Headquarters,
Department of the Army

FIELD MANUAL
24-7

Tactical Local Area Network (LAN) Management

Field Manual
No 24-7

Headquarters,
Department of the Army
Washington, DC 8 October 1999

Tactical Local Area Network (LAN) Management

Contents

*This publication supersedes FM 11-75, 20 September 1994 and FM 24-16, 7 April 1978.

Page

Preface

This manual concentrates on tactical local area network (LAN) management at echelons corps and below (ECB). Command and control (C2) systems in a tactical LAN are integrated to collect, combine, process, exchange and present information to support the commander across the battlefield. The commander can effectively plan, coordinate, control, and direct the battle when the proper procedures in establishing, managing, and maintaining a tactical LAN are met. This manual outlines the responsibilities and procedures that apply to all levels of command.

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@emh.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

Tactical Operations Center LAN Overview

Commanders depend on command and control (C2) systems to collect, combine, process, and exchange vital information needed to gain information dominance. The C2 systems in each tactical operations center (TOC) connect forming a local area network (LAN). These systems connected to the TOC LAN enhance C2 of the forces. This chapter gives an overview of a TOC, LAN, Army Battle Command and Control System (ABCS), Standard Army Management Information System (STAMIS), and data transport systems.

TOC

1-1. The TOC serves as the unit's C2 hub and assists the commander in synchronizing operations. Most of the staff coordination, planning, and monitoring of key events occurs at the TOC. Its personnel must ensure all resources are in the right place at the right time. They must function efficiently and effectively as a team in a fast-paced, unforgiving environment. All users, individually and collectively, must understand the overall function of the TOC. Basic TOC functions include–

- Receiving, distributing, and analyzing information.
- Submitting recommendations to the commander.
- Integrating and synchronizing resources.

1-2. The TOC functions primarily as an information center processing a high volume of message traffic, reports, and orders. It must act, direct, inform, and decide based on that information. An efficient TOC communicates internally and externally, and it integrates all its players. It is very easy for units to experience information overload unless they have simple and effective systems in place to receive and process information.

TOC LAYOUT

1-3. The physical layout of a TOC contributes to how efficiently information is passed from one staff section to another, and how easily sections communicate with one another. There is no standardized method on how a TOC should be configured. It is basically at the discretion of the individual unit. However, the most effective TOCs have the following factors in common:

- A high degree of organization.
- Configured in a manner that was functional to the unit and did not segregate staff sections.
- Planning areas were segregated from TOC briefing and operations areas.

1-4. Each TOC is configured differently depending on the unit's modification table of organization and equipment (MTOE) and mission. In each TOC, the different types of LANs vary as they depend on the mission, enemy, terrain, troops, time, and civilian consideration (METT-TC).

LAN

1-5. A LAN is a data communications network that interconnects a community of digital devices and other peripherals. These are linked over a network and are distributed over a localized area. The LAN consists of a communications channel that connects a series of computer terminals connected to a central computer or, more commonly, connects a group of computers to one another. Figure 1-1 shows an example of a LAN.

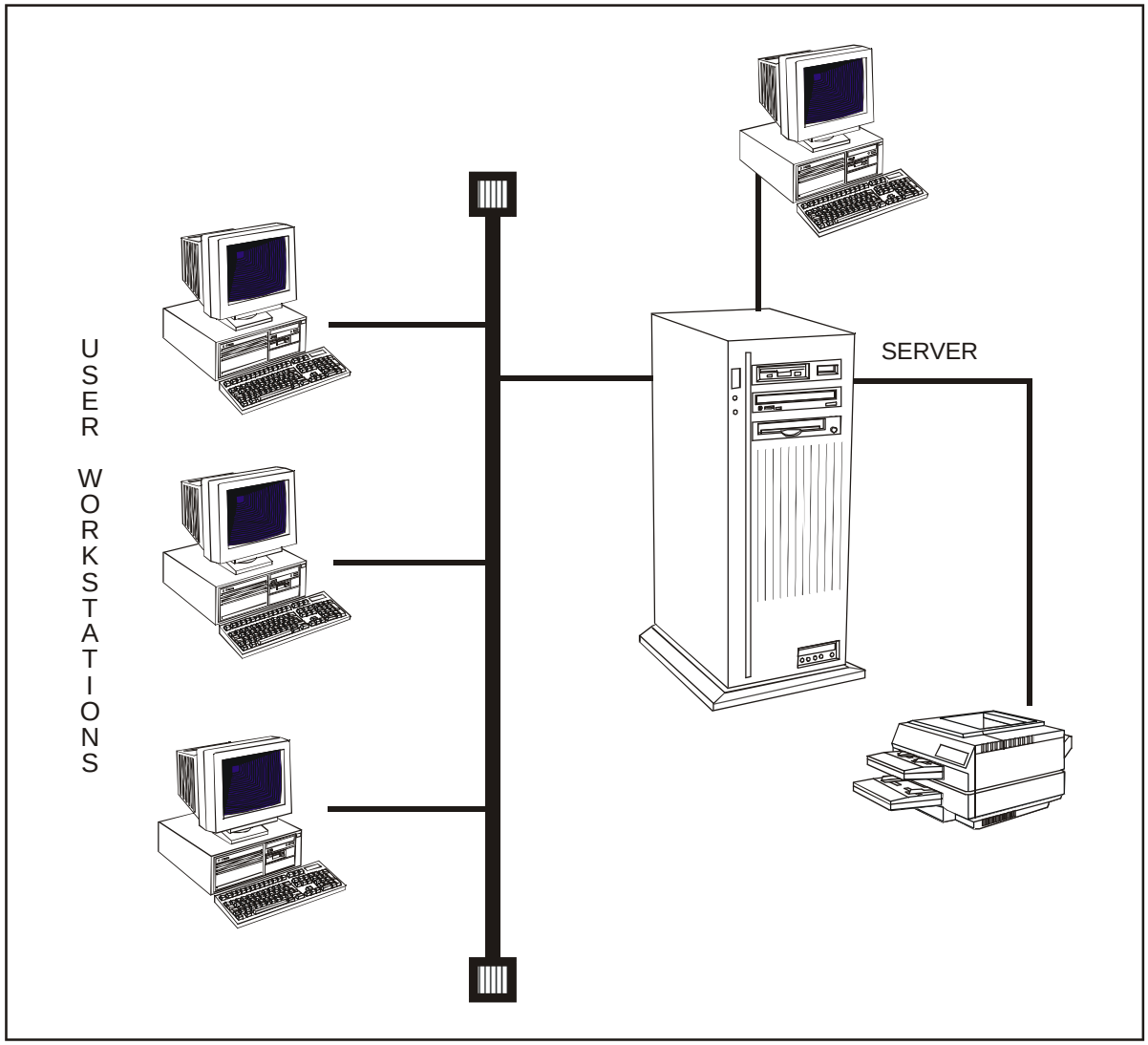

Figure 1-1. Example of a LAN

1-6. A LAN is connected by cables or by wireless technology. All Army LANs use the Institute of Electrical and Electronic Engineers (IEEE) 802.3/802.3u standard.

1-7. A LAN can be configured in a multitude of configurations depending on the unit's MTOE. A LAN includes–

- Digital devices (computers, scanners, printers, and other peripherals).
- A communications medium that exchanges data from one device to another.
- Network adapters that provide devices with an interface to the communications medium.
- A physical topology extending the medium between adapters.
- An access protocol carried out by the adapters to ensure an orderly use of the medium.
- A logical format for transmitting data over the medium.
- An electrical specification for data encoding and transmission.

1-8. Three common applications of a LAN are hardware, software, and information resource sharing. The communications resources of a LAN are shared among all devices attached to the network.

- Hardware resource sharing allows each computer on a network to access and use devices that are too costly to provide for each user or cannot be justified for each user because they are used infrequently.
- Software resource sharing involves storing frequently used software on the server's hard disk so multiple users can access the software on each computer.
- Information resource sharing allows anyone using a computer on a LAN to access data stored on any other computer in the network.

ABCS

1-9. 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 supports the mission by integrating the automation and communications systems that link strategic and tactical headquarters.

1-10. ABCS is interoperable with joint and multinational C2 systems at upper echelons, and it is vertically and horizontally integrated at the tactical and operational levels.

BATTLEFIELD FUNCTIONAL AREA CONTROL SYSTEMS (BFACSs)

1-11. Integrating the BFACSs and the Force XXI Battle Command – Brigade and Below (FBCB2) system supports requirements at brigade and below for situational understanding (SU) and C2 data. Within this integration of systems, the force-level database first forms at the battalion to meet the tactical commander's requirements for the common picture and SU. The BFACSs are heavily oriented toward combat operations. Figure 1-2 shows the objective architecture of BFACSs.

1-12. The combined arms team commanders and staffs integrate and synchronize the BFAs to exercise force-level control (FLC). This is achieved by managing, manipulating, and assessing information from the BFAs and developing tactical plans and orders based on that information. FLC functions by providing automated support to the force commander and staff in planning, directing, coordinating, and controlling the combined arms team. FLC software supports the maintenance of force status, monitors the current situation, plans force missions, and controls FLC information transactions.

Maneuver Control System (MCS)

1-13. The MCS is the primary maneuver information system that allows the commander to collect, coordinate, and act on near-real-time battlefield information. The MCS quickly and accurately transfers tactical information and rapidly disseminates the commander's orders.

1-14. The database of the MCS maintains and displays critical and current information on friendly and enemy forces obtained from the BFACSs. This information is displayed in text and graphic formats. The commander and staff use common decision graphics for identifying possible courses of action. Commanders can make supporting decisions that mesh with the decisions and capabilities of other commanders.

Advanced Field Artillery Tactical Data System (AFATDS)

1-15. Fire missions flow through the FS chain where the most effective weapon system at the lowest echelon satisfies the target attack criteria. The AFATDS provides the automation that enables the maneuver commander to influence the battle. It provides the right mix of firing platforms and munitions to defeat enemy targets based on the commander's guidance and priorities. Also, the AFATDS facilitates the FS coordinator commander's ability to control assets and allocate resources.

1-16. Integrating all FS systems creates greater tactical mobility for FS units and allows missions to be planned and completed in less time using the best attack system to defeat a target. The AFATDS also meets field artillery needs by managing critical resources; supporting personnel assignments; collecting and passing intelligence information; and controlling supply, maintenance, and other logistics functions.

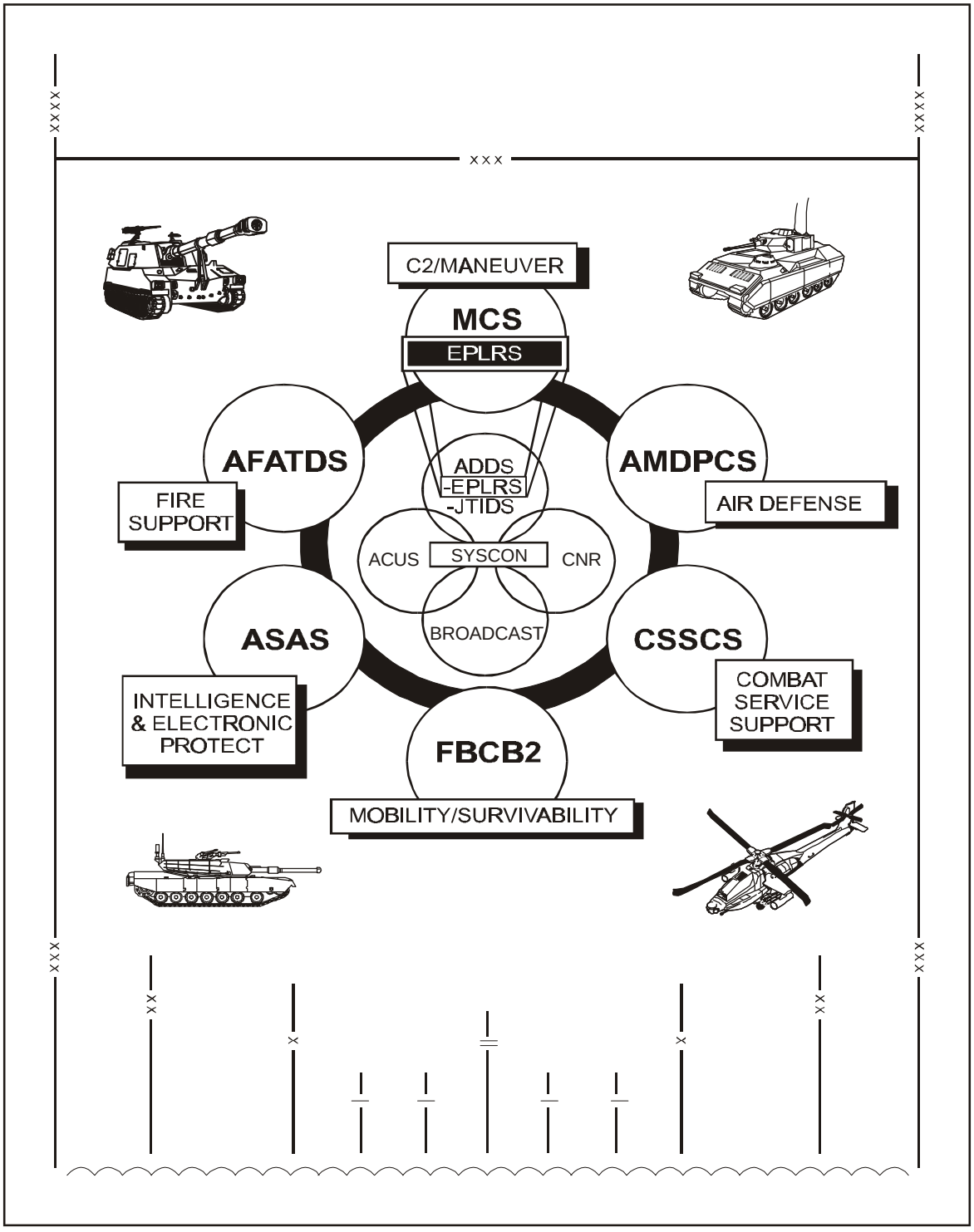

Figure 1-2. Objective Architecture of BFACSs

Air and Missile Defense Planning and Control System (AMDPCS)

1-17. The AMDPCS is an automated C2 system supporting AD operations within the battlespace. It controls and integrates AD engagement operations and combined arms force operations for the AD BFA. The system assists battle managers in planning, coordinating, synchronizing, directing, and controlling the counter air fight. It also assists the battle manager in developing and disseminating timely target data to all air and missile defense (AMD) components.

1-18. The AMDPCS responds to air attack threats by integrating targeting functions to support engagement operations. It acquires and tracks incoming air threats, identifies friendly and enemy aircraft, and automatically alerts forward AD weapons. To support force operations, the AMDPCS provides force-level commanders with the information to integrate AD into the overall tactical plan.

All Source Analysis System (ASAS)

1-19. The ASAS is a functionally integrated intelligence support system. It manages sensors and other resources and collects, processes, and fuses intelligence data. The ASAS stores, manipulates, and displays this data and quickly disseminates it to all commanders. This provides a common picture of enemy activity to the force-level database used by all BFAs.

1-20. The ASAS supports the commander's decision-making process. By facilitating the decision process, the ASAS allows the commander to generate opportunities to seize and to retain the initiative. The ASAS provides timely and accurate intelligence information that enables tactical commanders to maneuver inside the enemy's decision cycle and significantly enhances the interoperability and support of all BFAs.

Combat Service Support Control System (CSSCS)

1-21. The CSSCS is a logistics, supply, and administrative information system. It provides timely and critical information to strategic, operational, and tactical commanders. This system allows commanders to conduct trade-off analysis and to evaluate potential courses of actions based on different logistic scenarios.

1-22. The CSSCS serves as the interface with STAMIS and the other BFACSs. It consolidates detailed data from the STAMIS into decision support information for both CSS and force-level commanders.

FBCB2 System

1-23. The FBCB2 system consists of computing hardware (AN/UYK-128), system and application software, and installation kits. FBCB2 computers use tactical radio systems to link to the network. They use the variable message format (VMF) to send or receive messages, both horizontally and vertically in near-real time. The FBCB2 system exchanges information with the MCS, AFATDS, AMDPCS, ASAS, and CSSCS.

1-24. The FBCB2 system–

- Is user-owned and -operated.
- Improves combat effectiveness of the force.
- Provides up-to-date combat situation data such as friendly and enemy, air/ground unit position, and map/terrain/elevation data based on echelon and location.
- Generates and disseminates messages and acknowledgments such as orders and requests, fires and alerts, and reports.
- Generates and disseminates overlays on the situation posture such as intelligence, obstacle, operations, and control measures, and geometry data.
- Exchanges selected mission-critical data between the FBCB2 system and the other information systems semiautomatically.

STAMIS

1-25. The STAMIS provides the essential data needed to supply, resupply, requisition, and repair the Army's equipment. Each STAMIS is different and has requirements governing specific site location and operations. Many STAMIS software packages feed data to the Joint Chiefs of Staff (JCS)-level and are time critical in delivery and execution.

1-26. The Global Combat Support System-Army (GCSS-A) will be the Army's combat service supply system to modernize and integrate the capabilities of the existing STAMIS. The GCSS-A will integrate manning, arming, fixing, fueling, moving, and sustaining functions. This system will interface with other CSS automated systems so users can maximize the amount of information available with the minimum amount of data entry. It will be a commercial-off-the-shelf (COTS) hardware solution using the Windows New Technology operating system.

