Headquarters,
Department of the Army

FIELD MANUAL
6-02.2
(11-2)

Command, Control, Communications, and Computer (C4) Operations: Stryker Brigade Combat Team

Final Draft
October 2002

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

FM 6-02.2
(FM 11-2)

Field Manual
No 6-02.2

Headquarters,
Department of the Army
Washington, DC Pending Date

Command, Control, Communications, and Computers (C4) Operations: Stryker Brigade Combat Team (SBCT)

Contents

Page

Preface

This manual provides a single source reference supporting the Brigade Signal Company (BSC), brigade, and battalion S6 in the Stryker Brigade Combat Team (SBCT). It provides tactics, techniques and procedures (TTPs) for personnel to use in predeployment and deployment planning, and in support of training. Use of Interim Division (IDIV) and Army Forces (ARFOR) indicate organizations that assume the role as Higher Controlling/Command (HICON). Signal sections indicated as supporting the Brigade Support Battalion (BSB) are defined as sections supporting the Brigade Support Area (BSA), BSB areas of operation (AOs), and associated logistics locations.

This manual is a companion manual to FM 3-21.31, *The Stryker Brigade Combat Team*, and wherever differences may appear between the two manuals FM 3-21.31 will have precedence.

The proponent for this publication is the United States Army Signal Center. Send comments and recommendations on DA Form 2028 directly to Commander, United States Army Signal Center and Fort Gordon, ATTN: ATZH-CDD (Doctrine Branch), Fort Gordon, Georgia 30905-5075 or via e-mail to doctrine@gordon.army.mil. Key comments and recommendations to pages and lines of text to which they apply. Provide reasons for your comments to ensure complete understanding and proper evaluation.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

Chapter 1

SBCT C4 Support Concept of Operations

The Stryker brigade combat team (SBCT) is a full-spectrum combat force that has utility in all operational environments and against all threats. This chapter discusses the command, control, communications, and computers (C4) support concept of operations.

OVERVIEW

1-1. The SBCT provides significant capabilities as a subordinate maneuver component to division or corps commanders in a major theater war (MTW). In a smaller-scale contingency (SSC), the SBCT deploys rapidly, executes early entry operations, and is prepared to conduct offensive operations immediately upon arrival to prevent, contain, stabilize, or resolve a conflict, or to promote peace. During a peacetime military engagement (PME), the SBCT conducts programs or training exercises with other nations to assist in shaping the international environment and improve interoperability with treaty partners or potential coalition partners.

1-2. The SBCT consists of elements that perform the brigade's C4 mission of continuous operations based on mission, enemy, terrain, troops, time, and civilian considerations (METT-TC). The brigade S6 has the overall responsibility of the SBCT's information network. He provides the connectivity for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) integration within the SBCT, its higher headquarters, and the Army forces (ARFORs). Additionally an organic brigade signal company (BSC), designed to support the entire range of operations, supports the SBCT.

1-3. The SBCT can be deployed rapidly (96 hours) and can be sustained by an austere support structure for up to 72 hours. The SBCT conducts operations against conventional or unconventional enemy forces in all types of terrain and climate conditions and all operational environments (MTW, SSC, PME). The SBCT can perform its mission throughout the entire spectrum of military operations (offensive, defensive, stability, and support) but may require some augmentation for certain missions. The SBCT may deploy as part of an early entry force and may fight by itself or as part of a division or corps. The SBCT's operational capabilities are--

- Combined arms assault in the close fight.
- Mobility.
- Reach-back.
- Enhanced situational understanding.
- Lethality.

- Force protection and survivability.
- Force effectiveness.
- Joint, multinational, or interagency operability.
- Full-spectrum flexibility and augmentation.
- Simultaneous operations.

BSC

1-4. The BSC is under the operational control (OPCON) of the brigade commander.

1-5. The brigade S6 develops the C4 plan in conjunction with the BSC commander, and the BSC executes the plan in support of the brigade S6.

1-6. The BSC commander maintains command authority over the company. The BSC commander is responsible for the technical design, planning, engineering, configuration, and management of the information network planned by the brigade S6 to support the mission of the SBCT.

1-7. The BSC installs, operates, and maintains the SBCT wide area network (WAN). The BSC configures and manages the tactical Internet (TI) and tactical operation center (TOC)-to-TOC data networks. The Network Operations (NETOPS) section establishes the brigade network operations and security center (BNOSC) at the SBCT main command post (CP) and the BNOSC at the tactical command post (TAC CP) when the tactical situation dictates. The BSB nodal platoon establishes the BNOSC (alternate [ALT]) located at the Brigade Support Area (BSA) or where primary logistic and C2 data traffic/users are deployed.

1-8. The BSC relies upon external support for airborne retransmission and relay assets, motor maintenance, heavy recovery operations, logistics and personnel operations support, and remote site force protection.

BNOSC

1-9. The BNOSC is the C4 Operations center for the SBCT. The BNOSC, under the supervision of the BSC commander, directs the NETOPS functions to support the plan developed by the brigade S6. The BNOSC controls all assets organic to the BSC. See Appendix A for more detailed information on the BNOSC.

NETWORK MANAGEMENT (NM)

1-10. Network Management activities, functions, and tasks that are required to manage the WAN, TI, and TOC-to-TOC data networks are organic to the BSC. This NM capability is established in the BNOSC that is collocated with the brigade subscriber node (BSN) at the SBCT main CP. The BNOSC will operate and maintain the NM tools that monitor and maintain the information networks supporting the SBCT. Under the supervision of the brigade S6, a combination of BSC and S6 section assets establish the BNOSC (FWD). The primary NM tool will be the Tactical Internet Management System (TIMS) and local area NM tools providing TI and local area network (LAN) management capabilities. The BNOSC (ALT) will provide LAN

management for the SBCT support area CP and maintain an alternate NM database as back up to the BNOSC at the SBCT main CP.

INFORMATION ASSURANCE (IA)

1-11. The BSC has an organic capability in the BNOSC to perform IA functions. The computer network defense (CND) team in the NETOPS section performs limited IA functions. The limited nature of IA within the SBCT necessitates that the ARFOR provide additional IA tools, software, and/or personnel to the SBCT. IA is a key component of NM and information operations (IO) as a whole and assures the availability, integrity, authentication, confidentiality, and non-repudiation of friendly information and information systems. IA protects the SBCT information networks against exploitation, degradation, and denial of service by incorporating a defense in depth (DID). Detection and reaction capabilities allow for the effective defensive measures and/or timely restoration of debilitated information systems. IA capabilities will reside at each BNOSC with a tool set tailored to the mission requirements and risk assessment established by the commander and through support from the ARFOR.

Chapter 2

Brigade Signal Company

The BSC is organic to the SBCT and is organized with equipment and capabilities not previously provided at the brigade level. This chapter discusses the unique structure and capabilities of the BSC.

OVERVIEW

2-1. The BSC is unique in structure and capabilities. It consists of the command and NETOPS sections, brigade support battalion (BSB), TOC nodal, and the signal support platoons. Figure 2-1 shows the initial BSC organizational structure.

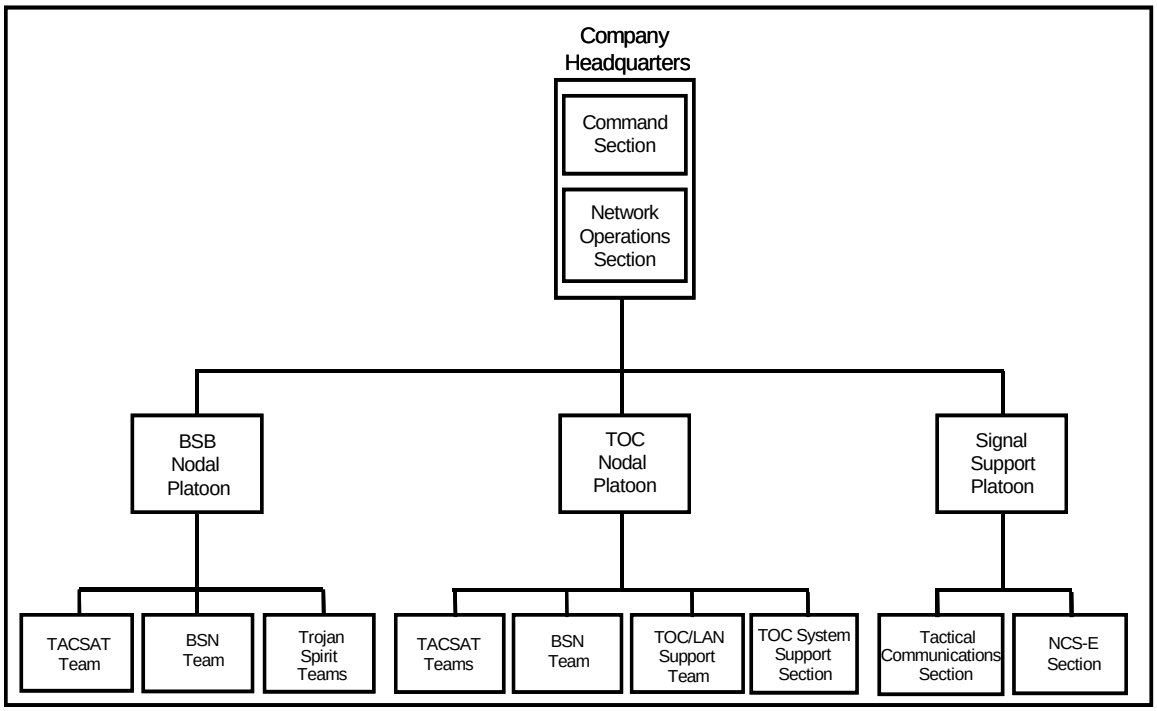


Figure 2-1. BSC Organizational Chart

BSC HEADQUARTERS

2-2. The BSC headquarters consists of the command and NETOPS sections.

COMMAND SECTION

2-3. The command section consists of the BSC commander, first sergeant, and supply noncommissioned officer (NCO). The command section is responsible for the administration and logistics support for the company.

NETOPS SECTION

2-4. The NETOPS section consists of the NM and computer and network defense teams. These teams execute the installation, operation, maintenance, and CND functions of the SBCT's information network. The NETOPS section establishes the BNOSC while operating closely with the TOC nodal platoon. The NETOPS section uses the organic NM capability of the TOC nodal platoon BSN to configure, monitor, and manage the information network. The BNOSC coordinates with the HICON for additional inorganic communications systems required, based on METT-TC, for network extension connectivity through ground, air, and satellite assets. The NETOPS section performs the IA functions of the BSC using the IA software and hardware located at the SBCT main and BSA/BSB CPs. The NETOPS section serves as the center for SBCT signal command and control (C2) operations. Figure 2-2 shows the NETOPS section structure.

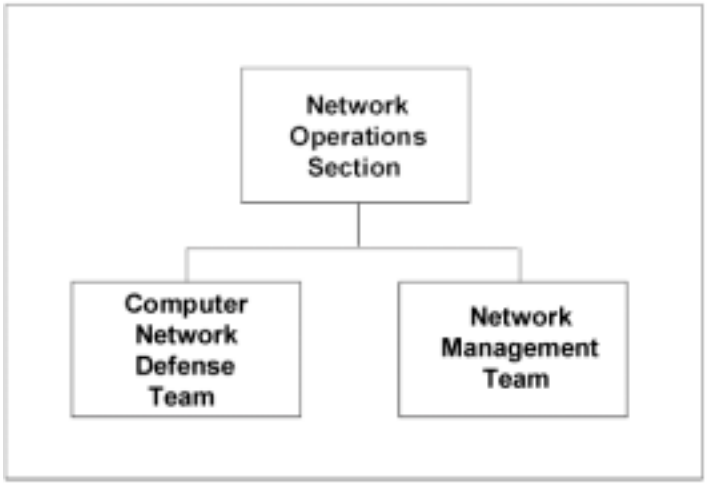


Figure 2-2. NETOPS Section Structure

BSB NODAL PLATOON

2-5. The BSB nodal platoon consists of the TACSAT, BSN, and Trojan Spirit teams. Figure 2-3 shows the BSB nodal platoon structure.

BSN Team

2-6. The BSN team provides the nucleus for voice, video, and data services to the SBCT main CP and the BSB. The BSN team maintains the BSN assemblage. See Appendix E for more information on the BSN.

TACSAT Team

2-7. The TACSAT team provides beyond line of sight (BLOS) connectivity from SBCT CPs into the BSA. The satellite system maintains the ability to terminate BSN circuits, provide data and battlefield video teleconferencing (BVTC) connectivity to host equipment, and through satellite assets provided by a HICON, interface special circuits, such as Defense Switched Network (DSN), North Atlantic Treaty Organization (NATO) circuits, and commercial gateways. TACSAT operators install, operate, and maintain (IOM) the Brigade Remote Switching System (BRSS) and can assist in operation of the BSN.

Trojan Spirit Teams

2-8. The Trojan Spirit teams provide the organic nonterrestrial reach-back capability required to access theater, joint, National Security Agency (NSA) analytic products. Trojan Spirit teams also provide the opportunity for collaboration internal (with the reconnaissance, surveillance, and target acquisition [RSTA] squadron) and external to the SBCT.

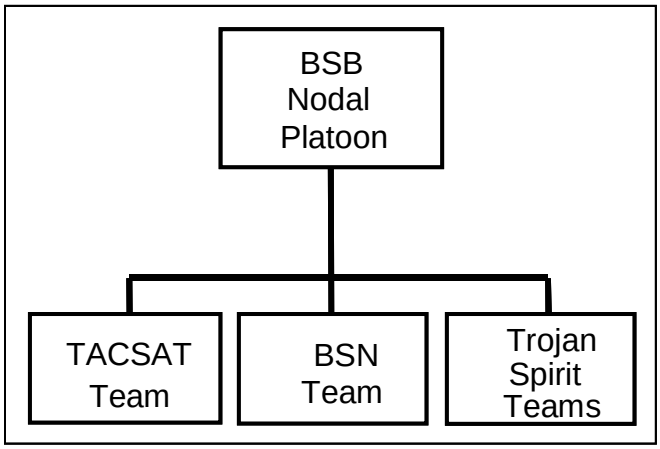


Figure 2-3. BSB Nodal Platoon Structure

TOC NODAL PLATOON

2-9. The TOC nodal platoon works closely with the NETOPS section to operate the BNOSC at the SBCT main CP. The BNOSC uses the organic NM capabilities of the BSN and has the primary NM responsibility for the information network. The TOC nodal platoon consists of TACSAT and BSN teams, and the TOC support section. Figure 2-4 shows the TOC nodal platoon personnel.

TACSAT Teams

2-10. The TACSAT teams provide habitual BLOS support to the SBCT main and forward CPs. Each system maintains the ability to terminate BSN circuits, provide data and BVTC connectivity to host equipment, and interface special circuits, such as DSN, NATO circuits, and commercial gateways. TACSAT operators IOM the BRSS and can help operate the BSN.

BSN Team

2-11. The BSN team provides voice, video and data services at the SBCT main CP. BSN NM capabilities will enable the BNOSC to manage the entire information network from the SBCT main CP. The BSN section maintains limited organic electronic maintenance support and provides an emergency response capability to immediately attend to and resolve SBCT communications infrastructure failures.

TOC LAN Support Team

2-12. The TOC LAN support team provides LAN support to the SBCT main CP.

TOC Support Section

2-13. The TOC support section provides BSC support functions and provides signal support for all communications systems supporting the BCT main and forward CPs.

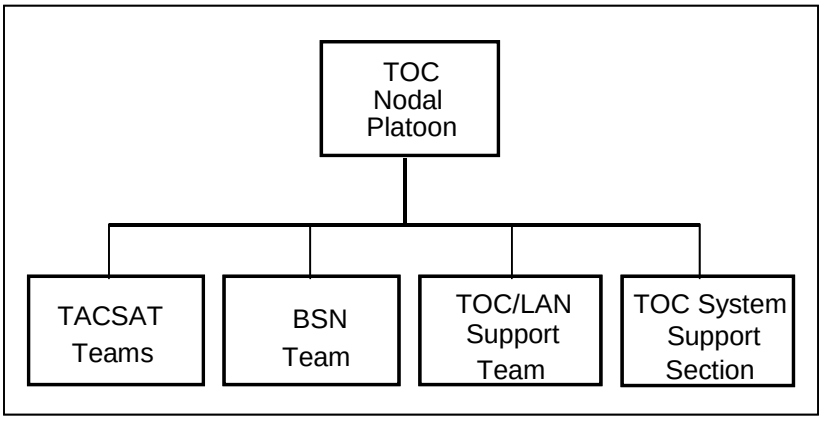


Figure 2-4. TOC Nodal Platoon Structure

SIGNAL SUPPORT PLATOON

2-14. The signal support platoon consists of the tactical communications section, and EPLRS network control station (NCS) team. The signal support platoon provides retransmission (Retrans), relay, EPLRS gateway, and EPLRS net control capabilities. Figure 2-5 shows the signal support platoon structure.

Tactical Communications Section

2-15. The tactical communications section provides range extension and network relay support for EPLRS, TOC-to-TOC data, and Single-Channel Ground and Airborne Radio System (SINCGARS) networks. The Retrans team is mission critical to SBCT C2 and situational understanding (SU) and may necessitate the commitment of force protection assets, in the absence of an airborne CRP. The gateway teams provide connectivity to adjacent EPLRS networks. The teams also provide dedicated relay support for the SBCT. These teams can be located in areas on the battlefield to provide additional support for TI backbone connectivity.

EPLRS NCS Team

2-16. The NCS-E section provides network initialization, monitoring, control, and configuration to maintain the EPLRS backbone of the TI. The NCS teams will reside in those locations to provide optimum connectivity and may be located in the vicinity of the SBCT main CP, BSB, and RSTA.

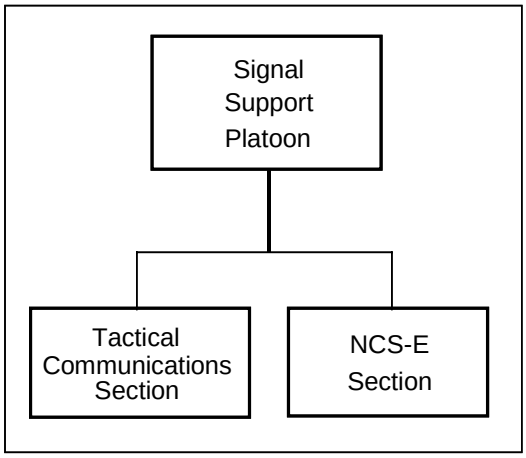


Figure 2-5 Signal Support Platoon Structure

Chapter 3

SBCT Information Network

This chapter discusses SBCT information network architecture, reach-back communications, subnetworks, and communications systems. It also discusses SBCT information network range extension and interoperability.

ARCHITECTURE

3-1. The SBCT information network provides the network connectivity for C4ISR. C4ISR is the integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications. C4ISR systems—

- Provide the information needed to develop situational understanding (SU) to support the commander's mission.
- Support the commander's implementation of C2 across the range of military operations by regulating forces and functions in accordance with (IAW) the commander's intent.
- Provide a link to develop a common operational picture of the situation.
- Locate, track, and engage critical targets.
- Conduct operations with lethal and nonlethal means.
- Operate with joint and multinational forces.
- Recognize and protect their forces.

3-2. The rapid aggregation and dissemination of relevant information (RI) with greater speed and precision becomes critical within the operational concept. This situation allows significantly enhanced synchronization of widely dispersed, highly mobile forces in the planning and execution of mass effects.

3-3. The operational environment characteristics of C4ISR are—

- Force projection that employs an SBCT within 96 hours from the first aircraft deployment.
- Reliance on the ARFOR/joint forces land component commander (JFLCC) for joint battlespace situational understanding (SU) and support.
- Joint operations are conducted in noncontiguous areas of operations (AOs) with tailored, widely dispersed units that are mobile and lethal.
- C4ISR activities support the force from alert through execution.

- Communications systems technologies provide access to the global information grid (GIG).
- SBCT footprint is minimized through reach-back.
- Increased interaction with information systems or people external to the SBCT.
- Enhanced C4ISR allows the commander to mass effects rather than forces.

ARMY BATTLE COMMAND SYSTEM (ABCS)

3-4. The ABCS is the primary user system designed to operate within the C4ISR architecture. The ABCS integrates the five battlefield functional areas (BFAs) of maneuver, fire support (FS), air defense (AD), intelligence and electronic protect (EP), and combat service support (CSS). Whether deployed for land combat or conducting peace operations, ABCS enables the commander to rapidly process and disseminate information within the battlespace.

3-5. The ABCS is interoperable with joint and multinational C2 systems at upper echelons. The ABCS is vertically and horizontally integrated at the tactical and operational levels.

REACH-BACK COMMUNICATIONS

3-6. The effectiveness of the SBCT as an early entry force will depend significantly on its ability to establish reach-back communications to compensate for the absence of combat, combat support (CS), and CSS capabilities.. The SBCT is designed to exploit nonorganic capabilities located within and outside the theater. Reach-back communications expand the capabilities of the force to operate across the spectrum of conflict, while reducing its in-theater footprint.

3-7. The SBCT's information network allows it to reach back to access existing databases, products, and analytic expertise resident in service, joint, and national surveillance and reconnaissance resources. Reach-back communications allow for collaboration, task sharing, and access to higher echelon databases.

3-8. The capability of reach-back communications to expand the power and effectiveness of the force comes from the precept that the commander can use resources external to the area of responsibility (AOR). Reach-back communications directly support—

- Fires and effects.
- Intelligence and IOs.
- Planning and analysis.
- Force protection.
- Logistics.

SUBNETWORKS

3-9. Table 3-2 shows the location of each SBCT C2 node information network by subnetwork. The following paragraphs provide an overview of each subnetwork.

Table 3.2 Information Network

SBCT Element	Subnetworks				
	WAN	TI	CNR	TOC to TOC	GBS
Main CP	X	X	X	X	X
TAC CP	X	X	X	X	
BSA	X	X	X	X	X
RSTA		X	X	X	X
Infantry battalion (x3)		X	X	X	X
FA Battalion		X	X	X	X

WAN

3-10. The WAN provides telephone, data, collaborative planning, and BVTC services to the SBCT main CP, TAC CP and BSB. This organic BVTC capability does not extend to the RSTA (unless collocated with the Main CP) or infantry battalions. The SBCT's WAN relies primarily on the organic AN/TSC-154 secure mobile anti-jam reliable tactical terminal (SMART-T) located at the SBCT main CP, BSA, and TAC-CP to achieve intra-theater connectivity. These multichannel TACSAT terminals provide transmission means for higher-bandwidth voice, video, and data applications.

TI

3-11. The TI integrates EPLRS, Force XXI Battle Command—Brigade and Below (FBCB2), and supporting communications equipment into a mobile data network. The TI provides situational awareness (SA) and C2 data exchange capabilities to all FBCB2 equipped platforms. The TI also enables users to access the network with the FBCB2 at any location as long as the system is within line of sight (LOS) of other TI assets. FBCB2 uses the TI to automatically exchange SA information among users as the tactical situation changes.

COMBAT NET RADIO (CNR)

3-12. The CNR provides the SBCT with very high frequency-frequency modulated (VHF-FM), high frequency (HF), and single-channel TACSAT capabilities to execute C2 of forces throughout the SBCT battlespace. The

primary role of the CNR network is voice communications using the SINCGARS, HF, or single-channel TACSAT for C2.

TOC-TO-TOC DATA NETWORK

3-13. The TOC-to-TOC data network enables users to exchange C2 information between TOCs and key C2 platforms. The near-term digital radio (NTDR) is a Joint Tactical Radio System (JTRS) surrogate and provides the TOC-to-TOC data network connectivity within the SBCT. The TOC-to-TOC data network uses each NTDR within the network as a relay.

GLOBAL BROADCAST SERVICE (GBS)

3-14. The GBS enables the SBCT staff to receive high-bandwidth products, such as imagery, logistics data, and digital map information. GBS is primarily located at the Main, BSA, RSTA, and Infantry Battalion CPs. The GBS allows tactical commanders to receive, access, retrieve, and archive this data. Examples of information that may be sent over the GBS include the following:

- Video broadcasts.
- Unmanned aerial vehicle (UAV) video feed.
- Common ground station sensor data.
- Maneuver Control System (MCS) overlays (friendly operational picture).
- All Source Analysis System (ASAS) overlays (enemy operational picture).
- Friendly operational picture overlaid with enemy picture from ASAS.
- Access to commercial television broadcasts (i.e. news)
- Other large volume data.

COMMUNICATIONS SYSTEMS

3-15. The following paragraphs describe the communications systems that support the SBCT information network.

MULTICHANNEL TACSAT TERMINALS

3-16. The SBCT will use the AN/TSC-154 SMART-T for intra-theater SBCT WAN links. The AN/TSC-154 is a high mobility multi-purpose wheeled vehicle (HMMWV)-mounted TACSAT communications terminal. It operates in the military strategic and tactical relay (MILSTAR) satellite low data rate and medium data rate advanced extreme high frequency (AEHF) communications payloads. MILSTAR provides BLOS range extension for the BSNs. The SMART-T terminals will provide military and commercial connectivity for data, imagery, video, and voice communications. The AN/TSC-154 SMART-Ts will reside at the SBCT main CP, BSB, and forward CP.

3-17. The SBCT will use the AN/TSC-85C or AN/TSC-93C for external network links and reach back into a HICON. The AN/TSC-85/93 is a tri-band

multichannel TACSAT communications terminal and operates in the SHF spectrum. These terminals will reside at the SBCT main CP and BSA.

JTRS/NTDR

3-18. The NTDR is a surrogate for the JTRS and will be used until the JTRS is fielded. The NTDR radio supports LAN (Ethernet) and serial interfaces inside the TOCs and selected C2 vehicles. The NTDR has a range of 10-20 kilometers (6-12 miles) and incorporates a Global Positioning System (GPS)-receive capability that provides the Military Grid Reference System (MGRS) position for the radio.

EPLRS

3-19. EPLRS provides the backbone for the SBCT's TI that is used to distribute SA and C2 information across the battlespace. The Network Control Station-EPLRS (NCS-E) or EPLRS Network Manager, dependant upon the system fielded to the unit, is used to establish, manage, and control the EPLRS network. EPLRS can also provide interfaces for numerous Army tactical computers to provide them access to the EPLRS network. Additionally, EPLRS provides a gateway function to adjacent networks and a relay capability with the EPLRS grid reference unit (EGRU).

SINCGARS

3-20. SINCGARS is a family of VHF-FM CNRs that provide the primary means of C2 communications for SBCT units. A common receiver/transmitter (RT) is used for manpack and vehicular configurations. SINCGARS radios can transmit and receive voice, data, and record traffic consistent with NATO interoperability requirements. See Appendix H for more information on SINCGARS.

HF

3-21. The SBCT will use a commercial off-the-shelf (COTS) HF radio system. The AN/PRC-150(C) manpack is automatic link establishment (ALE)-capable and has embedded COMSEC. The primary component of HF system is the RT-1694D (P)(C)/U. This RT will be common to all configurations of the SBCT's HF radios. The vehicular radio communications (VRC) and base station ground radio communications (GRC) nomenclatures are currently under development. See Appendix I for more information on HF radios.

BSN

3-22. The BSN includes asynchronous transfer mode (ATM) switching, routing, transmission, NM, and security services within a single shelter. The BSN provides a high-speed WAN infrastructure and extends network connectivity to the SBCT main CP, BSB and TAC CP when the tactical situation dictates. Commercial standards-based equipment allows the BSN to interface with the GIG, host nation, joint/coalition force, joint task forces (JTF), and ARFOR communications networks. The BSN is also interoperable with commercial networks and legacy Army communications systems (mobile subscriber equipment [MSE] and tri-service tactical communications [TRI-TAC]). The BSN interfaces with BLOS and LOS transmission systems and

can provide integrated services digital network (ISDN) loops off a post branch exchange (PBX), ISDN/Internet protocol (IP) video teleconferencing (VTC) through the multi-conference/gateway units, and e-mail services. BSN provides wireless LAN, wireless loops (cordless telephones), JTRS interface, and redundant LOS links between BSNs with the High Capacity Line of Sight (HCLOS) Radio System. See Appendix E for more information on the BSN.

Brigade Access Remote Terminal (BART)

3-23. The BART provides secure voice, video, and data network services up to Secret High and can interface via fiber optic cable with the multichannel satellite terminals, network operations control-vehicle (NOC-V), and BSN. The BART is stored and transported within two transit cases and has the following operational capabilities:

- Twenty tactical analog or commercial phones.
- Two Secret High LANs.
- One SBU LAN.

Single-Channel TACSAT Terminals

3-24. The AN/PSC-5 Spitfire is a lightweight, ultra high frequency (UHF), demand assigned multiple access (DAMA)-capable satellite terminal that supports single-channel communications at all echelons. The terminal includes embedded communications security (COMSEC), narrow-band voice capability and LOS communications for voice and data. The Spitfire's data capability is limited to non-DAMA (satellite) mode. The terminal can support command and control on the move (C2OTM) (when equipped with the appropriate amplifier and antenna) and extend SINCGARS communications when paired with SINCGARS as a Retrans.

GBS Receive Suite

3-25. The GBS receive suite operates in the Department of Defense (DOD) GBS information distribution system. The GBS receive suite receives the products programmed for the users serviced by each receive terminal at SBCT and battalion levels. The GBS can handle SECRET and Unclassified products.

NM Systems

3-26. The BSN has organic NM capabilities and provides the SBCT with an open system, integrated, planning, and engineering capability. These BSN organic NM capabilities provide management tools for the SBCT WAN, radio frequency (RF) spectrum, SBU traffic, and COMSEC. The ISYSCON V(4) provides TI and LAN management tools for the TI and TOC LANs. The EPLRS network will be managed using the NCS-E/ENM.

Defense Message System (DMS) Extension into a Tactical Environment

3-27. Tactical DMS provides a record traffic messaging system in the SBCT. Tactical DMS software components are installed on pre-existing platforms within each TOC at SBCT and battalion levels. The brigade and battalion S6

sections are responsible for the message transfer agent (MTA) located on each TOC server supported by tactical DMS. Tactical DMS is supported by the Tactical Messaging System (TMS) at the ARFOR that provides the backbone connectivity and management services to the SBCT.

TACTICAL RANGE EXTENSION

3-28. The tactical communications section employs a relay/retransmission capability for range extension of the TI, CNR, and TOC-to-TOC data networks. The primary role of relay/Retrans is range extension of the TI. The relay/Retrans is specifically focused on providing relay for the NTDR/JTRS network.

3-29. Under most circumstances, relay/Retrans capabilities in the SBCT's subordinate units remain under the control of the respective unit commander. This authority provides the commander with the flexibility to employ tactical range extension as the situation dictates. Although doctrinal signal support is from higher to lower and supporting to supported, the existence of the brigade-wide NTDR/JTRS network necessitates each relay/Retrans vehicle in the SBCT to be positioned for optimum area coverage.

3-30. The Airborne Communications Relay Package (CRP) is the preferred option to provide range extension. The CRP reduces the need to deploy isolated ground relay/Retrans teams, and overcomes ground LOS restrictions. The BSC, RSTA, FA, and Infantry Battalions maintain relay/Retrans assets in support of range extension in the absence of airborne CRP assets.

3-31. Operations in a noncontiguous battlespace will demand coverage beyond the capabilities of the SBCT terrestrial relay/Retrans systems. Aerial CRP, in addition to terrestrial relay/Retrans systems, significantly enhances information network coverage throughout the SBCT battlespace. Given METT-TC, the TI, CNR, and TOC-to-TOC data networks must be able to use some aerial CRP assets to ensure full coverage of the SBCT's battlespace. Network infrastructure, intelligence, surveillance, and reconnaissance (ISR) missions should be prioritized IAW the commander's intent.

Chapter 4

The S6 and Brigade Signal Company Commander

The brigade S6 has the overall responsibility for the SBCT's information network. The brigade signal company commander has overall responsibility to execute the signal plan in support of the commander. The S6 ensures the SBCT information network provides the connectivity for information network integration within the SBCT elements and the ARFOR. The signal company commander is responsible for installing, operating, and maintaining the SBCT information network. This chapter provides an overview of the duties and responsibilities of the S6 and the responsibilities unique to the brigade and battalion and the signal company commander. It also discusses the systems and network administrators.

S6 RESPONSIBILITIES

4-1. The S6 has the overall responsibility for the SBCT information network at brigade and battalion. As a principal staff officer, the S6 interacts closely with the XO, S3 and other staff officers. The S6–

- Is the signal expert to the commander.
- Advises the commander and staff on all signal support matters and information systems connectivity.
- Develops and coordinates the signal support plan.
- Coordinates with higher, adjacent, and subordinate units in development of the signal support plan.
- Establishes COMSEC accountability, distribution, destruction, and security procedures within the unit.
- Inspects subordinate unit signal support sections.

4-2. Table 4-1 lists the critical responsibilities of the S6. Due to the unique structure and mission of the SBCT, many tasks of the brigade S6 are shared with the BSC.

