defense information network.

wide-area network

A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network and is usually spread over a larger geographic area than that of a local area network. Note 1: Wide-area networks may include physical networks, such as Integrated Services Digital Networks, X.25 networks, and T1 networks. Note 2: A metropolitan area network is a wide-area network that serves all the users in a metropolitan area. Wide-area networks may be nationwide or worldwide. Also called WAN. (American National Standard T1.523.2011)

References

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

ADRP 1-02. *Terms and Military Symbols*. 7 December 2015.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 8 November 2010.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT PUBLICATIONS

Most joint publications are available online: http://www.dtic.mil/doctrine/new_pubs/jointpub.htm

DOD instructions are available at: http://www.dtic.mil/whs/directives/index.html

DODI 8500.01. *Cybersecurity*. 14 March 2014.

DODI 8510.01. *Risk Management Framework (RMF) for DOD Information Technology (IT).* 12 March 2014.

JP 3-14. *Space Operations*. 29 May 2013.

JP 3-30. *Command and Control of Joint Air Operations*. 10 February 2014.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: http://www.apd.army.mil

ADP 1. *The Army*. 17 September 2012.

ADP 3-0. *Unified Land Operations*. 10 October 2011.

ADP 5-0. *The Operations Process.*17 May 2012.

ADRP 1. *The Army Profession*. 14 June 2015.

ADRP 3-0. *Unified Land Operations.* 16 May 2012.

ADRP 5-0. *The Operations Process.*17 May 2012.

AR 25-2. *Information Assurance.* 24 October 2007.

ATP 6-02.53, *Techniques for Tactical Radio Operations.* 7 January 2016.

FM 3-14, *Army Space Operations.* 19 August 2014.

FM 6-0. *Commander and Staff Organization and Operations.* 5 May 2014.

FM 6-02. *Signal Support to Operations*. 22 January 2014.

FM 27-10. *The Law of Land Warfare*. 18 July 1956.

OTHER PUBLICATIONS

American National Standard T1.523.2011. *Alliance for Telecommunications Industry Solutions Telecom Glossary 2011*. http://www.atis.org/glossary/

Army Information Assurance Best Business Practices Document 04-IA-O-0001. *Army Password Standards*. 1 May 2008. https://www.milsuite.mil/book/servlet/JiveServlet/download/22894-1-114498/04-IA-O-0001_Army_Password_Standards.pdf

RECOMMENDED READINGS

ATP 5-19. *Risk Management*. 14 April 2014.

FM 3-94. *Theater Army, Corps, and Division Operations*. 21 April 2014.

JP 3-0. *Joint Operations*. 11 August 2011.

JP 3-12. *Cyberspace Operations*. 5 February 2013.

JP 3-33. *Joint Task Force Headquarters*. 30 July 2012.

JP 6-0. *Joint Communications System.* 10 June 2015.

PRESCRIBED FORMS

None.

REFERENCED FORMS

Unless otherwise indicated, DA Forms are available on the Army Publishing Directorate (APD) web site: http://www.apd.army.mil

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

WEBSITES

These are the websites quoted or paraphrased in this publication:

Army Centralized Army Service Request System https://acas.army.mil/ (Requires DOD-approved certificate login and user account).

Army Information Assurance/Best Business Practices Library: https://informationassurance.us.army.mil (Requires DOD-approved certificate login).

Army Information Assurance Reference Library: https://ia.signal.army.mil/refLib.asp

Center for Army Lessons Learned: https://call2.army.mil/Login.aspx?ReturnUrl=%2f (Requires DOD-approved certificate login).

Information Assurance Support Environment http://iase.disa.mil/stigs/Pages/index.aspx (Requires DOD-approved certificate login).

Joint Integrated Satellite Communications Tool portal (SIPRNET) https://jist.afspc.af.smil.mil/jist

Project Manager Warfighter Information Network-Tactical Information and Support Exchange (Requires DOD-approved certificate login and user account). https://win-t.army.mil/wint/menu.cfm

Index

Entries are by paragraph number unless otherwise specified.