1-27. A brief description of each STAMIS application follows below.

DEPARTMENT OF THE ARMY MOVEMENT MANAGEMENT SYSTEM-REDESIGN (DAMMS-R)

1-28. The DAMMS-R provides automation support for transportation staffs and organizations within a tactical theater of operations. It supports transportation units within the continental United States (CONUS) and supports the Army's strategic mobility programs. It is a vital link in maintaining in-transit visibility over units, personnel, and materiel. DAMMS-R is the most complex of the retail STAMISs. DAMMS-R interfaces with all STAMISs, services, and foreign governments where the Army is deployed.

STANDARD ARMY AMMUNITION SYSTEM (SAAS)

1-29. The SAAS-modified provides centralized information management to support CONUS, overseas, and within the major commands.

STANDARD ARMY MAINTENANCE SYSTEM (SAMS)

1-30. The SAMS increases the productivity of maintenance shops, and it provides the commanders with accurate and timely maintenance management information. It operates in the direct support/general support (DS/GS) maintenance and/or aviation intermediate maintenance activity, the forward support battalion, main support battalion, corps support battalion, area support battalion, and the materiel management center (MMC) within division, corps, and echelons above corps (EAC) environments.

STANDARD ARMY RETAIL SUPPLY SYSTEM (SARSS)

1-31. The SARSS is a multiechelon supply management and stock control system that operates in tactical and garrison environments. It supports the STAMIS, SAMS-level 1, standard property book system-redesign (SPBS-R), unit-level logistics systems (ULLSs), nonautomated customers, and the split operations concept. Throughout the Army, SARSS is used in–

- DS and GS units' supply support activities (SSAs).
- Division MMCs.
- Armored cavalry regiments.
- Separate combat brigade MMCs.

SPBS-R

1-32. The SPBS-R provides on-line management information and automated reporting procedures for the property book officer and produces updated company-level hand receipts, when needed. It also provides automated interfaces with–

- SSAs for request and receipt of equipment.
- Continuing balance system-expanded for worldwide asset reporting.
- Logistics support activity for total asset visibility and catalog updates.
- Unique item tracking for weapons serial number tracking.
- Automated records management system for nondevelopmental item computer serial number tracking and warranty information.

ULLS

1-33. The ULLS is a standard, automated, logistics system for unit prescribed load list (PLL) and maintenance management operations. The ULLS automates repair parts, supply functions, maintenance management operations, aircraft records, and historical data. This automation improves accuracy and timeliness. The ULLS provides the tactical line companies and supporting CSS companies the capability to automate logistics at the unit level.

Unit Level Logistics System-Ground (ULLS-G)

1-34. Any unit that has an organizational maintenance facility has an ULLS-G. It automates vehicle dispatching, PLL management, and the Army Maintenance Management System. The ULLS-G interfaces with the SARSS-level 1, SAMS-level 1, ULLS-S4, vehicle sensors, and intervehicular information system. The automatic information technology interrogator is connected directly to the ULLS-G. It is linked to the wholesale supply system through objective supply capability.

Unit Level Logistics System-Aviation (ULLS-A)

1-35. All aviation units have an ULLS-A. It performs those functions for aviation that the ULLS-G performs for ground units.

Unit Level Logistics System-S4 (ULLS-S4)

1-36. Unit-level supply rooms and battalion and brigade level S4 staff sections have an ULLS-S4. It automates the supply property requisitioning/ document register process, hand/subhand receipts, component, budget, and logistical planning activities.

STANDARD INSTALLATION/DIVISION PERSONNEL SYSTEM-3 (SIDPERS-3)

1-37. SIDPERS-3 provides an integrated personnel support environment for the active Army. SIDPERS-3 consists of hardware, software, communications, and training that provides a minimum essential set of software applications to support a relational database. This database contains information about soldiers and units that commanders and staff officers use to properly manage the active Army force and maintain field personnel data in an automated form.

1-38. All decision-makers can use SIDPERS-3 to manage personnel assets in combat, meet mobilization contingencies, and achieve peace and wartime readiness goals. Through the Total Army Personnel Database (TAPDB), SIDPERS-3 indirectly interfaces with the Army Authorization and Documents System-Redesign. Also through the TAPDB, future interfaces may include the installation support module, the CSSCS, and the Reserve Component Automation System.

THEATER ARMY MEDICAL MANAGEMENT INFORMATION SYSTEM (TAMMIS)

1-39. TAMMIS can interface with other Department of Defense (DOD) management information systems and programs such as the Defense Medical Regulating Information System, SIDPERS, Prime Vendor Programs, Standard Financial System, and more.

1-40. TAMMIS automates communications by setting up a transmission schedule to remote locations and automating retransmissions. TAMMIS can relay information between units in various ways. The preferred methods use tactical terminal adapters, LAN, telephone lines, defense data networks, or an international maritime satellite using a commercial modem, stand-alone LAN, and floppy diskette or tape delivered by courier.

1-41. TAMMIS consists of six subsystems that support logistics and patient administration.

Logistics Subsystems

1-42. The subsystems supporting logistics are medical supply, medical assemblage management, and medical maintenance.

Patient Administration Subsystems

1-43. The subsystems supporting patient administration are medical regulating, medical patient accounting and reporting, and medical patient accounting and reporting-command and control.

DATA TRANSPORT SYSTEMS

1-44. Data is moved outside the LAN by accessing the data transport systems through a gateway. A gateway is a combination of hardware and software that allows users on one network to access the resources on a different network. The communications systems covered below can be used as data transport systems.

NOTE: The equipment available to a specific unit depends on the unit's mission and table(s) of organization and equipment (TOE).

COMBAT NET RADIO (CNR)

1-45. The CNR consists of the Single-Channel Ground and Airborne Radio System (SINCGARS), a tactical satellite (TACSAT) communications system, and high frequency (HF) radios. CNRs are the primary means of voice communications, but they can also transport data. CNRs are used in command, administrative/logistical, and intelligence/operations networks.

AREA COMMON USER SYSTEM (ACUS)

1-46. The ACUS is a communications system of network node switching centers connected primarily by line-of-sight (LOS) multichannel radios and TACSATs. Army ACUS networks include Tri-Service Tactical Communications (TRI-TAC) at EAC and mobile subscriber equipment (MSE) at echelons corps and below (ECB). The ACUS provides a multiuser, common-user area system for voice and data communications.

MSE

1-47. The MSE system is the primary ACUS configuration for ECB. MSE forms a network that covers the area occupied by unit subscribers. For a division, the grid is made up of four to six centralized node centers (NCs) These NCs make up the hub or backbone of the network. Throughout the maneuver area, subscribers connect to small extension nodes/large extension nodes (SENs/LENs) by radio or wire. These extension nodes serve as local call switching centers and provide access to the network by connecting to the NCs. The MSE system provides both voice and data communications on an automatic, discrete-addressed, fixed-directory basis using flood search routing. The system supports both wire and mobile subscribers.

Tactical Packet Network (TPN)

1-48. The TPN is overlaid on the MSE network and uses existing trunks exclusively for data transmission. Users can connect computers and LANs to the TPN from their command posts (CPs). The TPN breaks up data into packets and routes them along their most efficient path to their destination. When all packets arrive, the receiving packet switch reassembles the data and sends it to its destination.

ARMY DATA DISTRIBUTION SYSTEM (ADDS)

1-49. The ADDS is an integrated command, control and communications system providing near-real-time transmission capabilities to support low to medium volume data networks. The system automatically relays information from the origin to the destination transparent to the user. Subsystems are the Enhanced Position Location Reporting System (EPLRS) and the Joint Tactical Information Distribution System (JTIDS).

BROADCAST

1-50. Broadcast communications systems use technology similar to commercial radio stations. Transmit-only stations send information to HF radio systems, satellites, unmanned aerial vehicles, or other means. Weather, intelligence, and position location/navigation information get support from broadcast systems.

SATELLITE COMMUNICATIONS SYSTEMS

1-51. There are four segments to the military satellite communications (MILSATCOM) architecture. First, ultra high frequency (UHF) satellites are the workhorses for tactical ground, sea, and air forces. Second, the super high frequency (SHF) Defense Satellite Communications System (DSCS) supports long-distance communications requirements of military forces. The DSCS satisfies most DOD medium- and high data-rate communications requirements. The Military Strategic and Tactical Relay (MILSTAR) will soon be integrated as the third segment of the MILSATCOM architecture. It will provide a worldwide, secure, jam-resistant communications capability to US civilian and military leaders for C2 of military forces. The fourth segment consists of commercial communications satellites, which are used to support DOD's MILSATCOM.

DEFENSE DATA NETWORK (DDN)

1-52. The DDN is a global communications network serving DOD. The DDN consists of military networks, portions of the Internet, and classified networks (which are not part of the Internet). The Defense Information Systems Agency (DISA) manages the DDN.

DEFENSE INFORMATION SYSTEMS NETWORK (DISN)

1-53. The DISN is a worldwide information transfer infrastructure. It consists of backbone, regional, and local components intended to support the DOD. The DISN provides sufficient value-added common user services and bandwidth for the high-volume exchange of voice, data, imagery, and video communications anywhere in the world. Its capabilities include–

- The long-haul transport component of the defense information infrastructure (DII).
- Providing seamless interoperability and assured connectivity.
- Providing positive control of network resources.
- Incorporating emerging technology, as it becomes available.

As a subset of the DII, the DISN provides switching and transmission within and across DII boundaries.

AUTOMATIC DIGITAL NETWORK (AUTODIN)

1-54. The AUTODIN currently provides all levels of message security classification services worldwide. AUTODIN is interconnected through a network of AUTODIN switching centers located within the CONUS and around the world. AUTODIN is an integrated multilevel secure network that supports the exchange of general service narrative, data pattern, and Defense Special Security Communications System (DSSCS) messages. These messages range from unclassified to Top Secret/Special Category Information (TS/SCI).

DEFENSE MESSAGING SYSTEM (DMS)

1-55. The Defense Message System (DMS) is a new way of doing electronic organizational messaging. DMS eliminates the need for AUTODIN and legacy electronic mail (e-mail) systems throughout DOD's Internet protocol (IP) router network and associated LANs. DMS is a flexible, secure, COTS-based system. It provides multimedia messaging and directory services that take advantage of the underlying DII network and services. The DMS will handle information of all classification levels, compartments, and handling instructions. DMS is an integrated suite of applications that run on the DISN. DMS is NOT a network and is the system of record for organizational messaging.

Chapter 2

LAN Installation

Linking BFACSs in a local geographical area creates a LAN. The LAN provides the path for data to travel gathering and sharing information. This chapter discusses the components used in installing a LAN, the different network configurations, and the router- and switched-based architectures.

LAN CONFIGURATION

2-1. The LAN configuration and protocols used depend on the mission of the unit and the commanders' intent. For a LAN to function effectively, it must be well planned. The hardware, software, and peripherals used must interoperate with one another. Certain hardware and software requirements must be met and installed

BFACSs

2-2. Computers are electronic devices operating under the instructions stored in the memory unit. Computers can accept and process data (input), produce results (output) from the processing, and store the data for future use. Computers can also communicate by sending and receiving data to other computers connected to a LAN.

2-3. The ABCS computers are the C2 systems that are software unique for each BFA. They provide maneuver, FS, AD, intelligence and EP, and CSS information. These systems can provide e-mail, facsimile, electronic data exchange, global positioning systems, and Internet and video teleconferencing. The configuration of these systems depends on the unit's mission.

NETWORK INTERFACE CARD (NIC)

2-4. A NIC is a circuit card that 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. A NIC has circuits that coordinate transmitting and receiving data and check errors of transmitted data.

2-5. NICs are built into hardware-like routers and switches and require no hardware configuration. For laptop computers, the NIC is the personal computer (PC) card and requires little or no configuration. The configuration process for many NICs will differ based on whether the NIC is installed in a server or a workstation. Different drivers are required for different operating systems. Figure 2-1 shows an example of a NIC connected by a T-connector with a coaxial cable or RJ-45 cable.

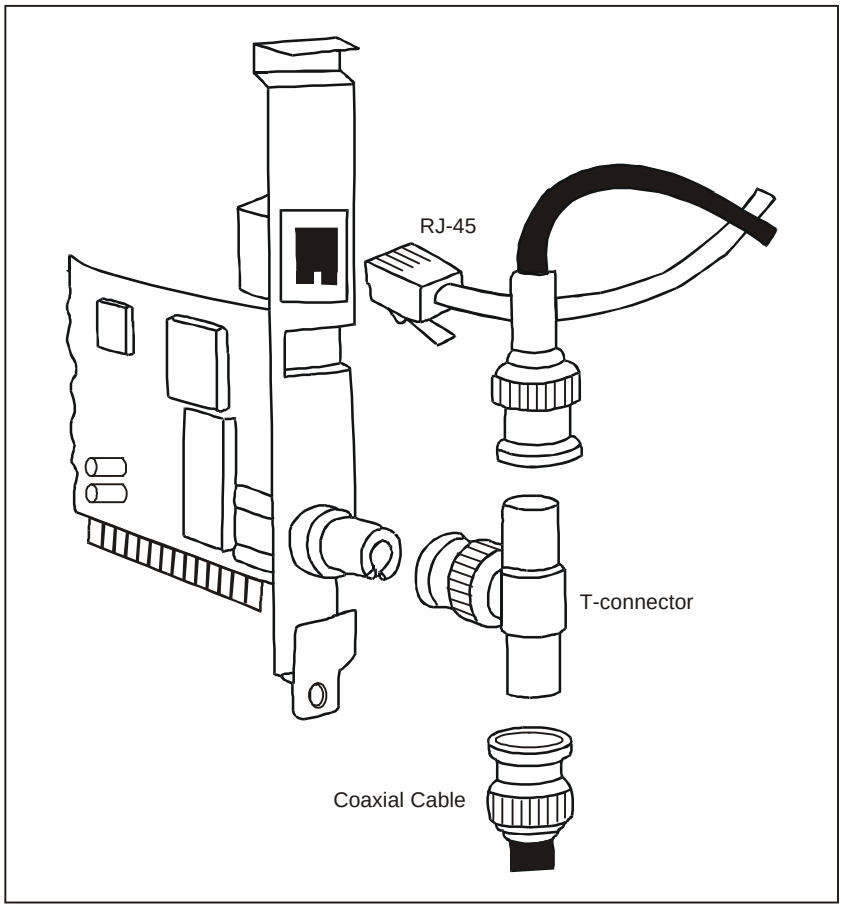

Figure 2-1. Example of a NIC

2-6. The NIC–

- Provides power to the transceiver.
- Buffers and decodes the received frames.
- Builds frames to be sent out on the network.
- Interfaces with PCs and the PC's central processing unit.
- Performs parallel to serial conversion.
- Provides a workstation with a unique address.
- Computes back off time when a collision is detected by the transceiver.

TRANSMISSION MEDIA

2-7. The TOC LAN can use coaxial cable, twisted-pair cable, fiber-optic (FO) cable, wire, radio frequency, infrared, or laser beam (wireless). The signals travel over these media from one device to another device.

COAXIAL CABLE

2-8. Coaxial cable is a high-quality, heavily insulated communications line. It consists of a nonconducting insulator surrounded by a woven metal outer conductor and a plastic outer coating. It is not susceptible to electrical interference and transmits data faster over longer distances.

10Base2 Thinnet

2-9. 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 2-2 shows an example of a basic 10Base2 LAN. Figure 2-3 shows an example of T-connectors to a NIC.