Table 4-1. Task Responsibilities

AOR/Tasks	Responsible
Network Employment	Both
• Advises the commander on communications requirements.	
• Establishes, manages, and maintains communications links, including reach-back communications.	Both/BSC

Table 4-1. Task Responsibilities (Continued)

AOR/Tasks	Responsible
• Plans and coordinates network terminals.	Both
• Configures and manages network terminals.	BSC
Network Configuration	Both/BSC
• Receives planning worksheets with LAN/WAN requirements.	
• Determines system requirements needed for support based on the tactical situation.	Both
• Determines communications and/or transmission connectivity requirements.	Both
• Informs the commander of primary and alternate communications capabilities.	Both
• Develops initialization instructions for new or modified communications systems.	Both
• Provides recommendations for database configurations.	Both
• Supervises and monitors network configuration, initialization, and tactical LAN (TACLAN) installation in the TOC. See Appendix N for more information on network configuration.	Battalion S6/BSC
• Establishes and enforces network policies and procedures.	Both/BSC
• Detects, reports, and takes corrective action on security violations and possible internal and external intrusions.	Battalion S6/BSC
• Develops Signal Annex K to the Operations Order (OPORD).	Both
• Develops network architecture diagram/annex.	BSC
• Prepares signal estimates.	Both/BSC
• Advises the commander and users on the requirements, capabilities, and use of the systems.	Both/BSC
• Plans and coordinates TACLAN configuration for the TOC.	Both
• Configure and maintain TOC TACLAN networks.	Battalion S6/BSC
• Coordinates signal interfaces with host nation and allied forces.	Brigade S6/BSC
Network Status Monitoring and Reporting	
• Monitors the status of the network using NM tools.	BSC
• Monitors the status of communications links, to include—	
▪ WAN.	Brigade S6/BSC
▪ CNR as reported by the NCS.	Both
▪ NTDR.	Both/BSC
▪ EPLRS/TI.	Both/BSC
▪ GBS.	Both/BSC
• Reports network changes to the commander.	Both/BSC

Table 4-1. Task Responsibilities (Continued)

AOR/Tasks	Responsible
Network Control and Reconfiguration	Both/BSC
• Monitors network performance and database configuration.	
• Provides supervision and guidance on troubleshooting, reconfiguration, and correction of network problems.	BSC
• Plans systems reconfigurations caused by changes in the tactical situation, communications connectivity, and system initialization instructions.	Both
• Ensures software distributed throughout the network is in compliance with appropriate regulation and unit standard operating procedures (SOPs).	Both/BSC
Training	Both
• Helps train users on automation information systems.	
• Supports the training of users and collective training for the unit.	Both
• Provides training in the establishment and interconnection of networks.	Both
Security	BSC
• Responsible for management, security, implementation, and utilization of all COMSEC issues.	
• Develops and distributes COMSEC within the unit.	BSC/Battalion S6
• Prepares communications network security plans, instructions, and SOPs.	Both/BSC
• Develops security policies and procedures for network operations.	Both/BSC
• Monitors the security integrity of the network and reports breaches in that security.	BSC
• Reports threats to network security.	Brigade S6/BSC
• Implements procedures to restrict entry of unauthorized users, transactions, or data.	BSC
• Determines network security requirements.	Both
• Ensures all users operate IAW AR 25-IA and local security SOPs.	Both/BSC
• Ensures information assurance security officers (IASO) are appointed for each BFA.	Brigade S6

SIGNAL COMPANY COMMANDER

4-3. The signal company commander is responsible for executing the installation, operation, and maintenance of the SBCT information network. The signal company (and its assets) is the only unit within the SBCT capable of network-wide communications support and management requirements in the brigade (see Chapter 2 for a description of the signal company). The signal company commander is the BNOSC officer in charge (OIC). With

support from the BNOSC, the signal company commander assists the brigade S6, and in some cases is the primary signal planner, during the MDMP. The signal company commander interacts very closely with the brigade S6, brigade XO, S3, and other staff officers. The signal company commander—

- Is the OIC of the BNOSC.
- Executes the Brigade S-6 signal plan.
- Assists the brigade S6 in the development of the signal plan (see Annex H).
- Inspects company signal support platoons.
- Supervises the establishment, operation, and sustainment of the brigade information network.
- Supervises brigade help desk.

BRIGADE S6

4-4. The brigade S6 operates primarily from the Network Operations Vehicle (NOC-V) located at the TAC CP when deployed. The brigade S6 is responsible for the development of the C4 plan in support of the brigade commander's intent. The brigade S6—

- Plans reach-back connectivity through the higher headquarters.
- Plans range extension of the brigade's communications services.
- Establishes the network management plan.
- Plans primary TOC voice and video capabilities.
- Plans network connectivity requirements.

4-5. The brigade S6 is responsible for supervision of all automation information systems, NM, and information security. As an active member of the military decision-making process (MDMP), he is the primary planner for all signal operations. He determines the supportability and feasibility of the signal plan versus the scheme of maneuver. Early involvement in the MDMP by the brigade S6 is critical to the successful development of a comprehensive and complimentary signal plan. See Appendix L for more information on the signal planning process.

BATTALION S6

4-6. The battalion S6 maintains the battalion's communications and C2 systems. As a principal staff officer, the battalion S6 interacts closely with the Commander, XO, S3 and other staff officers to determine specific or unique signal requirements and develop SU of the AO. The battalion S6—

- Is the signal support expert and advisor to the maneuver battalion commander.
- Advises the commander and staff on all signal support operations.
- Plans and executes range extension assets.

- Develops network-supportable battalion TOC locations in conjunction with the brigade S6 and battalion S3.
- Coordinates with the brigade S6 for additional communications support.

4-7. The battalion S6 is responsible for supervision of all automation information systems, NM, and information assurance. As an active member of the MDMP, he is the primary planner for all signal operations. He determines the supportability and feasibility of the signal plan versus the scheme of maneuver. Early involvement in the MDMP by the battalion S6 is critical to the successful development of a comprehensive and complimentary signal plan.

4-8. Additionally, the battalion S6 located at the BSA operates closely with the BSA nodal platoon and is responsible for establishing the BNOSC (ALT). The S6 is responsible for the installation and maintenance of the non-secure Internet protocol router network (NIPRNET) LAN supporting the BSA. The S6 provides the commander with the status of all the information systems on the TOC LAN.

SYSTEMS AND NETWORK ADMINISTRATOR

4-9. The systems and network administrators helps the S6 manage the network. They plan and coordinate with the BFA mission application administrators (MAAs) in linking the Battlefield Functional Area Control System (BFACS) devices in the brigade and battalion TOCs.

Appendix A

Satellite Operations

Multichannel and single-channel SATCOM extends the range of the WAN. This appendix discusses the multichannel, Trojan Spirit, and AN/PSC-5 satellite terminals.

MULTICHANNEL

A-1. The SBCT will use the AN/TSC-154, SMART-T, for intra-theater BCT WAN links. The AN/TSC-154 is a HMMWV-mounted tactical satellite communications terminal. It operates in the military strategic and tactical relay (MILSTAR) satellite low data rate and medium data rate advanced extreme high frequency (AEHF) communications payloads. MILSTAR provides BLOS range extension for the BSNs and NOC-V. The SMART-T terminals will provide military and commercial connectivity for data, imagery, video, and voice communications. The AN/TSC-154, SMART-Ts will be located at the SBCT main CP, BSB, and when the situation dictates at the TAC CP. Figure A-1 provides a photo of the SMART-T.

Figure A-1 SMART-T

A-2. The SBCT will use ARFOR that are provided AN/TSC-85C and AN/TSC-93C for external network links and reach back. The AN/TSC-85C and AN/TSC-93C tri-band multichannel TACSAT communications terminal is mounted on a high mobility multipurpose wheeled vehicle (HMMWV) and operates in the SHF spectrum with improved DTG data rate capabilities. AN/TSC-85C and AN/TSC-93C will be located at the BCT main CP and BSB. Figure A-2 shows an AN/TSC-85C and AN/TSC-93C.

AN/PSC-5

A-3. The AN/PSC-5, Spitfire, is a lightweight, UHF, DAMA - capable satellite terminal that supports single-channel communications at all echelons. The terminal includes embedded COMSEC, narrow-band voice capability and LOS communications for voice and data. The AN/PSC-5 data capability is limited to non-DAMA (satellite) mode. The terminal can support command and C2OTM (when equipped with the appropriate amplifier and antenna) and extend SINCGARS communications when paired with SINCGARS as a Retrans. AN/PSC-5 radio set components include the following:

- **RT-1672/U(C)—**contains RF and digital circuitry to perform the radio functions, embedded COMSEC, and modulation/demodulation of LOS, DAMA, and SATCOM communication modes. It provides the user with the capability of multiband operations within the frequency range of 30-400 MHz.
- **LOS antenna—**an omni-directional antenna optimized for the use in the UHF range. Figure A-3 shows an AN/PSC-5 and LOS antenna.
- **Satellite antenna system AS-4326/P (user supplied)—**used for satellite operations. Figure A-4 shows satellite antenna systems
- **Battery box—**contains two user-supplied BA-5590/U lithium batteries or two user-supplied rechargeable BB-590/U batteries.
- **Handset H-250 ()/U—**provides audio input/output for the unit.
- **Interface cable assemblies (W1 through W5)—**connects the radio set to various external devices. Figure A-5 shows interface cable assemblies.
- **Satellite antenna cable assembly (W6)—**interfaces to a satellite antenna. Figure A-5 shows a satellite antenna and other cable assemblies.

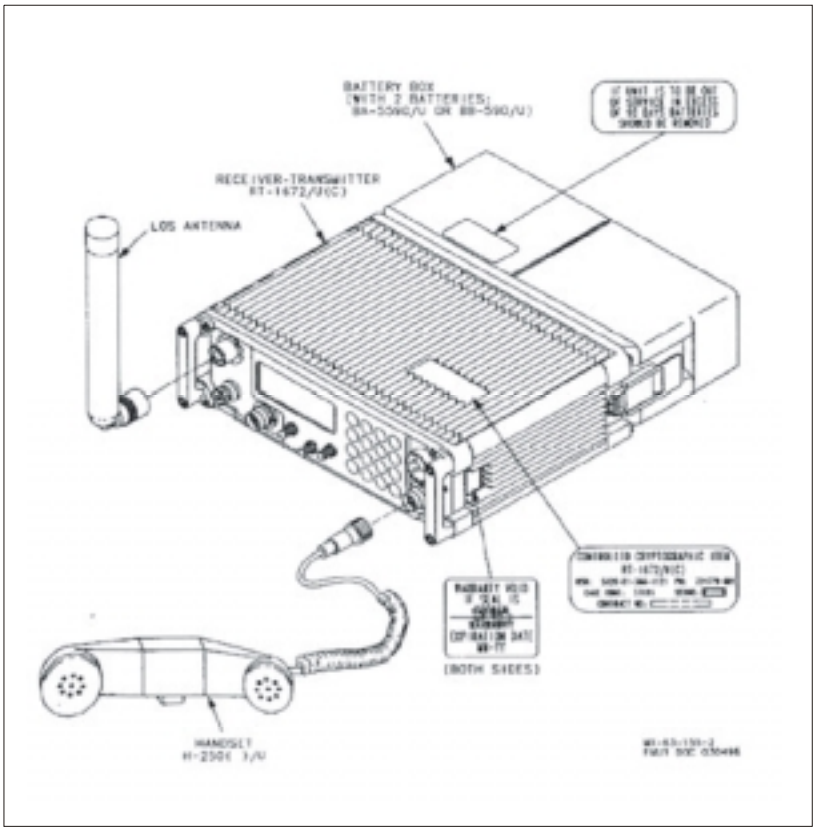


Figure A-3. AN/PSC-5 Radio Set Components

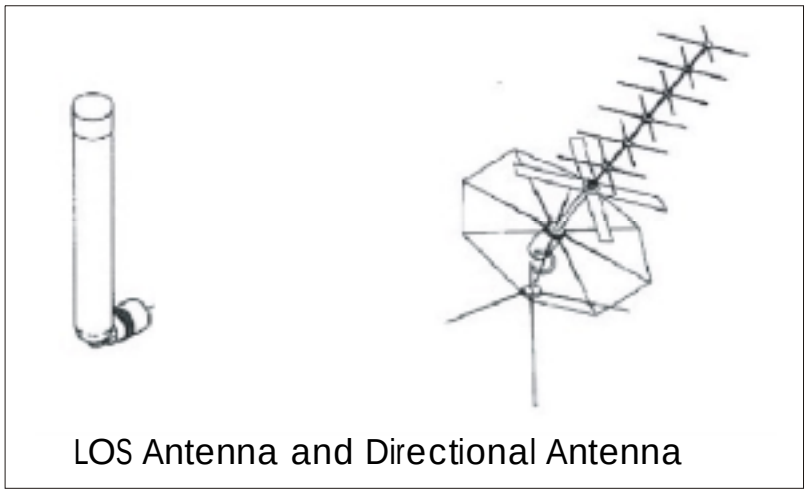


Figure A-4. AN/PSC-5 Antennas

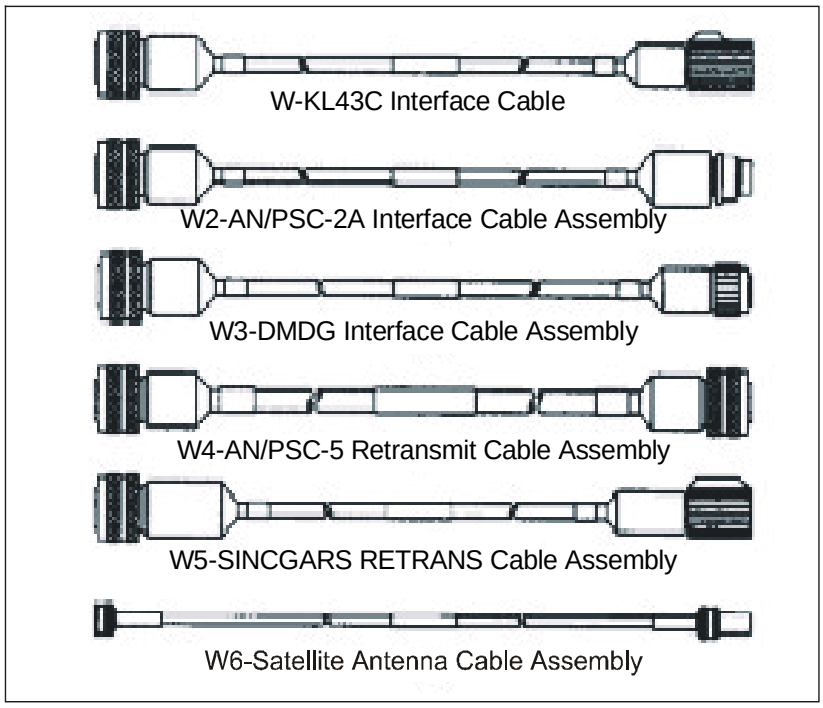


Figure A-5. Interface Cable Assemblies

Interface Equipment

A-4. Although the AN/PSC-5 cannot perform the frequency-hopping capability of the SINCGARS bandwidth, it communicates single channel with the SINCGARS terminals in the LOS mode. The AN/PSC-5 can also communicate with SINCGARS terminals in the abbreviated Retrans mode. This is when the SINCGARS network is Retransmitted through one AN/PSC-5 (which cannot communicate with the radios since it is in plain text [PT] mode) to another AN/PSC-5 that is set up for reception instead of Retrans. The distant end terminal will be used in the cipher text (CT) mode. The distant end terminal will be able to transmit and receive the messages sent within the SINCGARS network. This ability provides the user a limited BLOS capability with SINCGARS equipment.

A-5. The AN/PSC-5 radio set can be used in a Retransmit (range extension) mode with either PT or CT voice/data in LOS communication or, CT voice/data when used in a SATCOM relay. The CT information is not decrypted at the relay station; it simply passes through the relay station. Figure A-7 shows an AN/PSC-5-to-AN/PSC-5 Retrans.

A-6. In the Retrans mode, radio sets and SINCGARS need to be up to 25 feet apart, with operating frequencies at least 40 MHz apart. This separation prevents the transmitter of one radio set from blanking the receiver of the second radio set.

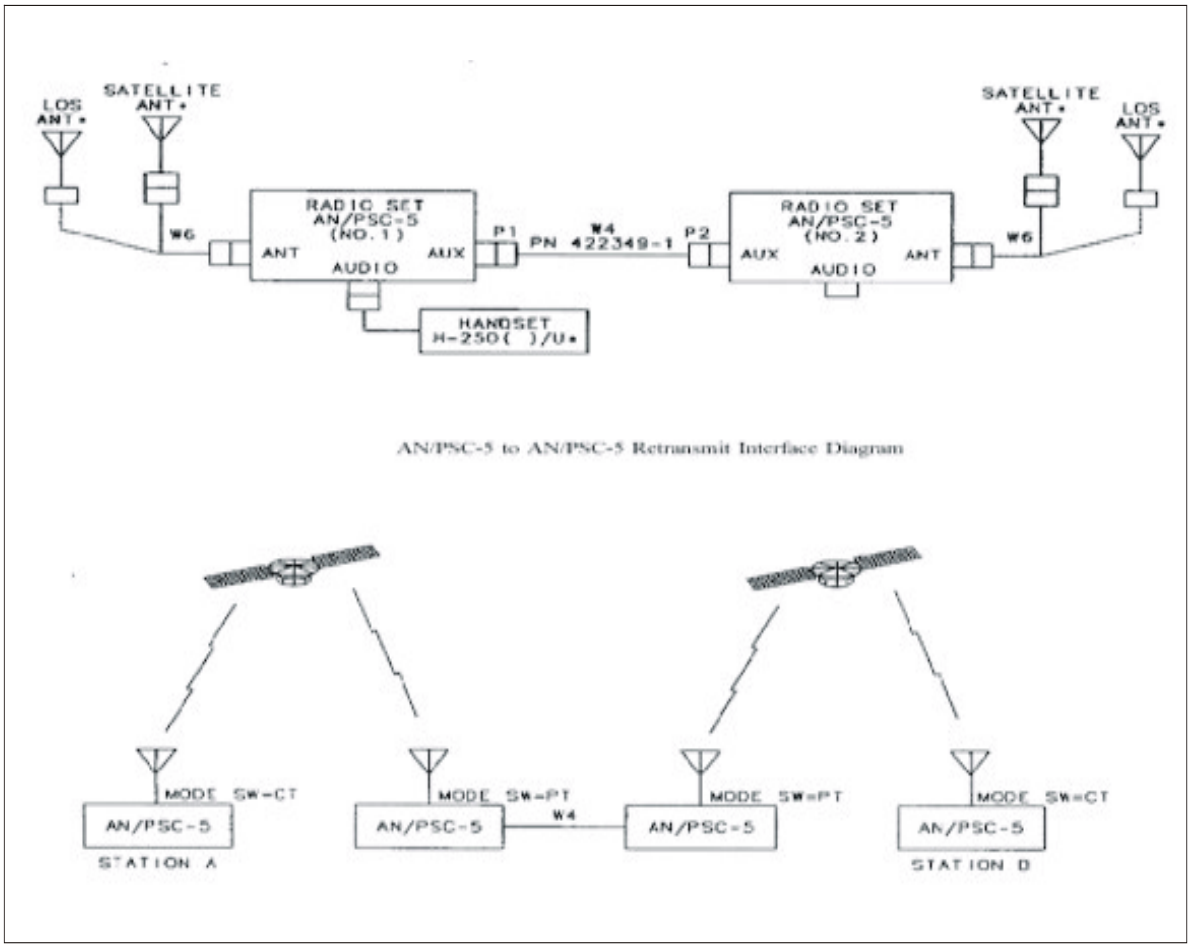


Figure A-7. AN/PSC-5-to-AN/PSC-5 Retrans

Appendix B

Relay/Retransmission Operations

A commander's ability to communicate with his subordinate elements/forces is imperative for a unit to accomplish its mission. Communication is critical in the planning and execution of any tactical operation. This appendix discusses the tasks required to employ a relay/retrans team in support of range extension.

OVERVIEW

B-1. Commanders are required to maintain C2 communications with appropriate headquarters and personnel. The BSC and battalion S6 deploy relay/Retrans teams to support the plan developed by the brigade S6. Each relay/Retrans team is equipped with an EPLRS radio set, NTDR, and two SINCGARS (AN/VRC-92F) to provide range extension for the TI, TOC-to-TOC data network, and SINCGARS nets. The placement of range extension equipment is critical for the SBCT information network; terrain and man-made obstacles restrict transmission distances.

PLANNING

B-2. Planning and coordinating a relay/retrans site is much like preparing for a combat mission. The BSC and S6—

- Take into consideration that a relay/retrans team will be moved to a remote location to support the battle, and may have limited to no force protection support.
- Ensure the relay/retrans team is trained and equipped to support the mission.
- Coordinate with the S2 and S3 to move the relay/retrans team to its new location.
- Ensure force protection measures are established for position ingress or egress.
- Develop C2 responsibilities for supervision and management of relay/retrans assets through out the network by the BNOSC.

MISSION ANALYSIS

B-3. The BSC and S6 perform the mission analysis based on the intent of the commander. The BSC and S6 must—

- Understand the threat in all phases of the unit's plan.
- Know the templated enemy air assaults, avenues of approach, chemical strikes, and obstacles.
- Develop a signal estimate.

- Look at branch/contingency plans and be prepared to cover them.
- Look for higher terrain further behind the forward line of troops (FLOT). Use the height and protection of corridor walls rather than isolated hills along valley floors.
- Coordinate with adjacent or higher unit assets.
- Analyze the impact of boundary changes, and consider how long it would take to move the Retrans team to support the change.
- Determine follow on mission relay/retrans requirements.

B-4. Once the S6 and signal company commander perform the mission analysis, they can collaborate on a course of action. Relay/Retrans missions must be planned in collaboration with the brigade S6 to ensure:

- Connectivity of the TOC to TOC data network.
- TI battlespace coverage.

RECONNAISSANCE

B-5. In parallel with the mission analysis and course of action (COA) development relay/retrans teams must assist in determining the route and site location as factors to mission accomplishment. Route reconnaissance can be conducted through-

- Aerial
- Ground
- Map

B-6. Prior to and during movement to relay/retrans sites teams ensure SA is obtained and validated through FBCB2 and the common tactical picture (CTP), focused on-

- Verified enemy locations
- Friendly unit locations
- Battlefield obstacles (minefields, NBC, etc.)
- Locations of friendly relay/retrans and TOC locations

B-7. Coordination for force protection assets is critical to mission success for emplacement and displacement of relay/retrans teams. Typically, scouts escort relay/retrans teams into position and ensures the site location is clear of enemy forces (Transition from HMMWV platforms to Interim Armored Vehicles (IAV) will provide the relay/retrans teams with organic force protection and may negate the need for route clearance by other forces.) Force protection of the relay/retrans site after occupation is the responsibility of the relay/retrans team.

PRIMARY AND ALTERNATE SITE LOCATIONS

B-8. The BSC and S6 should select two alternate relay/retrans sites for every phase of the mission. The relay/retrans team chief must understand the conditions and procedures for relocating the team. Alternate locations must be plotted and identified on the signal overlay through FBCB2.

RELAY/RETRANS TEAM CONSIDERATIONS

B-9. The relay/retrans team chief should consider—

- Supplemental force protection assets (Class IV, anti-tank weapons, etc).
- Accessibility of the relay/retrans site for resupply.
- Logistical support (coordinate with the S4 for fuel, rations, and equipment).
- Decontamination routes.
- Nearest medical support and the casualty evacuation plan.
- Situational awareness of the battlefield via FBCB2. Has the authority on mission withdrawal criteria.
- Evacuation plans (vehicular and non-vehicular).
- Establishment of signal communications nets for network operations(ie. High frequency radio, SINCGARS, FBCB2 messaging)

SECURITY

B-10. The relay/Retrans team establishes a perimeter defense of the site, remote radios, and antennas, when possible, and through the S6 provides the S3 grid coordinates for the location of aerial and ground support.

B-11. Relay/Retrans teams consist of either two or three soldiers for 24-hour operations. While one soldier conducts relay/retrans duty, one soldier sleeps and the other soldier is on perimeter security. If possible, the BSC and S6 will collocate relay/Retrans teams to help provide force protection and security.

B-12. If possible, an additional CNR asset should be assigned with the relay/Retrans team to allow for team updates and to receive updates from the BSC or S6.

MANAGEMENT

B-13. All relay/retrans teams within the SBCT will be monitored and managed, based on METT_TC, by the BNOSC. Critical battalion and SIGO relay/retrans teams identified by the brigade S-6 and tasked to provide brigade network support will be directly managed by the BNOSC. Battalion teams identified will be managed directly by the BNOSC in conjunction with their organic battalion S-6/NCOIC. Management of relay/retrans teams consists of-

- Determine and track current and future site locations to support network changes.
- Alerting, sending overlays, and messaging relay/retrans teams for changes, updates, and current situations.
- Directing unit task organization (UTO) or unit task reorganization (UTR) for critical relay/retrans teams.
- Providing logistical support, through relay/retrans team chiefs, to deployed teams.

Appendix C

Network Operations

The SBCT will establish network operations and security centers (NOSCs) to provide the NETOPS functions of NM and IA for the networks and information systems employed by the SBCT. This appendix covers the NM and IA responsibilities within the NOSC.

BNOSC

C-1. Two BNOSCs are established to perform NETOPS at the main CP and BSB, when the tactical situation dictates a third (BNOSC [FWD]) being deployed with the TAC CP. SBCT level NM and IA activities, functions, and tasks are performed primarily at the brigade main CP and the BSB support operations center.

C-2. The primary component of the BNOSC at the SBCT main CP is the BSN. The BNOSC provides the BSC commander and the brigade S6 with their primary NM capability. The BNOSC is used to manage the brigade WAN and LAN, and perform some IA functions to support combat forces, weapon systems, and battlefield automated systems (BASs). The BNOSC also contains the ISYSCON (V)4, TOC LAN, LKMS, TOC LAN management laptops, NTDR/JTRS systems, terrestrial communications links, Network Planning Tool (NPT), and the IA monitoring client. The NCS-E or ENM may not be collocated with the BNOSC at the SBCT main CP; however, EPLRS NM is the responsibility of the BNOSC operations personnel. Additionally, the BNOSC diagnoses, tracks, and in some cases repairs LAN or client system problems.

C-3. The BNOSC (FWD) can be located at the SBCT TAC CP and will have limited NETOPS capability. The BNOSC (FWD) will normally consist of brigade S6, S6 network operations center-vehicle (NOC-V), and a limited staff. The NM capability will be limited to the ISYSCON (V)4 and the NTDR manager terminal (NMT). IA capabilities will be available, although limited to software packages loaded on existing systems.

C-4. The alternate BNOSC resides at the BSB support operations center. It has the same basic NM and IA capabilities as the main BNOSC, and will assume the primary NETOPS responsibilities when required. Figure C-3 shows an example of alternate BNOSC configuration and functions.

NM

C-5. The objective of NM in the SBCT is to coordinate and manage the installation, operation, and maintenance of the networks and information systems that support warfighters' information requirements. Effective NM allocates network, information system, and security resources more efficiently to directly support operational forces. NM requires the

performance of a set of activities, functions, and tasks to control the network topology, maintain its operational capability, optimize its performance, and reconfigure networks to meet changing mission requirements. Specific NM activities include—

- Service provisioning.
- Planning.
- Engineering.
- Logistics.
- Fault, performance, configuration, and security management.

C-6. C-6. The SBCT will coordinate network requirements and planning with the ARFOR G6. The ARFOR and SBCT network must be planned collaboratively to ensure the optimal use of assets. The ARFOR will support the SBCT with complex network planning, network engineering, fault management, and battlefield spectrum management. This NM relationship requires that network management systems for the ARFOR and the SBCT be compatible and interoperable to allow exchange of mission planning and engineering data. Compatible systems will provide the tools for the transfer of authority and permit a shared view of the operational network.

C-7. Performance, configuration, fault, and security management will be the primary focus of NM during the initial deployment. As the AO matures and the networks are adjusted to meet changing mission requirements, the NM cycle will begin again. Figure C-1 shows the network management cycle.

NOTE: In the tactical environment, all activities found in the normal NM cycle are not conducted. For example, chargeback, procurement, and accounting management are normally not performed. See FM 6-02.71 for more information on the NM cycle.

Service Provisioning

C-8. This NM activity adds, deletes, or changes network and information systems services available to the warfighter. It covers the non-engineering tasks associated with providing users access to required services. During the pre-deployment phase, most information services will be provided as part of the SOPs for contingency operations. Some services will be changed based on mission-unique requirements established in the OPORD. During the deployment phase of an operation, information services will be tailored to changing mission requirements. The primary functions associated with service provisioning include–

- Reviewing, validating, and tracking new communications and information processing requests that are in addition to SOP services.
- Selecting new or existing network and information systems resources to meet the warfighters' service requirements.
- Changing the network configuration to provide new or modified services.
- Validating system modifications and verifying the users' requirements have been met.

- Reconfiguring end-user equipment to make it compatible with the supporting communications and information systems.

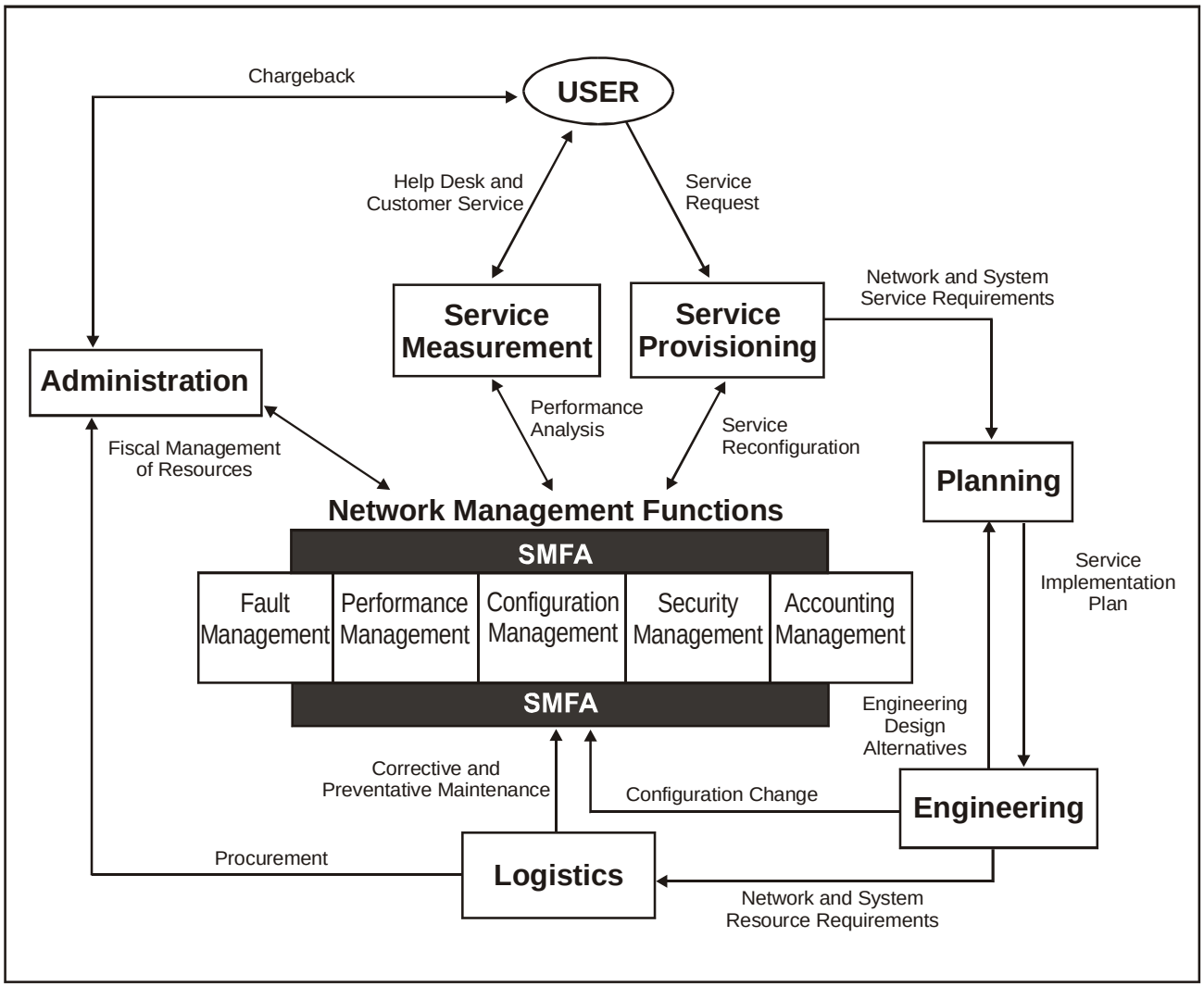


Figure C-1. NM Functions and Activity Cycle

Planning

C-9. In the pre-deployment phase, the planning activity consists of non-real-time functions that involve acting on the information service requirements identified through the service provisioning analysis. The ultimate goal of planning is to ensure resources are available to meet the deployment phase requirements. Additional planning will be required to meet changing mission requirements during the deployment phase of the operation. Functions associated with planning include–

- Analyzing user needs by gathering, forecasting, and assessing warfighters' requirements, which includes planning for future contingencies, deployments, and re-deployments.
- Determining the network and information systems resources needed.
- Identifying contingency and restoration capabilities, such as alternate routing and spare equipment to overcome system failures.
- Planning the configuration of the network and information systems to meet established performance and capacity requirements.
- Developing a security plan by performing a risk assessment and continuously conducting reviews of current or potential threats to and vulnerabilities of the networks and information systems.
- Determining and resolving network protocol conflicts and resourcing provisions from the HICON.
- Optimizing the placement of resources against subscriber requirements, terrain considerations, and the tactical situation.