A

ad hoc network, 1-17

B

blackout, NIPRNET, 3-70

C

colorless architecture, 3-74

Command Post Node, 2-13

communications on-the-move, 2-74

components, increment 1b, 2-6

components, increment 2, 2-22

cybersecurity, 3-4

cybersecurity, policies, 3-7

D

defense-in-depth, 3-6

DODIN operations, 3-1

drills, battle, 3-68

E

employment, brigade combat team, 4-11

employment, brigade combat team, main command post, 4-13

employment, brigade combat team, tactical command post, 4-14

employment, corps, 4-23

employment, corps, main command post, 4-24

employment, corps, tactical command post, 4-25

employment, division, 4-6

employment, division, main command post, 4-9

employment, division, tactical command post, 4-10

employment, expeditionary signal battalion, 4-30

employment, expeditionary signal company, 4-34

employment, increment 1b, 4-21

employment, increment 2, 4-4

employment, joint/area signal company, 4-35

employment, maneuver battalion (brigade combat team), 4-15

employment, maneuver company (brigade combat team), 4-17

employment, Point of Presence, 2-55

employment, Soldier Network Extension, 2-64

employment, support battalion (brigade combat team), 4-19

employment, support battalion (support brigade), 4-28

employment, support brigade (corps), 4-26

equipment upgrades, increment 1, 1-5

equipment upgrades, increment 1a, 1-6

equipment upgrades, increment 1b, 1-7

establishing WIN-T networks, 3-29

H

High Capacity Line of Sight, 2-12; 2-40

highband networking waveform, 1-16

I

internet, tactical, 1-32

internet, tactical, lower tier, 1-38

internet, tactical, mid tier, 1-36

internet, tactical, upper tier, 1-34

interoperability, 4-1

J

Joint Network Node, 2-7

M

maintaining WIN-T networks, 3-38

management, configuration, 3-84

management, firewall, 3-54

management, internet protocol, 3-47

management, network, functions, 3-12

management, network, software, 3-16

management, node, distributed, 3-71

management, password, 3-51

management, ports, protocols, and services, 3-56

management, quality of service, 3-83

management, Simple Network Management Protocol, 3-39

Modular Communications Node-Basic, 2-69

monitoring, network, 3-58

N

network diagrams, 3-34

Network Operations and Security Center, 2-32; 3-8

Network Operations and Security Center, equipment, 3-9

network transport, 1-26

network transport, line of sight, 1-28

network transport, satellite communications, 1-30

O

overview, increment 1, 1-3

overview, increment 2, 1-14

overview, WIN-T, 1-1

P

planning, network, 3-21

planning, satellite communications, 3-24

Point of Presence, 2-45

Point of Presence, ground-to-ground communications, 2-51

Point of Presence, satellite communications, 2-54

Point of Presence, services, 2-49

Point of Presence, transmission technologies, 2-50
priorities of work, 3-30

Q

quality of service, 3-78
quality of service, planning and configuration, 3-80
quality of service, prioritizing information, 3-81

R

reachback, 1-25
regional hub node, 2-15
regional hub node, coordination, 3-27

S

Satellite Transportable Terminal, 2-10; 2-27
Secure Wireless Local Area Network, 2-70
security, port, 3-32
self-forming network, 1-17
self-healing network, 1-19
shift changes, 3-67
Soldier Network Extension, 2-58
Soldier Network Extension, enclaves, 2-61
Soldier Network Extension, services, 2-62
Soldier Network Extension, transmission technologies, 2-63
system allocation, increment 1, 2-21
system allocation, increment 2, 2-73
system description, 2-1

T

Tactical Communications Node, 2-24
tactical hub node, 2-23
Tactical Relay-Tower, 2-35
Tactical Relay-Tower, site selection, 2-38
training and exercise, 4-37
training, cross, 4-42
training, individual, 4-41
training, unit, 4-37

V

Vehicle Wireless Package, 2-41

ATP 6-02.60

03 Februaray 2016

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army
1601401

DISTRIBUTION:

Active Army, Army National Guard, and United States Army Reserve: Distributed in electronic media only (EMO).