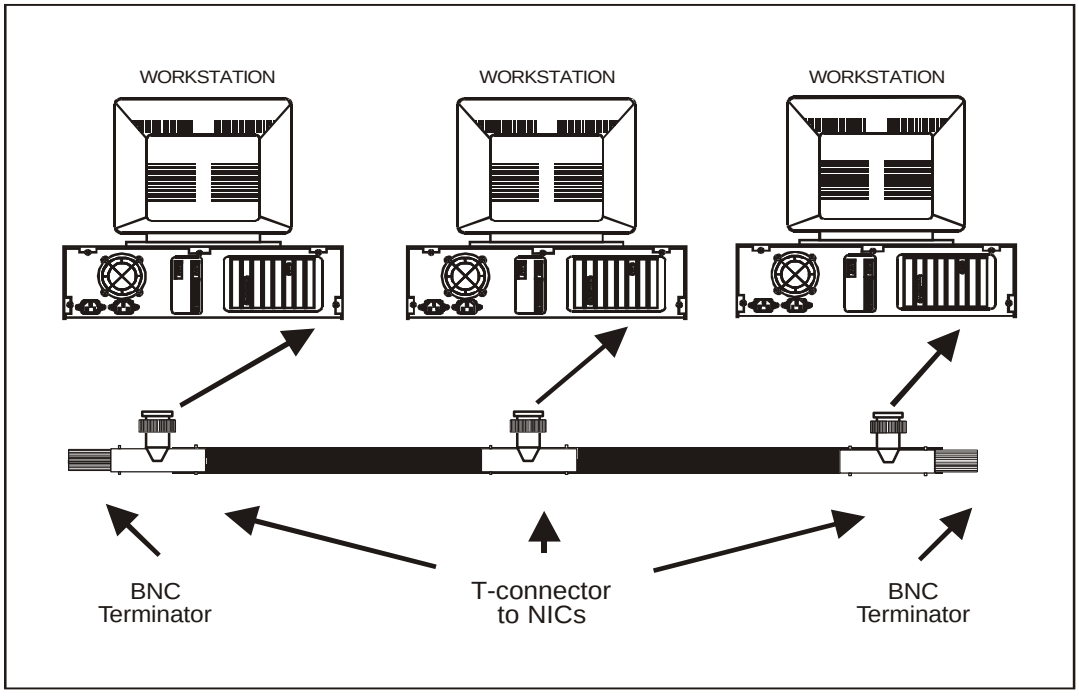

Figure 2-2. Example of a Basic 10Base2 LAN

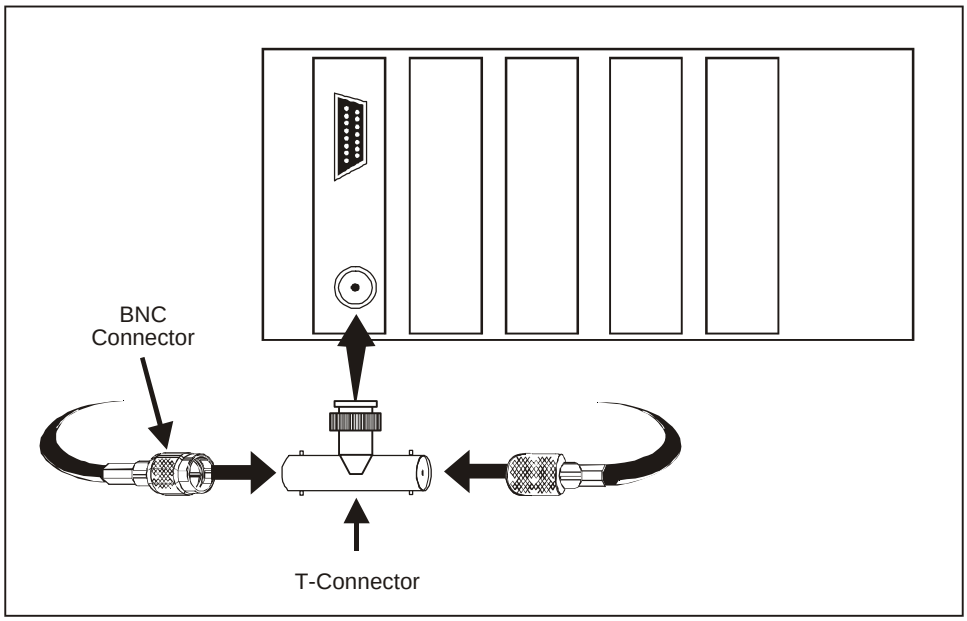

Figure 2-3. Example of T-connectors to a NIC

10Base5 Thicknet

2-10. 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 2-4 shows an example of the basic connections for a 10Base5 bus LAN. DIX connectors refer to the three companies (Digital, Intel, and Xerox) that developed Ethernet. These connectors have 15-pin male and female connectors. Figure 2-5 shows an example of the male and female DIX connectors.

TWISTED-PAIR CABLE

2-11. 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. UTP cable does not have the foil wrapper. Twisted-pair cable is an inexpensive transmission medium that can be installed easily.

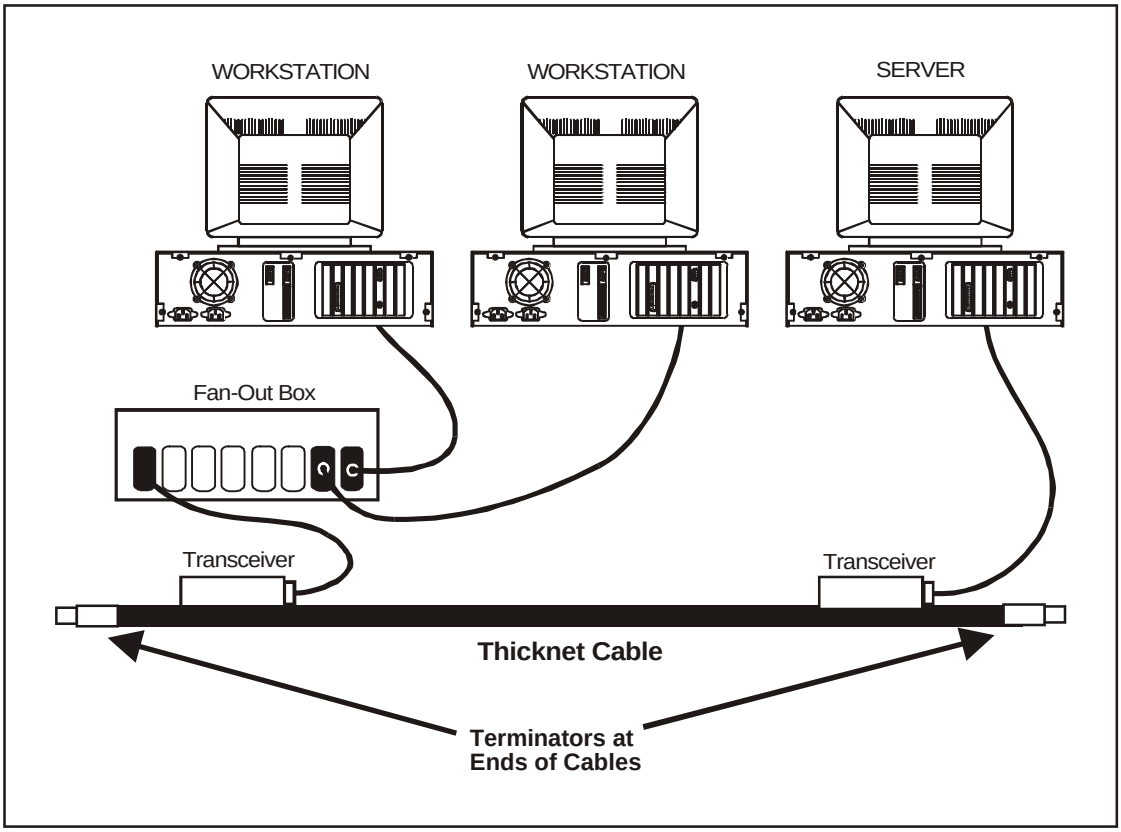

Figure 2-4. Example of Basic Connections for a 10Base5 Bus LAN

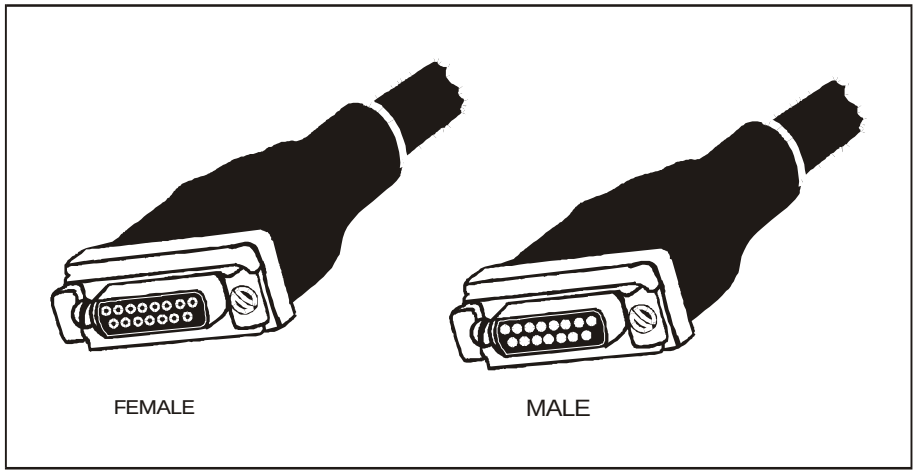

Figure 2-5. Example of the Male and Female DIX Connectors

100BaseTX

2-12. 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

2-13. The 10BaseT is a UTP cable used to connect 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 (mbps)). The 10BaseT's maximum segment length 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 2-6 shows an example of a 10BaseT LAN.

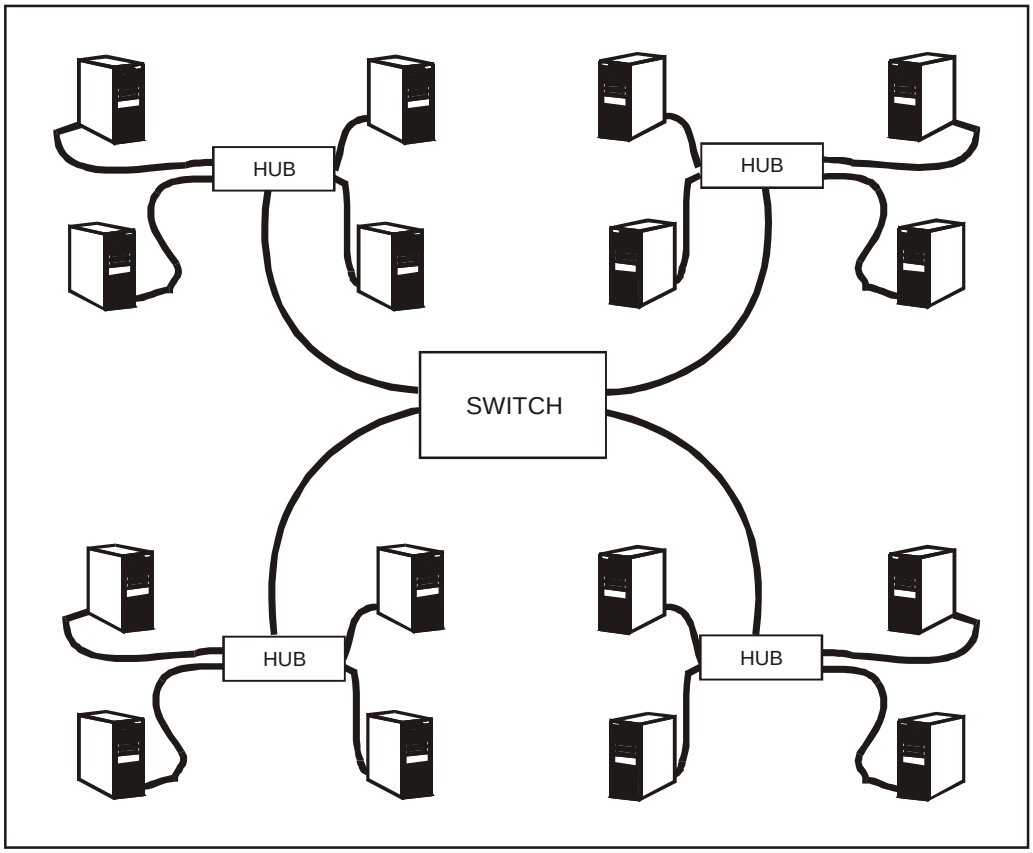

Figure 2-6. Example of a 10BaseT LAN

FO CABLE

2-14. 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

2-15. 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 2-7 gives an example of a 10BaseFL fiber link between sites.

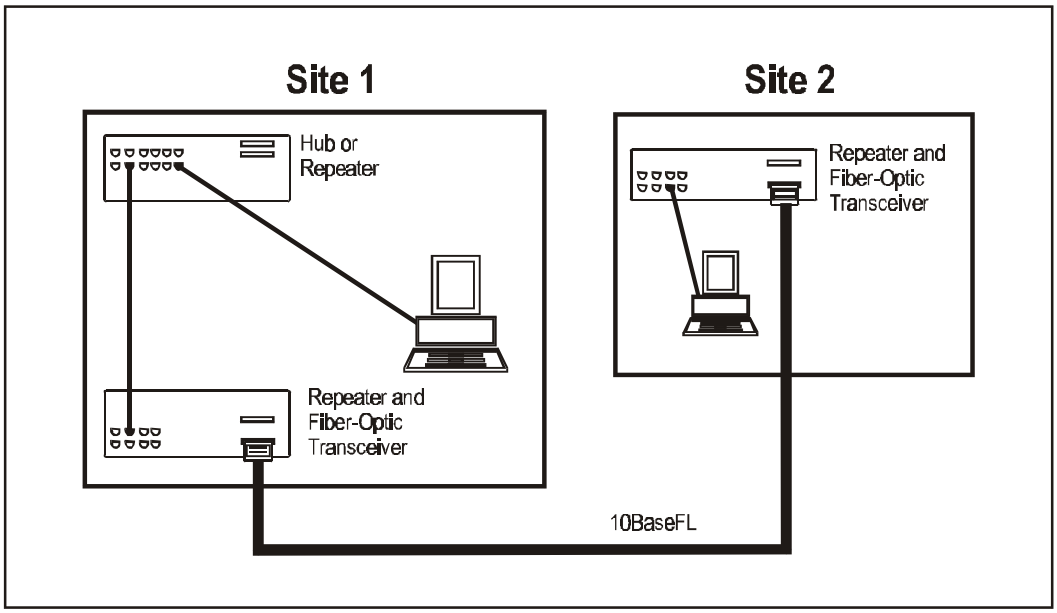

Figure 2-7. Example of a 10BaseFL Fiber Link Between Sites

100BaseFX

2-16. 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 2-8 shows an example of a 100BaseFX LAN.

WIRELESS

2-17. Wireless transmission technology uses infrared or laser beams to transmit data between computers without connecting them with a cable.

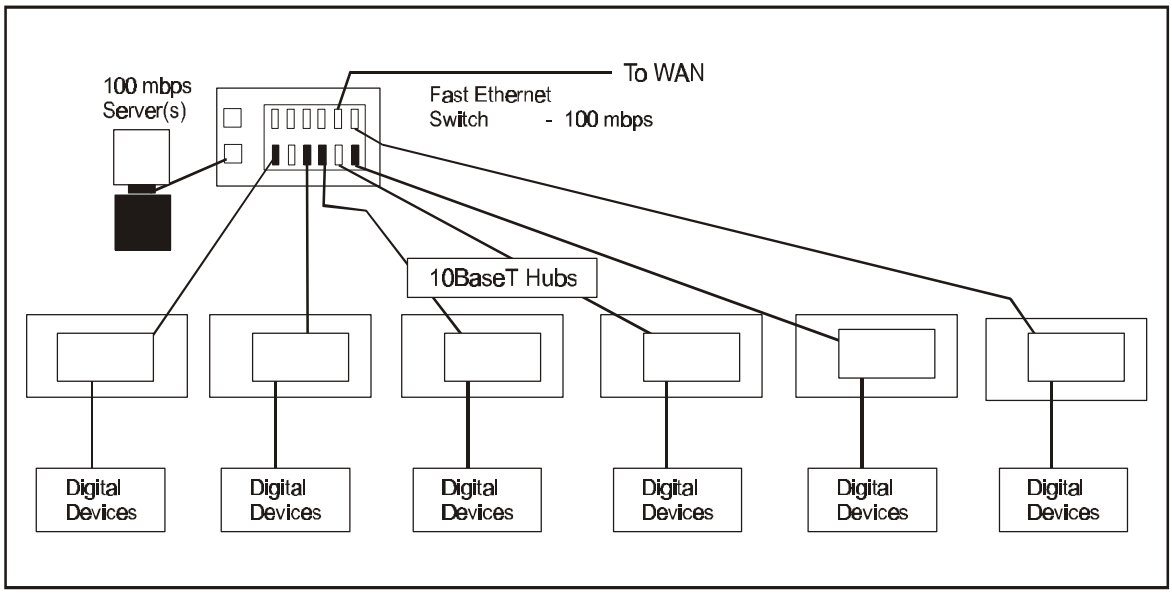

Figure 2-8. Example of a 100BaseFX LAN

COMMUNICATION PROTOCOLS

2-18. A protocol is a set of rules and procedures for exchanging information between computers. Protocols define how the communications link is established, how information is transmitted, and how errors are detected and corrected. The two most used protocols are Ethernet and token ring.

ETHERNET

2-19. Ethernet is the most widely used network protocol for LAN networks. Ethernet is based on a bus topology but can be wired in a star pattern by using a wiring hub. Most networks transmit data at 10 mbps. A higher speed version of Ethernet is the Fast Ethernet, and it can transmit data at 100 mbps.

2-20. A packet of data can be sent in both directions along the bus whenever a node is ready to transmit. The packet, which contains the destination address and sending address, travels along the network until it arrives at the designated receiving device. When a collision occurs, the network adapter cards send out a jam signal. This signal lets the conflicting nodes know that there is a collision. Each adapter stops transmitting and a unique back off period calculates when to retransmit the data. This ensures that the collision does not occur again when the nodes try to resend the data.

2-21. When a network uses carrier sense multiple access/collision detect (CSMA/CD), all computers are equal when it comes to accessing the media. Every computer on the network receives every frame that is transmitted, unless switches are used.

CONNECTIVITY DEVICES

2-22. Tactical LANs are interconnected using routers, switches, bridges, repeaters, and hubs.

ROUTERS

2-23. Routers allow addressees to change as needed for jump and/or split TOC operations. Routers are used when several networks are connected together. A router is an intelligent network-connecting device that sends (routes) communications traffic directly to the appropriate network. In the event of a network failure, routers are smart enough to determine alternate routes.

SWITCHES

2-24. A switch connects LAN segments and a high-speed port. A LAN switch has a dedicated bandwidth per port. When a LAN switch is powered up and the devices that are connected to it request services from other devices, the switch builds a table that associates addresses of each local device with the port number through which that device is reachable.