Engineering

C-10. Within this activity, the networks and information systems are tailored to meet warfighters' requirements. Engineering bases design requirements on the planning provisions that relate to capacity allocation and the new services to be implemented. Some functions associated with the engineering activity include–

- Specifying user requirements and designing the overall networks and information systems to meet user communications and processing requirements.
- Specifying the security capabilities of the networks and information systems to assure user services are protected.
- Configuring equipment to meet warfighters' requirements within designated performance parameters and available resources.
- Providing a centralized source of system expertise to help resolve technical issues with the users.
- Battlefield spectrum management to eliminate or minimize adverse collateral effects of co-site and adjacent frequency interference as it considers all battlefield systems (including non-signal emitters) in managing the spectrum.
- Resolving network conflicts and developing processes to merge network protocols from HICON and adjacent units.

Logistics

C-11. This NM activity provides for the logistical support of the networks and information systems. Logistics includes storage, distribution, maintenance, and replacement of materiel, such as spare and repair parts and consumable items. Logistics functions include–

- Performing preventive maintenance on a scheduled basis to lower the probability of trouble occurrences and to maintain optimum performance levels.

- Performing corrective maintenance to quickly restore information services as a part of the real-time fault management function.
- Requisition processing to ensure spare and/or replacement parts are available for network and information systems preventive and corrective maintenance.
- Maintaining the established levels of supply items to satisfy anticipated requisitions.

Fault Management

C-12. Fault management provides the status of the networks and information systems to detect, isolate, and correct problems before they cause a major interruption to information services. Network managers will perform scheduled maintenance activities and initiate tests to detect or correct problems before service troubles or outages are reported. This process allows the network manager to initiate service restoration and perform activities necessary to repair the diagnosed fault. Fault management tasks include–

- Monitoring specific events or alarms to detect or predict faults and identify specific equipment or network problems.
- Initiating tests and diagnostics to isolate faults to a replacement component level.
- Restoring the network or information system to working order by applying corrective actions, such as switching to standby components, replacing components, or reinitializing systems or components.

Performance Management

C-13. Performance management ensures the most efficient use of network resources (such as bandwidth) and their ability to meet user service-level objectives. It enables network managers to ensure networks and information systems are at their peak performance and deliver voice, data, imagery, and video services to the warfighter. Specific performance management tasks include–

- Monitoring selected events and network resources and analyzing performance indicators, such as traffic load, usage trends, and capacity limitations.
- Controlling performance by fine-tuning the network and information systems configuration by optimizing storage, transmission, and processing resources.
- Analyzing periodic reports that provide baseline performance parameters.
- Monitoring LANs and WANs for network-loading analysis to identify potential problem areas and direct the reconfiguration of the network as required to support changing user requirements or network outages.

Configuration Management

C-14. Configuration management enables the network manager to configure networks and information systems to meet the support requirements of the warfighter. It also allows control over changes as resources are reallocated for

priority of service to support the commander's operational requirements. Configuration management also overlaps with resource provisioning (timely deployment of resources to satisfy the expected service demand), service provisioning (assigning services and features to end-users), and network planning and engineering (automated planning, design, and engineering of all communications networks to support the various tactical courses of action). This capability is critical for preparing, initializing, and providing for the operation and termination of services. Specific configuration management tasks include–

- Maintaining the desired real-time network and information systems configuration status.
- Maintaining a combination of tools, tests, reports, policies, and procedures needed by network managers to implement, monitor, and maintain an end-user information system.

Security Management

C-15. Security management provides for network and information systems security services and a portion of the overall IA management function. It protects against intentional or accidental abuse, unauthorized access, and communications loss. Security mechanisms will accommodate ranges of control and inquiry privileges that result from the variety of access modes by operations systems, service provider groups, and customers whom need to be administratively independent. Security management tasks include–

- Controlling access to the entire network or information system, or selected portions, by granting or restricting the password capability of users.
- Gathering, storing, and accessing relevant information for analysis, detection, and control purposes.
- Managing COMSEC using the Army Key Management System (AKMS) hardware and software to automate cryptonet planning, management, and engineering, including COMSEC record keeping and audit trails. COMSEC management also includes the development of an operational plan—initialization of system (cold start) planned keying, rekeying, movement and displacement (renetting), expiration of cryptographic period, and compromise.

IA

C-16. IA assures the availability, integrity, authentication, confidentiality, and non-repudiation of friendly information and information systems. IA provides a defense in depth (DID) that protects networks and information systems against exploitation, degradation, and denial of service by incorporating vigorous detection, reaction, and restoration capabilities. DID allows for effective defensive measures and/or timely restoration of debilitated information systems.

C-17. IA capabilities are limited within the SBCT. The SBCT higher control (HICON) has the responsibility to perform IA for the SBCT. The BSN and NOC-V contain the following IA systems:

- Cisco 7206.

- WatchDog.
- Sniper.
- CiscoWorks 2000.
- NetRanger.
- Intrusion Detection System 2000 (IDS 2000).

C-18. The IA process ensures that authorized users have guaranteed access to appropriate friendly information systems. Friendly information systems are protected from unauthorized change or tampering; authorized users are verified. The system protects information from unauthorized disclosure. Friendly information systems provide an undeniable record of proof of user participation and transactions. An information system or process that lacks any of the above IA components is vulnerable to adversary disruption or exploitation and must be considered unreliable.

C-19. Typically the greatest risk for network intrusion and integrity is from the users within the network. Protection from such user corruption is accomplished through efficient and comprehensive password and access management. Without effective levels of IA security starting at client terminals up to gateways compromise of information and the integrity of the network is assured.

Risk Management

C-20. A comprehensive risk management program is the most effective way to protect the SBCT's networks or information systems. Risk management identifies, measures, controls and eliminates, or minimizes uncertain events that may adversely affect system resources. The objective of risk management is to achieve the most effective safeguards against threats of both intentional and unintentional intrusions into a network or system. Intentional intrusions are planned attacks against an IO resource and must be protected against by an effective DID. Risk management also includes identifying system and network vulnerabilities created by weaknesses in design, ineffective security procedures, or faulty internal controls that are susceptible to exploitation by authorized or unauthorized users.

C-21. **Threats.** Threats to the SBCT's networks and information systems are genuine, and can come from individuals and groups motivated by military, political, social, cultural, ethnic, religious, personal, or industrial gain. They vary by the level of hostility (peacetime, conflict, or war), technical capabilities, and motivation of the perpetrator. It is virtually impossible to defend against all possible threats. However, IA programs will include a threat assessment ensuring the necessary protection and defense mechanisms are in place. Threats generally fall into three categories: intentional, unintentional, and environmental intrusion.

C-22. **Attack.** Attacks are intentional intrusions against a network or information system and are generally aimed at software or data contained in either end-user or network infrastructure computers. Attacks can be from an opposing military force, mischievous or vengeful insiders, terrorists, hackers, or foreign espionage agents.

C-23. **Vulnerabilities.** The warfighter's increased dependence on commercial reach-back information capabilities has created vulnerabilities to networks and information systems employed by the SBCT. Attackers can quickly take advantage of weaknesses in design, ineffective or lax security procedures, or insufficient internal controls. A periodic vulnerability analysis will be conducted on all of the SBCT's networks and information systems to assess their security capabilities.

Protection, Detection, and Reaction Capabilities

C-24. The warfighter's assurance that the SBCT's networks and information systems are defended adequately against attack requires the ability to protect the information that is passed and stored, detect when an intrusion happens, and react to contain the damage and repair the network or information system.

C-25. **Protection.** Information protection applies to any medium and form, including hard copy, electronic, video, imagery, voice, computer, and human. Network managers must devise and implement comprehensive plans for using a full range of protective measures. Protection measures for network and information systems should consist of firewalls, intrusion detection systems, router filtering and access control lists, password control, COMSEC, in-line encryption devices, security guards, physical isolation, and software that hardens them against intruders. Protection plans will include external and internal perimeter defense.

C-26. **Detection.** Real-time security management and intrusion detection should be a part of routine operations for the IA cell (IAC) located in the BNOSC. To detect occurrences that constitute violations of security policies, selected events or occurrences (such as numerous log on attempts within a specified period) are monitored using the above-mentioned protection and detection tools, devices, and capabilities. When violations are detected, the network manager must prevent further violations and report the event to the commander, IAM, and supporting computer emergency response team (CERT).

C-27. **Reaction.** Reaction to a network or information system intrusion incorporates the capability to restore essential information services, change existing protective measures, and initiate attack response processes.

C-28. Restoration of information services can be quickly accomplished by following a detailed continuity of operations plan (COOP).

C-29. Changing protective measures incorporates actions, such as reconfiguring firewalls, guards, and routers; rerouting traffic; changing encryption levels or rekeying; zeroizing suspected compromised communications; re-establishing nets without selected members; or changing passwords and authentication.

C-30. The response processes begin when the emergency is under control and information services are restored. Responses can be offensive or defensive. Offensive measures are restricted to law enforcement agencies during peacetime operations. During hostilities, the commander may use military force to eliminate or disrupt the means or systems that an adversary uses to

conduct an information attack. Defensive responses include all measures and countermeasures available to a commander to limit or counter an adversary's attack, exploitation, deception, or electronic warfare (EW) capability to protect against further attacks.

IA Management Structure

C-31. The SBCT commander appoints an IA manager (IAM), with the brigade S6 normally performing the IAM mission. The IAM's responsibilities include–

- Developing, staffing, and managing IA plans for the SBCT.
- Coordinating IA activities with HICON and adjacent units.
- Conducting individual network and information systems risk assessment to determine potential threats and vulnerabilities, and determining appropriate measures to effectively manage the risks.
- Conducting IA training and awareness programs.
- Implementing IA and information assurance vulnerability alert (IAVA) reporting and compliance procedures, to include IA incidents and technical vulnerabilities.
- Ensuring that an information assurance security officer (IASO) is appointed for each battalion and/or separate network and information system.
- Ensuring that the BSC appoints an information assurance network manager (IANM).
- Establishing the scope of responsibility for each IASO and the IANM.

C-32. The BSC commander appoints an IANM. The IANM's responsibilities include–

- Supervising the IA cell in the BNOSC and ensuring all protection devices are monitored and maintained.
- Implementing the IA program for the SBCT's WAN, NTDR/JTRS, LAN, and TI networks IAW policy established by the IAM.
- Ensuring procedures are in place to support security integrity of the networks, provide protection for the networks, and support secure access controls and connectivity.
- Determining the network plan for IA to distribute the IA tools to the network and information system managers.
- Downloading the appropriate tools as they are updated or new tools are introduced.
- Downloading and distributing the current network intrusion detection system (NIDS) attack and virus files and the relevant software security patches.
- Monitoring the NIDS for possible attacks and reconfiguring the network, if necessary.
- Ensuring that password integrity is maintained.

- Developing and implementing security procedures and protocols for the networks.
- Conducting reviews of network threats and vulnerabilities, and reporting to the IAM any attempts to gain unauthorized access to the network.
- Implementing IA and IAVA reporting and compliance procedures to include the use of only Army-approved IA products.

C-33. The commander of each battalion or information system appoints an IASO. The battalion commanders will normally appoint the battalion S6 as the IASO. The IASO's responsibilities include–

- Preparing, distributing, and maintaining plans, instructions, guidance, and SOPs for information systems security.
- Preparing or overseeing the certification and accreditation documentation of systems IAW AR 25-IA.
- Coordinating with the battalion and brigade S2s to ensure users have the required security investigations, clearances, authorizations, and need-to-know.
- Establishing and implementing a system for issuing, protecting, and changing systems' passwords.
- Establishing the training and awareness programs.
- Ensuring and monitoring the proper security of systems connected to the network.
- Assessing direct threat and vulnerability, enabling the commander to analyze the risks to interconnected systems.
- Determining appropriate measures to manage network risks effectively.
- Overseeing the review of network and information systems' audit trails, resolving discrepancies, and reporting incidents to the brigade and battalion S2s for evaluation and reporting.
- Performing password control duties as assigned.

MANAGEMENT SYSTEM CAPABILITIES

C-34. The BNOSC employs management tools and techniques that reach the user terminal level throughout the various networks. The BNOSC provides network managers with automated tools to plan, manage, and engineer tactical communication networks. The BSN, ISYSCON V(4), NCS-E/ENM, and NTDR management tool provide the NM tools employed in the BNOSC. Figures C-2, C-3, and C-4 show the full array of NM and IA tools and functions that may be available in the BNOSCs.

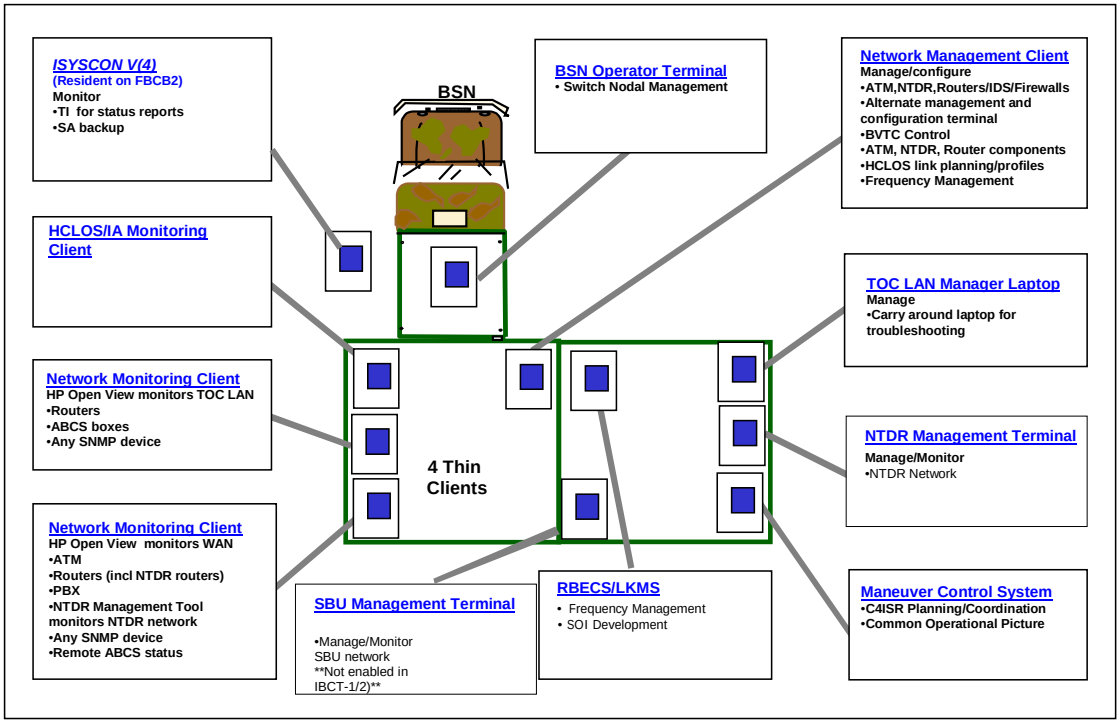


Figure C-2. BNOSC

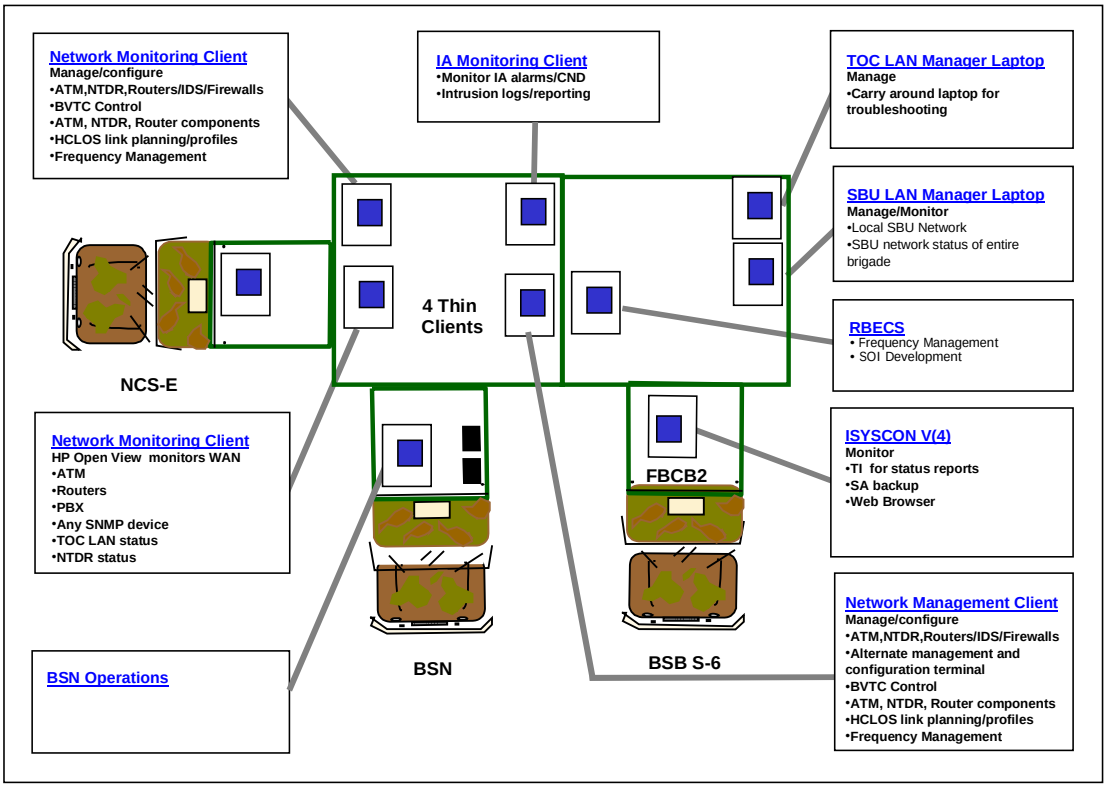


Figure C-3. BNOSC (Alternate)

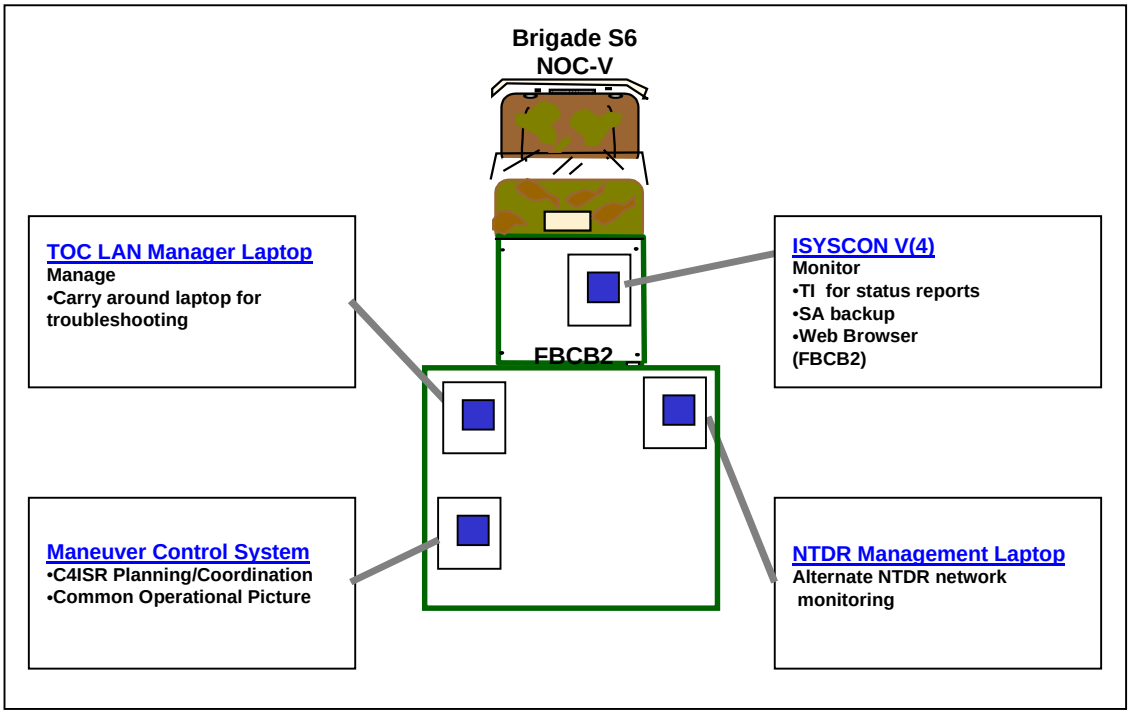


Figure C-4. BNOSC (Forward)

ISYSCON V(4)

C-35. The ISYSCON V(4) manages the TI and enables the exchange of information with organizations and individuals not directly connected to the TI. In addition to the BNOSCs, ISYSCON V(4) reside in the S6 sections of the battalions. Each ISYSCON V(4) is associated with a designated LAN and one or several remote LANs or extended networks. The ISYSCON V(4) exchanges technical and operational database information for network and subscriber device management. This information is needed to monitor and control the networks under its domain, and to modify and disseminate data concerning subscriber requirements with other ISYSCON V(4).

C-36. The ISYSCON V(4)—

- Establishes automated interfaces with all maneuver brigade communications systems.
- Monitors single and/or multiple LANs in the TOC.
- Monitors connectivity through the access points in the TOC.
- Maintains TOC LAN status reports on the performance and use of the ABCS and Global Combat Support System-Army (GCSS-A).
- Sends and receives LAN status reports to subordinate and higher headquarters.
- UTO/UTR Capable.

C-37. The ISYSCON (4) engineers and plans the network configuration prior to initiation of operations based upon pre-deployment OPORD and plans. However, changes to operational requirements call for automated network reconfigurations, parameter changes, and configurable network modeling tools. The objective ISYSCON (4) will provide network configuration planning, network device configuration, network monitoring, NM, network services, event and action logging, and troubleshooting tools.

NCS-E/ENM

C-38. The NCS-E/ENM are used for system initialization, monitoring, management, and control of the EPLRS network. They may be located primarily in the vicinity of the SBCT main CP and TAC CP, and collocated with the BNOSC (alternate) at the BSB. The NCS-E/ENM contains tactical computers that provide automated technical control and centralized NM of EPLRS. It is the primary technical control interface. NCS-E/ENM software provides network monitoring and resource assignment that satisfies communications, navigation, identification data distribution, and position location requirements. The NCS-E/ENM sets up and monitors communications needlines used for host-to-host communication between the NCSs and other computer systems. for more detailed information on the NCS-E/ENM.

NTDR NMT

C-39. The S6 uses the NTDR NMT to initialize, monitor, and reconfigure the network links to the battalion TOCs.

DEFENSE MESSAGE SYSTEM (DMS) MANAGEMENT

C-40. The DMS management responsibility resides with the TMS team at the ARFOR, along with all of the hardware and software performing this function. The SBCT S6 section is responsible for the DMS software functionality in the brigade and battalion C2 information systems.

Appendix D

Enhanced Position Location Reporting System Operations

The EPLRS provides communications backbone for the TI within the SBCT. The system is jam-resistant and provides secure data transfer for the FBCB2 and other C2 systems. This appendix is arranged into two sections providing an overview of the EPLRS functions and the network architecture. Section I is focused on the EPLRS supported by the sheltered NCS and fielded in the initial SBCT's. Section II is focused on the downsized EPLRS network management (ENM) system designed to replace the sheltered NCS and fielded in the SBCT's in FY03.

SECTION I – FUNCTIONAL DESCRIPTION

D-1. EPLRS is a LOS, data-only digital radio system primarily used in the SBCT for the TI backbone. It can be used as a position, location, navigation, identification, and communications system.

COMPONENTS

D-2. The SBCT will employ four major components of the EPLRS: the NCS-E, EGRU, gateway, and radio sets (RSs). These components support the TI and other SBCT data requirements. Supporting United States Air Force (USAF) elements may deploy with the SA data link (SADL) to enable aircraft to receive ground forces SA data.

NCS-E

D-3. The NCS-E is used for system initialization, monitoring, and controlling of the network. The BSC is assigned three NCS-E assemblages. The NCS-Es will be located primarily in the vicinity of the SBCT main CP and the third being deployed per METT-TC. The NCS-E contains tactical computers that provide the focal point for automated technical control and centralized EPLRS NM. It is the primary technical control interface. NCS-E software provides network monitoring and resource assignment that satisfies communications, navigation, identification, data distribution, and position location requirements. The NCS-E sets up and monitors communications needlines used for host-to-host communications between the NCSs and other computer systems. Figures D-1 and D-2 show the interior curbside and roadside view, respectively, of the downsized NCS-E.

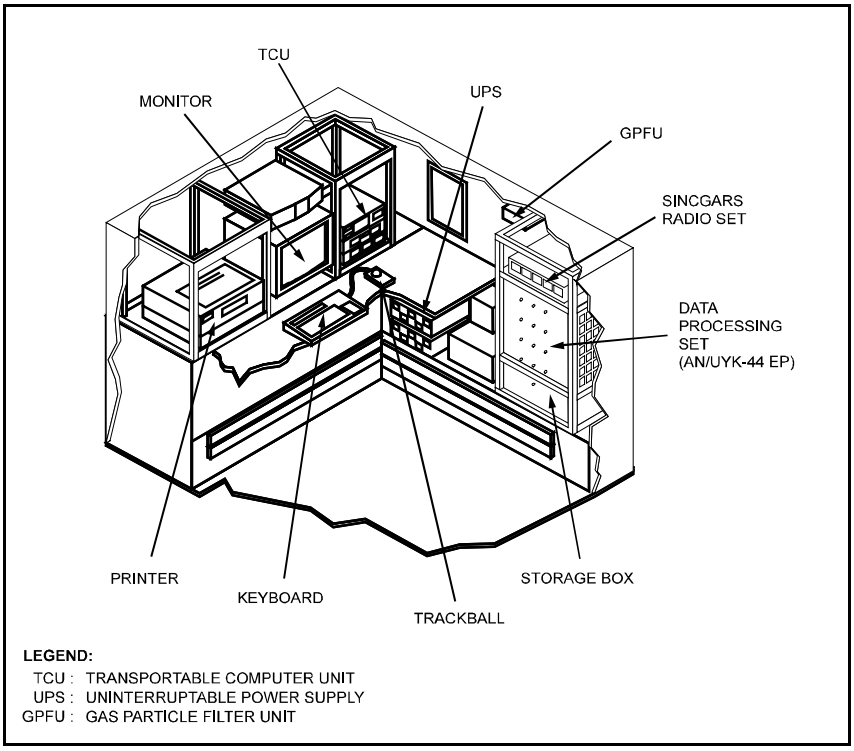


Figure D-1. NCS-E Interior Curbside View

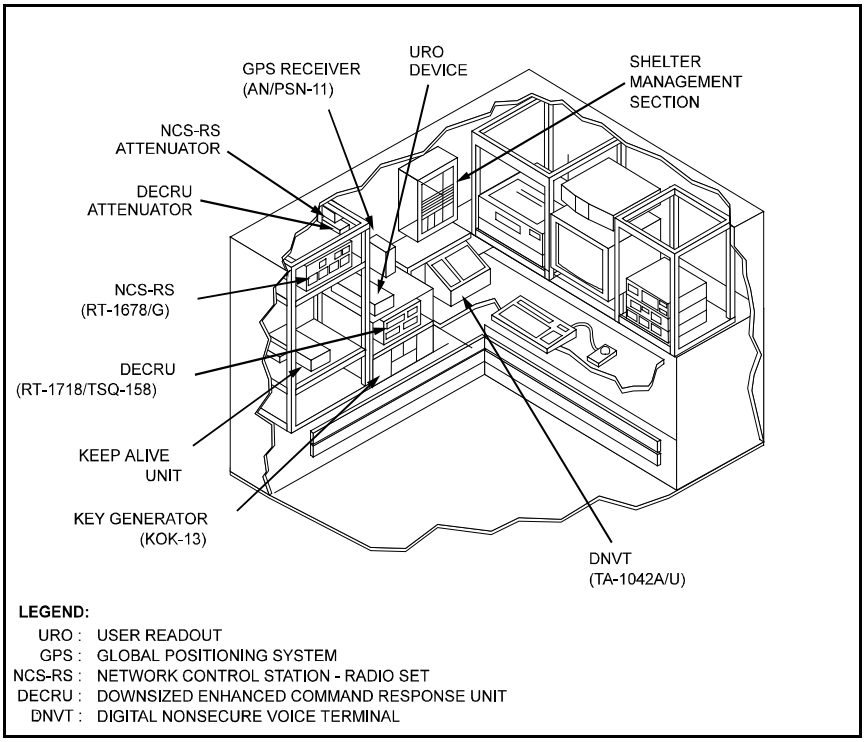


Figure D-2. NCS-E Interior Roadside View

D-4. The NCS-E is mounted on an HMMWV and is equipped with a 10-kilowatt generator. Figures D-3 and D-4 show external roadside and curbside views, respectively, of the NCS-E. The NCS-E is a central processing facility that provides position location, identification, and navigation information to the forces it supports.

D-5. The NCS-E controls the EPLRS control network, performs all the necessary calculations, routes control net messages and queries, and graphically displays the positions of all active radio sets. The NCS-E controls access to cryptographic keys and uses over-the-air rekeying (OTAR) to transmit required keys to radio sets.

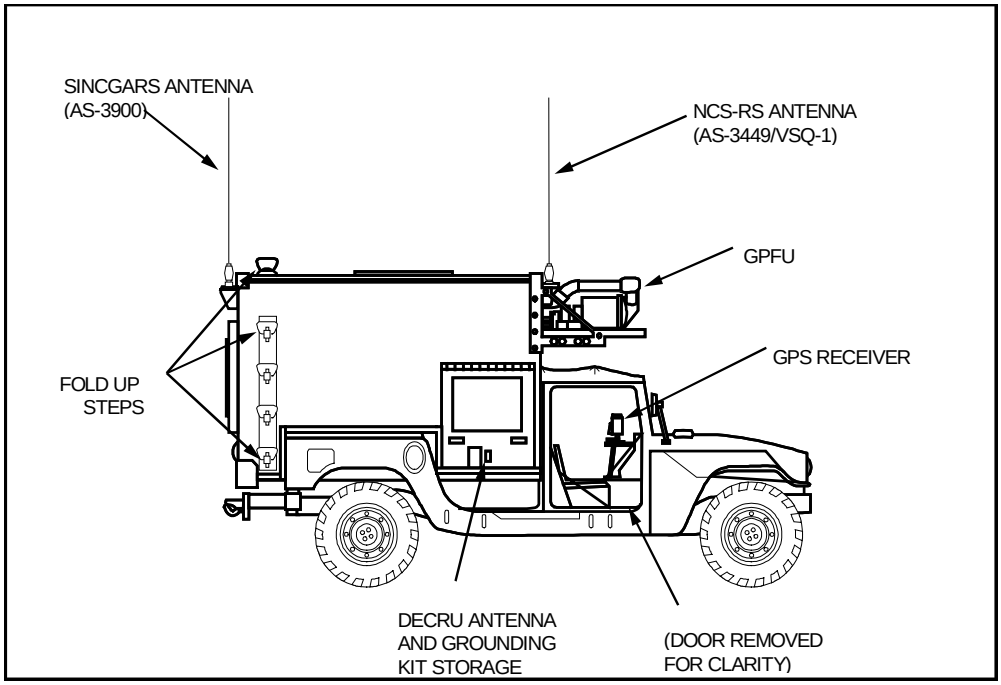


Figure D-3. NCS-E External Curbside View

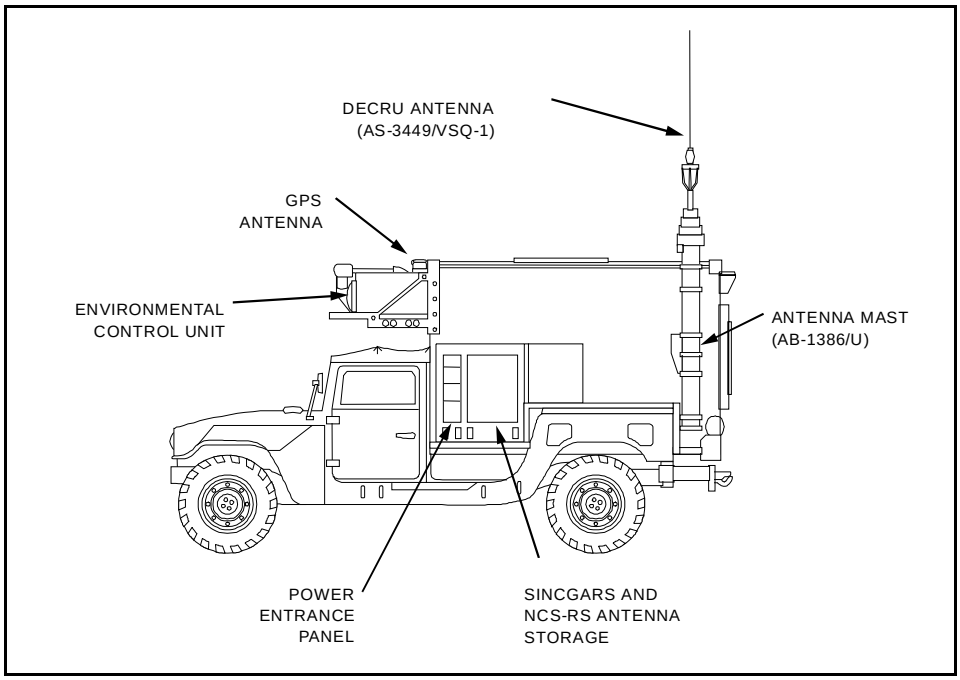


Figure D-4. NCS-E External Roadside View

EGRU

D-6. The BSC personnel operate and maintain the EGRU. The EGRU provides dedicated grid reference EPLRS NCS-to-NCS relay support for the EPLRS network. It also has the functional capability to be used as a relay or a gateway unit. The utility of the EGRU is most beneficial during mission occurring in urban terrain (MOUT) operations where locating an EGRU atop a building would provide the greatest SA relay coverage.