BRIDGES

2-25. A bridge connects two or more LANs that use identical LAN media access control (MAC) layer protocols. A bridge forwards frames between LAN segments using information it finds in the open systems interconnect reference model (OSI RM) Layer 2 of a packet. It looks at the destination address and compares the address to its address tables. If it finds the address associated with a port, it sends the packet out on that port. If it does not find an address, it sends the packet out on all ports.

2-26. Multibridges usually communicate with each other using the IEEE 802.1d spanning tree algorithm protocol or other protocol. Pure transparent and source routing bridging are most effective when there are fewer links in the network. Larger networks usually use routers where links are numerous. Transparent bridges send frames or packets out a port; they do not route them to another device.

REPEATERS

2-27. Repeaters provide the cheapest and least intelligent connections between segments of a LAN or between closely located LANs. Repeaters simply take the input (signals) and regenerate the signals on all other ports on the repeater at its original voltage.

2-28. Multiport repeaters primarily connect several 10Base2 segments of an Ethernet/802.3 LAN. This repeater has one AUI port and six 10Base2 ports. Repeater (half) sets generally connect segments of a LAN located more than 100 meters apart. FO is the generally accepted media between repeater sets. For less than 100 meters, AUI cable can connect 10Base5 segments.

NOTE: Repeaters do not control or reduce traffic between LAN segments or between LANs. Attempting to run too many segments can result in too long a distance and increased collisions due to that distance. IEEE standards say that a frame cannot pass through more than four repeaters between a sending and a receiving station.

HUBS

2-29. Wiring hubs allow devices such as computers, printers, and storage devices to connect to the server. The hub acts as the central connecting point for cables that run to the server and each of the devices on a network. A stackable hub can connect with another hub to increase the number of devices attached to the server.

NETWORK CONFIGURATIONS

2-30. Topology is the way equipment is configured in a LAN. The logical connection of the devices in the network determines the typology and the path the data follows as it is routed from one device to another. The actual physical connections may form a different shape than the one formed by the devices in the network. The more common topologies are bus, star, and ring. Combinations of these topologies also are used.

BUS NETWORK

2-31. In a bus network, all the devices or nodes are connected to and share a single path. Bus networks allow data to be transmitted in both directions. Each time data is sent out a destination address is included with the transmission so the data is routed to the appropriate receiving station. A bus network can be wired with a wiring hub at the center so it looks like a star network. An advantage of the bus network is that devices can be attached or detached from the network at any point without disturbing the rest of the network. Also if one computer in the network fails, this does not effect the rest of the network. Figure 2-9 shows an example of a bus network.

STAR NETWORK

2-32. In a star network, a central computer with one or more terminals or smaller computers are connected forming a star. A star network consists of only point-to-point lines between the central computer and the other computers on the network. The disadvantage of a star network is that the network relies on the central computer's hardware and software. If any of these elements fail, the entire network is disabled. In a star network, back-up computer systems are kept available in case of system failure. Figure 2-10 shows an example of a star network.

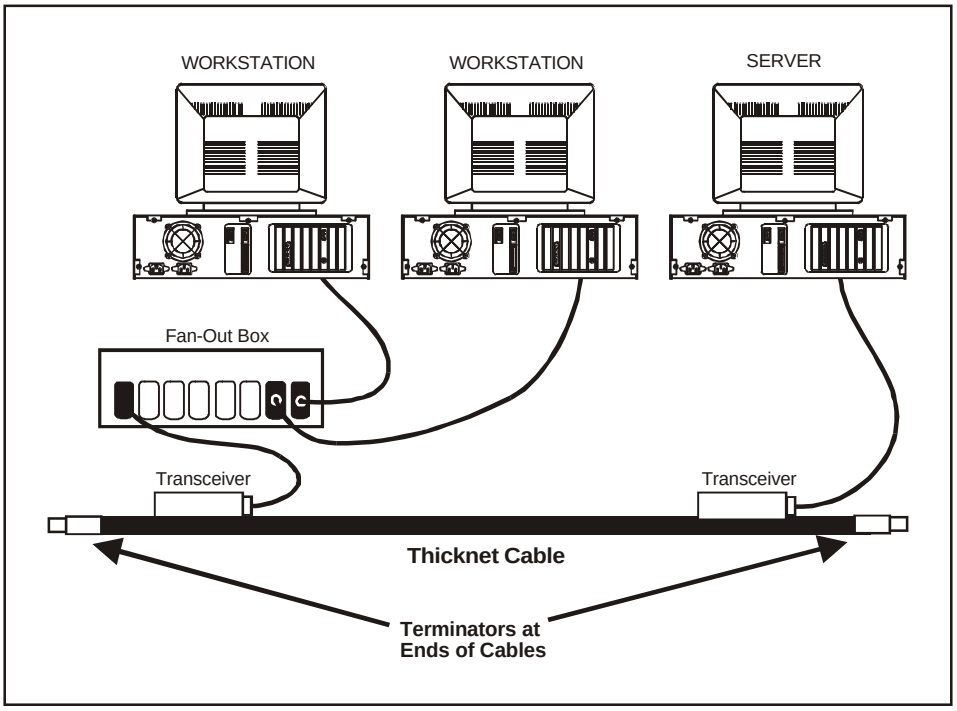

Figure 2-9. Example of a Bus Network

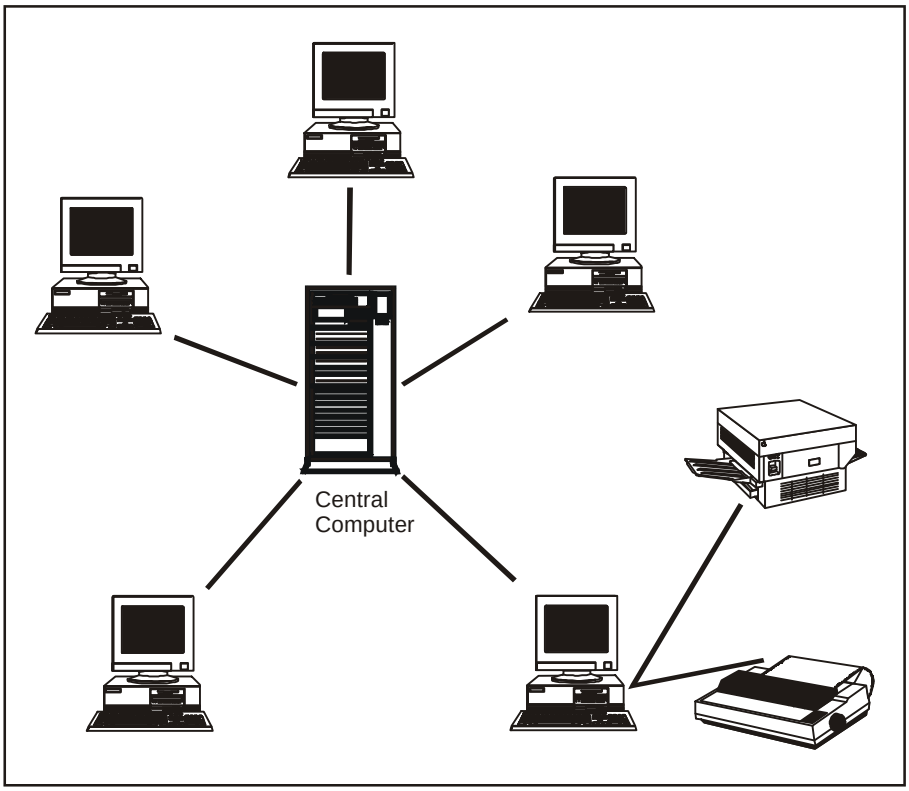

Figure 2-10. Example of a Star Network

RING NETWORK

2-33. In a ring network, all devices on the network are connected in a continuous loop or ring. A ring network does not use a centralized host computer. In the ring network, computers connect and communicate in a circular pattern. Data travels around in one direction only and passes through each computer. Ring networks sometimes connect large computers in the same area that share data frequently. One disadvantage of a ring network is that if one computer fails, the entire network fails because the data cannot be transmitted past the failed computer. Figure 2-11 shows an example of a ring network.

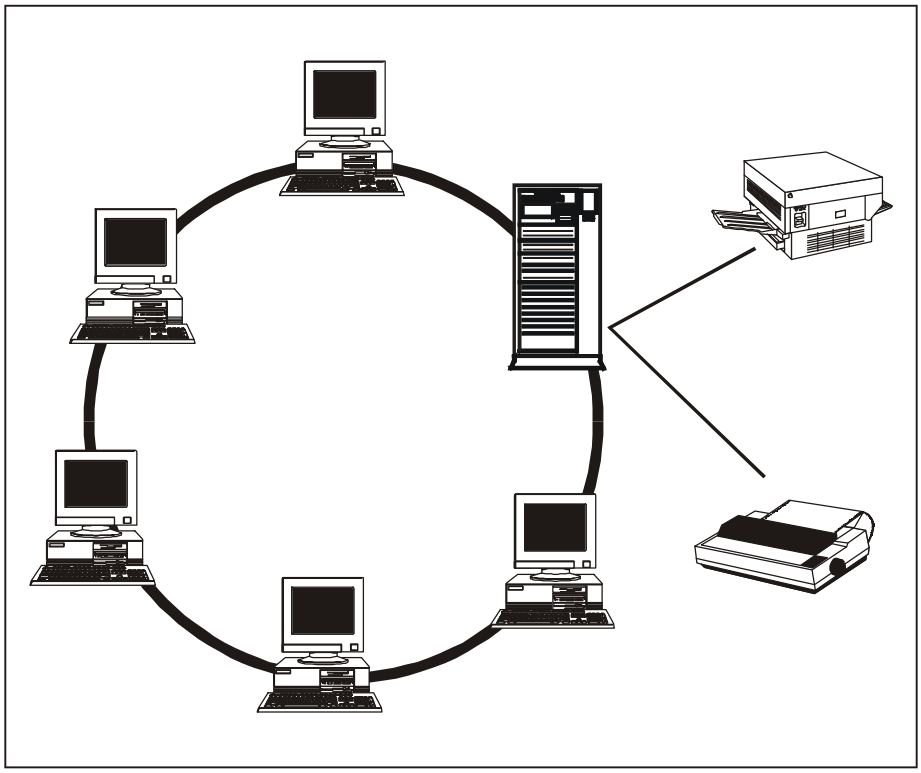

Figure 2-11. Example of a Ring Network

TOKEN RING

2-34. In a token-ring network, computers are configured in a ring and a message called a token is passed from computer to computer The token is used to avoid conflicts in transmission. A computer can only transmit messages while it holds the token. The computer keeps the token while transmitting a message and then passes it on to the next computer. While the computer is transmitting a message, other stations must wait.

2-35. The receiving computer copies the data and it continues around the ring until it gets to the computer that transmitted the original message. That computer then purges the busy token and inserts a new free token and the process starts over with a new computer transmitting a message.

2-36. Token-ring networks run over twisted-pair cabling with a length limited to 150 feet between the MAU and the computer. This cable can be either STP or UTP. UTP is cheaper but tends to have interference problems. STP is the more stable.

ROUTER-BASED ARCHITECTURE

2-37. The TOC LAN consists of several separate LANs interconnected by routers. The TOC LAN interconnects the various TOC shelters. The intervehicle LAN is external and uses a router AUI 1 LAN port. The intravehicle LAN is internal and uses a router AUI 0 LAN port. The intervehicle LAN interconnects the BFA workstations within a shelter. Thus, the host can keep their IP address wherever their vehicle attaches to the network. The host tables can stay the same while the routing protocols quickly announce the new route. The fire support element shelter has an additional LAN that extends the AFATDS workstation into the TOC Standard Integrated Command Post Systems (SICPSs). So, within a multiple shelter TOC, there could be multiple intervehicle LANs. Figure 2-12 shows an example of tactical LAN connectivity.

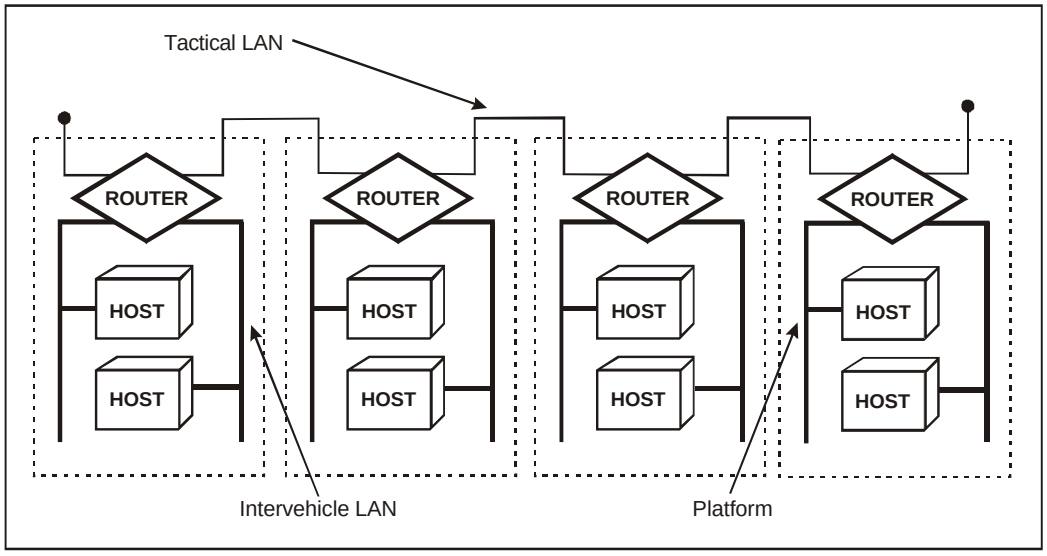

Figure 2-12. Example of Tactical LAN Connectivity

2-38. The LAN is configured as a single continuous bus and is terminated at each end with a 50-ohm terminator. To minimize coaxial stub lengths, T-connectors connect directly to the equipment. The IEEE 802.3 Type 10Base2 LAN is limited to 185 meters (about 600 feet) and 30 MAUs. Each shelter has about 50 feet of internal cabling. Four interconnected SICPSs will give an internal total cable length of about 200 feet.

2-39. The LAN must have a single-point ground for the coaxial cable segment, even if the segment consists of cable sections from multiple SICPSs. Standing operating procedures (SOPs) must be established for grounding TOC LANs. This helps the user understand who is responsible for grounding the LAN and in which vehicle.

2-40. For a single SICPS LAN with no coaxial connections to other SICPSs, the terminator plugs connect to the LAN connectors at the single entry panel (SEP) and the tent interface panel (TIP). A multiple SICPS LAN requires a terminator at the SEP of the first SICPS and another terminator at the TIP of the last SICPS on the Thinlan bus.

2-41. The FO LAN connects to the TOC LAN when the 185-meter maximum cable run is exceeded. All equipment connected to the FO LAN must be IEEE 802.3. The FO cable is not subject to the electrical constraints limiting the coaxial LAN. These electrical constraints include lightning, electromagnetic interference (EMI), grounding, and shock hazards.

2-42. The battalion/brigade support area (BSA) and the battalion TOC intervehicle LANs connect in daisy chain configuration. They connect to the TOC LAN at the vehicle's TIP of the first vehicle and to LAN B on the SEP of the second vehicle. This method continues until the last vehicle is connected. The BSA and the battalion TOC intervehicle LANs terminate at LAN B on the SEP of the first vehicle and LAN B on the TIP of the last vehicle. The vehicle of the deputy G6 and/or the S6 connects onto the TOC LAN. Figure 2-13 shows an example of a router-based architecture.

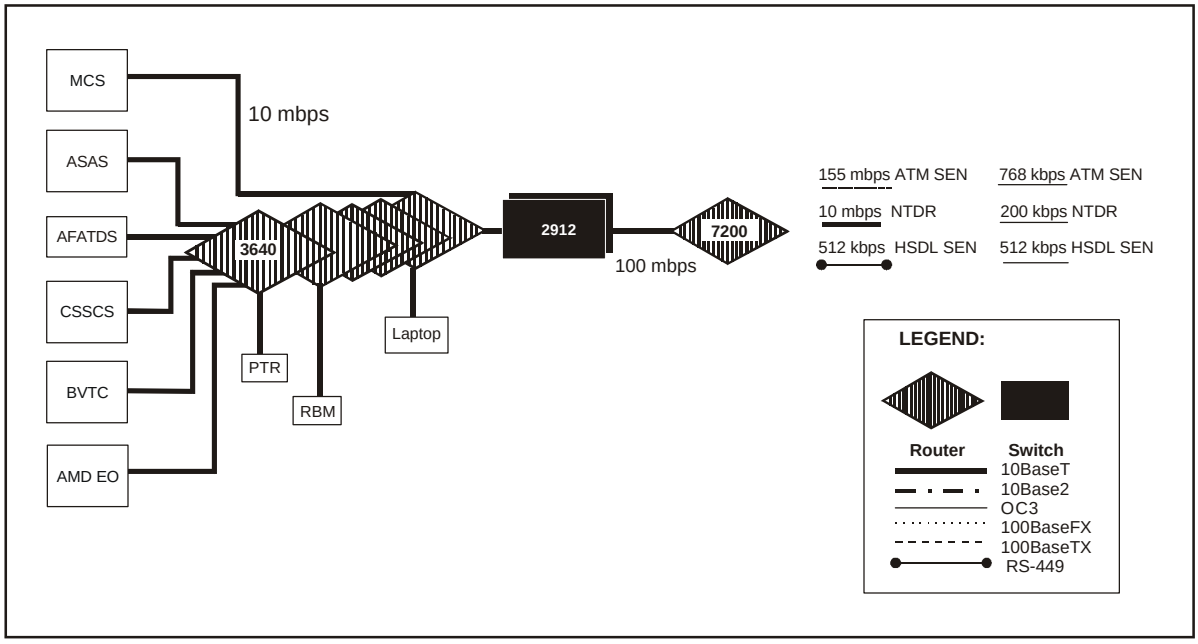

Figure 2-13. Example of a Router-Based Architecture

2-43. The division and the brigade TOC intervehicle LANs connect in a star configuration with a central Ethernet switch hub. Separate intervehicle TOC LAN segments connect to the LAN hub. Each intervehicle LAN segment directly connects to the vehicle TIP LAN B connector without a tee and at the Ethernet switch using a coaxial tee and terminator. LAN A and B ports terminate on the vehicle's SEP. The intravehicle LAN's TIP LAN A port extends the LAN's access to workstations in the TOC's tent complexes. When intravehicle LANs extend from a vehicle to a TOC tent complex, the TIP LAN

A terminator is removed and is replaced with a LAN segment (a coaxial T-connector and terminator). Extended intravehicle LANs terminate at the workstation.