GATEWAY

D-7. Gateways are primarily suited to provide connectivity to adjacent EPLRS networks. Gateways can also be used to provide dedicated relay support for the SBCT. In cases where adjacent unit gateway requirements exist, the systems will reside in areas on the battlefield to provide TI backbone connectivity.

RS

D-8. The RS is allocated to EPLRS users and operators, and provides secure, jam-resistant, digital communications. The RS interfaces with the FBCB2 platforms within the SBCT.

D-9. The RS is a small, lightweight radio providing data throughput and a sophisticated POS/NAV capability. The RS accepts and implements NCS-issued commands and reports its status to the NCS-E. These reports are essential for accomplishing the automatic control of the EPLRS. Figures D-5 shows the frontal view of the EPLRS RS.

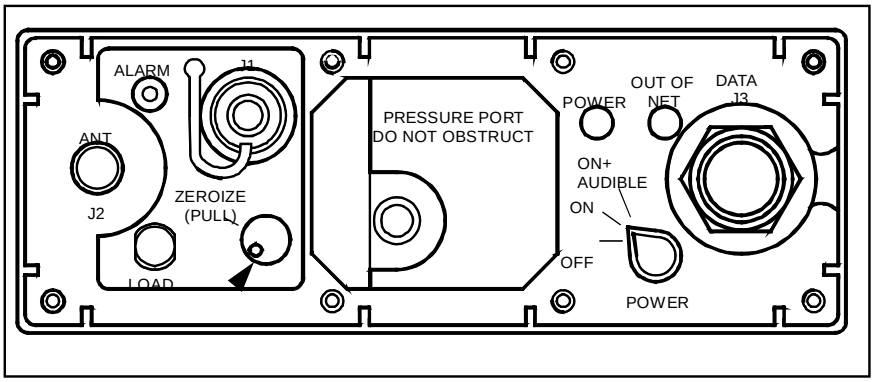


Figure D-5. Frontal View of the EPLRS RS

SADL SYSTEM

D-10. The SADL uses the EPLRS to provide a data-link for fighter-to-fighter, fighter-to-ground, and ground-to-fighter information transfer. SADL takes advantage of EPLRS being a secure, jam-resistant communications system with low probability of intercept qualities to provide a near-term data link capability for older USAF aircraft.

D-11. The SADL enhances a pilot's SA of friendly ground troop concentrations and position to prevent fratricide when operating in the air-to-ground role. It capitalizes on developing Army digitized battlefield architectures.

D-14. **Planning**. Planning USAF SADL assets entering the SBCT area of operations requires close coordination on the part of the brigade S6, BSC operations section, and USAF personnel. The BSC operations section requires the RS identification from the USAF prior to the aircraft entering the SBCT AO. The USAF requires COMSEC from the brigade EPLRS network to operate in the SBCT EPLRS network.

NETWORK ARCHITECTURE

D-15. EPLRS network architecture supports the transmission of C2, SA, and position/navigation (POS/NAV) data throughout the battlespace on the battlefield. The network architectural concept is based on EPLRS communities configured to support a SBCT AO.

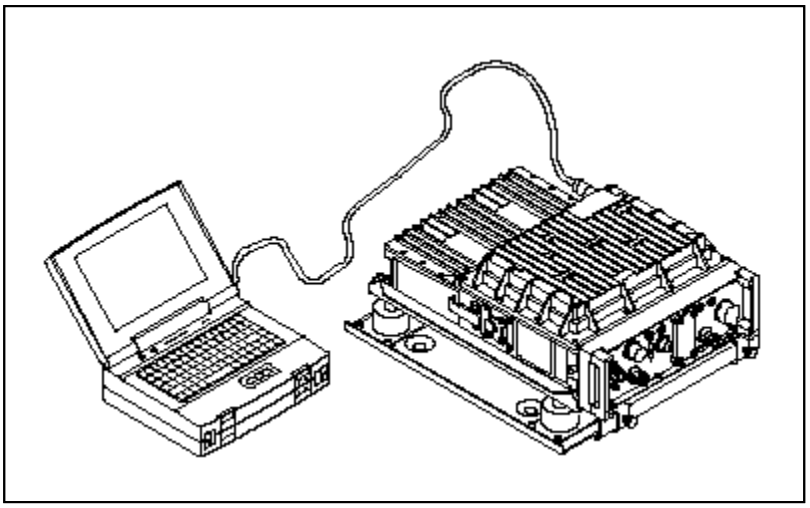
D-16. The company operations section of the BSC, as part of the BNOSC, directs the employment of NCS-E and EGRUs based on direction provided by the brigade S6. The SBCT EPLRS network community (generally made up of three NCS AORs) has its own time synchronization and cryptographic keys. Gateways, consisting of a pair of interconnected radio sets, achieve data communications between these communities. EPLRS allows users to move between a division's communities while retaining system services.

SECTION II - EPLRS NETWORK MANAGEMENT (ENM)

D-17. The ENM was developed to configure, control, and monitor an EPLRS network, thereby taking the place of the EPLRS NCS. With the elimination of the EPLRS NCS, the ENM and the EPLRS Radio Set (RS) now perform the EPLRS network management functions formerly handled by the EPLRS NCS.

D-18. ENM will enable the BSC and S6s at all levels to monitor, configure, manage, and plan the EPLRS network for the SBCT. Additionally, ENM will enable UTO/UTR to occur seamlessly between the planning and execution of task organization changes. Figure D-6 shows the ENM laptop connected to the EPLRS radio set.

Figure D-6. ENM with Radio Set



D-19. As with the original EPLRS configuration addressed in Section I the gateway vehicles and EGRU's will remain as critical nodes to provide relay and adjacent linking of other EPLRS networks.

FUNCTIONAL DESCRIPTION

D-20. The ENM system consists of three distinct functions:

- Planning
- Operations
- Monitoring

D-21. The ENM software encompasses all three mission areas as a single software application, thus any ENM can be initialized to perform any ENM mission. Access to the separate mission areas is controlled through software passwords.

D-22. The ENM supports two levels of management privilege, determined by user login. Each ENM can be designated to have Network ENM privileges and Monitor ENM privileges.

- Network ENM - All ENM functions are available.
- Monitor ENM – Only those functions required to manage the ENM RS and perform passive network monitoring are supported. May do auto reconfiguration and OTAR of COMSEC keys as a selection option when initializing as an ENM Monitor.

D-23. To perform the operations and planning missions, the ENM is initialized as a Network ENM. To perform the monitor function, the ENM will be initialized as a Monitor ENM. For additional detailed ENM operational procedures see Technical Bulletin (TB) 11–5825–298–10–1, *Operator's Manual for Net Control Station (AN/TSQ–158A) EPLRS Network Manager (ENM),* and TB 11–5825–298–10–2, *Operator's Manual for Communication Subsystem (AN/USQ-165).*

PLANNING

D-24. EPLRS network planning is the function of creating the EPLRS deployment plan, which is electronically documented in the ENM as an EPLRS network configuration file. This configuration file is a deployment wide file, which contains the configuration information for all EPLRS radios in the network. Once generated, this configuration file is copied and distributed to all Network ENM's (planners, operations, and monitors) in the deployment. The Tactical Internet Manager (TIM) provides the initial parameters for the generation of the EPLRS configuration file to the planner (currently a manual process via spreadsheet, but in the future, an electronic file via LAN/floppy). Changes to the configuration file (such as unit task organization (UTO) changes) or new cryptographic key files will be created by the planner and distributed to operations and monitor ENM's. There is only one active planner per deployment. If this planner is compromised, another ENM node (usually an operations ENM) will be designated as the planner by the BNOSC.

D-25. The ENM is not used to design the EPLRS network. The role of ENM in the planning process is to provide a computer–based tool for data entry and deployment plan file generation. This tool is the EPLRS Network Planner (ENP) and this tool helps the planner or designated operator create or modify a deployment plan database file and the corresponding RS configuration data files for network RSs. ENP handles operational parameter data but does not directly handle cryptographic keys. ENP enables you to generate a deployment plan database file, which is in turn used by ENM to generate individual RS configuration files. ENM sends the RS configuration files to the RSs during the configuration or reconfiguration process. ENP can generate a deployment plan database file by any one of three methods:

- Modifying an existing deployment plan file
- Inputting a Tactical Internet Manager (TIM) database file
- Creating a completely new deployment plan file

D-26. Figure D-7 shows the flow of data for the network configuration planning function, illustrating the three methods listed above. Planning can be performed either on–line or off–line. The ENM operator can use ENP to import a TIM file and create a deployment plan file from the TIM file. The operator can also load and modify an existing deployment plan file and use

ENP to edit it. ENP generates the final deployment plan file, which is then distributed to the network. The deployment plan file contains RS configuration files for each RS in the network. After the network is activated, these files are sent over the air to individual RSs whenever ENM determines that a specific RS needs to be reconfigured.

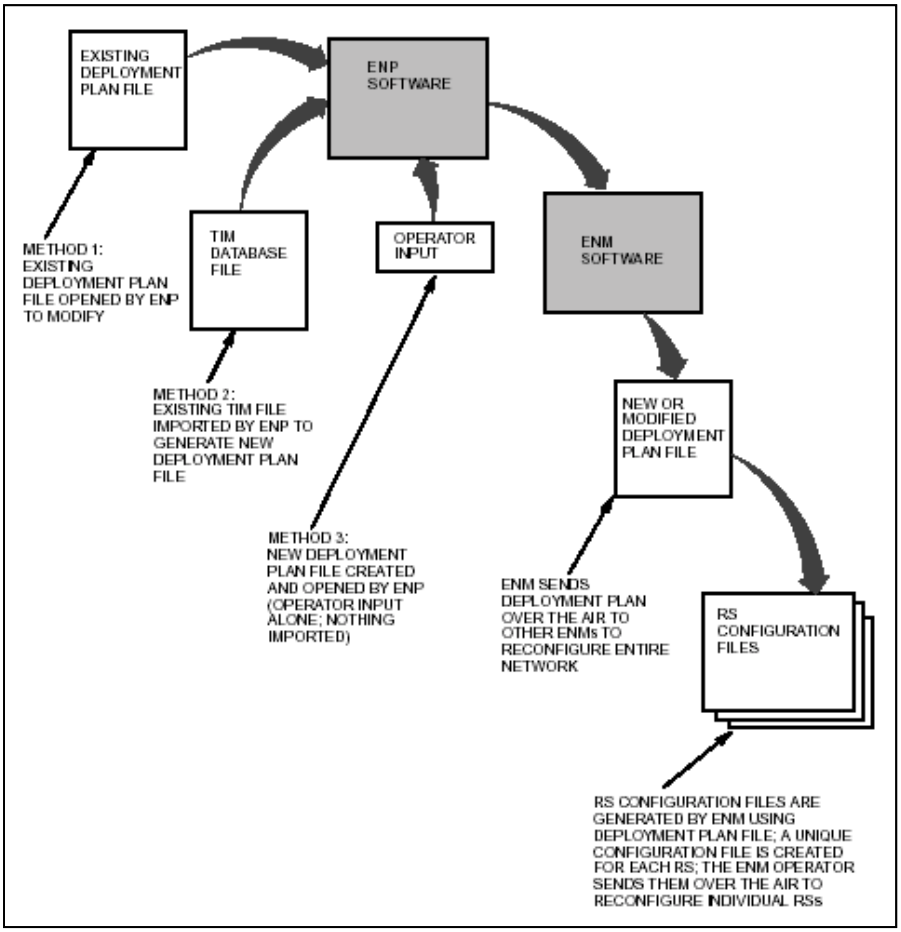


Figure D-7 Network Configuration Planning Function

OPERATIONS

D-27. The ENM operations perform the functions of controlling and managing the EPLRS network. This includes the monitoring, troubleshooting, key generation and key distribution, and configuration file distribution functions. The ENM operations will be performed out of the vehicle configurations dedicated to ENM operations. The operations nodes are configured with a KOK-13 to primarily generate COMSEC keys and to be available to take over the ENP function if necessary. The SBCT will deploy two ENM operations nodes.

D-28. The ENM operations vehicular system leverages the importance of employment flexibility and mobility. Nominal ENM operations will require one ENM operations vehicle (linked with the ENM monitors) to initialize,

manage, and monitor the EPLRS network. One ENM operations node will be the network master timing source, generating and distributing configuration files, generating and distributing COMSEC keys. The two BSC ENM operations vehicles will normally be co-located with the BNOSC at the main CP, BSB, or when the tactical situation dictates the TAC CP. Multiple ENM operations vehicles may be employed in an EPLRS network for the following reasons:

- Primary ENM operations vehicle backup (both hardware and operationally)
- Split-based or Non-contiguous operations (Multiple ENM operations vehicles providing management to greatly disjointed EPLRS networks)
- Redeployment operations (Continuous ENM management during hot-jump)

D-29. ENM operations vehicles also provide the flexibility and mobility to manage an EPLRS network without being tethered to CP or BNOSC. This flexibility allows relocating in the network to minimize the "hops" to the ENM monitoronitors or maximize the number of EPLRS RS's the ENM can "touch" directly. The ENM operations vehicular system also allows an ENM to deploy into theater separately from a CP or BNOSC for quick EPLRS network initialization/control.

MONITORING

D-30. The ENM monitoring mission is the function associated with monitoring the network and providing COMSEC key and configuration file updates to radios. The Tactical Internet Manager (TIM) will ultimately perform this monitoring function. The ENM monitor's are located in all the NOC-Vs in the SBCT.

D-31. The ENM monitors provide the unit commander (battalion and higher) visibility into the wellness of their EPLRS network and provide enhanced EPLRS network connectivity for the network mangers located at the BNOSC

D-32. **Network Visibility.** ENM monitors will provide the span of reach required to monitor all the radios in the EPLRS network. Reliance on the ENM operations vehicles at a small number of locations in the expanded areas of operation of a SBCT for monitoring is not adequate. The ENM monitor's at battalion level provide enhanced connectivity and act as relays for the EPLRS network.

D-33. **EPLRS Network Management Connectivity.** The ENM monitors effectively increase the number of automatic relay links available for network management functions. Reliance on a small number of ENM operations nodes to perform monitoring, key and configuration file distribution in the expanded geographic areas associated with SBCTs can result in radios not being in contact with an ENM (based on EPLRS 4 levels of relay capability). By utilizing ENM monitor's at battalion level ensures that all radios will be in contact with an ENM to obtain the required COMSEC key and Configuration File updates needed to continually operate in the network.

D-34. S6 personnel are responsible for installing, operating and maintaining the ENM monitor. There are seven (7) ENM monitor's in an SBCT with each located in the NOC-V.

D-35. The ENM monitor's provide the unit commander (battalion and higher) visibility into the wellness of their EPLRS network and provide enhanced EPLRS network connectivity for the network mangers located at the BNOSC.

D-36. **Network Visibility.** ENM monitor's will provide the span of reach required to monitor all the radios in the EPLRS network. Reliance on the ENM operations vehicles at a small number of locations in the expanded areas of operation of a SBCT for monitoring is not adequate. The ENM monitor's at battalion level provide enhanced connectivity and act as relays for the EPLRS network.

D-37. **EPLRS Network Management Connectivity.** The ENM monitors effectively increase the number of automatic relay links available for network management functions. Reliance on a small number of ENM operations nodes to perform monitoring, key and configuration file distribution in the expanded geographic areas associated with SBCTs can result in radios not being in contact with an ENM (based on EPLRS 4 levels of relay capability). By utilizing ENM monitor's at battalion level ensures that all radios will be in contact with an ENM to obtain the required COMSEC key and Configuration File updates needed to continually operate in the network.

D-38. S6 personnel are responsible for installing, operating and maintaining the ENM monitor. There are seven (7) ENM monitor's in an SBCT with each located in the NOC-V.

CONCEPT OF OPERATIONS

D-39. EPLRS network management will continue to be the responsibility of the BSC with ENM management vehicles being co-located at the main CP, BSB, or when the tactical situation dictates TAC CP. When the tactical situation dictates ENM management vehicles may also be co-located at battalion level CP's with the ENM retaining the mobility to deploy to alternate locations in the network at the direction of the BNOSC. Other than the ENM being hosted on a laptop and requiring less personnel to operate, EPLRS network management continues to be consistent with the EPLRS NCS-E operations discussed in Section I. Figure D-8 shows a simplified conceptual view of the ENM computer and RS installed in the vehicle configuration.

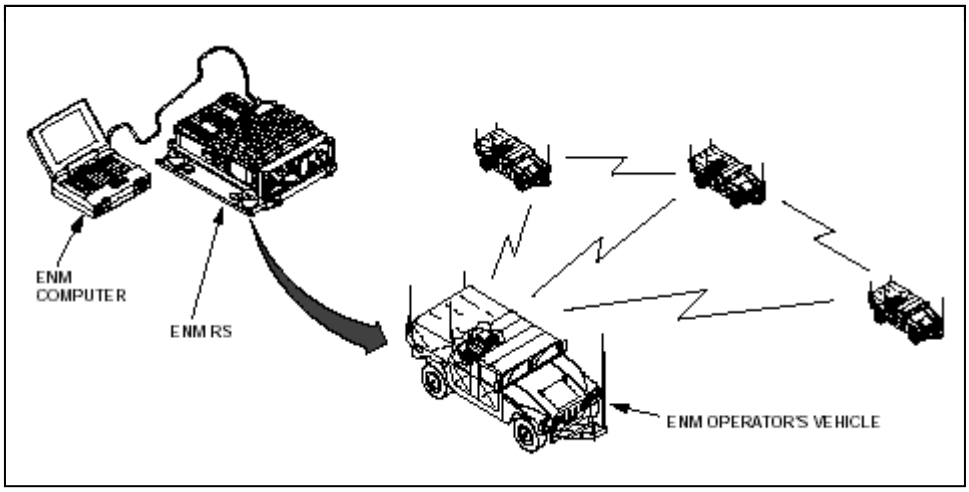


Figure D-8 ENM Vehicle Configuration

EGRU

D-40. The EGRU performs relay and/or grid reference position functions. The BSC personnel install, operate and maintain the EGRU. Employment of an EGRU is based on the deployment and density of the user radios sets (RSs) over the occupied terrain. EGRUs are necessary to supplement the network when unit RSs are not in the most advantageous position for system connectivity or grid reference. Reference units can also be a combination of EGRUs and any stable Radio Set. It is recommended that EGRUs comprise ten percent of the deployed community.

D-41. Pockets of small numbers of RSs dispersed over large areas, non-contiguous areas, or difficult limited line of site terrain may require relay and or dedicated reference units. The ENM planner/manager and ENM operator will implement resources and or assignments to support grid references via an EGRU or designated stable RSs.

Gateways

D-42. The gateway performs two critical missions for the EPLRS network: network gateway and dedicated relay.

D-43. **Network Gateway.** The primary mission for the Gateway Vehicle is performing network gateway functions between different EPLRS networks. Generally these networks will be between different units. Time synchronization and TRANSEC differences between the networks make it necessary for a gateway to establish a common link between the networks. The Gateway vehicle contains the necessary EPLRS gateway components and two radio sets to accomplish this mission. The two radio sets are cabled between their host data ports and each radio set becomes a member of the different network community. A needline is created between the two community radio sets and the inter network gateway or communications path is formed.

D-44. **Dedicated Relay.** The secondary Mission for the Gateway Vehicle is performing Dedicated Relay functions. The vehicle can be quickly dispatched by the BNOSC to perform relay and/or grid reference missions. These missions become critical when deployments consist of few RSs over extended or non-contiguous areas.

NETWORK ARCHITECTURE

D-45. EPLRS network architecture supports the transmission of C2, SA, and position/navigation (POS/NAV) data throughout the battlespace. The network architectural concept is based on EPLRS communities configured to support a SBCT AO.

D-46. The company operations section of the BSC, as part of the BNOSC, directs the employment of ENM, Gateways and EGRUs based on direction provided by the brigade S6. The SBCT EPLRS network community has its own time synchronization and cryptographic keys.

Appendix E

Brigade Subscriber Node Operations

The BSC employs the BSN as the primary node in the SBCT WAN. This appendix discusses the capabilities, interfaces, transmission systems, and architecture of the BSN.

CAPABILITIES

E-1. The BSN provides ATM switching, routing, transmission, NM, and security services within a single shelter. These components form the communications network infrastructure that enables the warfighter to transfer voice, video, data, and imagery information throughout the battlespace. The BSC contains two (2) BSNs for network servicing. Traditionally these assemblages are placed at the Brigade Main CP and the Brigade Support Area CP. Figures E-1, E-2, and E3 are diagrams of the BSN internal component locations.

E-2. The Brigade Subscriber Node provides the operator an effective and expedient way to configure, monitor, print reports, and maintain a network by usage of a variety of Commercial Off The Shelf Systems (COTS). The capabilities of the Brigade Subscriber Node are:

- Provides 96 Internodal Voice Trunks (Analog).
- 8 kbps Voice Compression.
- 32 kbps for secure analog voice call (STU III).
- 2 SATCOM Links (SMART-T or 85/93).

E-3. Video Services:

- H.323 Gatekeeper software.
- MCU (multiconference unit).

E-4. LAN capabilities:

- 10 Base-FX LAN Fiber 10 Mbps TOC LAN (1).
- 100-Base FX LAN Fiber 100 Mbps TOC LAN (2).
- 10-Base T LAN D.
- Local LAN Port (2).
- 100 Base FX LAN Fiber 100 Mbps Sun Rays (1).

E-5. ATM services:

- PNNI for auto re-route.
- Quality of Service.
- Dynamic Bandwidth Allocation.
- Vantage Software (participates in MSE flood search).

- Logical voice networking.
- User affiliation/disaffiliation.
- Ninety-six analog lines and one ISDN line.
- HCLOS radio links.

MANAGEMENT CAPABILITIES

E-6. The BSN and its capabilities define the location of the BNOSC and alternate BNOSC. Traditionally the Network Operations Support Center (NOSC) is located with each BSN. As part of providing the primary links to the WAN each BSN possesses the management tools, systems, and interfaces to manage the entire network.

E-7. The BSN provides the interfaces to manage the network through the Network Management (AXMP) server. Four (4) Thin Client terminals are remoted into the NOSC. Any of the thin client terminals can run whatever software the operator chooses to load from the server. Typically, each client runs separate software. Appendix C, Network Management, describes the management tools in more detail. Below describes the management capabilities and additional systems attached to the BSN:

- HCLOS/IA Monitoring Thin Client.
- Network Monitoring (WAN) Client.
- Network Monitoring (LAN) Client.
- Network Management (NTDR/NPT) Client.
- Additional management systems attached to the BSN:
  - LKMS
  - SBU Management Laptop
  - ISYSCON V(4)
  - NTDR NMT
  - ABCS Client system

INTERFACES

E-8. The BSN supports direct connectivity to commercial networks and legacy Army communications (MSE and TRI-TAC) systems. This dual functionality allows the switch to adapt to direct, switch-to-switch MSE and TRI-TAC standards or accept commercial interface functions built into sister service and allied switching assemblages. MSE and TRI-TAC standards allow the use of existing Standardization Agreement (NATO) (STANAG)-based communications interface devices. These devices - such as the CV-4002 NATO analog interface device - exist within US and allied inventories.

E-9. To provide voice, video and data network services for remote TOC subscribers, the Brigade Remote Subscriber Service (BRSS) can be connected via a fiber optic remote extension into the BSN.

TRANSMISSION SYSTEMS

E-10. The BSN can use either organic HCLOS radio transmission systems, BSC-supplied multichannel satellite, and/or satellite assets provided by HICON for connectivity. The BSN can terminate ISDN, BVTC, and e-mail services, and it provides wireless LAN, wireless loops (cordless telephones), and an NTDR interface.

E-11. The transmission assets connect the BSN WAN nodes, subscriber nodes, LANs, and the Defense Information Systems Network (DISN). The BSN can operate independently of a WAN node, providing local users with secure and Sensitive but Unclassified (SBU) wired and wireless multimedia subscriber services. The BSN may draw services from other nodes when employed as part of a network.

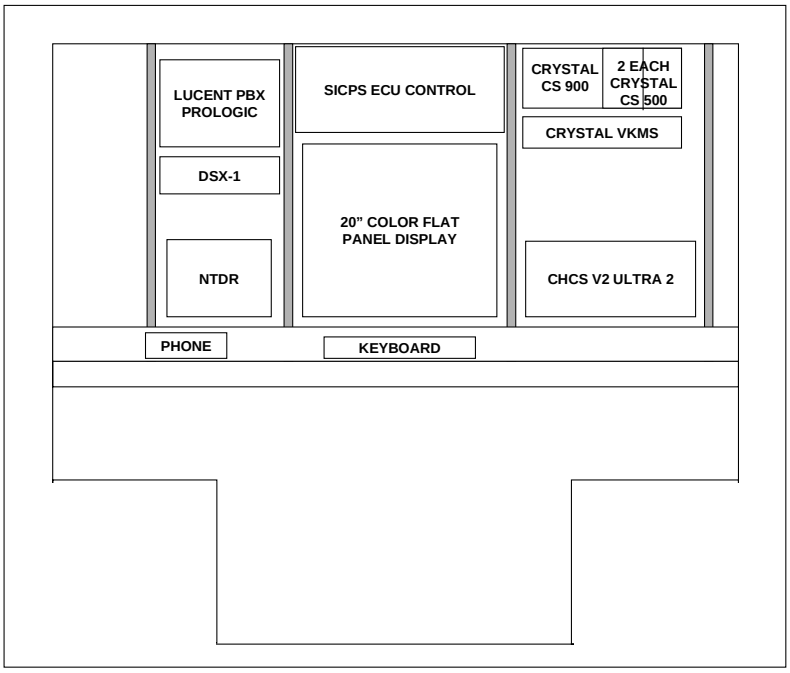


Figure E-1. BSN Shelter (End View) (Not to Scale)

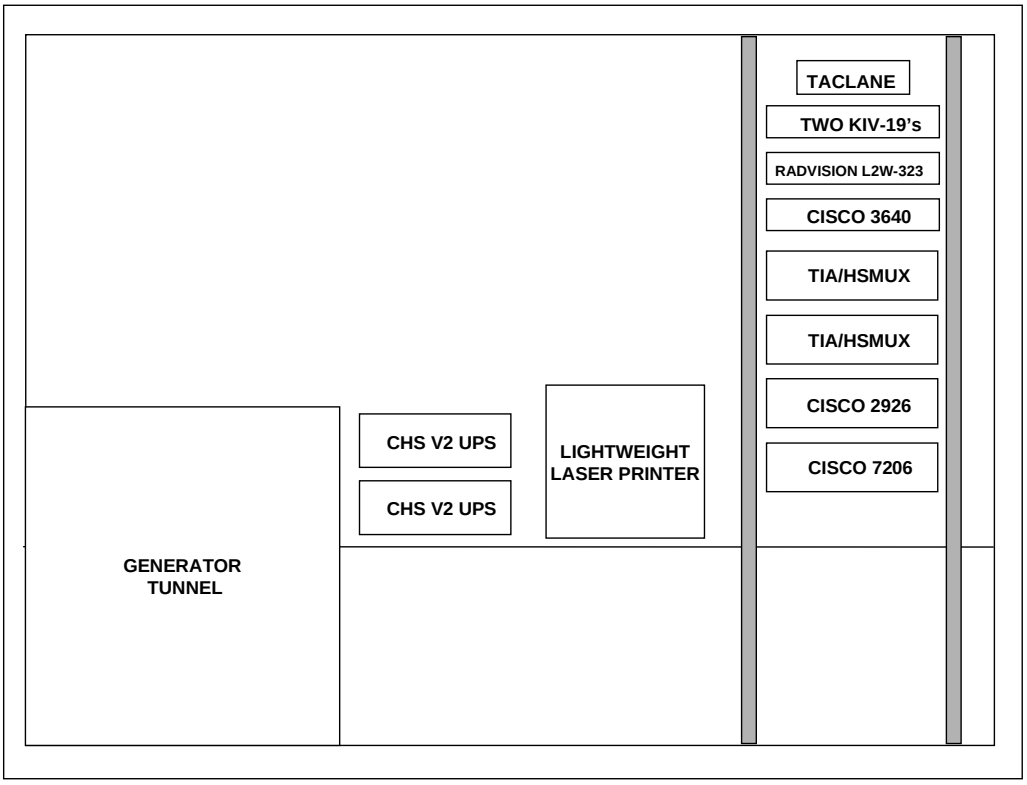


Figure E-2. BSN Shelter (Curb Side View) (Not to Scale)

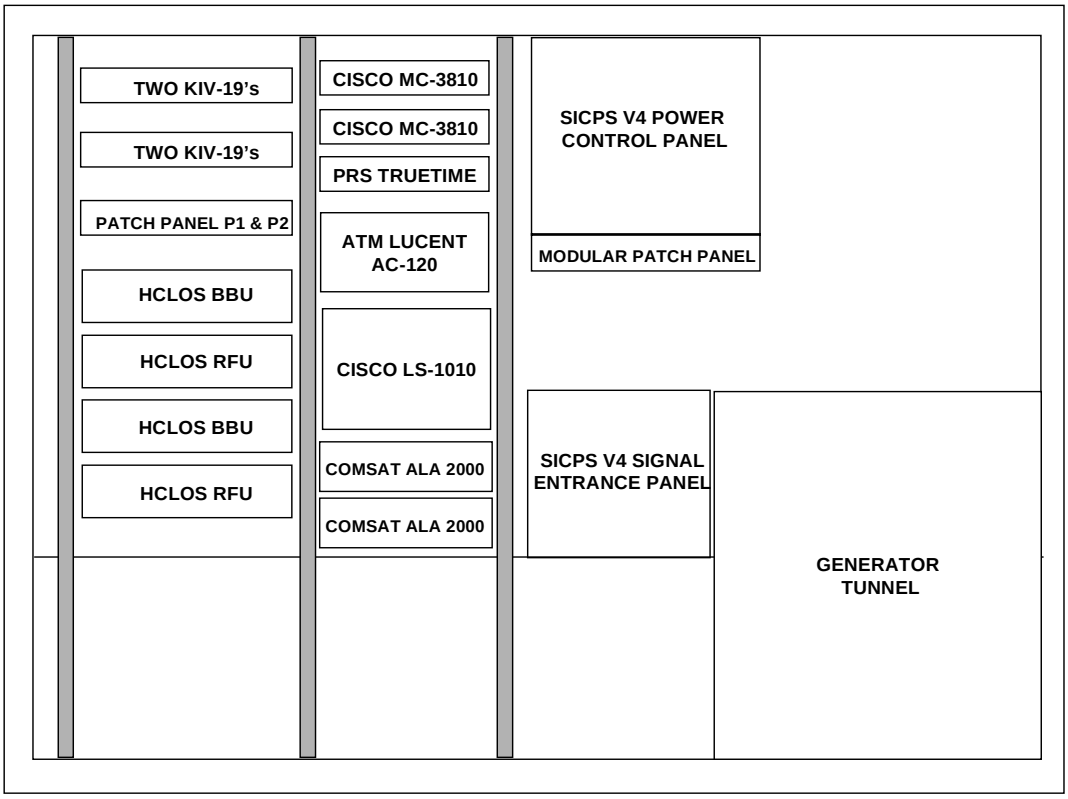


Figure E-3. BSN Shelter (Road Side View) (Not to Scale)

ARCHITECTURE

E-12. The BSN supports the SBCT information network by providing a tactical WAN that operates in complex, rolling, and urban terrain. The BSN will extend data connectivity to forward elements and route information efficiently anywhere in the battlespace while reducing the signal presence on the battlefield. The BSN will establish an environment in which commanders at all echelons can operate with virtual staffs that are located at remote locations.

E-13. With multichannel TACSAT providing reach back to the standardized tactical entry point (STEP) and access to sustaining base networks, the BSN provides the full suite of subscriber services to the warfighter.

Appendix F

Tactical Internet

The Tactical Internet (TI) is the tactical communications network in the SBCT that supports the FBCB2 while on the move. The TI provides SA and C2 data exchange between maneuver, CSS, and C2 platforms. This appendix addresses the TI and components in the SBCT.

TI IN THE SBCT

F-1. The TI is an automated, router-based communications network consisting of servers, routers, hubs, EPLRS data radios, and other supporting communications equipment. The network uses commercial Internet standard protocols to move data vertically and horizontally throughout the SBCT area. The ISYSCON V(4) enables S6s to plan, monitor, and reconfigure the TI at the brigade and battalion levels.

F-2. The TI supports the operational deployment of host FBCB2, supporting communications, networks, and integrated management at each echelon. Terms associated with the TI are–

- Autonomous system (AS)—a collection of networks, under a common administration that shares a common routing strategy. An AS consists of one or many networks, and each network may or may not have an internal structure.
- Routing area—a network within an AS. Routing areas and the AS to which they belong share the same routing strategy.

F-3. Figure F-1 shows a generic example of the complexity of the TI architecture with the TOC-to-TOC data network supporting the TOCs and the TI supporting the mobile platforms. It indicates the TI employment that supports them in terms of hosts, communications, networks, and management elements. This representation of the TI focuses on operating and managing the advanced systems that will provide enhanced data transfer and communications support to the SBCT.

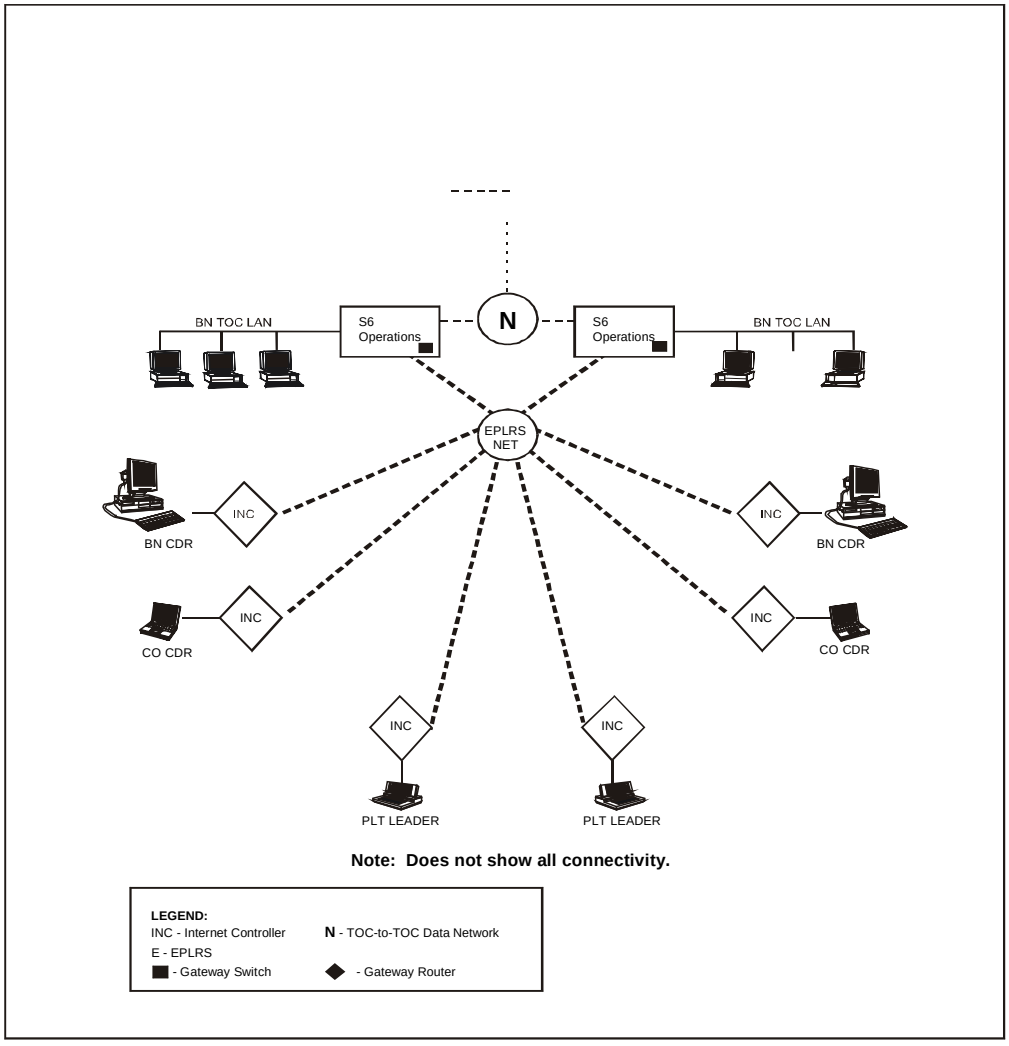


Figure F-1. SBCT TI Generic Connectivity

FUNCTIONS

F-4. The TI is the primary communications architecture supporting the warfighter at brigade and below. The TI enables the sharing of C2 data by commanders, staffs, units, and soldiers down to an individual platform. The greatest benefit of the TI is providing the information pathway for FBCB2. Through FBCB2 users obtain unprecedented situational awareness (SA) of friendly forces and enables improved survivability, increased lethality, and economy of forces. Additionally FBCB2 provides realtime messaging and directly interfaces with ABCS, allowing users to access information databases from higher.

F-5. This information exchange consists of selected, interoperable, joint variable message format (JVMF) messages used to communicate between the ABCS automated components.

TI COMPONENTS

F-6. The TI integrates tactical radios, computers, and supporting communications equipment into a mobile data network. It enables users to access the network with the FBCB2 at any location and send and receive information automatically to support changing operational requirements and task organizations for tactical operations.

ISYSCON V(4)

F-7. The ISYSCON V(4) manager provides semi-autonomous management capability to help plan, initialize, monitor/troubleshoot and reconfigure the TI. The ISYSCON V(4) will reside at all NOSCs and battalion S6 sections.

ABCS

F-8. The ABCS, although not part of the total TI, is the primary user of the TI with the FBCB2. The ABCS provides the SBCT an enhanced C2 capability that is a significant force multiplier. The BSC provides the communications paths over which the SBCT exchanges battle command information within the larger ABCS operational environment.

F-9. The TI is integrated with ABCS through an interface at TOCs. It enhances the necessary information for battle command at brigade and below. The FBCB2 functionality of the TI is integrated into the TOC LANs at battalion and brigade echelons using embedded battle command (EBC). This integration enables information flow between the soldier/platform level and the SBCT and throughout the ABCS.

F-10. The integration of six principal ABCS automation components provides situational awareness and decision support to the battlefield operating systems of the SBCT. These components are the–

- Maneuver Control System (MCS).
- Advanced Field Artillery Tactical Data System (AFATDS).
- Air Missile Defense Work Station (AMDWS).
- All Source Analysis System (ASAS).
- Combat Service Support Control System (CSSCS).
- Force XXI Battle Command Brigade and Below (FBCB2).

COMMUNICATIONS COMPONENTS

F-11. The paragraphs below discuss the principal communications components supporting the TI and ABCS.

EPLRS

F-12. EPLRS is an integral communications system that provides the backbone for the TI. The NETOPS section maintains the SBCT EPLRS network. The EPLRS network consists of NCS or ENM, EGRU, gateway and RS deployed throughout the SBCT area.

TOC-to-TOC Data Network

F-13. The TOC-to TOC data network, although not part of the TI, links the TI to the ABCS at brigade and battalion TOCs. The TOC-to-TOC data network is the sole means for data transmission system between TOC's ABCS at the battalion level. Although EPLRS can 'bridge' data between TOCs, traditionally the injection of data into the ABCS network is accomplished by data transmissions system above EPLRS.

WAN

F-14. The WAN, although not part of the TI, supports the TI by providing connectivity to the HICON through the BSN at the SBCT main CP and BSB support operations center.

Appendix G

Near-Term Digital Radio/Joint Tactical Radio System Operations

The NTDR is the primary SBCT TOC-to-TOC data radio and this appendix provides information on the functional description, employment, operational software, operational procedures, and tactics and techniques of the NTDR. The Joint Tactical Radio System (JTRS) is an objective scaleable multi-wave form radio designed to communicate throughout the frequency spectrum from 2 MHz to 2 GHz. The JTRS is mentioned in this section for information purposes only.

NTDR

G-1. The following paragraphs discuss the NTDR.

FUNCTIONAL DESCRIPTION

G-2. The NTDR is a digital radio that operates in the UHF band (225-450 MHz) in discrete tuning steps of 0.625 MHz. Transmitted data is encrypted, protected with forward error correction and detection codes, and modulated onto a RF carrier. Received data is recovered following the same process, but in reverse. Direct sequence spreading at a chip rate of 8 MHz enhances performance with respect to multipath, jamming, and enemy interception. Nominal digital throughput is 200 kilobits per second (kbps). The NTDR supports LAN (Ethernet) and serial (RS-423 asynchronous and RS-422 synchronous and asynchronous) interfaces. The NTDR has a range of 10-20 kilometers (6-12 miles) and incorporates a GPS-receive capability that provides the MGRS position for the radio.

EMPLOYMENT

G-3. The NTDR is the primary data communications transmission system linking the ABCS at the brigade and battalion echelons. The TOC-to-TOC data network provides a wireless WAN for the SBCT using the ABCS host terminals located in TOCs and C2 platforms. The NTDR WAN allows users to transmit information between C2 nodes to support C2 data and imagery information flow.

OPERATIONAL SOFTWARE

G-4. The protocol processor software for the NTDR is downloaded from a personal computer. The software is accessed using the function switch and display on the front panel of the NTDR. The display provides visual feedback about the radio's status. It has the following three message areas:

- MGRS—displays the latest MGRS position of the radio.

- Receiver transmitter (RT) STATUS—displays messages about the status of the RT.
- Hold-up battery (HUB) LOW—Indicates when the HUB is low and needs replacing. The display is blank when the HUB power is adequate.

G-5. Table G-1 lists the NTDR function switches, and table G-2 lists the NTDR control and connections.

G-6. As the operator sets up the NTDR operation and selects the appropriate function, the software automatically executes the function and displays the result in the display area.

Table G-1. NTDR Function Switches

Switch	Function
OFF[1]	Removes operating power from the radio but saves fill data, if a good HUB is installed.
Communicate (COM)	Used for normal radio operation.
FILL	Used for loading fill data into the radio.
Built in test (BIT)	Starts the radio self-test.
Zeroize (Z)[1]	Clears all fill data from the radio's memory.
Store (STO)[1]	Removes all operating power from the radio. Extends the life of the HUB.

[1] OFF, Z, and STO are pull-to-turn positions.

Table G-2. NTDR Controls and Connections

Controls and Connections	Function
Display	Provides two lines of visual radio status feedback. The display has three message areas. 1) LAT/LON. Displays the latest position of the radio in latitude (LAT) and longitude (LON) when the radio is connected to a GPS antenna. 2) RT STATUS. Displays messages about the status of the radio. 3) HUB LOW. Provides an X indication when the HUB is low and should be replaced. The display is blank when the

	HUB's power is adequate.

Table G-2. NTDR Controls and Connections (Continued)

Controls and Connections	Function
POWER ON light	Lit when the radio is turned on and primary power is present.
PORT 1 connector	Used for a cable that connects the radio using point-to-point protocols (PPP) to a SINCGARS INC or equivalent RS-432-compliant device.
PORT 2 connector	Used for a cable that connects the radio using a PPP to a SINCGARS INC or equivalent RS-422- or RS-423-compliant device.
E-NET (Ethernet) connector	Used for a cable that connects the radio to an Ethernet (Institute of Electrical and Electronics Engineers [IEEE] 802.3, 10base2)-compliant device.
MAINT (maintenance) connector	Used for a cable that connects the radio to a maintenance terminal (RS-232 signal levels).
FILL connector	Used for a cable that connects the radio to an ANCD fill device.

SECURE OPERATION

G-7. The NTDR requires fill data for normal operation. The fill data is loaded into the radio using the automated net control device (ANCD) and NTDR interim fill device (NIFD). The ANCD loads the COMSEC data and the NIFD loads the transmission security (TRANSEC) and GPS data. To load the NTDR, the operator–

- Ensures fill data is available.
- Sets the function switch to FILL; verifies this by viewing the display.
- Connects the NIFD to the radio fill connector.
- Turns the NIFD on and sets it to the appropriate fill setting; verifies this by viewing the display.
- Disconnects the NIFD, connects the ANCD, and turns it to the appropriate fill setting; verifies this by viewing the display.

OPERATIONAL PROCEDURES

G-8. The brigade S6 establishes TOC-to-TOC data networks to support the brigade operation plan (OPLAN) or OPORD. The NTDR network is defined as the brigade information network. This network extends throughout the depth of the battlespace and utilizes both battalion and brigade resources for successful operation (brigade and battalion TOCs, commander platforms, relay/retrans vehicles). The NTDR structure ensures successful network

operation. Successful operation requires establishing separate cluster nets and a backbone net to connect the clusters. Clusterheads form within the clusters to link the backbone and to maintain connectivity. The NTDR has a self-organizing networking capability that provides highly mobile operations. End-to-end routing within the NTDR net structure is based on IP addressing schemes. A cluster may be formed by linking elements of a maneuver battalion together with the backbone that links the battalion clusters with the brigade TOC.

TACTICS AND TECHNIQUES

G-9. For successful NTDR operations, the antenna and cables must be installed properly. Also, the proper NTDR sight location must be consistent with LOS RF propagation.

G-10. The network operations section, operating from the BNOSC, plans and manages the TOC-to-TOC data network.

JTRS

G-11. The JTRS is a multi-service, multi-platform data and voice communications system. It is designed to utilize legacy and newly designed communications waveforms. A single JTRS will be capable of communicating with any current communications system (legacy and in some cases foreign waveforms) and switch to any other system loaded with the appropriate waveform.

G-12. Essentially, the JTRS will be the only radio necessary to communicate with other voice and data systems operating within the available 41 waveforms loaded. The JTRS will be capable of operating on two different waveforms simultaneously (for example, a voice SINCGARS and a data EPLRS waveform).

G-13. An additional benefit of the JTRS will be the advent of the Wideband Network Waveform (WNW). This waveform will provide a high bandwidth (2.5 Mbps-projected) path for TOC-to-TOC transmissions and will be able to support battlefield video teleconferencing (BVTC) between users.

Appendix H

Single-Channel Ground and Airborne Radio System Operations

This appendix provides a description of SINCGARS. It discusses the SINCGARS components, planning ranges, and the frequency hopping (FH) multiplexer.

SINCGARS DESCRIPTION

H-1. The SINCGARS family of radio systems is designed on a modular basis to achieve maximum commonality among various ground configurations. A common RT is used in the manpack and all vehicle configurations. The RT is totally interchangeable from one configuration to the next. Additionally, the modular design reduces the burden on the logistics system to provide repair parts.

H-2. SINCGARS operates in either the single-channel or FH mode. It is compatible with all current US and allied VHF radios in the single-channel nonsecure mode. Currently, in the FH mode, SINCGARS is only compatible with other Air Force, Marine, or Navy SINCGARS radios. SINCGARS stores eight single-channel frequencies and six separate hopsets. The eight single-channel frequencies include the cue and manual frequencies.

H-3. Radio systems using special encoding techniques must provide outside network access through some hailing method. The cue frequency provides the hailing ability to the SINCGARS radio. When hailing a network, an individual outside the network contacts the NCS on the cue frequency. In the active FH mode, the SINCGARS radio gives audible and visual signals to the operator that an external subscriber wants to communicate with the FH network. The SINCGARS NCS operator must change to the cue frequency to communicate with the outside radio system.

H-4. The network uses the manual frequency for initial network activation. The manual frequency provides a common frequency for all members of the network to verify the equipment is operational. During initial net activation, all operators in the net tune to the manual frequency. After communications are established, the net switches to the FH mode and the NCS transfers the hopping variables to the out stations.

H-5. SINCGARS directly accepts either analog (voice or frequency shift key) or digital input signals. SINCGARS provides data rates of 600, 1,200, 2,400, 4,800, and 16,000 bits per second. It also provides enhanced data modes of 1,200N, 2,400N, 4,800N, 9,600N, packet data modes, and RS 232 data modes.

H-6. System Improvement Program (SIP) and Advanced System Improvement Program (ASIP) radios provide enhanced data modes.

Enhanced data modes provide forward error correction, speed, range, and data transmission accuracy. The packet data mode is used only with the FBCB2 system. The RS-232 data mode allows file transfers to be sent from net members of a common net. By attaching a host computer directly to the ASIP radio, the RS-232 data mode uses an auto-baud detect process to select one of four data rates of 1,200, 2,400, 4,800 and 9,600 bits per second used by the host computer. The RS-232 mode will support X, Y, or Z modem protocols that are normally a selection on any commercial communications program. Communications software must be set to half duplex operations.

H-7. SINCGARS can control output power. The RT alone has three power settings that vary transmission range from 200 meters (660 feet) to 10 kilometers (6.2 miles). Adding a power amplifier increases the range to 40 kilometers (25 miles) for LOS. The variable output power level allows users to lessen the electromagnetic signal (signature) given off by the radio set.

H-8. Using lower power is particularly important at major CPs that operates in multiple networks. The ultimate goal is to reduce the electronic signature at the CP. The NCS should ensure that all members of the network operate on the minimum power necessary to maintain reliable communications. SINCGARS has built-in test (BIT) functions that tell the operator the RT is malfunctioning and identifies the faulty circuits for repair or maintenance.

H-9. The SINCGARS ASIP program increases the performance of the SINCGARS SIP. It increases its operational capability to support the TI, specifically, improved data capability, manpower and personnel integration (MANPRINT) requirement compliance, and flexibility to interface with other systems. Figure H-1 shows the SINCGARS ASIP (front panel integrated COMSEC (ICOM) RT-1523F).

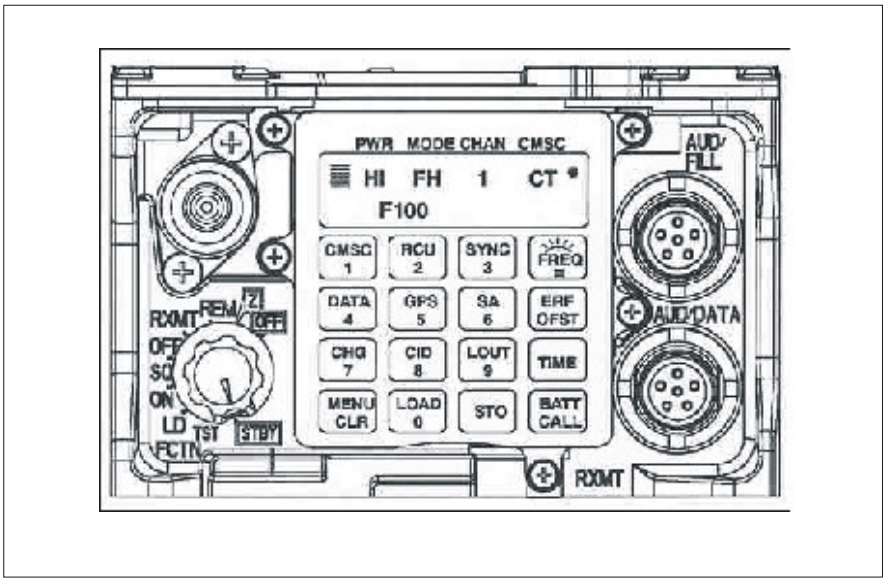


Figure H-1. Front Panel ICOM RT-1523F

H-10. The SINCGARS ASIP radio incorporates an enhanced system improvement program (ESIP) waveform. The waveform includes optimizations to the algorithms of noisy channel avoidance (NCA) scheme, the time of day (TOD) tracking scheme, and end of message (EOM) scheme. Enhancements include—

- **ESIP waveform—**implements a faster channel access protocol, which reduces net fragmentation by shortening the collision intervals between voice and data transmissions. The result is the reduction of voice and data contention problems associated with shared voice and data networks.
- **NCA algorithm—**always reverts to a known good frequency instead of constantly searching for clear frequencies, thus increasing the FH synchronization probability in high noise and jamming conditions.
- **TOD enhancement—**uses a reference bit that assures time constraints are the same during each transmission.
- **End of message (EOM) enhancement—**reduces fade bridging, whereby the transmission would linger even though adding extra EOM hops to increase the detection and probability of synchronization completes the message.

H-11. In the ASIP radio, the forward error correction scheme, combined with COMSEC, reduces the over the air transmission time of a message by half, and essentially allows more data to be processed over the net more efficiently under severe jamming, mutual interference, and co-site environments.

H-12. The ASIP radio incorporates the same functionality and features of the full-size SIP radio in a package that is half the size and approximately one-third less weight. The ASIP radio has a lower voltage application specific integrated circuit (ASIC), ASIC insertion, and a digital signal processor (DSP)-based architecture that contribute to the smaller size and lower weight. The ASIP radio in the manpack configuration (including a battery, handset, and antenna) weighs approximately 8 pounds.

H-13. Range performance is the same as the SINCGARS SIP radios in both dismounted and vehicular configurations. Power consumption is reduced, thereby increasing the usefulness of the primary battery to more than 33 hours of mission life at a 9:1 duty cycle. The ASIP radio, much like the Internet controller (INC), is fully field-programmable, and is capable of supporting future growth or hosting a different waveform. The ASIP radio eliminates the need for an external mounted battery box. The BA-5590/U primary lithium battery now resides within the radio itself, and acts as the HUB when the radio is in the standby mode. In its current configuration, there is still space above the battery compartment for expansion modules and/or functions. Due to the reduction in size and fewer component parts, the reliability of the ASIP radio is greatly increased.

COMPONENTS

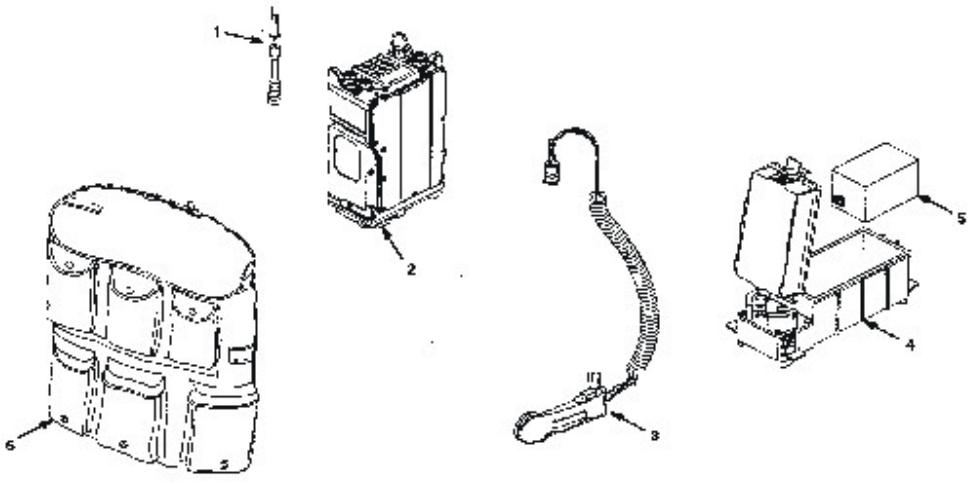
H-14. The components of the RS determine its capabilities. Common components are the key to tailoring radio sets for specific missions. The RT is the basic building block for all radio configurations. The number of RTs and amplifiers, the installation kit, and the backpack component determine the model.

CONFIGURATIONS

H-15. Radio set configurations include a manpack (AN/PRC-119F), and six ground (AN/VRC-87F through AN/VRC-92F). These versions are discussed below.

Manpack

H-16. Manpack radio AN/PRC-119F consists of one RT, a battery, a battery box, a handset, a manpack antenna (AS/4266), and an all-purpose lightweight individual carrying equipment (ALICE) pack. Figure H-2 shows manpack radio AN/PRC-119F. The non-integrated COMSEC (non-ICOM) radio must be used with TSEC/KY-57 Vinson to provide secure communications.



1. ANTENNA
2. SINCGARS ASIP RT
3. HANDSET H-250
4. BATTERY BOX
5. BATTERY BA-5590
6. MANPACK (AS/2466)

Figure H-2. Manpack Radio AN/PRC-119F

Ground Versions

H-17. Table H-1 briefly compares the ground radio systems. These radios are discussed further in the following paragraphs.

Table H-1. Comparison of Ground Radio Systems

Radio System/Component	Short Range	Long Range	Power Amplifier	Dismount Manpack	INC (AM-7239C/E)
AN/VRC 87F	X				X
AN/VRC 88F	X			X	X
AN/VRC 89F	X		X		X
AN/VRC 90F		X	X		X
AN/VRC 91F	X	X	X	X	X
AN/VRC 92F		X	X (two each)		X

H-18. **AN/VRC-87F.** The AN/VRC-87F is a short-range radio and is the base vehicular RS. The radio consists of one RT, a radio mount, a mounting adapter, a vehicular antenna, and associated handsets and cabling. Figure H-3 shows an AN/VRC-87F.

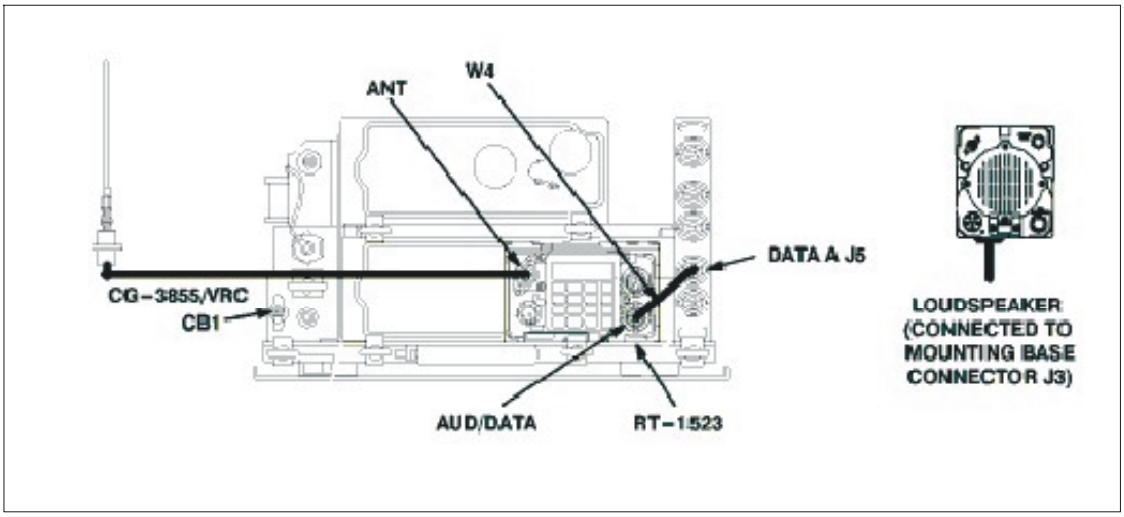


Figure H-3. AN/VRC-87F

H-19. **AN/VRC-88F.** The AN/VRC-88F is a vehicular dismountable short-range radio. It is identical to the AN/VRC-87F but has added components needed to operate as a manpack radio (battery box, manpack antenna, and ALICE pack).

H-20. **AN/VRC-89F.** The AN/VRC-89F is a vehicular short-range/long-range radio. It is built from the AN/VRC-87F with another RT and a power amplifier added. The RT provides increased capabilities over a receiver alone. Figure H-4 shows an AN/VRC-89F.

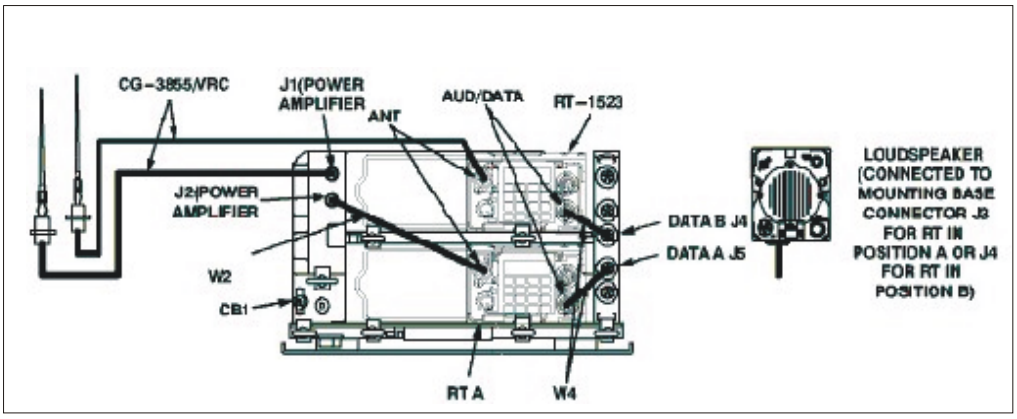


Figure H-4. AN/VRC-89F

H-21. **AN/VRC-90F.** The AN/VRC-90F is a vehicular long-range radio. It is identical to the AN/VRC-87F but with a power amplifier added for long-range capability. Figure H-5 shows an AN/VRC-90F.

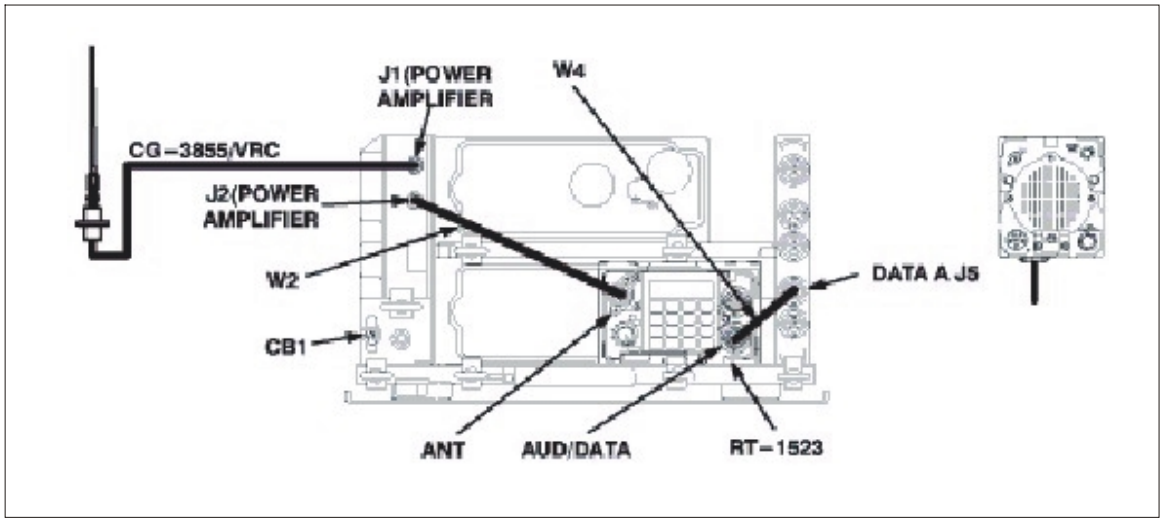


Figure H-5. AN/VRC-90F

H-22. **AN/VRC-91F.** The AN/VRC-91F is a vehicular short-range/long-range dismountable radio. It is identical to AN/VRC-89F but has added components needed to operate as a manpack radio.

H-23. **AN/VRC-92F**. The AN/VRC-92F is a vehicular dual long-range/retransmission radio. It is identical to the AN/VRC-89F but has a second power amplifier to provide high-power capability for both radios in the mount. The second amplifier has its own mount (MT-6353/VRC) and obtains its power from a cable connected to one of the auxiliary power outputs from the radio mount. In the mounting adapter, the co-mounted amplifier can only be used with the lower radio, and the separate amplifier can only be used with the upper radio. Figure H-6 shows an AN/VRC-92F.

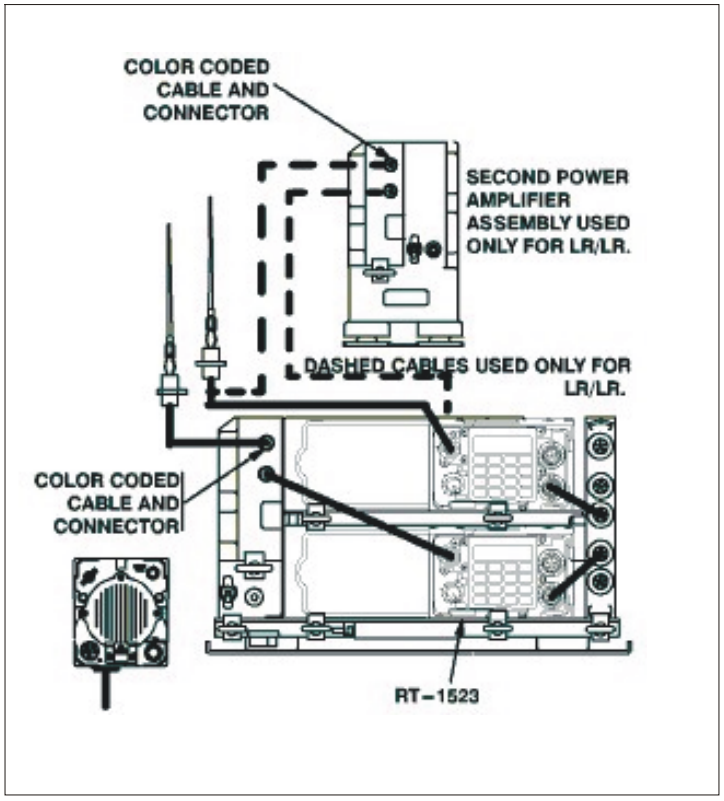


Figure H-6. AN/VRC-92F

Planning Range

H-24. The FM radio planning ranges differ for voice and digital communications. Normally, if voice communications are clear and if the radio is properly aligned, digital communications should be clear. Although limited in range, SINCGARS range can be significantly extended with directional antennas, retransmission stations, or relays. Table H-2 shows the planning ranges for using SINCGARS manpack and ground radios. Planning ranges for data transmission are usually less than for voice.