2-44. Division and brigade jump and/or split TOC operations use the battalion TOC LAN daisy chain configuration until the TOC hub arrives. AFATDS intervehicle LANs will use additional LAN C ports and the daisy chain configuration.

SWITCHED-BASED ARCHITECTURE

2-45. A switched LAN consists of several Ethernet switches that extend to a central switch and a central router. Some TOCs may have multiple central switches and central routers. The central switch provides the interface from the cell switches to the central router. At the designated vehicle, the central router provides communications between cells and connectivity to the wide area network (WAN). The C LAN exists for the AFATDS intervehicle LANs. The switches in these TOCs automatically identify who is connected to its ports by the MAC address. Thus, the switch can broadcast traffic immediately to a port using the store and forward procedure. The procedure increases the performance of the LAN since there is no collision factor. The central router will have the open shortest-path first and the border gateway protocol to allow for inter- and intra-administrative borders. Figure 2-14 shows an example of a switched-based architecture.

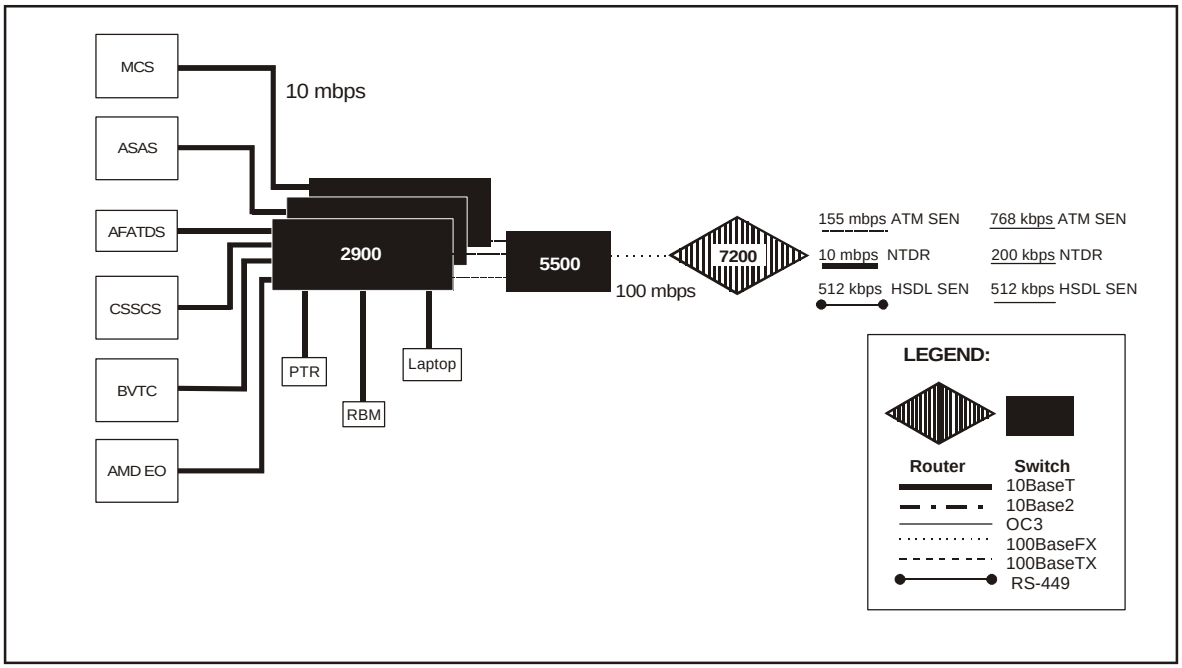

Figure 2-14. Example of a Switched-Based Architecture

2-46. The intervehicle LANs connect in a star configuration to a central Ethernet switch. The FO cable has one pair per connection: one transmit and one receive. When connecting the fiber, the ends must be swapped so one end transmits and one end receives. The IEEE 802.3 Type 10BaseT and 100BaseTX LAN distance limitation is 100 meters (about 328 feet). The 100BaseFX distance limitation is 412 meters (about 1351 feet). The optical carrier (level 3) OC3 distance limitation is 2 kilometers (about 1.2 miles). Straight through patch cords connect the hosts to the switch, and the crossover patch cords connect the switch to another switch or router.

Chapter 3

Tactical LAN Management Responsibilities

An effective, well-structured, and managed network should not require user intervention. Users must concentrate on understanding and interpreting the information they receive. This information must be readily available, and the user should not have to understand the process by which information is made available. This chapter covers the management personnel, tasks, and functions at all levels for establishing, managing, and maintaining a TOC LAN.

MANAGEMENT PERSONNEL

3-1. Establishing, managing, and maintaining any network is an essential task. Management personnel perform their tasks, duties, and responsibilities under network employment, network configuration, network status monitoring and reporting, network control and reconfiguration, training, and security. Appendix A provides a detailed sample of a security SOP.

3-2. The complexity of the Army's networks requires highly-skilled individuals with the necessary tools to install, operate, and maintain the LANs. Table 3-1 identifies the personnel directly involved in the management process.

Table 3-1. Management Personnel

Title	Location
G3, Operations and Plans Officer	Corps and Division
S3, Operations and Training Officer	Brigade and Battalion
G6, Signal Officer	Signal Commander Corps/Division
Deputy G6, Assistant Corps/Division G6	Corps/Division – Main (Signal Office)
S6, Signal Officer	Brigade/Battalion (Signal Office)
Systems Administrator (SA) Network Administrator (NA)	Signal Office at every echelon
Combat Service Support Automation Officer (CSSAMO)	Division Support Command (DISCOM)
Mission Applications Administrator	BFA Cell
Mission Applications User	BFA Cell

G3/S3, OPERATIONS AND PLANS/TRAINING OFFICER

3-3. The G3/S3 is the principal staff officer for tactical network training, operations and plans, force development, and modernization. Figure 3-1 lists the tasks and functions of the G3/S3.

G3/S3, Operations and Plans/Training Officer
Network Employment– • Coordinates tactical LAN employment issues with the deputy G6 or S6.
Network Configuration– • Establishes and enforces network policies and procedures as outlined in Signal Annex K and the unit's SOP. • Receives guidance from the deputy G6 or S6 on TOC LAN configuration and connectivity for the BFACSs. • Includes completed worksheets in the tactical SOP for the deputy G6 or S6. **Note: See Figure 3-5 for a sample of a completed system planning worksheet.**
Network Status Monitoring and Reporting– • Monitors the tactical situation. • Receives updates on the status and availability of the tactical LAN.
Network Control and Reconfiguration– • Coordinates with the deputy G6 or S6 on changes to the signal annex of the operation order (OPORD). • Transmits changes to subordinate elements. • Implements unit SOPs for system back up and recovery. • Coordinates network for initialization or recovery, as needed. • Conducts database initialization and back ups, as needed.
Training– • Plans, executes, and supervises training. • Develops a sustainment training program that addresses– ▪ User training on hardware and system software for staff officers and noncommissioned officers (NCOs). ▪ Unit maintainer and support personnel training for information systems. ▪ Training for users and/or staff users. • Collective information systems and C2 protect (C2P) security training for the unit.
Security– • Implements information security plans, instructions, and SOPs. • Implements procedures to restrict entry of unauthorized transactions or data. • Ensures systems operate IAW current Army regulations (ARs) and local security SOPs. • Ensures the information systems security officer (ISSO) is appointed. • Conducts C2P training. • Reports threats to network security.

Figure 3-1. G3/S3 Tasks and Functions

G6/S6, SIGNAL OFFICER

3-4. The G6/S6 at all echelons must develop a routine interaction with the unit staff and must take an active role in the staff planning process. He must ensure the staff understands the capabilities and limitations of the units' organic signal assets and external support.

3-5. The G6/S6 plans, designs, engineers, maintains, and evaluates network management. He is also responsible for communications, visual information systems, and IP networks. He provides technical guidance and direction to subordinate operating elements. Figure 3-2 lists the tasks and functions of the G6, deputy G6 and S6, and the SA/NA.

Corps G6

3-6. The G6 is responsible to the corps commander for installing, operating, and maintaining the network. He supervises the corps communications security (COMSEC) office of record. The G6 controls radio frequency allocations, IP addresses, and spectrum management for the corps and the distribution and reproduction section. The corps signal office's primary mission is to perform signal planning for the corps. The corps signal office is part of the corps and the deputy G6 oversees the operation of the office.

Division G6

3-7. The signal battalion commander serves in the dual role of commander of the signal battalion and as a member of the general staff as the G6. These two functional roles are separate but related. The G6 consults directly with the Chief of Staff (CofS) on all communications matters.

3-8. The G6 is the general staff officer for signal operations, automation and network management, and information security. He also presents the communication aspects for tactical operations for all staff planning. The system control center-2 (SCC-2) assists the G6 and the deputy G6 in managing the division's communications systems.

Deputy G6, Assistant Corps/Division G6

3-9. The deputy G6 represents the G6 on the division staff. The deputy G6 locates at the corps and/or division signal office and represents the G6 in providing communications support. The deputy G6 performs management operations and maintenance of the command's communications and information systems. He coordinates with the supporting signal battalion for connectivity to the WAN, and he is responsible to the commander for information systems connectivity to the WAN.

3-10. The deputy G6 locates and supervises the division tactical signal office and works closely with the division G3. The deputy G6–

- Monitors the TI.
- Prepares and distributes the division signal operation instructions (SOI).
- Coordinates signal interfaces with host and allied nations in stand-alone divisions.
- Requests and manages satellite access for TACSAT.

G6, Deputy G6 and S6, and the SA/NA
Network Employment– • Establishes, manages, and maintains communications links. • Advises the commander on communications support requirements. • Plans, coordinates, and manages network terminals (regardless of affiliation).
Network Configuration– • Receives planning worksheets with LAN/WAN requirements. • Determines system requirements needed for support based on the tactical situation. • Determines communications and/or transmission connectivity requirements. • Links separate TOCs through the WAN. • Informs the commander on primary and alternate communications. • Develops initialization instructions for new or modified communications systems. • Assists the mission applications administrator with database configurations. • Supervises network configuration, initialization, and tactical LAN installation in the TOC. • Establishes and enforces network policies and procedures. • Detects, reports, and takes corrective action on security violations and possible internal and external intrusions. • Develops signal annex K to the OPORD. • Prepares signal estimates. • Advises the commander and users on the requirements, capabilities, and use of systems. • Determines tactical LAN configuration for the TOC. • Monitors network configuration in the TOC. • Coordinates signal interfaces with host nation and allied forces.
Network Status Monitoring and Reporting– • Monitors the status of the network using network management tools and reports from the mission applications administrator. • Monitors the status of communication links through automated reports from integrated system control (ISYSCON) to include– ▪ MSE TPN. ▪ MSE circuit switch network. ▪ CNR as reported by subordinates. ▪ EPLRS/joint tactical data radio (JTDR) as reported by their net control stations. ▪ Broadcast systems as reported by their net control stations. ▪ Tactical Internet (TI). • Reports network changes to the commander. • Monitors network performance and database configuration and reconfiguration.
Network Control and Reconfiguration– • Provides supervision and guidance on troubleshooting and correcting network problems. • Troubleshoots interconnection device problems throughout the system. • Determines the need for configuration changes. • Plans system reconfigurations caused by changes in the tactical situation, communications connectivity, and system initialization instructions. • Supervises changes in system configuration, initialization, and LAN installation. • Provides supervision and guidance on initialization and configuration instructions. • Replicates, distributes, and controls all software by ensuring software is current, compatible, and standardized IAW appropriate technical bulletins (TBs) and SOPs.

Figure 3-2. G6, Deputy G6 and S6, and the SA/NA Tasks and Functions

G6, Deputy G6 and S6, and the SA/NA (Continued)
Training– • Assists in training users on automation systems. • Supports the development and execution of training users and collective training for the unit. • Provides training in establishing and interconnecting networks.
Security– • Manages all operational and contingency COMSEC matters. • Prepares communications network security plans, instructions, and SOPs. • Develops security policies and procedures for network operations. • Monitors the security integrity of the network and reports breaches in that security. • Reports threats to network security. • Establishes procedures to restrict entry of unauthorized users, transactions, or data. • Ensures all users operate IAW AR 380-19 and local security SOPs. • Ensures the implementation of access control procedures. • Ensures ISSOs are appointed for each BFA.

Figure 3-2. G6, Deputy G6 and S6, and the SA/NA Tasks and Functions (Continued)

S6, SIGNAL OFFICER, PRINCIPAL STAFF OFFICER

3-11. The S6 manages operations and maintains the command's communications and C2 systems. As the principal staff officer, he works for the unit executive officer and closely interacts with the S3 and other staff officers.

Brigade/Battalion S6

3-12. The brigade/battalion S6–

- Is the signal expert to the maneuver commander.
- Advises the commander and staff on all signal support matters.
- Coordinates with higher echelon signal officers for additional communications support.
- Coordinates with the supporting signal battalion for connectivity to the WAN.
- Identifies, coordinates, and provides for task force communication requirements.
- Is responsible for all COMSEC items within the unit to include accountability, distribution, destruction, and security.
- Inspects subordinate unit signal support sections.
- Is responsible to the commander for information systems connectivity to the WAN.

CSS S6

3-13. The CSS S6 section is responsible for network management, systems administration, and systems/software security IAW AR 380-19 and the unit SOP. The S6 section troubleshoots TOC LAN problems, hardware, and network operating systems failures. As SAs/NAs and system/software security managers, the S6 performs all tasks normally associated with information technology operations ranging from issuing passwords to installing antivirus software. The S6 assists the CSSAMO in troubleshooting hardware/software application software problems. The S6 oversees the installation and maintenance of the LAN supporting DISCOM, forward support battalion, division support battalion, and aviation support battalion operations. The S6 provides the commander with the status of all information systems on the TOC LAN. The S6 coordinates with the supporting signal unit for connectivity to the WAN.

SA/NA

3-14. Each G6/S6 signal office has an SA/NA that plans and coordinates with the BFA mission applications administrator in linking the BFACS devices to the TOC LAN.

CSSAMO

3-15. The CSSAMO assigns a mission applications administrator for each of the STAMIS software applications. The CSSAMO–

- Provides customer support in operating and sustaining the Army's CSS STAMIS.
- Monitors the TOC LAN that the STAMIS resides. (However, the S6 is responsible to the commander for the LAN.)
- Provides support for all STAMIS applications.
- Loads, reloads, and copies STAMIS application software.
- Troubleshoots STAMIS hardware/software problems.
- Restores, rebuilds, edits, and reconfigures corrupt files.
- Loads, reproduces, and maintains tape libraries.
- Provides, rebuilds, and reproduces catalogs.
- Monitors user training programs and the fielding of new STAMIS equipment.
- Tests user suggestions.
- Conducts customer assistance visits.
- Assists units during deployments.
- Organizes resources to support deployments.
- Maintains hand receipts and small computer exchange line replaceable units (LRUs).

MISSION APPLICATIONS ADMINISTRATOR

3-16. A mission applications administrator is located within the BFA cell. He must be familiar with his cell's specific hardware and software applications. Within each BFA, the information flow, processing, and storing of information is managed according to the needs of the commander. Figure 3-3 lists the tasks and functions of the mission applications administrator.

Mission Applications Administrator
Network Employment– • Plans, coordinates, and manages BFACSs and software. • Receives the tactical plan from the G3 and/or S3. • Determines, identifies, and coordinates the unique BFA requirements with the deputy G6 and/or S6.
Network Configuration– • Determines tactical disposition of BFA elements and receives configurations guidance from the deputy G6 or S6. • Determines and provides information systems LAN configuration and communication requirements to the deputy G6 or S6. • Develops configuration and/or initialization instructions. • Plans BFACS database configuration and management responsibilities. • Defines database replication schemes. • Develops database configuration instructions and back up and recovery plans. • Supervises system configuration in his immediate area. • Establishes and enforces system policies and procedures IAW unit SOPs or BFA SOPs. • Prepares the C2 system Annex to the BFA OPORD.
Network Status Monitoring and Reporting– • Monitors the tactical situation. • Reports network changes to the deputy G6 or S6. • Monitors database configuration and/or reconfiguration and operations of his information systems. • Monitors his BFACS performance.
Network Control and Reconfiguration– • Provides supervision and guidance on initialization and configuration instructions to user and/or staff users. • Assists in troubleshooting problems in his immediate area. • Controls changes on configuration and initialization. • Provides information management for his commander and staff. • Replicates, distributes, and controls software IAW BFA TBs and SOPs. • Implements unit SOPs for network back up and recovery. • Plans system reconfiguration. • Transmits changes to subordinate elements. • Supervises system configuration in his immediate area. • Plans changes in the local system configuration.