Table H-2. Planning Ranges for Voice and Data Transmissions Using SINCGARS

Manpack Radio		
Communications Mode	**RF Power**	**Range**
Voice	Low (LO)	200 meters to 400 meters
	Medium (M)	400 meters to 5 kilometers
	High (HI)	5 kilometers to 10 kilometers
SDM Data (600–4,800 bps)	HI	3 kilometers to 5 kilometers
SDM Data (16,000 bps)	HI	1 kilometer to 3 kilometers
EDM Data (1,200N)	HI	5 kilometers to 10 kilometers
EDM Data (2,400N)	HI	5 kilometers to 8 kilometers
EDM Data (4,800N)	HI	3 kilometers to 5 kilometers
EDM Data (9,600N)	HI	1 kilometer to 3 kilometers
Ground Radio		
Communications Mode	**RF Power**	**Range**
Voice (slant range [SR] or long range [LR] radio)	LO	200 meters to 400 meters
Voice (SR or LR radio)	M	400 meters to 5 kilometers
Voice (SR or LR radio)	HI	5 kilometers to 10 kilometers
Voice	Power Amplified (PA)	10 kilometers to 40 kilometers
SDM data (LR radio)		
600–4,800 bps	HI	3 kilometers to 5 kilometers
16,000 bps	HI	1 kilometer to 3 kilometers
SDM data (LR radio)		
600–2,400 bps	PA	5 kilometers to 25 kilometers
4,800 bps	PA	5 kilometers to 22 kilometers
16,000 bps	PA	3 kilometers to 10 kilometers
EDM data (SR radio)		
1,200N–2,400N bps	HI	5 kilometers to 10 kilometers
4,800N bps/packet	HI	5 kilometers to 10 kilometers
9,600N bps	HI	5 kilometers to 10 Kilometers
EDM data (LR radio)		
1,200N–2,400N bps	PA	20 kilometers to 35 kilometers
4,800N bps/packet	PA	15 kilometers to 25 kilometers
9,600N bps	PA	10 kilometers to 25 kilometers

H-25. Planning ranges are based on LOS and are average for normal conditions. Ranges depend on factors like location, sighting, weather, and surrounding noise levels. Users of the OE-254 antenna will increase the ranges for both voice and data transmissions. Adversary jamming and mutual interference conditions will degrade these ranges. In data transmissions, use of low data rates will increase the range. Special consideration must be given to SINCGARS SIP manpack radios (AN/PRC-119D), as they are not TI-compatible without internal reprogramming.

FH MULTIPLEXER (FHMUX), TD-1456/VRC

H-26. The FHMUX combines any mix of up to four low to high power FH transceivers to a single antenna. The FHMUX unit operates across the 30.000 to 87.975 MHz frequency range. The primary function is to extend the multiplexing capability to FH radios. The FHMUX also prevents frequency collisions and provides the selectivity necessary to attenuate any local interfering signal that might otherwise degrade the receiver sensitivity. The FHMUX is digitally tuned via the steerable null antenna processor (SNAP) interface when controlled by a SINCGARS radio. Figure H-8 shows the FHMUX, and Table H-3 lists FHMUX physical data.

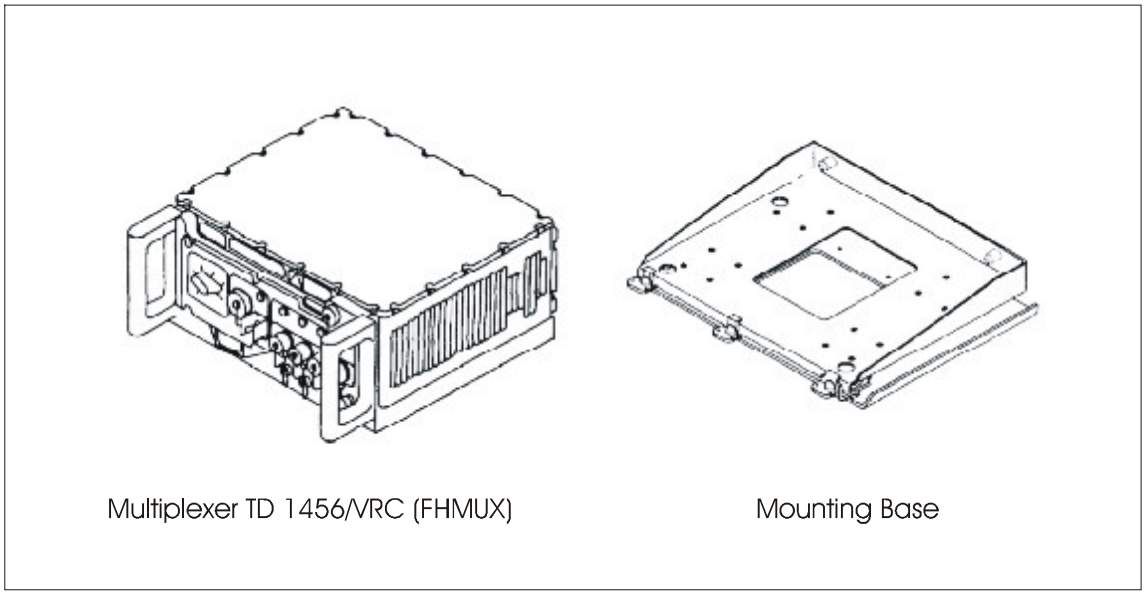


Figure H-8. FHMUX

Table H-3. FHMUX Physical Data[1]

Item	Length	Width	Height	Weight
Multiplexer	43.2 centimeters (17.0 inches)	40.6 centimeters (16.0 inches)	21.6 centimeters (8.5 inches)	25 kilograms (56 pounds)
Mounting base	40.6 centimeters (16.0 inches)	41.4 centimeters (16.6 inches)	8.9 centimeters (3.5 inches)	8.6 kilograms (19 pounds)

[1] All weights are approximate; all measurements are maximums.

FHMUX Performance Data

H-27. Figure H-9 shows a typical vehicular configuration using one multiplexer and two VRC-92F radios. The introduction of the multiplexer into the radio system is transparent; therefore, it does not affect the way the radios are operated. The number of vehicular antennas needed is reduced from four to one. Instead of each radio going directly to its own antenna, the antenna connections of the four radios are routed to the multiplexer and the multiplexer then connects to a single common antenna. To provide FH information to the multiplexer, the SNAP control signals provided by the vehicular amplifier adapter (VAA) must be connected to the multiplexer with one SNAP cable per VAA. Vehicular direct current (DC) power (22 to 32 volt direct current [Vdc]) must also be supplied to the multiplexer through the J2 on the power amplifier mount (MT-6353/VRC) or on the mounting base (MT-6576/VRC).

H-28. The only two operator controls on the multiplexer are the POWER switch and the RADIO PRIORITY switch. The POWER switch must be placed in the ON position to use the FHMUX. The POWER switch can be turned on and left on if the DC power is controlled remotely by CB1 on the VAA.

H-29. The RADIO PRIORITY switch position is set based on the desired operating scenario. In the EQUAL position, all four radios connected to the multiplexer will have equal communications priority. In the 1A, 1B, 2A, and 2B positions, the selected radio will have a slightly higher priority than the other radios whenever there is frequency conflict. (A frequency conflict is when two or more hopping radios want to communicate on the same frequency simultaneously.) In the retransmit (1A+1B) position, radios 1A and 1B (operating in the retransmit mode) have higher priority than radios 2A and 2B. Normally, the switch will be set in the EQUAL position; however, higher priority can be given to a critical communications link. Figure H-10 shows a radio priority switch.

H-30. The TEST position is used only for off-line BIT and the switch should not be placed in this position except as directed in the -20 and -30 maintenance manuals.

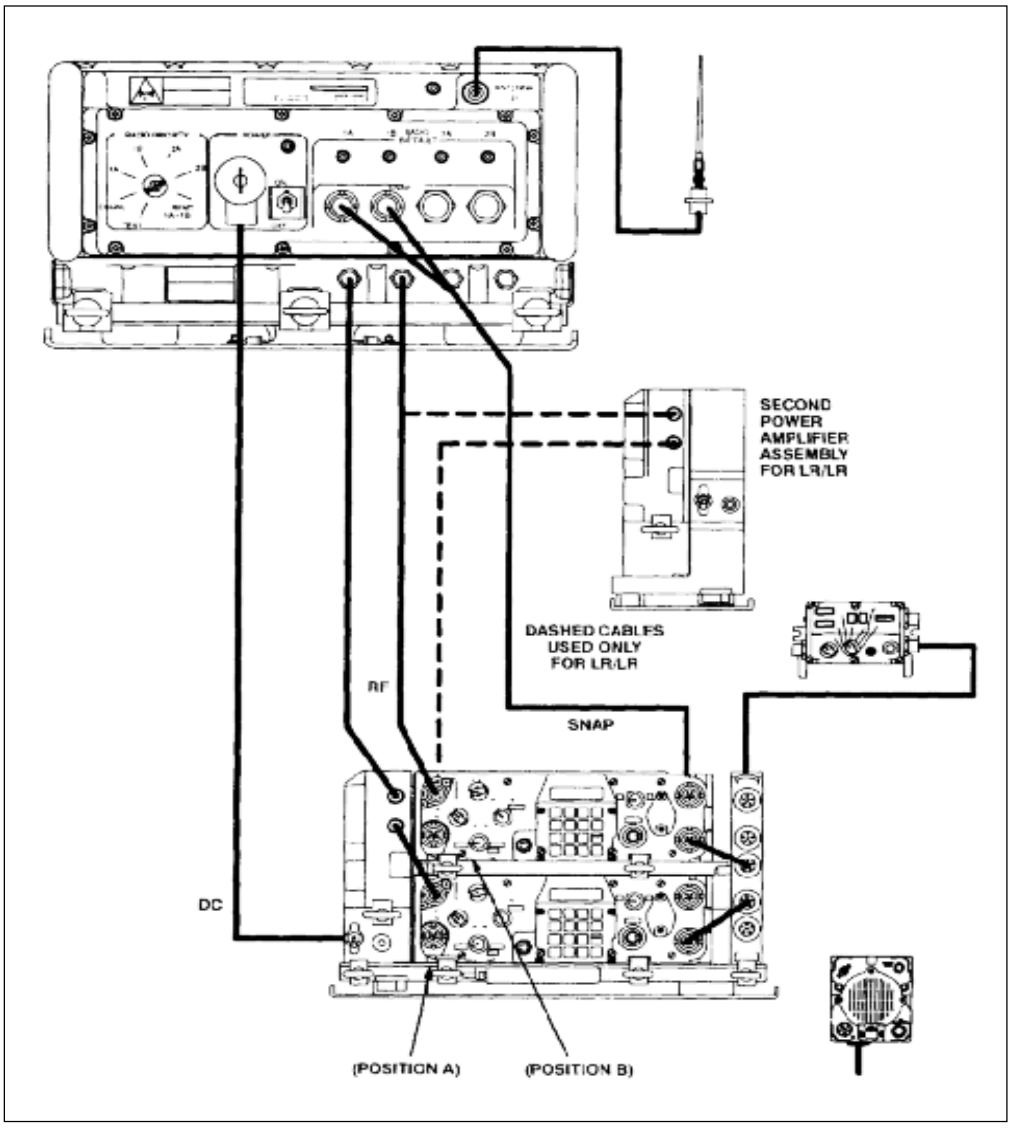


Figure H-9. AN/VRC-92 with Multiplexer

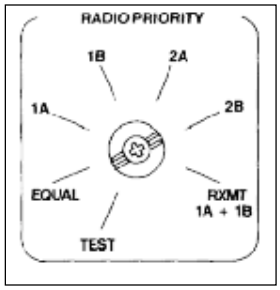


Figure H-10. Radio Priority Switch

Appendix I

High Frequency Radio Operations

The HF radio provides the SBCT with the only long-range communications capability independent of terrestrial or satellite relays. This appendix provides an overview and functional description of the capabilities and limitations of the HF radio systems employed by the SBCT.

OVERVIEW

I-1. The SBCT uses the HF radio to support elements employed BLOS and out of reach of other SBCT communications systems, or as a redundant communications system supporting other C2 systems. The HF Radio System provides the SBCT the only long-range communications asset that is independent of terrestrial or satellite relays. It provides medium-to-long range communications (50 to 300 kilometers [31 to 186 miles]). HF has a limited data capability and is used primarily for voice communications within the SBCT.

I-2. The COTS HF radio fielded to the SBCT is a user-owned and -operated ALE-capable system. The ALE capable system increases the ability of the unit to provide a C2 means, but continues to be dependent upon trained users and spectrum planners. Brigade and battalion S6s maintain operators capable of determining the proper antenna and antennas IAW current conditions and frequencies.

FUNCTIONAL DESCRIPTION

I-3. The COTS HF Radio System is modular and supports manpack, vehicular, and transit case mounted operations. The primary component of the COTS HF Radio System is the RT-1694D(P)(C)/U. Depending on the mission of the unit the RT-1694D(P)(C)/U is combined with other components to create manpacked, vehicular (20 and 150 watt configurations), or fixed station radios (transit cased - 400 watt configuration). The system is ALE-capable and provides an increased capability over legacy HF radios by automatically establishing communications on the best frequency available loaded in the HF radio. The system operates in the 1.6 to 59.999 MHz range using ground and sky wave propagation paths for medium-to-long-range communications. It is a HF single-side band (SSB) radio that operates in either the upper or lower sideband. The COTS HF radio accepts input of voice and data rates up to 4,800 bps when used with the appropriate ancillary equipment. All three-radio configurations can provide secured communications with an embedded COMSEC module.

I-4. Planning ranges for HF transmission distances are a function of the radio wave propagation (ground wave, short sky wave, or long sky wave) and the

antenna being used. Ground wave communications distance is primarily LOS. The short sky wave communications distance is less than 800 kilometers (500 miles) and generally involves a single hop. The long sky wave communications distance is greater than 800 kilometers (500 miles) and involves multiple hops.

MANPACK SYSTEM

I-5. The AN/PRC-150(C) manpack is a lightweight, battery-powered system. The AN/PRC-150(C) operates in the HF-SSB/VHF-FM bands and can operate in the 1, 5, 10, or 20-watt range (1-, 5-, 10-watt range for VHF-FM). The manpack set consists of the following equipment and accessories

- Radio chassis assembly, RT-1694D(P)(C)/U.
- Handset.
- Ground stake kit.
- OE-505 whip antenna (10 ft).
- Y-adapter cable assembly.
- Cable assembly, KDU.
- Battery box.
- Operator manual.
- Backpack.
- Cable assembly remote.
- Continuous Wave (CW) key.
- Antenna, manpack, and long wire.

VEHICULAR SYSTEMS

I-6. The COTS HF vehicular radio systems are available in 20- and 150-watt configurations. Both configurations are equipped with complete manpack accessories and can be converted into a manpack configuration. The vehicular systems allow for C2OTM when operating on the vehicle whip antenna

Vehicular 20-Watt HF Radio System

I-7. The Vehicular 20-Watt HF Radio System consists of the following equipment and accessories:

- Radio chassis assembly, RT-1694D(P)(C)/U.
- Speaker.
- Vehicular system - 20 watt consisting of –
  - Antenna mounting kit.
  - Power amplifier (PA) - 20 watt.
  - Coax cable assembly.
  - Control cable assembly.
  - Power cable assembly.
  - Installation manual.
  - Ground strap.

I-8. Figure I-1 shows a Vehicular Mounted 20-Watt HF Radio System.

Figure I-1 Vehicular Mounted 20-Watt HF Radio System

Vehicular 150-Watt HF Radio System

I-9. The Vehicular 150-watt HF Radio System consists of the following equipment and accessories:

- Radio chassis assembly, RT-1694D(P)(C)/U.
- Speaker.
- HF fast-tune automatic antenna coupler.
- Shock-mount antenna coupler.
- Coupler control cable.
- Coupler coax cable.
- HF whip antenna.
- Tilt whip adapter.
- Antenna mounting kit.
- Vehicular System - 150 watt consists of:
  - PA vehicular shock mount.
  - 150 watt PA with RF-5245 pre-post selector.
  - 25 MHz low pass filter.
  - Coax cable assembly.
  - Audio cable assembly.
  - Power cable assembly (20 ft).
  - 150-watt installation manual.
  - Control cable assembly.
  - Ground strap.

TRANSIT CASE SYSTEM

I-10.The Transit Case System is the high-powered configuration of the COTS HF family and is generally used in a fixed station configuration.

I-11.The Transit Case HF Radio System - 400 watt – consists of the following equipments and accessories:

- Radio chassis assembly, RT-1694D(P)(C)/U.
- Speaker.
- Transportable ground stake antenna.
- Transportable dipole antenna.
- 400W HF Mini-Transit Case System adapter consisting of –
  - FALCON II 400 watt PA.
  - RF-5054 power supply.
  - Loudspeaker.
  - Speaker audio cable assembly.
  - Speaker power assembly.
  - Coax cable assembly (4 ft).
  - Direct current (DC) power cable assembly (4 ft).
  - 400-watt installation manual.
  - Control cable assembly PA-RT (4 ft).
  - Alternating current (AC) power cable (9 ft).
  - Ground strap.
  - Mini transit cases (quantity three).
- Antenna coupler mini transit (two-case set) consisting of –
  - HF fast-tune automatic antenna coupler.
  - 250-ft control cable.
  - 250-ft coax cable.
  - Mini transit cases (quantity two).
- RF-5845 pre/post selector.

Appendix J

Battlefield Spectrum Management

The SBCT has a unique mission to support any US Army division or JTF. This support requirement, along with the SBCT information network, will drive spectrum management requirements for the SBCT. This appendix discusses the battlefield spectrum manager (BSM), database management, electromagnetic interference resolution, deconfliction, joint restricted frequency lists (JRFLs), and definitions of functions and frequencies.

OVERVIEW

J-1. Battlefield spectrum management is the systematic planning, management, engineering, and coordination of the electromagnetic spectrum used by units engaged in combat and training for combat. The SBCT is unique with the authorization of a Spectrum Management Additional Skill Identifier (ASI) D9 soldier. The D9 residing in the NETOPS section, operating from the BNOSC, performs the daily battlefield spectrum management functions for the SBCT. A BSM is assigned to the SIGCO and coordinates with higher, subordinate, and adjacent units and with other staff sections. Success in accomplishing the battlefield spectrum management mission will eliminate or minimize adverse collateral effects of co-site and adjacent frequency interference, because all battlefield systems, including non-Signal Corps emitters, are considered. The automated battlefield spectrum management tools and shared databases will provide automatic, accurate, and timely frequency allocation, assignment, and distribution.

BSM TACTICAL CHALLENGES

J-2. An unprecedented number of spectrum-dependant systems help the commander to win on the modern battlefield. Most of these systems are wireless and rely on the electromagnetic spectrum to operate. Thus, the electromagnetic spectrum is an increasingly limited resource. Without proper management, use of the electromagnetic spectrum could quickly reach saturation and could seriously degrade mission performance.

J-3. The BSM must consider sharing and reusing SBCT spectrum resources (allocations and assignments), not only by communications systems, but also by intelligence, surveillance, data, navigational, radar, and sensor systems.

BSM FUNCTIONS

J-4. The primary mission of the BSM is to ensure spectrum-dependent systems in the SBCT function as intended.

J-5. Coordination is the key to effective spectrum management. By direct coordination with higher, lower, and adjacent elements, the BSM can reduce or eliminate harmful interference from friendly force operations. The BSM coordinates with the S2/electronic warfare officer (EWO) before conducting intelligence and electronic warfare (IEW) operations. This coordination reduces adverse impacts on friendly force operations and helps to increase the effectiveness of friendly IEW. The BSM –

- Maintains the frequency database.
- Determines the SBCT's RF spectrum requirements.
- Ensures spectrum use considerations are in SBCT operation plan (OPLAN).
- Helps staff determine spectrum requirements.
- Requests frequencies to support the force operations.
- Coordinates with subordinate units to develop and distribute the signal operating instructions (SOIs).
- Deconflicts frequency assignments for SINCGARS and small unit radios.
- Deconflicts frequency assignments for TACSAT, EPLRS, NTDR, and air-ground-air systems.
- Assists higher BSM in coordinating and deconflicting SBCT emitters with other systems resident in the battlespace.
- Coordinates for the SBCT's RF spectrum-dependent equipment (COTS, government off the shelf (GOTS) and Army-fielded communications systems).
- Performs interference resolution.
- Coordinates with the S2, S3, and EWO to develop the restricted frequency list and JRFL.
- Conserves spectrum resources.
- Helps resolve co-site interference.
- Makes all frequency assignments for all subsystems, based on requests.
- Operates automated spectrum management tools and associated spectrum management programs.
- Manages satellite access, to include—
  - Satellite access request (SAR) and satellite access authorization (SAA) messages.
  - Network addresses.
  - Channel numbers.
  - Ephemeris data.
  - Demand assigned single access (DASA) or DAMA access.
  - Satellite interference reporting.
  - Satellite interference analysis.

- This is a HICON responsibility
- Coordinates (TUAV) communications payloads (SINCGARS and EPLRS).

J-6. The misperception of spectrum management is that it consists solely of assigning frequencies to the user's equipment. On the modern battlefield, this misperception continues to be a problem. The five functions of spectrum assignments are—

- Determining user requirements.
- Obtaining required frequency resources.
- Matching resources to requirements.
- Distributing frequency assignments to the user.
- Evaluating and optimizing spectrum use.

J-7. Battlefield spectrum requirements are determined by the user's operational needs and not items that would be nice to have. Based on doctrine and experience, the spectrum manager must estimate a unit's spectrum requirements. The type of operation and the equipment available determine the actual requirement. This information is drawn from operation orders (OPORDs), standard operating procedures (SOPs), coordination with the S6, and higher headquarters' G6 (HICON).

J-8. Frequency assignments are made from existing SBCT resources or are obtained from the supported HICON G6. The BSM will use automated spectrum management tools to assign and request frequencies to support the SBCT.

J-9. Spectrum resources are matched to requirements through allocation, allotment, and assignment.

Allocation

J-10. Allocation is the designation of frequency bands for use in performing specific functions or services, such as fixed, mobile, and amateur broadcast. When more than one type of service is authorized in a band, services are ranked as primary, permitted, or secondary. Primary and permitted services have equal rights except in preparing frequency plans. The primary service has first choice of frequencies. Secondary services are on a non-interference basis (NIB). The International Telecommunications Union (ITU) allocates frequencies on a global basis. An example is ITU allocation of the bandwidth from 230 to 235 MHz for fixed and mobile aeronautical and radio navigation. In the continental United States (CONUS), the Federal Communications Commission (FCC) allocates frequency for commercial use, and the National Telecommunications and Information Administration (NTIA) further allocates frequencies for the federal government (including military) as government exclusive, nongovernment exclusive, or government and non-government shared. Most frequencies used by the military/Army are on a sharing non-interference basis. An example is the allocation of 225 to 328.6 MHz for military air traffic control and air-to-air and air-to-ground communications in CONUS and US possessions. Likewise, each foreign country/host nation allocates frequencies for use within its geographic boundary.

Allotment

J-11. Allotment is the establishment of specific bands or frequencies within a prescribed nationally or internationally allocated band.

Assignment

J-12. Assignment is the designation of a specific frequency or frequencies for use by a radio station under specific conditions. An assignment grants permission to operate or turn on authorized equipment. An example is the assignment by the I Corps spectrum manager of frequency 226.075 MHz for the Corp's aviation net.

J-13. Most assignment requirements are identified at company and battalion level and are passed to the spectrum manager at the NOSC. If the BSM does not have the resources to fill the requirement, the BSM requests support from the ARFOR and division BSM.

J-14. Assignment of spectrum resources is basically a bottom-top-bottom process. Spectrum requirements are identified at companies and battalions within the SBCT. The BSM consolidates the requirements, makes assignments from available resources, or submits requests to next higher spectrum manager. The frequency assignment notification is then sent down through those same channels until it reaches the requesting unit.

BSM AUTOMATED TOOLS

J-15. To assist in the spectrum management mission, the BSM may have one or more of the following automated tools:

- Network planning terminal (NPT).
- Army Key Management System (AKMS).
- Local Key Management System (LKMS).
- Integrated Systems Control (ISYSCON).
- Spectrum XXI – replacing JSMSWIN.

DATABASE MANAGEMENT

J-16. Equipment technical characteristics are required to assign frequencies and to resolve interference. These characteristics include equipment tuning range, emission, channelization, and method of tuning (crystal or continuous). This information may be maintained on one or more of the automated spectrum management tools. The BSM will be required to update this database to include characteristics for new, commercial, or coalition force equipment or systems. Equipment characteristics for commercial equipment are available from the manufacturer or vendor and must be included in the emitter database. Information on other local or regional commercial/civilian emitters should be available from the HICON or supporting division. A spectrum manager's database may include—

- Frequency Resource Record System (FRRS).
- Database containing signal equipment parameters.
- Frequency allocation tables.
- International frequency list.

- Non-government frequency list.
- Government master file.
- Combined frequency allocation list (CFAL).
- Spectrum engineering tools.
- Equipment allocation documents.
- ITU and NTIA radio regulations.
- Military regulations.
- Manuals and pamphlets.
- Various other tools of the trade.

ELECTROMAGNETIC INTERFERENCE RESOLUTION

J-17. Electromagnetic interference is defined as any electromagnetic disturbance that obstructs, or otherwise degrades or limits, the effective performance of electromagnetic and electrical equipment. Electromagnetic interference can be induced intentionally, as in some forms of electronic warfare (EW), or unintentionally, as a result of spurious emissions, co-site effects, or intermodulation products.

J-18. Interference resolution is handled at the lowest level possible. Interference may come from signal devices (such as unintentional friendly and unfriendly radios and radars) and from non-signal devices (such as welders, vehicle engines, or computers).

J-19. After being informed of unresolved interference, the SBCT BSM can-

- Seek assistance from the EWO in identifying the source.
- Advise on and assist with the physical relocation of the affected user.
- Advise tolerance of the interference (working through it).
- Make appropriate changes in frequency assignments.

J-20. The EWO or S2 may detect hostile interference or jamming before it is recognized and reported to the BSM. A spectrum interference report should be initiated. Most instances of spectrum interference will be resolved locally within the SBCT, division, or corps.

J-21. During training exercises, CONUS-based Army forces (SBCTs) will attempt to resolve interference problems with their division or corps, or report interference to the supporting directorate of information management (DOIM), who will make every effort to resolve problems locally. If the interference cannot be resolved locally, the supporting DOIM will report the problem to the service-engineering agency responsible for interference resolution for assistance. The Army Signal Command (ASC) provides operational electromagnetic compatibility (EMC) and propagation engineering (PE) support for the Army. See the ASC Web site, www.asc.army.mil/EAC, for more information.

J-22. Army forces located outside CONUS (OCONUS) will report spectrum interference to the supporting joint frequency management office (JFMO) in accordance with the guidelines contained in the Joint Spectrum Interference Resolution (JSIR) Program. When division and corps units cannot resolve

interference problems locally, a report will be sent to the theater Army and commander-in-chief (CINC) JFMO headquarters for resolution. The JFMO will interface with the host nation through the status of forces agreements, where required.

J-23. In certain cases, the JFMO cannot resolve the spectrum interference problem after working with the host nation, and the interference incident cannot be resolved by the affected DOD component or the service engineering agency responsible for spectrum interference resolution. In such instances, the spectrum interference problem is referred to the JSC JSIR office for resolution.

J-24. The Joint Spectrum Center (JSC) JSIR office will analyze and attempt to recommend corrective action for reported interference problems by first using the JSC and JSIR databases and analytical tools, and then, if needed, by providing personnel and equipment to perform on-site direction finding, equipment tests, and problem solution.

J-25. Interference to HF, satellite, or troposcatter communications may involve reporting the interference to activities outside the theater or CINC AOR.

J-26. The initial interference report should be sent to the BSM. He has the database to quickly check friendly frequency assignments. He may go to the next higher-level spectrum manager for assistance.

J-27. The skill of signal systems operators and maintenance personnel can mean the difference between minor inconvenience and complete system disablement. On experiencing harmful interference, the operator should be able to discern whether the interference is coming from natural phenomena or man-made sources.

J-28. If natural phenomena are the cause, the operator should try to work through the interference. Should it persist, a BSM-coordinated frequency change may be in order.

J-29. If the operator suspects man-made interference, he makes an internal equipment check to exclude equipment malfunctions. In many cases, improper alignment, degraded components, antenna disorientation, or poor maintenance is the culprit. After the operator has ruled out internal causes, a check with other friendly units in the area may reveal incompatibilities between operations. If a compromise cannot be worked out between the units, the case is referred to the spectrum manager at the next higher echelon.

Appendix K

Digital Signal Planning Process

The brigade and battalion S6s are principal staff officers for all matters concerning C4 Operations. The SBCT provides a unique situation where the SIGCO performs many functions at brigade level historically performed by the brigade S6. This appendix provides the necessary steps to effectively execute the digital signal planning process.

DIGITAL MILITARY DECISION MAKING PROCESS (DMDMP)

K-1. The DMDMP relies on network and system enablers to foster a parallel and collaborative planning process. The DMDMP enables commanders and staff at all levels to initiate planning in conjunction with higher headquarters. Thus a subordinate staff could begin planning and developing a course of action (COA) prior to receiving a complete operations order from higher headquarters. The parallel and collaborative DMDMP has six actions that are utilized concurrently throughout the process; these actions are:

- Update and ensure SU.
- Receive the mission.
- Collaborate on the COA.
- Refine and synchronize the selected COA.
- Commander's approval of the plan.
- Rehearsing.

SITUATIONAL UNDERSTANDING

K-2. A key component of DMDMP is the ability to maintain SU throughout the battlespace, thus providing a common operating picture. SU is an ongoing process conducted throughout an operation that provides a complete picture of the battlespace (friendly and threat). SU is derived using the following collection devices:

- All Source Analysis System (ASAS).
- Manuever Control System (MCS).
- Air and Missile Defense Work Station (AMDWS).
- Combat Service Support Control System (CSSCS).
- FBCB2.
- Unmanned Aerial Vehicle (UAV).
- Joint Surveillance Target Attack Radar System (JSTARS).
- External intelligence collection assets.

RECEIVE/ANTICIPATE MISSION

K-3. Utilizing collaborative planning tools (such as VTC and whiteboard) the S6 and signal commander can anticipate mission requirements and potential AOs by observing the DMDMP at a higher echelon or HICON. By combining the anticipated higher mission and the current SU, the S6 and signal commander can begin a collaborative and parallel planning process.

COLLABORATE ON A COA

K-4. The brigade S6 and signal commander will collaborate on a COA that will collectively support the scheme of maneuver and commander's intent. This may include collaboration of Relay/Retrans/relay assets with the battalion level S6's. Collaborating on a COA combines three COA steps: COA development, COA comparison, and COA decision into a single action. When executed in parallel with higher, adjacent, and subordinate units this COA should sufficiently provide the most effective coverage with the greatest flexibility and redundancy possible.

REFINE/SYNCHRONIZE SELECTED COA

K-5. The S6 and signal commander participates in this action through war games and coordination with other battlefield operating systems (BOSs). Through this process a decision support template (DST), synchronization matrix, and a clear understanding of the plan is developed. After this action the signal support plan should be validated for supportability and survivability in relation to the intent of the commander.

COMMANDER'S APPROVAL OF THE PLAN

K-6. This military decision-making process (MDMP) step remains unchanged when used in the DMDMP.

REHEARSALS

K-7. Rehearsals are performed at all levels and sometimes with the back briefs to verify what the commander briefed. Rehearsals can be conducted virtually (such as with VTC and whiteboard) or physically at a specific location. Rehearsals are usually conducted by phase of an operation, and are an opportunity to ensure all elements of an operation understand critical events or actions. The rehearsal is not the time to make key staff coordination or plan alterations.

K-8. The S6 and signal commander should be involved in the rehearsal and address –

- Potential communications problem areas at the maneuver rehearsal.
- Demonstrate how the signal plan will support the scheme of maneuver.
- Define locations of the Relay/Relay/Retrans and ensure anti-jam plans are understood.
- Specific NM issues.

K-9. As a final step to conducting a rehearsal, the brigade S6 and subordinate S6s must collaborate and conduct a signal rehearsal . Personnel from the BNOSC and the SIGCO must attend and fully understand the intent of the signal network plan and the subsequent execution of the network.

K-10. Reconnaissance and surveillance assets, such as scouts and other observation teams, frequently conduct separate rehearsals run by the RSTA commander or S2. These are critical assets requiring detailed instructions and redundant communications. The S6 or his representative should attend this rehearsal, ensuring various teams fully understand the instructions and contingencies.

WARNING ORDER

K-11. A warning order will be provided to subordinate units when they are slated for a possible mission. The warning order will allow the brigade S6 to provide guidance to the SIGCO and subordinate battalion S6s.

S6 INTERNAL PLANNING

K-12. Table L-1 is a checklist of S6 internal planning requirements that helps ensure a successful operation. The table lists internal planning considerations to be used by the S6. Add to this list of planning, COMMEX as a separate step, add IP addressing scheme requirements, Satellite planning considerations, TOC-to-TOC radio cluster identification, management responsibilities, identification of primary node locations (jump), attachments of client systems or unique equipment, HICON satellite assets or other equipment.

Table L-1 Internal Planning

Identify	Result
Combat Net Radio	Ensure CNR is integrated into the communications exercise (COMMEX).
Communications contact team	Determine what triggers contact team employment and what actions are expected.
Net control station (NCS) procedures	Determine who controls what brigade and battalion nets.
Relay/Relay/Retrans teams	Plan requirements for employment, support, and site selection based on tactical situation and LOS requirements, triggers, frequencies, and distribution plan. Make sure the Relay/Retrans chief back briefs the plan.
Communications problem solving	Use an alternate net to resolve problems; do not use the command net. If available provide the Relay/Relay/Retrans team an additional radio (HF) to resolve any problems.
Security	Coordinate with the brigade or battalion S3 for security support.