Figure 3-3. Mission Applications Administrator Tasks and Functions

Mission Applications Administrator (Continued)
Training– • Plans, executes, and supervises the training of personnel. • Develops a sustainment training program that addresses– ▪ User training on hardware and BFA software for users and/or staff users. ▪ Collective training with the unit.
Security– • Develops information security plans, instructions, and SOPs. • Establishes BFA procedures to restrict entry of unauthorized transactions or data. • Ensures systems operate IAW AR 380-19 and local security SOPs. • Implements access control procedures. • Ensures physical security of terminals. • Ensures an ISSO is appointed for their system. • Develops and conducts training for security policies and procedures. • Reports threats to the SA/NA or ISSO.

Figure 3-3. Mission Applications Administrator Tasks and Functions (Continued)

MISSION APPLICATIONS USER

3-17. The mission applications user is located within the BFA cell. Users install, operate, and maintain their specific C2 systems. Figure 3-4 lists the tasks and functions of the user. Appendix B gives more information on basic system troubleshooting.

Mission Applications User
System Employment– • Installs, operates, maintains, and troubleshoots assigned hardware and software IAW SOPs, TBs, and technical manuals (TMs). (See Appendix B for troubleshooting.)
System Status and Reporting– • Monitors the information network. • Reports technical problems and changes to the mission applications administrator or supervisor.
Security– • Operates the systems IAW AR 380-19 and local security SOPs. • Implements access control procedures. • Provides physical security of terminals. • Reports threats to the mission applications administrator or SA/NA.

Figure 3-4. Mission Applications User Tasks and Functions

SYSTEM PLANNING WORKSHEET

3-18. The mission applications administrator provides the system planning worksheet to the deputy G6 or the S6 signal office for his systems requirements. Figure 3-5 shows a sample system planning worksheet.

Device Type	Seq No	Organization	User	Platform	LAN	TPN	Circuit Switched Network	CNR	EPLRS	JTIDS	BDCST
Division Main CP Headquarters Cell											
Mvr TCU	3	Division	Chief of Staff	5-Ton Van 03	HQ&Ops LAN	X	DNVT				
Mvr LCU	2	Division	LNO #1	M-998	HQ&Ops LAN	X	DNVT				
Mvr LCU	3	Division	LNO #2	M-998	HQ&Ops LAN	X	DNVT				
Mvr LCU	4	Division	LNO #3	M-998	HQ&Ops LAN	X	DNVT				
Division Main CP Operations Cell											
Mvr TCU	1	52d Engr Bde	ADA Main	M-998	HQ&Ops LAN	X	DNVT				
Mvr LCU	1	52d Signal Bn	Div Signal Office	MSC-31	HQ&Ops LAN	X					
Mvr TCU	5	Division	G3 Main Ops	5-Ton Van 04	HQ&Ops LAN	X	DNVT				
Mvr TCU	7	Division	G3 Main Ops	5-Ton Van 04	HQ&Ops LAN	X					
Mvr TCU	4	Division	G2 Main Ops	5-Ton Van 05	HQ&Ops LAN	X	DNVT				
Division Main CP Fire Support Cell											
FS HCU	1	DIVARTY	FSE Main Deep Ops	5-Ton Van 01	FSE LAN	X					
FSCT	2	DIVARTY	FSE Main Plans	5-Ton Van 01	FSE LAN	X					
FSCT	3	DIVARTY	FSE Main Plans	5-Ton Van 01	FSE LAN	X					
FSCT	4	DIVARTY	FSE Main Ops	5-Ton Van 01	FSE LAN	X		DA Ops 1	X		
								DA Ops 2			
								DA Ops 3			
Mvr TCU	1	52d Chem Co	Div Chem Section	M-109 Van	FS Cell LAN	X	DNVT				
AD TCU	1	4-441 ADA	ADA A2C2 Node	SICPS RWS 01	FS Cell LAN	X			X	X	
AD DTCU	1	4-441 ADA	ADA A2C2 Node	SICPS RWS 01	FS Cell LAN	X					

Figure 3-5. Sample of a System Planning Worksheet

Chapter 4

Network and Systems Management Hierarchy

A well-managed network or system ensures reliable and efficient communications to support the commander. The hierarchy of network and systems management facilitates the areas of responsibility of the WAN, TOC LAN, and the TI. This chapter covers the WAN, TOC LAN, network management, information management, and the TI at brigade and below.

WAN

4-1. The WAN consists of the following networks–

- MSE (ACUS) network.
- Global broadcast service (GBS) network.
- Near-term data radio (NTDR) network. (The Joint Tactical Radio System (JTRS) will replace the NTDR.)

4-2. The signal brigade headquarters conducts management and control in an MSE corps network. The supporting signal brigade/battalion provides configuration, performance, accounting, security communications, and fault management. The TOC LAN must connect to the SEN to communicate with higher, lower, and adjacent units. The SEN serves as the gateway to the WAN. Appendix C provides more information on MSE support.

TOC LAN

4-3. Each unit uses a TOC LAN to share information among the linked computers and other LANs. Gateways provide a connection to other LANs or WANs. The unit TOC LAN provides–

- File sharing and transfer.
- Application sharing and accessibility.
- Printer sharing.
- Security.

4-4. The unit installs, operates, and maintains all information systems connectivity requirements and peripherals within the TOC area. The deputy G6 and/or S6 plan, configure, manage, and maintain the unit's TOC LAN. Under the direction of the TOC noncommissioned officer in charge (NCOIC), the personnel install the unit's TOC LAN. The signal offices assist with and provide technical support in the installation of the TOC LAN.

4-5. The deputy G6 and/or S6 ensure connectivity to the supporting SEN. The supporting signal brigade/battalion and the G6/S6 share the responsibility to configure, operate, and maintain connectivity of the TOC LAN to the WAN. Figure 4-1 shows the WAN/LAN area of responsibility.

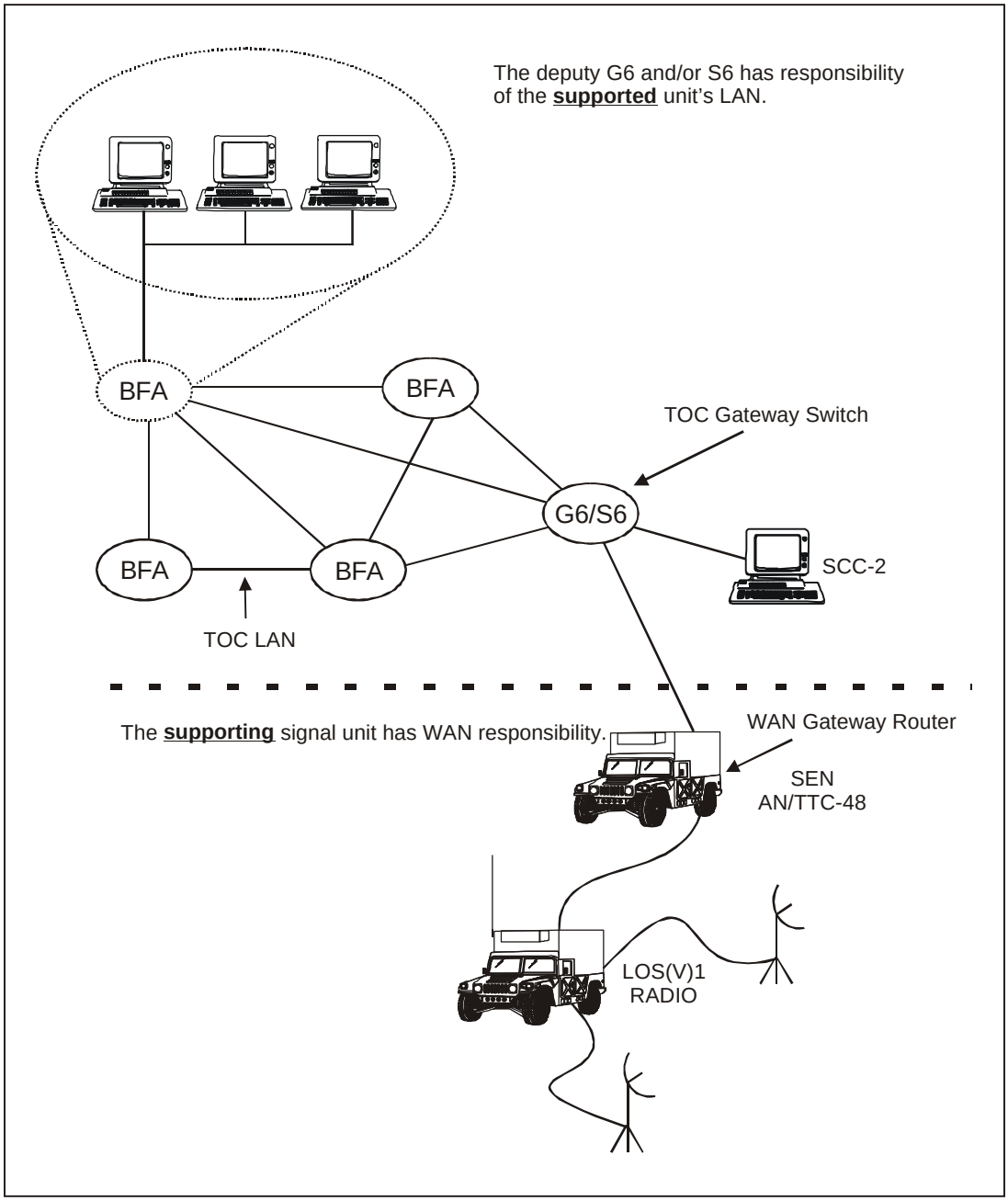

Figure 4-1. WAN/LAN Area of Responsibility

NETWORK MANAGEMENT

4-6. The corps and division signal battalions deploy their MSE signal assets under the overall direction of the corps signal brigade. The corps signal brigade SYSCON manages and controls the corps MSE network using the SCC-2. The SCC-2 performs all automated network planning, management, and control for the corps. The corps signal brigade maintains network

integrity, coverage and service. The division SCC-2 functions in an active role but remains under the technical control of the corps' active SCC-2 (Figure 4-2). In a division stand-alone configuration, the division SCC-2 assumes these functions and responsibility for the division network elements. SYSCON begins managing signal resources that support the TOC LANs on which the information systems operate.

4-7. Signal support organizations exist at every echelon to support the commander. These organizations provide reliable and flexible communications, automation, and information services. Effective network management provides an efficient and rapid means of retrieving information and enabling the battle staff to develop and maintain a single, virtual (or logical) database. This allows battle staffs to continue coordinating, integrating, and synchronizing current and future information operations. Network management ensures information systems, LANs, and WANs integrate into a single and seamless system.

4-8. The base requirement for establishing and controlling communications remains from higher to lower, left to right, supporting to supported, and reinforcing to reinforced. The element in the higher, left, or supporting category coordinates frequency plans, COMSEC keys, software, and edition and control mechanisms. Figure 4-2 shows the hierarchy from corps, division, brigade, and battalion. It indicates the network management hierarchy of communications, networks, and management elements.

CORPS

4-9. The corps signal brigade provides support through the corps area common-user network providing management and control in an MSE corps network. It provides special staff and technical assistance for planning and controlling all corps signal functions and the extension of signal services to higher and adjacent commands. MSE is the principal corps common-user system providing reachback capabilities and connectivity to subordinate divisions, adjacent units, and joint and allied services.

4-10. The corps G6, as a staff planner, plans for adequate and continuous area coverage throughout the corps area. In the division area, the organic four or six nodes often require augmentation. The corps G6 provides the assets needed to ensure area coverage. Normally, this requires two nodes. Allocation to the division depends on corpswide commitments. The division G6 employs his assets to support the C2 needs of the division. He has direct control of overall network assets and planning within the division switching control group. The corps SYSCON provides centralized control of the MSE network and is responsible for installation and operation. The division SYSCON works closely with the corps SYSCON for effective technical control.

4-11. In a corps network, each division SCC-2 controls the planning, engineering, and executing of all signal support requirements and assets within the division switching control group. The corps SCC-2 provides technical control for the integrated corps network while assisting the divisions.

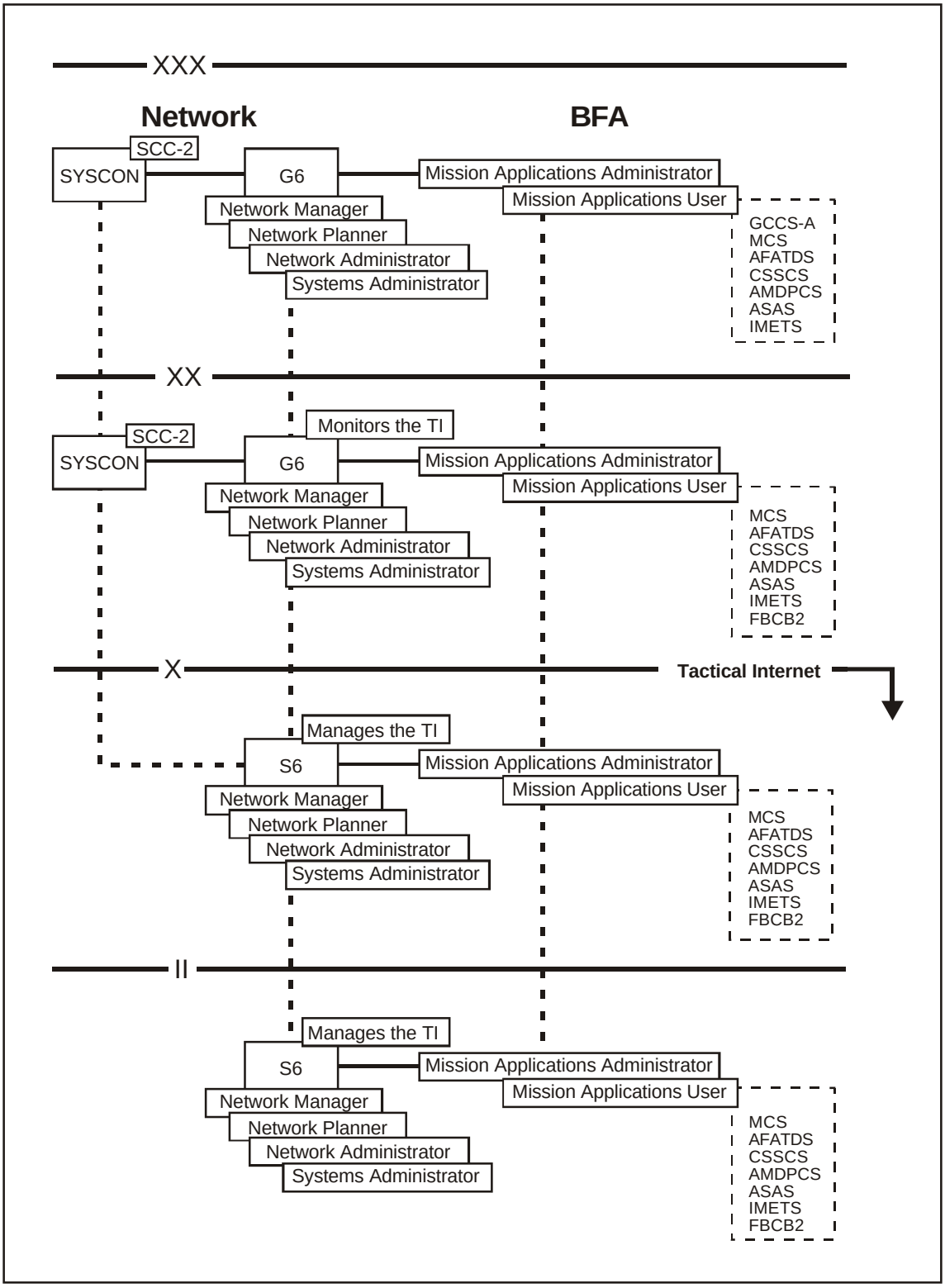

Figure 4-2. Network and Systems Management Hierarchy

DIVISION

4-12. The division signal battalion is the principal signal organization supporting the division. The battalion's primary mission is to establish a division area common-user network. The signal battalion also provides signal support and staff assistance to plan and control division communications, automation, visual information, and information systems.

4-13. The division signal battalion headquarters conducts management and control in a stand-alone division MSE network. Within these headquarters, SYSCON conducts MSE network planning and operation. SYSCON maintains technical control of the network and–

- Plans, engineers, controls, and maintains the network.
- Assigns and reassigns variable network operating parameters.
- Distributes all operating parameters networkwide.
- Establishes relationships among network components.

BRIGADE

4-14. At corps/division, the G6 provides the supporting signal brigade the network requirements needed to support the corps/division commanders' intent. The S6 at brigade provides his network/communications requirements to the division G6. The S6 at battalion provides his network/communications requirements to the brigade S6.