Table L-1 Internal Planning (Continued)

Identify	Result
Relay/Relay/Retrans OPORD	One-page matrix with only key information needed for operations.
Rehearsals	Attend rehearsals/rockdrills. The CSS and the reconnaissance and surveillance rehearsals are critical to success.
SOP	Provide a thorough, well-planned SOP; this is essential for success.

ORDER RECEIVED FROM HIGHER COMMAND

K-13. Once the order is received, a list of checks and balances must be performed to ensure the mission is successful. A mission analysis is conducted including specified and implied tasks. These tasks are to –

- UTO/UTR.
- Determine network initialization for TOC servers (boot sequence).
- Determine network reconfiguration requirements to support mission.
- Verify the location of the BSA for coverage of the administrative and logistics net.
- Coordinate for signal support and frequency and COMSEC support. relay/retrans.
- Collaborate all SBCT retrans/relay location.
- Ensure the backup Relay/Retrans team is briefed and preloaded.
- Validate Relay/Retrans/relay locations with automated profiling tools.
- Define time-sharing and procedures for critical nets to overcome problems with inter-/intra- service operations.
- COP and CTP rewrite digital. Ensure the S3 has key communications events on the execution matrix and net calls are done daily or tied to a specific event in the planning process.
- Confirm receipt of updated ASAS Receive a copy of all the intelligence updates; verify the terrain on slow go/no go areas and potential threats to the Relay/Retrans team(s).
- Verify the type of mission and priority of effort.
- Relay/RetransCoordiante to ensure RSTA squadron reconnaissance and surveillance plan is supported.
- Coordinate a timeline for the COMMEX.
- Coordinate with the G3/S3 to identify the brevity codes.
- Coordinate with the maintenance officer to verify deadlined vehicles with radios.
- Coordinate with the engineer officer for assets so the Relay/Retrans team can be protected for survivability.

- Coordinate with the fire support officer (FSO) and ensure the Relay/Retrans team is plotted and covered by supporting fires.
- Coordinate with the chemical officer for possible nuclear, biological, chemical (NBC) hazards in and around Relay/Retrans locations.
- Ensure Relay/Retrans sites are plotted for CSS/medical evacuation (MEDEVAC) plan.
- Coordinate with Medical officer and verify MEDEVAC frequency/network identification (Net ID) and call signs. Verify whether the net is secure or nonsecure. Determine the net procedures of the MEDEVAC and if they change channels once they are on the site.

LOSS OF COMMUNICATIONS

K-14. Backup and even tertiary plans should be developed in case communications is lost between higher, lower, and lateral units.

- **Primary —** Contact higher command on frequency modulated (FM) command net
- **Alternate —** FBCB2-Conduct troubleshooting procedures.
- **Contingency —** Move to a better location.
- **Emergency —** Contact an adjacent unit to pass the message traffic.

K-15. Contact points should be included on graphic overlays for units to meet if no contact is made within a specified amount of time. Particular attention should be paid to units that habitually operate independently, such as scouts, engineers, air defense artillery (ADA), and improved remotely monitored battlefield sensor system (IREMBASS)/ground surveillance radar (GSR).

COMSEC

K-16. Verify all COMSEC keys prior to distribution.

RELAY/RETRANS OPERATIONS

K-17. Prepare an alternate communications plan in case Relay/Retrans fails, nets are compromised, or the Relay/Retrans team must relocate. Refer to Appendix B.

TOC RECONNAISSANCE/TOC SIGNAL CONSIDERATIONS

K-18. Identify locations for network connectivity. Determine unique network requirements during TOC split based operations.

COMPROMISE OF SINCGARS NETS

K-19. Wartime communications are susceptible to enemy compromise. Avoiding and recovering from a compromise are vital in maintaining C2 communications. Steps to minimize effects from lost or captured equipment on the battlefield include –

- Automated network control devices (ANCDs) below the battalion level (S6) will only have the current unit traffic encryption key (TEK)

and key encryption key (KEK) and the minimum SOI data to perform the mission.

- ANCD loadsets will be loaded with the Net ID 999 in each fill position so not to compromise unit nets if captured. Net ID 999 will not be assigned as an operational net.
- ANCDs and the cryptographic ignition key (CIK) are always stored or transported separately to increase the difficulty of equipment operation by the adversary.
- Unique KEKs are assigned down to company level; however, situations may arise that require unique KEKs at lower levels.
- Units assign specific Net IDs as COMSEC recovery nets; predetermined Net IDs are addressed in tactical standing operating procedures (TSOPs) and/or OPORDs.

SYSTEMS OPERATORS

K-20. Radio operators must understand their respective radio systems and the tactical maneuver plan; they should be included in the battalion rehearsal. The radio operator continuously monitors the radio and promptly reports all tactical developments to the commander. Radio operators are not radio carriers and will take an active role in monitoring and controlling the operation.

K-21. Identify troubleshooting procedures regarding ABCS operators and when to enact a call to the brigade trouble desk.

K-22. Continuity books on each individual system.

BATTERY MANAGEMENT

K-23. Battery management is the most critical area for operations and sustainment planning. Use SB 11-6 to plan the battery basic load. The battery basic load must be in the SOP and in CSS planning. Rechargeable batteries should be used whenever generator power is available (at tactical CPs and BSB locations). The company's three-day basic load should be pushed as far forward as possible to avoid delays when a change in mission or the operational tempo (OPTEMPO) is high. Make sure the units return used lithium batteries through the resupply system (the enemy can use these batteries). Common commercial batteries (D-cell, AA, and 9-volt) run much of the unit's equipment. Most of these items have adapters, such as the AN/PVS-7 and GPSs. Incorporate technical bulletins and maintenance tips into the unit's tactical SOP.

K-24. Table L-2 is an example of a unit battery stockage chart. The S6 must develop a stockage chart for all batteries used in the unit.

Table L-2 Unit Battery Stockage Chart (Example)

Battery	Equipment	Hours at 70 °F	Operating Temp Max	Hours at Max Temp	Operating Temp Min	Hours at Min Temp	National Stock Number (NSN) 6135-01
BA-5372/U	TSEC/KY-68	1800	140°F	1800	-40°F	1000	214-6441
BA-5590/U	AN/PRC-119	20	125°F	20	-20°F	12	036-3495

Appendix L

Tactical Wire and Cable Operations

Establishing telephone cable systems within a CP requires careful planning and routing. This appendix covers tactical wire and the different types of cables used within a CP.

OVERVIEW

L-1. The relative transmission characteristics of telephone cable laid on the ground, buried, or installed on aerial supports is an important consideration in tactical wire and cable operations. An aerial line generally provides the most satisfactory type of service. Aerial construction is easier to maintain than surface construction and provides better quality circuits. However, aerial construction takes longer to lay than surface construction.

L-2. Surface cables require immediate and continuous maintenance. Carefully installed surface wire lines provide reliable circuits suitable for most combat operations. Cable and wire may initially be laid with only a minimum of servicing to ensure continuous communication.

NOTE: Proper policing should be accomplished immediately afterwards.

L-3. Buried wire lines are rarely used in forward areas. However, it may be necessary at times to bury cable and wire lines to protect the lines from troops and vehicles. Buried wire lines are more electrically stable than aerial or surface lines, and are rarely affected by weather and temperature. However, disadvantages of the buried wire include—

- More time is required for installation.
- They are more difficult to maintain and recover.
- The wire and cable is generally damaged during recovery and is not reusable.

TELEPHONE CABLE SYSTEM

L-4. Telephone devices are portable, self-contained equipment requiring cable to provide the link into the network. These devices combine durable construction with portability. Telephone cables that can be use to link the different telephone devices to the network include—

- Twenty-six pair cable, CX-4566/G.
- Special purpose cable assembly CX-11230(*)/G.
- Special purpose cable assembly CX-10734/G.
- Fiber optic cable assembly (FOCA).

TWENTY-SIX PAIR CABLE CX-4566/G

L-5. Twenty-six pair cable is a stranded conductor with 26 pairs of color-coded wires. It provides cable distribution for local telephone lines and circuits, interconnects communications shelters, and is used in conjunction with distribution boxes and cable stub CX-4760/U. Twenty-six pair cable terminates in a universal connector at each end. It is sturdy enough for both ground and aerial use. It is supplied in 250-foot lengths on metal cable reel RC-435/U.

L-6. Twenty-six pair cable can be used in the following three ways:

- **Aerial –** Aerial cable is installed on A-frames, trees, or poles using basket hitch tie and weave tie. The cable must have a minimum clearance over main roads of 18 feet above the center of the road and 14 feet over the secondary road and in command areas.
- **Surface –** Twenty-six pair cable is not normally surface cable, but when used as surface installation, installers must take measures to prevent it from being damaged by vehicles.
- **Buried –** Twenty-six pair cable is recommended for above ground use only. However, if construction requires it to be buried, bury the cable 6 to 12 inches deep.

L-7. To connect the twenty-six pair cable, join the conductors and hand-tighten the connection by turning both sleeves on the conductor. Make a tension bridge after the connection. For each span between poles or trees, allow the cable to sag. Table M-1 lists the recommended sags. If the span falls between two of the cited values, use the higher figure.

NOTE: Do not permit the sag tension to exceed 100 pounds.

Table M-1. Cable Sags

Span	100 ft.	125 ft.	150 ft.	175 ft.	200 ft.	Over 200 ft.
Sag	16 in.	24 in.	36 in.	48 in.	72 in.	Use messenger cable

L-8. Table M-2 lists the procedures required to recover a twenty-six pair cable.

Table M-2. Twenty-Six Pair Cable Recovery Procedures

Step	Procedure
1	Remove all wires, tags, ties, junction boxes, and telephones.
2	Lower aerial cable and remove buried road crossing cable.
3	Install RL-31-( ) with empty reel and reel in cable with first 6 feet of cable into the reel center storage area, place the connector into storage compartment, and secure the cable with storage straps.
4	Station one team member by the reel with the crank, one member to hold the end of cable connector, and a third member to guide the cable on the reel.

SPECIAL PURPOSE CABLE ASSEMBLIES CX-11230(*)/G AND CX-10734/G

L-9. Cable assembly CX-11230(*)/G is an inter-area coaxial cable. It provides a four-wire cable transmission medium for wideband pulse code modulation (PCM) and time division multiplexing (TDM) carrier systems. The CX-11230/G and CX-11230A/G are the two types of CX-11230(*)/G. The CX-11230/G is a twisted spiral construction. Figure M-1 shows the CX-11230/G. The CX-11230A/G is similar to the CX-11230/G, with internal differences and a smooth outer cover (not shown).

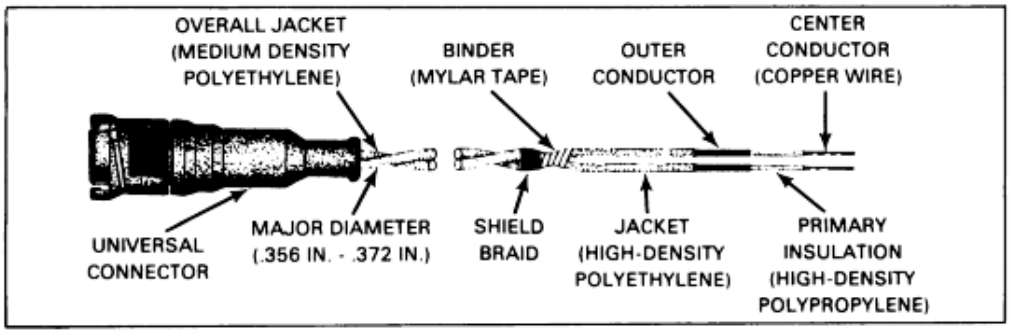


Figure M-1. Cable Assembly CX-11230/G

L-10. Cable assembly CX-11230(*)/G is available in 0.4-kilometer (1/4- mile) and 33-meter (100-feet) lengths. The 33-meter cable is used with the 0.4-kilometer cable to obtain the required length of a transmission line. Both are terminated at each end with universal connector UG-1870/U. Each connector has a waterproof cover that should be kept in place whenever the cable is disconnected. Figure M-2 shows the 0.4-kilometer cable mounted on reel DR-15-B. Figure M-3 shows the 33-meter cable mounted on reel RC-435/U.

L-11. Cable assembly CX-11230(*)/G provides a transmission line for 12-, 24-, and 48-channel TDM-PCM systems and 96-channel time division multiplexer (TDM)-PCM systems. When constructing cable systems for digital group multiplexer (DGM) networks, use only the CX-11230A/G to prevent an impedance mismatch that may hinder communications.

L-12. Construction of CX-11230 (*)/G cable systems may be as long as 384 kilometers (240 miles), but they must have an unattended restorer at 1.6 kilometers (1 mile) and an attended restorer facility every 64 kilometers (40 miles).

NOTE: Cable assembly CX-11230(*)/G replaces inter-area cable assembly CX-4245/G.

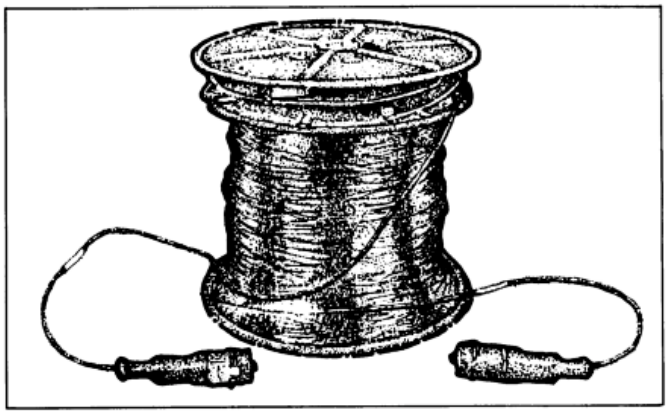


Figure M-2. Cable Assembly CX-11230( )/G, 0.4-Kilometer Length Mounted on Reel DR-15-B

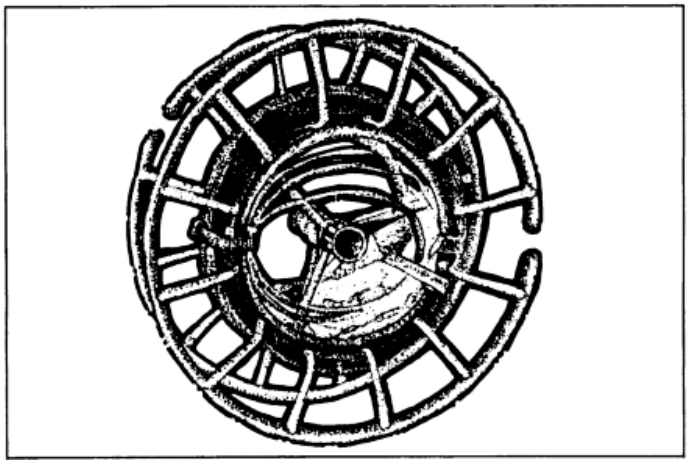


Figure M-3. Cable Assembly CX-11230( )/G, 33 Meters, Mounted on Reel RC-435/U

L-13. The CX-11230/G has two conductors, each covered by a plastic insulation, separate shield, and plastic jacket. The conductors are twisted, shielded again, and covered with an outer plastic jacket. The cable is oval in shape and terminates at each end with a connector, plug, and electrical UG-1870/U.

L-14. The CX-11230A/G has two conductors, each covered by a plastic insulation, separate shield, and plastic jacket. The conductors are twisted with plastic and paper fillers and secured with a thin, clear plastic. They are shielded again, wrapped with a thin aluminum, and covered with an outer plastic jacket. The CX-11230A/G is round, has a smooth covering, and terminates at each end with a connector, plug, and electrical UG-1870A.

NOTE: Refer to TM 11-5995-208-10 for more information.

L-15. Cable assembly CX-11230(*)/G connects to CX-10734/G, which consists of two 4-foot long coaxial tubes with a universal connector on one end, and a male and female connector on the other end. Cable assembly CX-10734/G is used to complete a connection to cable assembly CX-4245, to a tactical communications shelter, to test set AN/PTM-7, or to repeater TD-206( )/G. Figure M-4 shows the CX-10734/G.

L-16. Preformed wire grip ND-0104 is used to relieve strain on the connectors, to secure the CX-11230/G to anchors, and to support the cable in aerial construction. Figure M-5 shows the ND-0104.

NOTE: ND-0104 is preformed to fit the twist and shape of the CX-11230( )/G.

L-17. Cable assembly CX-11230A/G uses preformed wire grip ND-0107 to support the cable in aerial construction. The ND-0107 is similar to ND-0104, but is larger and specially constructed for use with the CX-11230A/G.

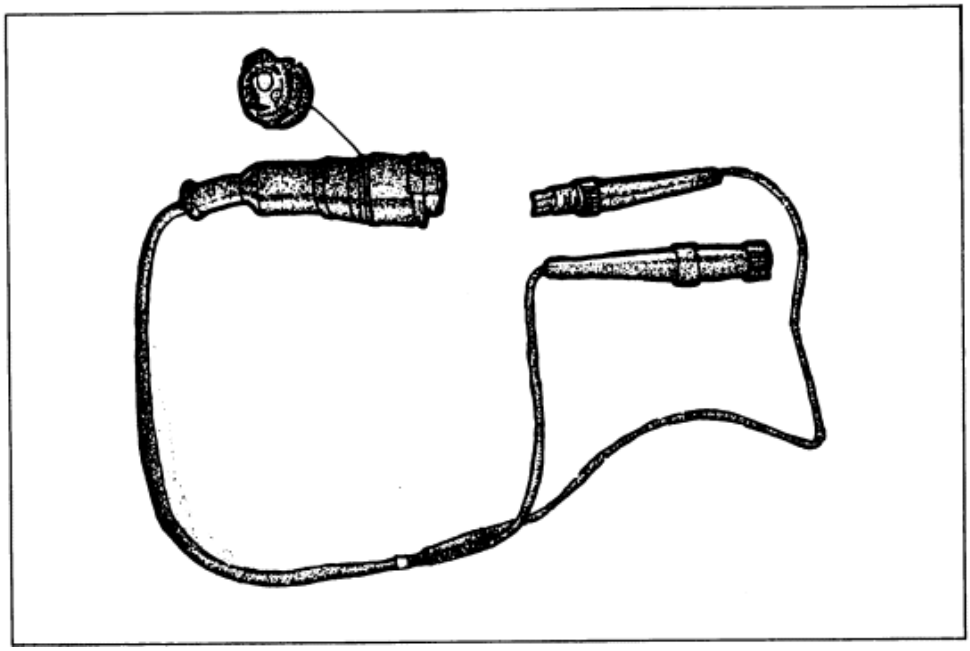


Figure M-4. Special Purpose Cable Assembly CX-10734/G

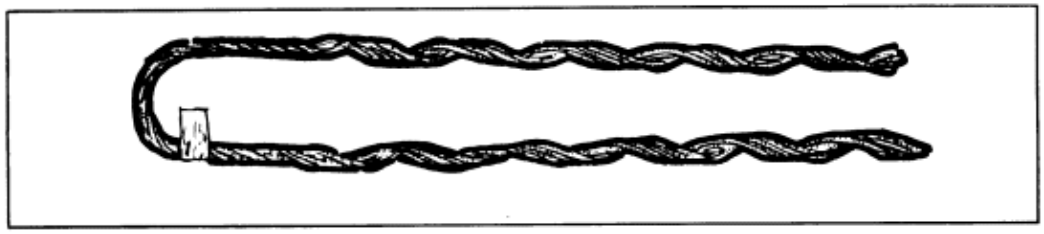


Figure M-5. Preformed Wire Grip ND-0104 and ND 0107

L-18. Table M-3 lists the procedures required to install cable assembly CX-11230(*)/G on poles, trees, or A-frames using preformed grips with safety loop.

Table M-3. Cable Assembly CX-11230(*)/G Installation Procedures

Step	Procedure
1	Mount the reel on the reeling machine RL-207/G, leaving enough slack at the beginning and end of the cable run as needed. Truck speed should be the speed of a fast walk.
2	Anchor the cable to a stake using the proper preformed grip. Feed off the cable on the RL-207/G using gloves and place the cable off the road in surface installation.
3	Test each section of cable before and after connection with test set AN/PTM-7. Interlock two preformed grips and form a loop after connecting the connectors. Never put the connector in the span.

WARNING

Do not install cable on or near power lines or a generator.

L-19. Cable assembly CX-11230(*)/G can be recovered using reeling machine RL-207/G. Remove all ties, cable grips, repeaters, tags, and the lower aerial cable, and then pull up buried cable. Using RL-207/G to recover cable by connecting cable to reel and reel approximately 12 feet of cable into reel storage compartment. One soldier guides the cable on the reel, one pulls in the slack, and one carries the connector. Inspect the condition of the cable during recovery. Reel in the last 5 to 10 feet of cable by hand. Refer to TM 11-5995-208-10 for more information.

L-20. Table M-4 lists the characteristics of various types of field cable.

Table M-4. Characteristics of Field Cable

Common Term	Basic Cable or Wire	Assembly	Length	Attn (db) per mile[1] (1.6 km)	Weight	Tensile Strength in lbs	Loading	Added Information
Inter-area coaxial cable		CX-11230/G (Std A) CX-11230A/G	1/4 mile (0.4 km) 100 ft	38@2.304 MHz	308 lb per mile (1.6 km)	750	None	Two coaxial conductors, improved connector, and improved shielding.
Twenty-six pair cable	WM-130/G (Std A)	CX-4566/G CX-4760/G	250 ft or 25 ft 15 ft	2.5	150 lb per 1,000 ft	700	None	Stranded conductors, six copper, and 1 steel-#24 AWG.

TFOCA

L-21. The TFOCA provides the physical connection between fiber optic modems (FOMs), repeaters, or other equipment capable of electrical-to-optical conversion. The TFOCA is a ruggedized, lightweight, and tactically superior fiber-optic cable that replaces CX-11230 coaxial cable. Figure M-5 depicts the TFOCA.

L-22. The TFOCA is designed for quick and easy deployment in rugged, harsh environments. It is engineered to satisfy the stringent environmental and mechanical requirements of military tactical operations.

L-23. The following are several advantages of fiber over traditional metal cable communications:

- Fiber offers much greater bandwidth.
- Fiber is less susceptible to interference.
- Fiber is thinner and lighter.
- Data can be transmitted digitally over fiber (a natural form for computer data).

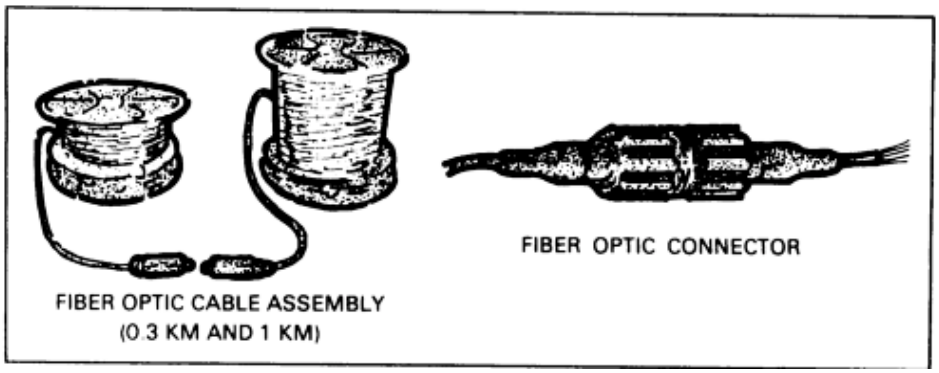


Figure M-5. TFOCA

L-24. The main disadvantage is that fiber is expensive, more fragile than metal wire, and difficult to split.

L-25. Install the TFOCA the same way as CX-11230(*)/G cable. Some deviations exist because of the bending limitations of TFOCA. Installing the TFOCA using the RL207 or RL31 is recommended. The preferred method is using the RL31 because of the extreme caution necessary to prevent damage and breakage of the TFOCA. Refer to TM 11-6020-200-10 for more information.

L-26. Use tactical multichannel connectors to couple the TFOCA to either node equipment or additional TFOCA links. The durable and environmentally sealed connectors provide for reliable, low loss performance in any environment while offering quick connect/disconnect using only bare or gloved hands. Figure G-5 shows a typical TFOCA application.

L-27. The following are the TFOCA technical specifications:

- Optical fiber bandwidth @1300nm: Greater than or equal to 400 MHz-km.
- Attenuation: Less than or equal to 2.75dB nominal (1km length with two connectors).
- Operating temperature range: -55°C to +85°C.
- Tensile load: (Newtons) - Deployment: 1,780 - Long Term: 500.
- Corner bend: 500 Newtons · Knot: 300 Newtons.
- Available lengths: 300m, 1km, 2km, and custom lengths.

CABLE REPAIR AND SERVICING

L-28. Various types of specialized test equipment are used to test different types of cables. This equipment enables the tester to quickly and accurately conduct the tests necessary during installation and maintenance of field cables.

L-29. Test instruments are delicate, precision devices that require careful handling while being transported or operated. The tester should be familiar with each test set, and should observe all required safety measures during the performance of any test.

SUBSCRIBER EQUIPMENT

L-30. Different types of field telephones may be used with communications equipment within a CP. The following paragraphs discuss information on the different telephone equipment found in the BCT. For more detailed information on any specific equipment, refer to the technical manual or other publications on that item.

LUCENT 8110

L-31. The Lucent 8110 is a COTS telephone that has seven fixed feature buttons: flash, redial, hold, speaker, mute, program, and pause.

L-32. The telephone has one-touch speed dialing for frequently called numbers, redial (last number dialed) button, built-in speakerphone, and auto answer and auto disconnect. Figure M-6 shows a Lucent 8110.

Figure M-6. Lucent 8110

LUCENT 8510T

L-33. The Lucent 8510T is a COTS telephone with nine fixed feature buttons: hold, transfer, speaker, conference, redial, volume, drop, mute, and edit. It has four fixed controls, including menus, directory, next, and previous buttons. The telephone also has acoustically adaptive built-in speakerphone, a hearing aid-compatible handset, and a personnel directory.

IP PHONE 12SP

L-34. The IP phone 12SP features twelve programmable buttons that can be programmed as any combination of access or feature buttons. It consists of a speakerphone, liquid crystal display (LCD), speaker mute button, integrated Ethernet hub, hearing aid-compatible handset, and an audio compression circuit. The telephone is also H.323- and net-meeting compatible, and may use IP addressing assignment. Figure M-7 shows the IP phone 12SP.

Figure M-7. IP Phone 12SP

IP PHONE 30 VIP

L-35. The IP phone 30 VIP uses 30 feature buttons with four fixed-feature buttons for transfer, display, hold, and redial. The telephone has 26 programmable buttons that can be used to perform any combination of features.

L-36. The telephone has numerous features, such as an integrated Ethernet hub, optional phone and PC port, convenient up-down buttons for control of speakerphone volume, handset volume, ring volume, ring tone, and display contrast. It also has a large 40-character two-line display with user-adjustable contrast. It uses the G.711/G.723 audio compression circuit. The telephone is also H.323- and net-meeting compatible, and may use IP addressing assignment. Figure M-8 shows an IP phone 30 VIP.

Figure M-8. IP Phone 30 VIP

Appendix M

Local Area Networks

Linking information systems within a local geographical area creates a LAN. The LAN provides a path for data to travel, gathering and sharing information. This appendix discusses the methods used in implementing a LAN at any echelon.

LAN CONFIGURATION

M-1.A LAN is planned and configured depending on the mission of the unit and the commander's intent. The hardware, software, and peripherals used must interoperate. Hardware and software requirements must be met and installed for a LAN to be fully operational and effective.

INFORMATION SYSTEMS

M-2.Computers are electronic devices operating under instructions stored in the memory unit. Computers can accept and process data (input), produce results (output), and store data for future use. Computers can communicate by sending and receiving data to other computers connected together forming a LAN. This configuration is accomplished by interconnecting the computers together with a wireless LAN or by using wire and cable to form a LAN.

NOTE: A LAN consists of two or more computers linked together by any means to share information. See FM 24-7 for more information.

LANs

M-3.A LAN is a data communications network that interconnects a community of digital devices and other peripherals. LANs vary as they depend on mission, enemy, terrain, troops, time, and civilian consideration (METT-TC).

M-4.A LAN consists of a communications channel that connects computer terminals to a central computer or, more commonly, connects a group of computers to one another. Figure N-1 shows an example of a LAN.

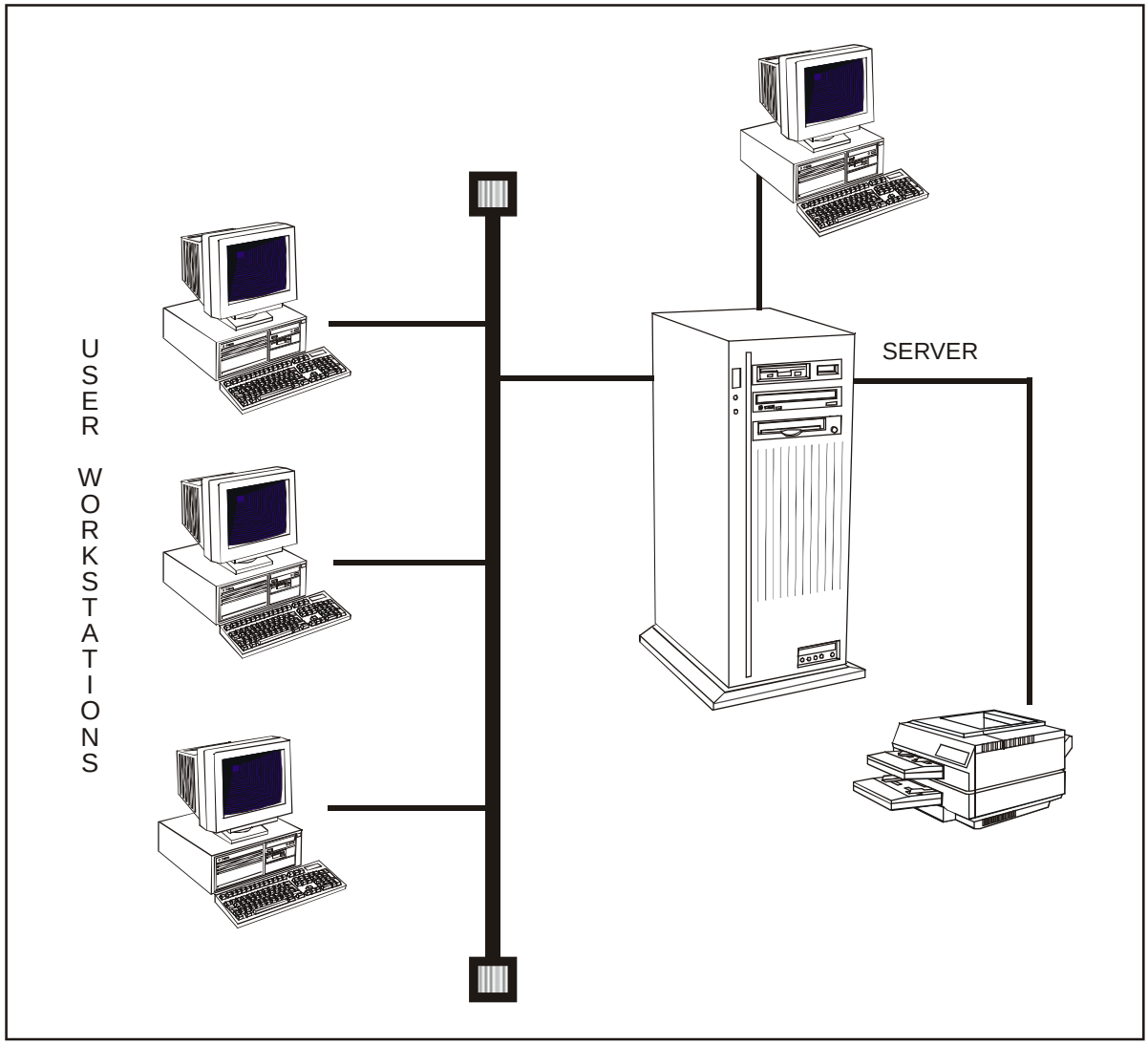


Figure N-1. Example of a LAN

NETWORK INTERFACE CARD (NIC)

M-5.A LAN connection is normally connected via coaxial cable, twisted-pair cable, and fiber-optic (FO) cable, which requires a (NIC). The NIC fits in an expansion slot of a computer or other device. Most NICs require a cable connection and have connectors on the card for different types of cables. Figure N-2 shows an example of a NIC connected by a T-connector with a coaxial cable or an RJ-45 cable.

NOTE: All Army LANs use the Institute of Electrical and Electronic Engineers (IEEE) 802.3/802.