4-15. The SCC-2 assists in managing, operating, and maintaining the command's communications and information systems. The deputy G6 and S6 provide assistance where needed to establish and maintain communications connectivity. The deputy G6 and/or S6 are responsible to the commander for connectivity to the WAN and for the operation of the TOC LAN. However, the commander is ultimately responsible for managing and operating the network.

4-16. The corps/division G6 and the deputy G6 use the SCC-2 to manage, operate, and maintain C2 of the network. The deputy G6 is responsible for all information systems in the division TOC LAN. He also monitors the TI at ECB.

4-17. The brigade/battalion S6 uses the SCC-2 to manage, operate, and maintain C2 of the information systems. The S6 is responsible for all information systems in his TOC LAN. The S6 manages, operates, and maintains the TI.

INFORMATION MANAGEMENT

4-18. ABCS, which works primarily at the SECRET classification level, poses both technical and tactical challenges. Technically, the ABCS network functions as a seamless network with redundant paths. Data flow among computers does not require intensive user action. However, tactically, understanding and interacting with the information received is a user requirement. The information systems architecture covers the entire battlefield.

4-19. Information systems management consists of prioritizing information in a limited communications environment. The automated and manual information systems use and manage information for timely and accurate decision making in any operation. The battle staffs use information systems that give the commander the desired information at the right time and place. The G6/S6 must approve all public domain, shareware, or other privately purchased software IAW AR 380-19.

4-20. Each information system will have an identified and authorized set of executable software, which will be protected from unauthorized modification. The software will be safeguarded and never used for actual production operations. Only personnel performing official system administration duties will be allowed access to this software. The G6/S6 approves all software on each information system connected to the unit's TOC LAN.

TI AT BRIGADE AND BELOW

4-21. The TI at brigade and below provides a more responsive information exchange capability supporting the battle command. The TI consists of FBCB2 computers, EPLRS, SINCGARS System Improvement Program (SIP), and other supporting communications equipment. Figure 4-3 shows TI employment at brigade and below.

4-22. The TI primarily supports brigade and below echelons. However, the division signal battalion planning and operation elements still play key roles in successfully operating the TI. A close working relationship must exist between the corps and division deputy G6s and the brigade and battalion S6s to ensure the satisfaction of user requirements and the proper allocation of communication resources. Since the TI links to ABCS, the G6 must ensure proper LAN management within the division TOCs and tactical CPs. The G6 ensures the ACUS provides an adequate WAN to support the TI information flow, via MSE.

4-23. The brigade S6 plans, monitors, and changes the TI to support the brigade's scheme of maneuver. For successful brigade communications, the S6 maintains continuous dialogue with the signal officers of the battalions assigned to the brigade. The brigade S6 staff section supports the planning, engineering, integration, and maintenance of the TI and all other communications systems. The S6 staff section has a signal support platoon which has the S6 vehicle that supports the maneuver brigade and battalion TOCs.

4-24. The battalion S6 is the staff signal expert supporting the battalion commander. In this role, the S6 advises the commander and other staff members on all signal support matters. He coordinates with the brigade S6 for exchanging communications information and assets, as required. He interacts primarily with the S3, and he takes a proactive part in the staff planning and operations process. He organizes, trains, and controls the brigade S6 section.

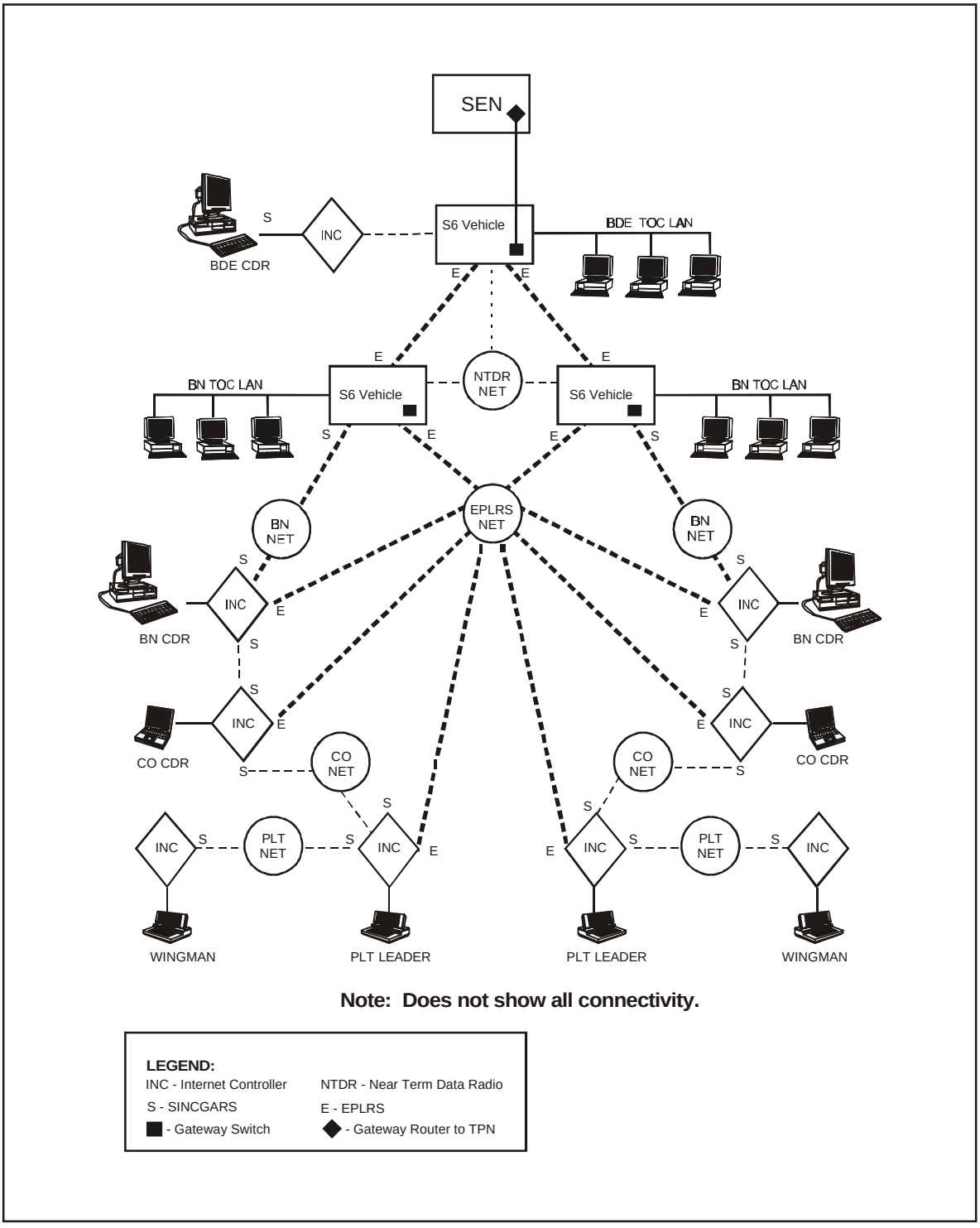

Figure 4-3. TI at Brigade and Below

4-25. The S6 signal office executes the network plan and initializes and operates the network. The radio operator-maintainer establishes the site for the S6 vehicle, and he installs, operates, and maintains the radio systems within the S6 vehicle.

4-26. The unit signal support system specialists perform system maintenance and TI system initialization and/or reinitialization functions. They also evacuate all defective digital devices to DS maintenance for replacement or repair. (See Appendix D.)

4-27. The SA/NA is also the TI manager at brigade and below. He supports all information systems and synchronizes information needed for successful battle command execution. The SA/NA is responsible for installing, operating, and maintaining the TOC LAN. This includes monitoring, controlling, troubleshooting, and reconfiguring LAN assets within the TOC. He also assists the mission applications administrator.

4-28. The mission applications administrator installs, operates, and maintains his information system. Each BFA will assign a mission applications administrator.

4-29. The G6/S6 vehicle is a mobile platform (S-250 shelter) on a high mobility multipurpose-wheeled vehicle (HMMWV). It contains the facilities for network planning, configuration, and management of the TI. It also serves as the integration platform that interfaces the TI with the MSE-based ACUS.

4-30. The TOC locations at brigade and battalion levels use the S6 vehicle to manage and interface the TI with ABCS, FBCB2, and ACUS. The major components of the S6 vehicle include–

- FBCB2 host running Solaris with ISYSCON(V)4.
- SINCGARS SIP with Internet controller (INC).
- X.25 interface to the MSE TPN.
- NTDR interfaces and TOC and tactical CP LANs.
- EPLRS.
- SunSPARC 20 workstation hosting the network management tool (brigade and below) (NMT(B2)) software.

4-31. The G6 vehicle uses the NMT(B2) software to plan, configure, monitor, and manage the TI. Thus, the division's G6 can track TI effectiveness in supporting the battle command information flow between the TI and ABCS.

4-32. The G6/S6 vehicle components can receive and send out position/ navigational data. It is deployed to support TOC and tactical CP locations throughout the battlespace, based on METT-TC.

Chapter 5

Command and Control Protect

The user is responsible for protecting his information system and its data. By failing to implement the correct C2 protect (C2P) measures, the user can experience data loss, hardware or software damage, and compromise of data. Any or all of these can result in the degradation of mission capability or the incapacity to support the mission. This chapter covers the procedures in protecting our systems. We must understand our system's vulnerabilities and what we must do to obtain assistance in protecting, detecting, and reacting to an intrusion or security violation.

THREAT

5-1. When deployed, information systems are subject to the same threats encountered in garrison. However, some of these threats are easier to exploit because of the deployed environment. Familiarization with the following terms is essential in understanding our systems' vulnerabilities.

INTENTIONAL

5-2. This threat is a deliberate attack on a computer system's resources or its ability to process. Insider threats are still the most serious while deployed because of greater access and knowledge of system assets and safeguards. However, threats from outside increase while deployed because of closer proximity and increased vulnerability.

UNINTENTIONAL

5-3. This threat results from an accident or procedural failure. The unintentional threat could increase while deployed because of longer and higher stress levels, different working environments, or poor training.

STRUCTURAL

5-4. This threat results from flaws in the construction of the physical environment, the physical configuration, or the system or application software. While deployed, computers often will not be operated in an office environment; rather, they will be operating in tents, vans, or other uncontrolled environmental facilities.

NATURAL

5-5. This threat can result from the locale or mode of operations. A varying degree of natural threats such as earthquakes, flood, dust, temperature, and humidity vary greatly between locations and must be considered.

ATTACKS

5-6. Some attacks against information systems can have a delayed effect and others are immediate. These attacks can corrupt databases, control programs, and degrade or physically destroy information systems.

COMPUTER

5-7. These attacks are aimed at software and data contained in individual computers or against computers connected to a network. Protecting information systems has become an important and everyday task. SAs/NAs must be trained in all aspects of information systems security (ISS). They must maintain and protect information systems and their networks. The SA/NA coordinates with the ISSO and reviews audit information for detecting system abuse.

PHYSICAL

5-8. These usually involve destruction, damage, overrun, or capture of the physical components.

THEFT

5-9. This is a physical attack that does not involve destruction or damage. However, theft of items, such as cryptographic keys and/or passwords, is of a particular concern. These items could support subsequent electronic or computer attacks.

ELECTRONIC

5-10. These attacks focus on specific or multiple targets within a specified area. Jamming, signal intercept, emitter direction finding, and geolocation can degrade communications.

HIGH ENERGY

5-11. High-energy attacks are electromagnetic pulses that destroy or damage electronic devices.

C2P MEASURES

5-12. C2P can be offensive or defensive. Offensive C2P measures use the five elements of C2 warfare to reduce the adversary's ability to conduct C2 attacks. These elements are–

- Operations security (OPSEC).
- Military deception.
- Psychological operations.
- Electronic warfare.
- Physical destruction.

Defensive C2P measures reduce friendly C2 vulnerabilities from adversary C2 attack by using adequate physical, electronic, and intelligence protection. FM 100-6 further explains the elements of C2 warfare, C2 attack, and information warfare affecting information operations.

SHARED C2P-NSM RESPONSIBILITIES

5-13. Command and control protect-network security management (C2P-NSM) encompasses those measures taken to maintain effective C2 of our forces. The goal of C2P-NSM is to integrate signal operations, technical engineering, security disciplines, and intelligence (or counterintelligence) support to ensure the availability, integrity, and confidentiality of information. The C2P-NSM strategy addresses protect, detect, and react measures. Figure 5-1 shows the shared and overlapping C2P-NSM responsibilities.

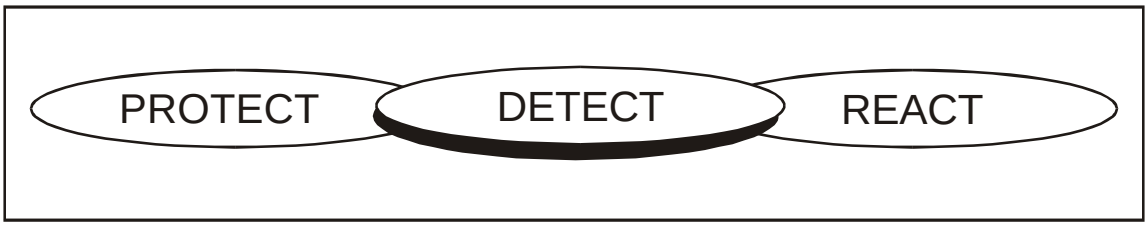

Figure 5-1. Shared C2P-NSM Responsibilities

PROTECT

5-14. Everyone must protect the information network from malicious threats. These threats can intentionally unleash computer viruses, trigger future attacks, or install software programs that compromise or damage data and systems. Users who are inexperienced or untrained that cannot identify security violations are jeopardizing their systems and networks which are vulnerable to all attacks. A comprehensive training program must be a part of the unit's training.

5-15. Information systems users must be trained to identify and to protect the system against intrusions. The most common intrusions include–

- Unauthorized users (hackers).
- Insiders (individuals with legitimate access).
- Terrorists (organized groups threatening national security).
- Nonstate groups (drug cartels and social activists).
- Foreign intelligence services.
- Opposing militaries or political opponents.

C2 Strategy

5-16. The Network Security Improvement Program is the primary plan for enhancing the overall network and systems security posture for the Army. This is a protection plan for all C2/information systems. Figure 5-2 gives an example of a typical network security plan.

5-17. **External Digital Perimeters.** These perimeters consist of COMSEC, firewalls, and security guards, and, where necessary, physical isolation which serves as a barrier to outside networks such as the Nonclassified Internet Protocol Router Network (NIPRNET).

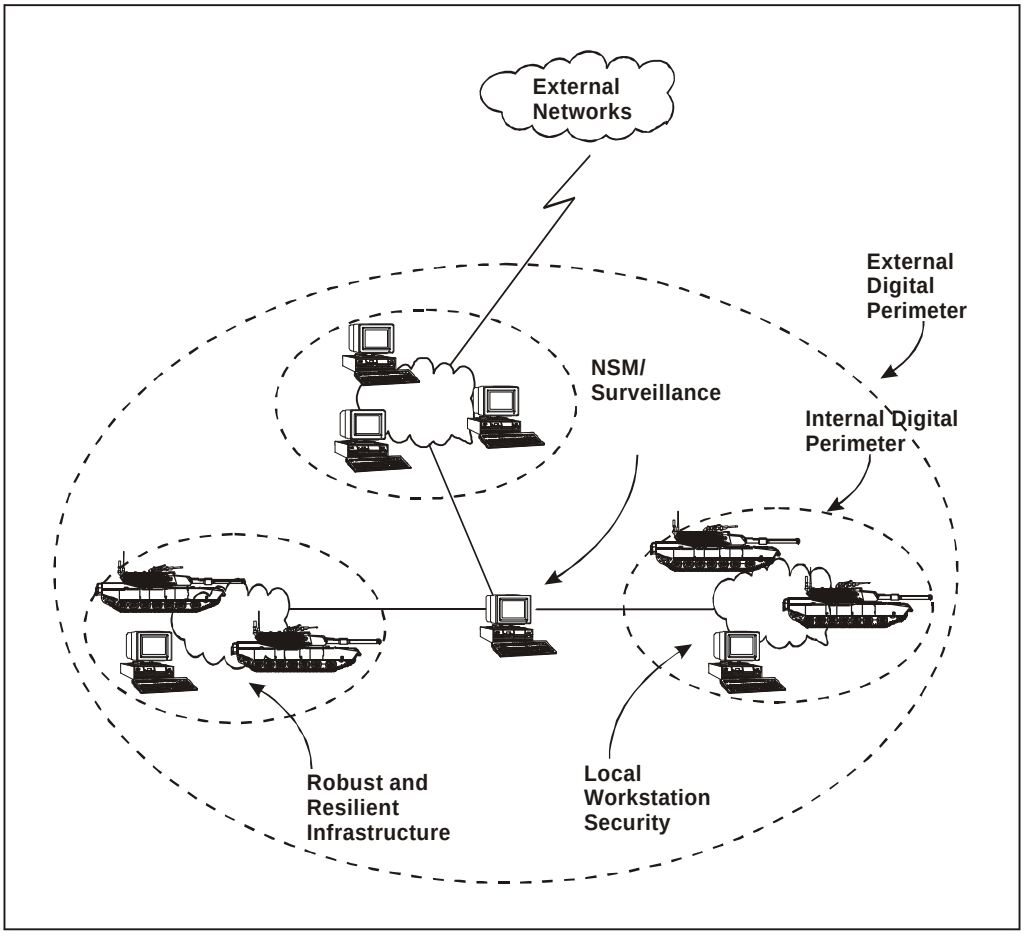

Figure 5-2. Example of a Typical Security Network Plan

5-18. **Internal Digital Perimeters.** These perimeters consist of firewalls and/or router filtering that serve as barriers between echelons and/or functional communities. Internal barriers may also use COMSEC and guards.