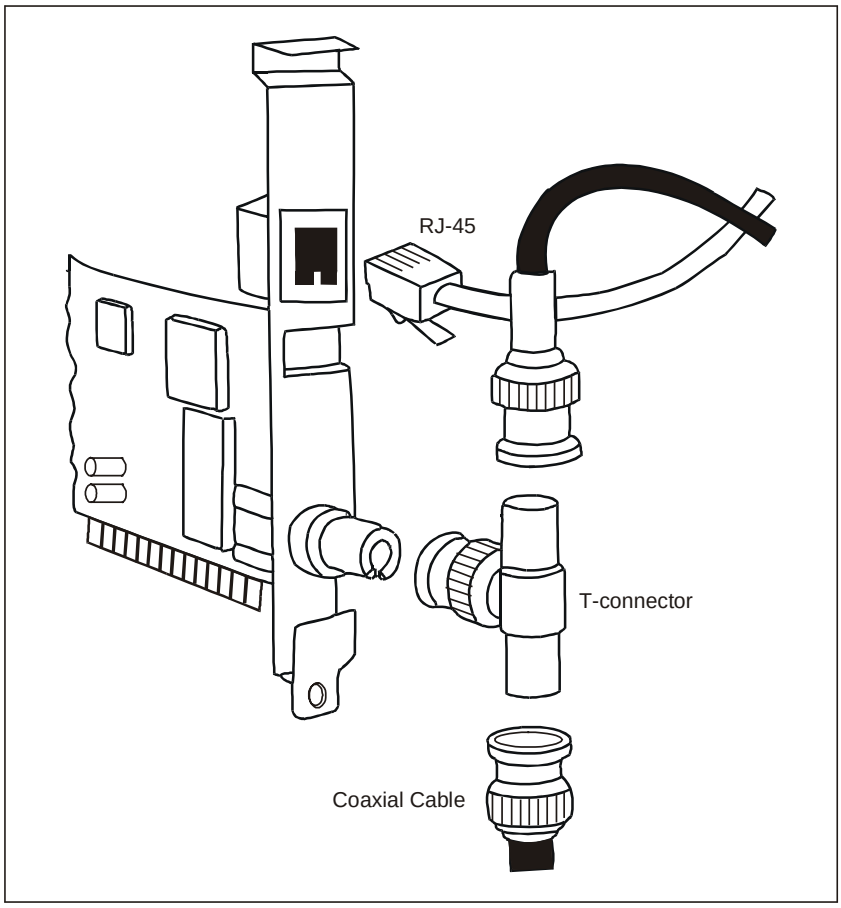


Figure N-2. Example of a NIC

WIRELESS LAN

M-6.A LAN can also be employed by wireless technology (radio frequency, infrared, or laser beam). Wireless transmission technology uses infrared or laser beams to transmit data between computers without connecting them with a cable. Use of wireless LANs reduces the time required to establish and dismantle TOC networks.

M-7.The wireless LAN allows the TOC to establish data connectivity quickly when the TOC's wired LAN is under construction or is being removed while preparing to jump the TOC. The wireless LAN supports C2OTMwhen the TOC vehicles are jumping. The two methods of interfacing with the wireless LAN are –

- Wireless radio interface on an individual computer.
- Wireless LAN interface connected to the TOC vehicle switch or router provides access for multiple computers on a wired LAN.

M-8.The wireless LAN requires a Type 1 encryption.

COAXIAL CABLE

M-9. Coaxial cable is a high-quality, heavily insulated communications line. It consists of a non-conducting insulator surrounded by a woven metal outer conductor and a plastic outer coating. Coaxial cable is not susceptible to electrical interference and transmits data faster over longer distances.

10Base2 Thinnet

M-10. The 10Base2 Thinnet is an RG-58 coaxial cable that is about 0.25 inches in diameter. The connectors are twist-on Bayonet Neill Concelman (BNC) with crimped connection to the wire. BNC always refers to 10Base2 connectors. The cable is limited to 185 meters in length. No more than 30 stations can be attached, and they must be separated by 0.5 meters. Multiple segments can be connected into a larger LAN with repeaters. The 10Base2 Thinnet coaxial cable uses T-connectors to connect a NIC to the medium. It must have a 50-ohm terminator at each segment end. Figure N-3 shows an example of a basic 10Base2 LAN, including T-connectors.

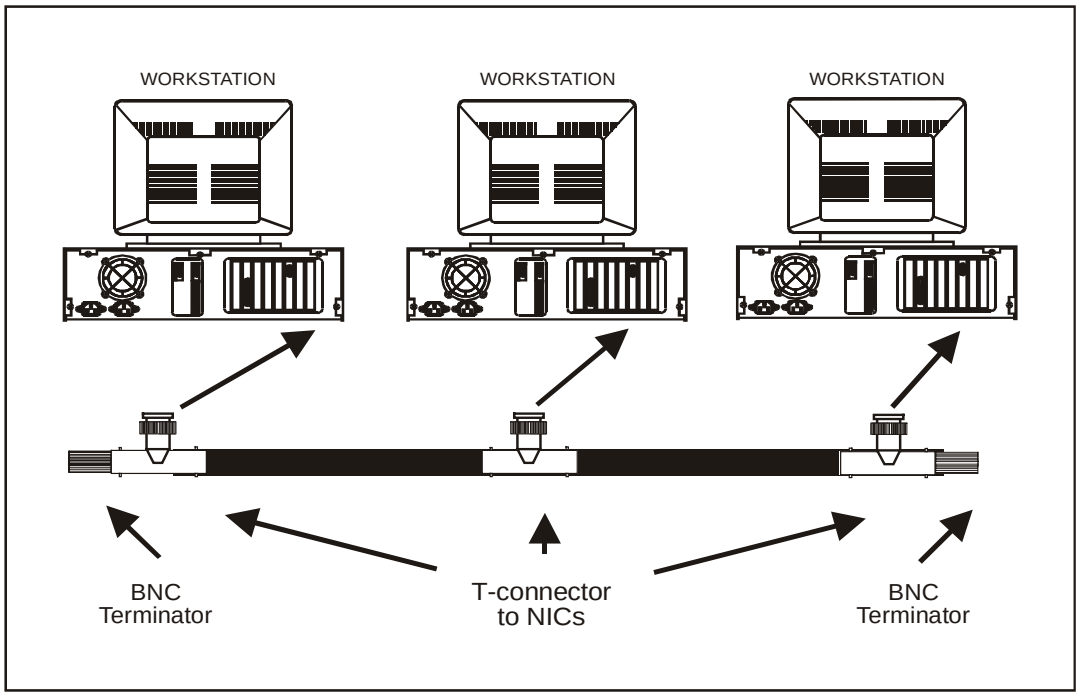


Figure N-3. Example of a Basic 10Base2 LAN

10Base5 Thicknet

M-11. The 10Base5 Thicknet coaxial cable is about 0.5 inches in diameter and limited to 100 connections per 500-meter length line segments. A repeater or bridge connects multiple segments. Thicknet coaxial cable has transceivers that attach to the medium. The attachment unit interface (AUI) cable attaches the media access unit (MAU) on the RG-8 cable to either a NIC or a multiport repeater. Workstations and servers are connected exactly the same way, either directly or through a repeater. However, the server attaches

directly to the transceiver. Figure N-4 shows an example of the basic connections for a 10Base5 bus LAN. Digital, Intel, and Xerox (DIX) connectors have 15-pin male and female connectors, and are named for the companies that developed Ethernet. These connectors. Figure N-5 shows an example of the male and female DIX connectors.

TWISTED-PAIR CABLE

M-12. Twisted-pair cable consists of plastic coated copper wires that are twisted together. A thin layer of colored plastic insulates and identifies each wire. The wires are twisted to reduce electrical interference. Shielded-twisted pair (STP) cable has a foil wrapper around each wire that further reduces electrical interference. Unshielded-twisted pair (UTP) cable does not have the foil wrapper. Twisted-pair cable is an inexpensive transmission medium that can be installed easily.

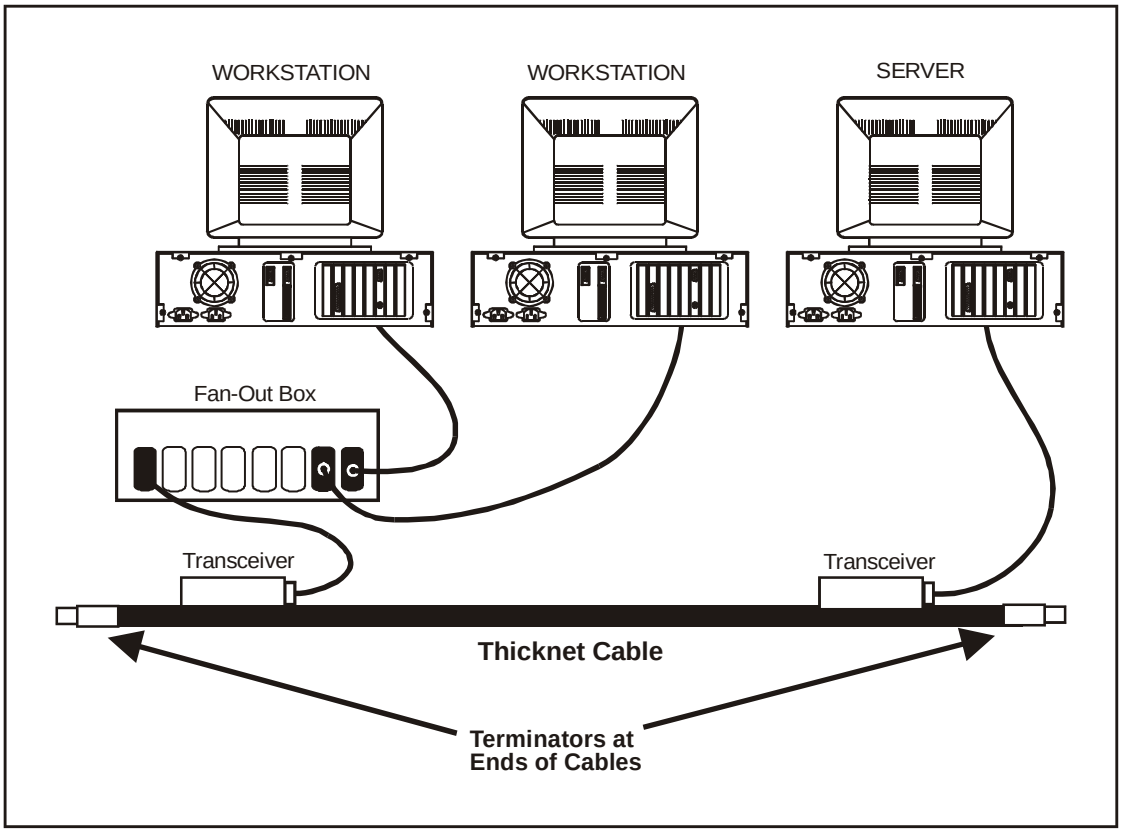


Figure N-4. Example of Basic Connections for a 10Base5 Bus LAN

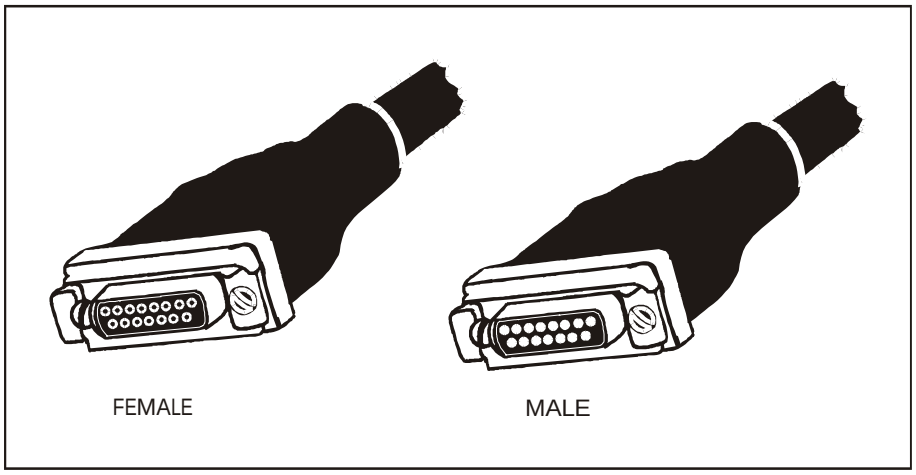


Figure N-5. Example of the Male and Female DIX Connectors

100BASETX

M-13. A specification of fast Ethernet is copper cables with one device per maximum segment length of 100 meters. Segments connected to 10BaseT hubs or 10/100Base switches normally use 4-pair, American wire gage (AWG) 22, 24, or 26 unshielded-twisted pair (UTP) cables. The connectors are RJ-45 connectors (8-wire telephone type connectors, category 5 UTP can be substituted for best results). Maximum distance is 205 meters unless additional switches or extension devices are used.

10BASET

M-14. The 10BaseT is a UTP cable that connects workstations to 10BaseT hubs and hubs-to-hubs. It is faster and has less chance of failure due to cabling, since it uses fewer parts than BNC. Each hub shares bandwidth and takes a portion of the total bandwidth (10 megabits per second [mbps]). The maximum segment length of the 10BaseT is 100 meters with one device per segment. Segments connect devices to 10BaseT hubs and each cable is a 4-pair, AWG 22, 24, or 26 UTP. The connectors are RJ-45 connectors (8-wire telephone type connectors). Figure N-6 shows an example of a 10BaseT LAN.

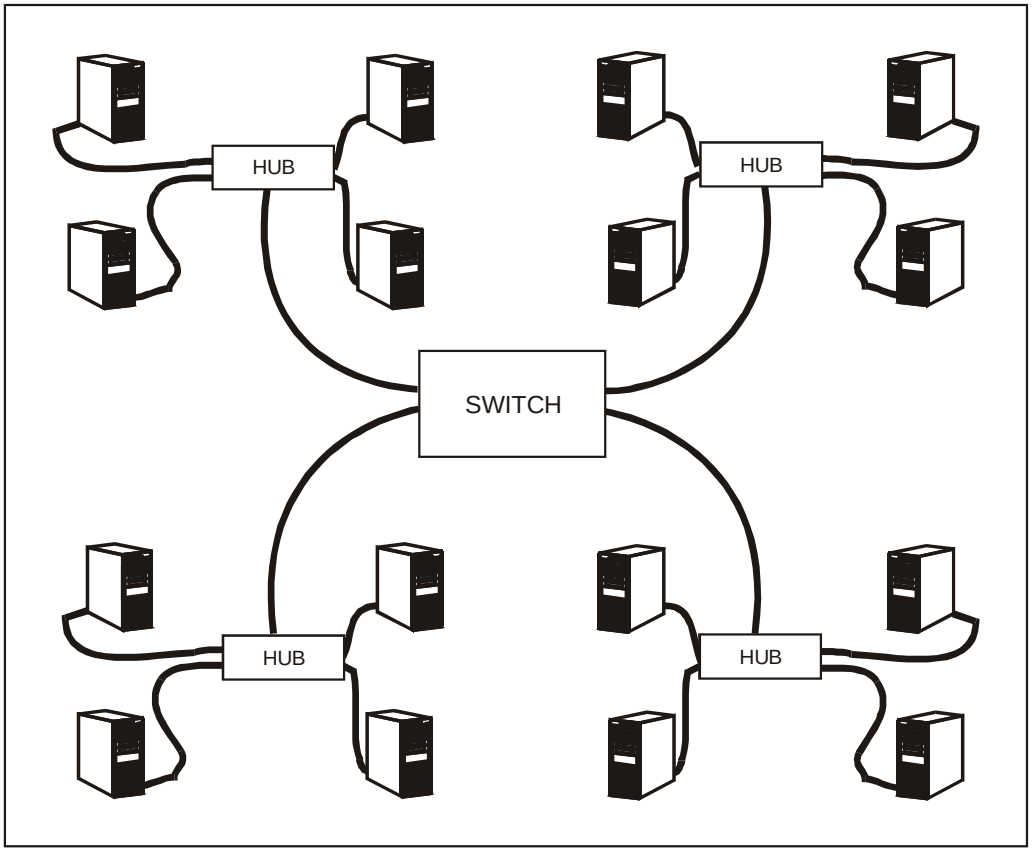


Figure N-6. Example of a 10BaseT LAN

FO CABLE

M-15. FO cable uses smooth, hair-thin strands of glass or plastic to transmit data as pulses of light. The major advantages of FO cables over wire cables include substantial weight and size savings and reduced electrical and magnetic interference. FO cable has a higher carrying capacity, carrying several hundred thousand voice communications simultaneously. FO cable is better than twisted pair or coaxial; however, it can be difficult to install and repair.

10BASEFL

M-16. The 10BaseFL can connect up to 2 kilometers (1.2 miles). The cable is either 50, 62.5, or 100-micron, duplex, multimode FO cable. Devices with AUI (DIX) connectors require an FO transceiver. The speed of the 10BaseFL is 10 mbps. Figure N-7 gives an example of a 10BaseFL fiber link between sites.

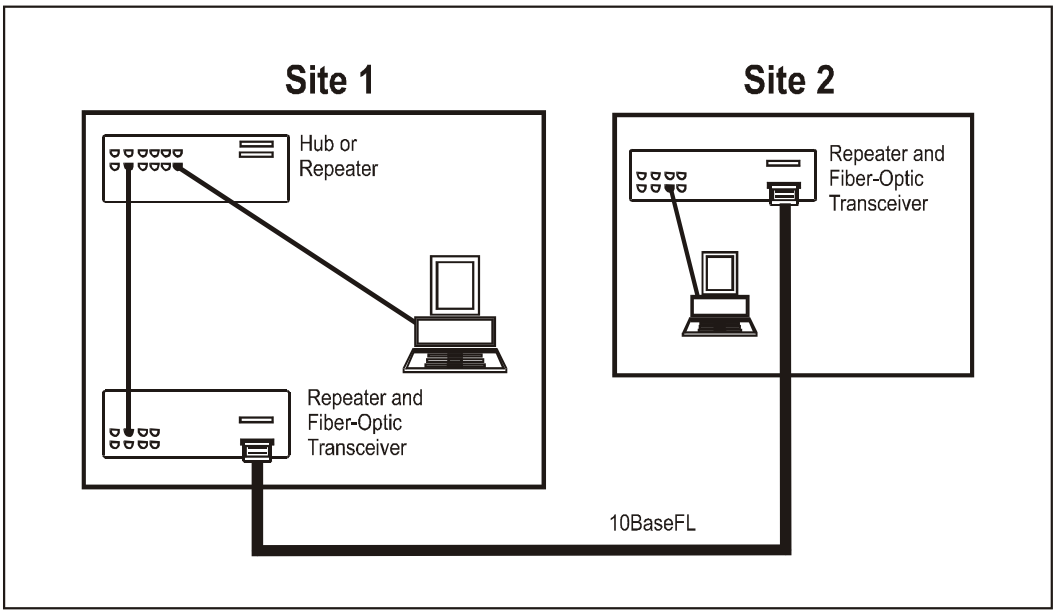


Figure N-7. Example of a 10BaseFL Fiber Link Between Sites

100BASEFX

M-17.The 100BaseFX is a physical layer standard using FO cables running at 100 mbps. They connect multiple Ethernet LANs, act as a high-speed bridge, and are most often set up in a star configuration. This configuration will access servers attached to one or more 100-mbps ports. The LANs are attached on 10-mbps ports for extremely fast transfer of packets from one LAN to another LAN or device through the switch. Figure N-8 shows an example of a 100BaseFX LAN.

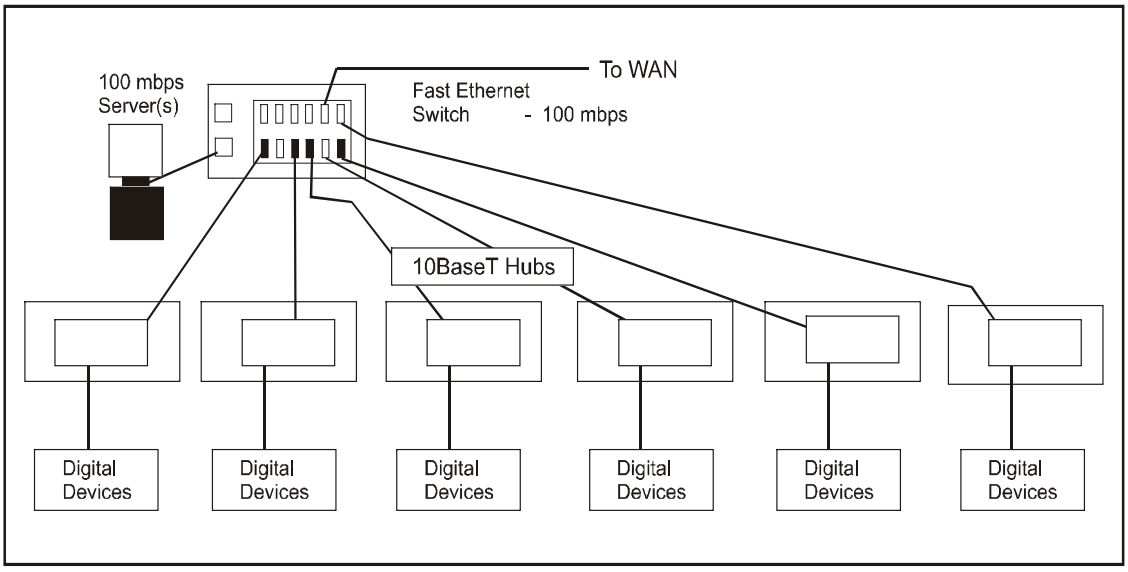


Figure N-8. Example of a 100BaseFX LAN

Glossary

A/L	administration and logistics
A2C2	Army Airspace Command and Control
ABCS	Army Battle Command System
AC	alternate current
ACUS	area common user system
AD	air defense
ADA	air defense artillery
ADDS	Army Data Distribution System
ADUA	administrative directory user agent
AFATDS	Advanced Field Artillery Tactical Data System
AFMO	Army Frequency Management Office
AKMS	Army key management system
ALICE	all-purpose lightweight individual carrying equipment
AMDPCS	Air and Missile Defense Planning and Control System
ANCD	automated net control device
ANCOC	Advanced Noncommissioned Officer Course
ANT	antenna
AO	area of operation
AOR	area of responsibility
AR	Army Regulation
ARFOR	Army Forces
AS	autonomous system
ASAS	All Source Analysis System
ASIC	application specific integrated circuit
ASIP	Advanced System Improvement Program
ATCCS	Army Tactical Command and Control System
ATM	asynchronous transfer mode
AUI	attachment unit interface
AUTODIN	automatic digital network
BFA	battlefield functional area

BFACS Battlefield Functional Area Control System

BIT built-in test

BLOS beyond-line of-sight

BNC Bayonet Neill Concelman [Electronics] (connector used with coaxial cable. Named after inventor.)

BNOSC Brigade Network Operations Support Center

BOS battlefield operating system

BRSS brigade remote subscriber system

BSB brigade support battalion

BSM battlefield spectrum management

BSN brigade subscriber node

BVTC battlefield video teleconferencing

C2 command and control

C2OTM command and control on the move .

C3I command, control, communications, and intelligence

C4 command, control, communications, and computers

C4ISR command, control, communications, computers, intelligence, reconnaissance, and surveillance

CA Certification Authority

CAW Certification Authority Workstation

CE communications-electronics

CINC Commander in Chief

CKL compromised key list

CNR combat net radio

CNRI combat net radio interface

COA course of action

CofS Chief of Staff

COM communications

COMMEX communications exercise

COMSEC communications security

CONUS continental United States

CP command post

CPU computer processor unit

CRL certificate relocation list

CRP communications relay payloads

CRYPTO cryptographic

CS combat support

CSS combat service support

CSSCS CSS control system

CT cipher text

DA directory agent

DAMA demand assigned multiple access

DASA demand assigned single access

DC direct current

DISN Defense Information System Network

DIT Directory Information Tree

DIVARTY division artillery

DIX refers to the Digital, Intel, Xerox companies

DMS Defense Messaging System

DOD Department of Defense

DOIM Directorate of Information Management

DRA data rate adapter

DSA directory services agent

DSN defense switched network

DSP digital signal processor

DTMF Dual tone multiple frequency

DVE Drivers Visual Enhancement

DUA directory user agent

EAC echelons above corps

EBC embedded battle command

ECB echelons of corps and below

ECCM electronic counter countermeasures

ECM electronic counter measures

EGRU EPLRS grid reference unit

EHF Extreme High Frequency

ELM electronic maintenance

e-mail electronic mail

EMCON emission control

ENM	EPLRS Network Management
EOM	end of message
EP	electronic protect
EPLRS	Enhanced Position Location Reporting System
ESIP	Enhanced System Improvement Program
ESIP	Enhanced System Improvement Program
EWO	Electronic Warfare Office
FAA	Federal Aviation Administration
FBCB2	Force XXI Battle Command - Brigade and Below
FCC	Federal Communications Commission
FCN	function
FEC	forward error correction
FH	frequency hopping
FH-MUX	frequency hopping-multiplexer
FLOT	forward line of troops
FM	frequency modulated; field manual
FO	fiber optic
FOCA	fiber optic cable assembly
TFOCA	Tactical Fiber Optic Cable Assembly
FOM	fiber optic modem
FS	fire support
FSO	Fire support officer
FWD	Forward
G1	Assistant Chief of Staff, Personnel
G2	Assistant Chief of Staff, Intelligence
G3	Assistant Chief of Staff, Operations and Plans
G3	Assistant Chief of Staff, G3 (Operations and Plans)
G4	Assistant Chief of Staff, Logistics
G5	Assistant Chief of Staff, Civil Affairs
G6	Assistant Chief of Staff, G6 (Signal Officer)
GBS	Global Broadcast Service
GCSS-A	Global Combat Support System-Army
GII	Global Information Infrastructure
GIG	Global Information Grid

GMF Ground Mobile Forces
GPS Global Positioning System
GWS groupware servers
HF high frequency
HFMUX high frequency multiplexer
HMMWV high mobility multipurpose wheeled vehicle
HQ headquarters
HQDA Headquarters, Department of the Army
HSMUX high-speed multiplexer
HUB hold up battery
IA information assurance
IAM Information Assurance Manager
IASO Information Assurance Security Officer
IAV Interim Armored Vehicle
IAW in accordance with
ICOM integrated COMSEC
ID Identification
IDM Information Dissemination Management
IEW intelligence and electronic warfare
IHFR improved high-frequency radio
INC Internet controller
INE Inline Network Encryption
IOM installation, operation, maintenance
IP Internet Protocol
IPB intelligent preparation of the battlefield
ISDN Internet subscriber data network
ISR Intelligence, surveillance, reconnaissance
ISSO Information Systems Security Officer
ISYSCON Integrated System Control
ITU International Telecommunications Union
JCS Joint Chiefs of Staff
JFMO Joint Frequency Management Office
JRFL joint restricted frequency list
JSIR joint spectrum interference resolution

JSMS joint spectrum management system

JTF joint task force

JTRS Joint Tactical Radio System

JVMF joint variable message format

kbps kilobits per second

KEK key encryption key

LAN local area network

LDR low data rate

LNO liaison officer

LOS line-of-sight

MAA mission application administrator

MAU mission application user

MCS maneuver control system

MCPTI MILSTAR Communications Planning Tool

MDMP military decision making process

MDR medium data rate

MEDEVAC medical evacuation

METT-TC mission, enemy, terrain, troops and time, and civilian consideration

MFI multifunctional interpretator

MGRS Military Grid Reference System

MHz megahertz

MI Military Intelligence

MILSTAR Military Strategic Tactical Relay

MLA mail list agent

MOS military occupational specialty

MP Military Police

MS message store

MSE mobile subscriber equipment

MSR Military supply route

MSRT mobile subscriber radiotelephone terminal

MSS Mobile subscriber service

MTA message transfer agent

MTW major theater of war

NATO	North Atlantic Treaty Organization
NCA	noisy channel avoidance
NCA	National Command Authority
NCS	network control station
NCS-E	network control station-EPLRS
NES	Network Encyrption System
NIB	noninterference basis
NIC	network interface card
NIFD	NTDR interim full device
NLOS	near line-of-sight
NMT	network management tool
NM	Network Management
NOC-V	Network Operations Center-Vehicle
NOSC	Network Operations Support Center
NPE	networking, planning, and engineering
NPT	network planning tool
NTDR	near term digital radio
NTIA	National Telecommunications and Information Systems Administration
NVIS	Near vertical incidence skywave
OCONUS	outside the continental United States
OPLAN	operation plan
OPORD	operation order
OPTEMPO	operation tempo
PACE	primary, alternate, contingency, and emergency
PC	personal computer
PLL	prescribed load list
POC	point of contact
POS/NAV	positioning and navigation
PS	packet switch
PT	plain text
PTR	problem trouble record (or report)
PVC	permanent virtual circuit
PWR	Power

QEAM	Quick Erect Antenna Mast
QUAL	quality
R&S	reconnaissance and surveillance
RA	routing area
RASI	remote access switching interface
RAU	radio access unit
RBECS	Revised Battlefield Electronic CEOI System
RELAY/RETRANS	Relay/Retransmission
RI	Relavent Information
RF	radio frequency
RS	radio set
RSTA	Reconnaissance, surveillance, and targeting acquisition
RT	receiver transmitter
S1	Adjutant
S2	Intelligence Officer
S2X	Intelligence Officer (Executive Officer in RSTA Squadron)
S3	Operations and Training Officer
S4	Supply Officer
S5	Civil Affairs Officer (US Army)
S6	Signal Officer (US Army)
SA	System Architecture
SAR	satellite access request
SASO	stability and support operations
SATCOM	satellite communications
SBCT	Stryker Brigade Combat Team
SBU	sensitive but unclassified
SFAF	standard frequency action format
SHF	super high frequency
SIGCO	Signal Company
SINCGARS	Single-Channel Ground and Airborne Radio System
SIP	System Improvement Program
SM	service management
SMART-T	secure mobile anti-jam reliable tactical terminal
SMS	service management system

SNMP simple network management protocol
SOI signal operation instructions
SOP standing operating procedures
SOTM SATCOM On The Move
SSB single-side band
SSC small-scale contingency
STANAG Standardization Agreement (NATO)
STBY Standby
STEP Strategic Tactical Entry Point
STO store
STP shielded twisted pair
SU Situational Understanding
TAC tactical command post
TACLAN tactical local area network
TACSAT tactical satellite
TACSOP tactical standing operating procedures
TB technical bulletin
TBD to be determined
TDM time division multiplexing
TF task force
TI tactical Internet
TIMS Tactical Internet Management System
TMS Tactical Message System
TOC tactical operations center
TOD time of day
TRANSEC transmission security
TRI-TAC tri-service tactical communications
tropo tropospheric scatter
TS TOP SECRET
TS Trojan Spirit
TTA tactics, techniques, and procedures
TTP tactics, techniques, and procedures
TUAV Tactical unmanned aerial vehicle
UA user agent

UHF	ultra high frequency
ULLS	unit-level logistics system
US	United States (of America)
USR	Unit status report
UTP	unshielded-twisted pair
VAA	vehicular amplifier-adapter
VEP	vertical error probable
VHF-AM	very high frequency-amplitude modulated
VHF-FM	very high frequency-frequency modulated
VHSIC	very high-speed integrated circuit
WAN	wide area network
WIN	warfighter information network
WIN-MS	Warfighter Information Network-Management System
XO	executive officer

S: 15 December 2002

ATZH-CD 15 October 2002

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Review of FM 6-02.2, (FM 11-2), *Command, Control, Communications, and Computers (C4) Operations: Stryker Brigade Combat Team (SBCT)* (Final Draft)

1. Request your review of FM 6-02.2, (FM 11-2), *Command, Control, Communications, and Computers (C4) Operations: Stryker Brigade Combat Team (SBCT)* (Final Draft).

2. FM 6-02.2 provides a single source reference supporting the Brigade Signal Company (BSC), brigade and battalion S6 in the Stryker Brigade Combat Team (SBCT). It provides tactics, techniques, and procedures (TTP) for use in predeployment and deployment planning, and in support of training. FM 6-02.2 targets commanders, staffs, the brigade and battalion S6, NCOs, and enlisted soldiers that are directly responsible for planning, establishing, and managing C4 operations in the SBCT.

3. FM 6-02.2 will not be mailed; it will only be available on the Signal Regiment Doctrine Digital Library Web site http://www.doctrine.gordon.army.mil on 25 October 2002.

4. Please review and provide comments and suggestions with rationale via e-mail: doctrine@gordon.army.mil, or mail to: COMMANDER, United States Army Signal Center & Fort Gordon, ATTN: ATZH-CDF (Doctrine Branch, Room 403A, Signal Towers), Fort Gordon, Georgia 30905-5075, NLT 15 December 2002.

5. Point of contact is Maj Steve Bolick, DSN 780-1184, e-mail: bolicks@gordon.army.mil or Mr. Rick San Miguel, DSN 780-1143, email: sanmigur@gordon.army.mil.

Encl

KEITH H. SNOOK
Colonel, Signal Corps
Director of Combat Developments

DISTRIBUTION:
Commandant, Regimental Officer Academy, ATTN: ATZH-LD
Commander, 15th Signal Brigade, ATTN: ATZH-TB
Director, Battle Command Battle Lab, ATTN: ATZH-BL
Director, Computer Science School, ATTN: ATZH-SS
TRADOC Systems Manager, Warfighter Information Network-Tactical, ATTN: ATZH-WT
TRADOC Systems Manager, Satellite Communications, ATTN: ATZH-TS
TRADOC Systems Manager, Tactical Radios, ATTN: ATZH-TR
Regimental Director of Training, ATTN: ATZH-DT
Commandant, Regimental Noncommissioned Officer Academy, ATTN: ATZH-LDN
AIG 6708 (All Signal Activities and Units)