5-19. **Local Workstation Security.** It consists of individual access controls, configuration audit capability, C2P tools, and procedures.

5-20. **NSM and/or Surveillance.** They provide real-time network surveillance and reaction to network intrusions.

5-21. **Robust and Resilient Infrastructure.** This infrastructure can contain the damage from attacks and is readily repairable if attacked.

DETECT

5-22. C2P-NSM facilities can detect security policy violations. Selected events or occurrences (such as numerous log-in attempts within a specified period) are monitored using conventional and C2P tools. Two violations of security policies are integrity and operational.

- Integrity violations indicate potential interruptions in information flow (such as illegally modified, inserted, or deleted information).
- Operational violations indicate a requested service is unavailable, malfunctioned, or an invocation of service.

REACT

5-23. Certain events will alert users and/or managers of possible internal or external intrusions. Users must be able to detect an intrusion and react accordingly to correct the problem. This includes operating during periods of degraded operations due to hostile attacks. The users and/or managers must–

- Report the incident to their immediate supervisor and/or ISSO.
- Follow the incident security network policy as outlined in the unit SOP and other applicable security regulations.
- Restore destroyed and/or compromised data (from backups).
- Report the incident to other activities, as required.

5-24. Appropriate reactive measures are taken when problems occur. Security management encompasses the means to alert the network and/or system manager when detecting intrusion attempts. The network and/or system managers react to intrusions by–

- Changing boundaries/perimeters.
- Reconfiguring firewalls, guards, and routers.
- Rerouting traffic.
- Changing the level of encryption or rekey.
- Zeroizing communications that are suspected of being compromised.
- Reestablishing a net with selected members.
- Changing authentication/passwords.

TOOLS

5-25. Software and hardware tools help network and security managers to prevent, detect, and monitor intrusions. These tools change constantly as technology continues to improve. The current list of approved network tools is available through the Office, Director of Information Systems for Command, Control, Communications, and Computers and distributed to subordinate activities. The G6/S6/ISSO representative has the list for the latest approved C2P-NSM tools.

5-26. C2P-NSM tools–

- Audit monitoring and intrusion detection systems.
- Isolate systems under attack by automated infrastructure management.
- Detect malicious code and eradicate systems.
- Analyze and assess vulnerability.

5-27. C2P tools with or embedded within the information systems to protect against external and internal hackers and virus attacks include–

- Antivirus software.
- Hard disk purge capability.
- Network mapping software.
- Audit profile software.
- Intrusion detection system.
- Secure password generation systems.
- In-line network encryption devices.
- Firewalls, high-assurance guards, and tactical security guards.
- Encryption key management systems.
- Security posture of systems and networks.

DUTIES AND RESPONSIBILITIES

5-28. The Army C2P-NSM program management plan and AR 380-19 requires a clearly defined structure of ISS personnel. (See Appendix A.)

INFORMATION SYSTEMS SECURITY PROGRAM MANAGER (ISSPM)

5-29. The program executive officer for the command, control, and communications system is the ISSPM and is responsible for–

- Developing the security architecture.
- Coordinating and reviewing operational concepts, SOPs, and security accreditation for C2 systems.
- Ensuring certifications of individual systems are completed.
- Ensuring transient electromagnetic pulse emanations standard (TEMPEST) certifications of individual systems are IAW AR 381-14.

INFORMATION SYSTEMS SECURITY MANAGERS (ISSM)

5-30. Individual program managers or battle lab sponsors for Task Force XXI Systems perform ISSM functions. ISSMs–

- Develop the systems operational concept, security SOP, and security accreditation. These are submitted through the ISSPM for review and to the designated accreditation authority (DAA) for approval.
- Conduct individual systems risk assessment for operating their systems.
- Conduct system-specific security training and awareness programs.

INTELLIGENCE OFFICER

5-31. The brigade intelligence officer (S2) is responsible for identifying and assessing foreign intelligence threats to command assets. The S2–

- Administers the Personnel Security Program IAW AR 380-67.
- Ensures the Command Statement of Intelligence Interest (AR 381-19) registers the receipt of validated intelligence impacting on the integrity and reliability of the network.
- Assists in identifying threat factors.
- Coordinates with the national intelligence agencies.
- Evaluates C2P-NSM incidents and implements reporting procedures.

ISSO

5-32. The G6/S6 is responsible for secure operations of the information systems. Therefore, the G6/S6 oversees the functions of the ISSO.

5-33. The automation officer and/or systems integration technician in the G6/S6 signal office normally serves as the ISSO. He–

- Prepares, distributes, and maintains plans, instructions, guidance, and SOPs for C2 systems security.
- Ensures all systems have approved accreditation (operational or generic) to operate at the SECRET level in the systems high mode of operation IAW AR 380-19.
- Coordinates with the brigade S2 to ensure users have the required security investigations, clearances, authorizations, and the need-to-know.
- Establishes and implements a system for issuing, protecting, and changing system passwords.
- Implements ISS training and awareness and incorporates this training into the overall unit security and training programs.
- Monitors, reviews, and evaluates the security impact of changes and coordinates this with the ISSM.
- Directs threat and vulnerability assessments to help the commander properly analyze the risks to the information systems and interconnected systems.

USER

5-34. The user is responsible for terminal security and must–

- Secure operations of the systems.
- Operate terminals IAW appropriate procedures and local SOPs.
- Perform other duties as assigned by the ISSO, SA/NA, and the mission applications administrator.

PASSWORD CONTROL

5-35. Passwords for processing classified or unclassified material over information systems must be randomly generated. Passwords must have at least an 8-character string using the 36 alphanumeric characters with at least 2 of the characters being numeric. The ISSO or designated representative generates, issues, and controls all passwords IAW the following guidelines:

- Users will not have any control over choosing their passwords.
- Passwords are handled and stored as the most sensitive data contained in the system.
- Knowledge of individual passwords will be limited to a need-to-know basis.
- Passwords will not be shared.
- Passwords will be issued only if the user has authorization to access the system.

5-36. Individual users will be briefed on–

- Password classification and exclusiveness.
- Measures to safeguard classified and unclassified passwords.
- Prohibitions against disclosure to unauthorized personnel.
- Immediate reporting of password disclosure or misuse.

5-37. Passwords are issued only once and are retired when the time limit has expired or the user has been transferred. Passwords, as unique identifiers of individual authority and privilege, **WILL NOT** pass between individuals, even if those individuals are employed on the same project.

5-38. All passwords on classified systems are changed at least quarterly. Passwords on nonsensitive and sensitive but unclassified systems will be changed semiannually.

5-39. Passwords are inhibited, overprinted, or otherwise protected from unauthorized observation on terminals and video displays.

COMSEC

5-40. The G6/S6 has overall COMSEC responsibility. Table 5-1 outlines various COMSEC systems to protect C2 data.

Table 5-1. COMSEC Systems

System Type	Key Source/Classification	Controlling Authority/POC
SINCGARS	Electronically Generated/SECRET	G6
EPLRS	Electronically Generated/SECRET	G6
GBS/BADD KG-194	TBD/TBD	NSA
NTDR	TBD	G6 COMSEC Office
TRI-TAC/MSE	Tape Generated/TBD	NSA/Signal Battalion
Wireless LAN	TBD	TBD

INCIDENT REPORTING

5-41. The user/ISSO will log and report all violations and insecurities as shown in Table 5-2. To facilitate detection and investigation of security breaches, all devices require reporting to an audit manager or providing an audit trail. The G6/S6 evaluate local and remote incidents and report to the brigade systems integrator for evaluation and investigation, if warranted. The brigade automation officer evaluates and/or investigates security breaches, coordinates recovery actions, and assists the brigade intelligence officer in preparing reports.

Table 5-2. C2P-NSM Incident Reporting (Internal to Brigade)[1]

Incident	Precedence	Action	Information
Copyright Violation	Routine	user>ISSO	S2/S3/S6
Virus Detection	Priority	user>ISSO	S2/S3/S6
Intrusion (internal)	Immediate	user>ISSO	S2/S3/S6
Intrusion (external)	Immediate	user>ISSO	S2/S3/S6
Malicious Code	Priority	user>ISSO	S2/S3/S6
Unauthorized Monitoring	Priority	user>ISSO	S2/S3/S6
Compromise	Priority	user>ISSO	S2/S3/S6

[1] The commander will determine external brigade reporting based on staff evaluation.

EMERGENCY PROCEDURES

5-42. Procedures for protecting our networks from being compromised are carried out only after directed to do so, or under extreme emergencies. These emergencies are normally covered in the unit SOP. Methods for denying access to sensitive and to classified systems are–

- Zeroize COMSEC devices.
- Purge systems.
- Destroy classified systems, **when capture is imminent.**

Appendix A

Network Security Management
(Sample Security SOP)

This appendix provides a sample security SOP. It gives examples of specific guidance and procedures for ISS personnel in establishing their unit's SOP. Its intent is to provide minimum security for operating at the SECRET level in the systems high mode of operation. In this mode, all users must have a SECRET security clearance. C2 systems will be accredited to process and store SECRET data. The security guidelines and procedures for all information systems should be distributed through the chain of command down to the user level. Information systems include ABCS, Army Tactical Command and Control System (ATCCS), COTS, and components connected to the network. These guidelines and procedures may be incorporated, when appropriate, into existing unit SOPs. It should apply to all units and to all elements assigned, attached, or under the operational control of the issuing headquarters. The OPLANs and OPORDs should note the exceptions to the established SOP. This SOP applies to information systems and their components.

ISS POSITIONS

A-1. Commanders should select personnel for ISS positions who can provide assistance in implementing security procedures. These personnel must have the authority to enforce security policies, to include shutting down information systems if warranted by the seriousness of a security incident. Personnel selected should serve as the commander's focal point for all network security matters.

COMMANDERS

A-2. Commanders have the overall responsibility for network security. They will–

- Operate systems within their command IAW AR 380-19 and unit SOPs.
- Appoint an ISSM.
- Establish reasonable procedures to protect information systems and data from compromise, theft, or damage.
- Include ISS in the unit's training program.
- Use information systems for their intended purpose.
- Incorporate information systems requirements into unit contingency planning.

ISSM

A-3. At all levels of command, an ISSM is appointed to establish and implement the ISS program. These ISSMs are normally the deputy G6 and/or S6, and they –

- Develop the systems operational concept, security SOP, and security accreditation.
- Conduct individual systems risk assessment for operating their information systems.
- Conduct system-specific security training and awareness programs.

INTELLIGENCE OFFICER

A-4. The brigade intelligence officer (S2) identifies and assesses foreign intelligence threats to command assets. The S2–

- Administers the Personnel Security Program IAW AR 380-67.
- Ensures the Command Statement of Intelligence Interest registers the receipt of validated intelligence impacting on the integrity and reliability of the network (AR 381-19).
- Assists in identifying threat factors.
- Coordinates with national intelligence agencies.
- Evaluates security incidents and implements reporting procedures.

ISSO

A-5. The automation officer and/or systems integration technician in the G6/S6 signal office normally serve as the ISSO. He–

- Prepares, distributes, and maintains plans, instructions, guidance, and SOPs for C2 systems security.
- Ensures all systems have approved accreditation (operational or generic) to operate at the SECRET level in the systems high mode of operation IAW AR 380-19.
- Coordinates with the brigade S2 to ensure users have the required security investigations, clearances, authorizations, and the need-to-know.
- Establishes and implements a system for issuing, protecting, and changing system passwords.
- Implements ISS training and awareness and incorporates this training into the overall unit security and training programs.
- Monitors, reviews, and evaluates the security impact of changes and coordinates this with the ISSM.
- Directs threat and vulnerability assessments to help the commander properly analyze the risks to the information systems and interconnected systems.
- Provides guidance to ensure maximum protection against compromise and theft of sensitive information and prevents the misuse or misappropriation of information systems.

- Maintains an accurate inventory of all hardware and software throughout their units. Ensures this inventory is reconciled with the appropriate property book officer at least annually.
- Ensures the unit's contingency plans incorporate information systems requirements.
- Conducts periodic inspections and reviews to ensure compliance with this SOP and other policies in operations and security.
- Suspends operations partially or completely upon detection of actions that may affect security.
- Oversees the review of system audit trails and investigates thoroughly any security violations. Ensures audit trails are reviewed at least weekly and audit files are backed up.
- Ensures information systems or workstations are operated, maintained, and secured IAW AR 380-19 and unit SOP.
- Immediately reports any attempt to gain unauthorized access to sensitive defense information, any system failure, or any suspected defect that could lead to unauthorized disclosure. Also advises the S2 and/or security manager of security incidents or violations.
- Performs ISSO duties as prescribed in AR 380-19.

NETWORK SECURITY OFFICER (NSO)

A-6. The NSO ensures the secure interconnection of information systems on the LAN. The NSO–

- Controls LAN access.
- Monitors assigned LANs to ensure systems comply with security policies and applicable directives.
- Assists the ISSO in preparing, distributing, and maintaining security SOPs IAW AR 380-19.
- Conducts risk assessment reviews with the ISSO, ISSM, and functional proponent.
- Assists the ISSO in evaluating the security impact of changes to the network, including interfaces with other networks.
- Coordinates and monitors periodic security indoctrination and training sessions for assigned personnel.
- Ensures audit trails and other system management reports are reviewed for internal security audits or testing.
- Ensures information systems are operated, maintained, and safeguarded IAW AR 380-5, AR 380-19, and the SOP.
- Conducts specific security training for users, as required.
- Reports to the ISSO any attempt to gain unauthorized access to sensitive defense information, any system failure, or any suspected defect that could lead to unauthorized disclosure.
- Maintains a current access roster of persons with authorized access to all systems.

- Ensures users are aware of the requirement to verify security clearances before granting access privileges to information systems.
- Provides positive control of the information systems within the user's area of responsibility.
- Prevents unauthorized tampering of hardware or software.

SECURITY MANAGERS

A-7. Unit security managers are responsible for the information security programs within their organizations, and they directly support ISS personnel in executing security policies and procedures. Security managers–

- Are responsible for information (documents), personnel, and physical security.
- Ensure all personnel who use or have access to information systems have been screened IAW AR 380-67 and have a SECRET security clearance, as a minimum.
- Implement security directives in managing classified information.
- Act as the staff focal point for security issues.
- Distribute changes to policies and similar security-related information to the ISSOs.
- Process applicants for security clearances, verify security clearance status for users, and support personnel within their units.
- Prepare security clearance access rosters for the ISSOs.
- Establish annual security training programs for persons having continued access to classified information.
- Conduct security-related inspections throughout their units for compliance with security standards.

COMSEC CUSTODIANS

A-8. The commander appoints the COMSEC custodian. He is responsible for access and control of accountable COMSEC material. Information systems do not require any new or unique COMSEC material or controlled cryptographic items (CCIs). The COMSEC custodian–

- Incorporates procedures for operating, handling, and securing COMSEC material into local COMSEC procedures currently in effect, including periodic inspections.
- Trains users on handling, using, and safeguarding COMSEC material, including key lists and CCIs.
- Maintains accountability of all CCIs.

MISSION APPLICATIONS USER

A-9. The mission applications user–

- Complies with the security requirements in this SOP and applies directives for safe and secure operation.
- Has a SECRET security clearance, need-to-know, and training.

- Maintains positive physical control of information systems, as a high dollar value item, within their area of responsibility.
- Secures the system IAW AR 380-19 as SECRET material is processed and stored on its hard disks or floppy disks.
- Reports to the SA/NA or ISSO any security violation, attempts to gain unauthorized access to sensitive defense information, any system failure, or any suspected defect.

SECURITY REVIEW

A-10. Secure operation of information systems requires constant vigilance and attention in an ever-changing environment. Command and managerial personnel must periodically reassess the risks their specific operating environments present to the security of information systems. To assist in conducting a security review, the following subparagraphs focus on specific areas that should be reevaluated on a regular basis.

COMPLYING WITH THE GENERIC ACCREDITATION

A-11. Information systems will process classified information at the SECRET level. Commanders and ISS personnel are responsible for meeting the minimum-security requirements of the generic accreditation IAW AR 380-19. Commanders and ISS personnel can use a security checklist to determine if their unit is complying with the generic accreditation. (See Table A-1 at the end of this appendix.)

RISK MANAGEMENT

A-12. The entire ISS staff shares the responsibility for properly operating information systems. Each BFA is responsible for conducting threat and vulnerability assessments and reviews to help commanders assess the risks. These assessments and reviews are an essential part of the risk management process. Local commanders and ISS personnel need to consider the security environment in garrison, tactical situations, and all operating environments. Deployable information systems must be accredited to operate in a deployed environment. A risk analysis of the system will determine the environment in which the system will operate. Since conditions, including the environment and threat, change as computer systems deploy, the following factors must be considered for deployment.

Sensitivity

A-13. Sensitivity relates to the information being processed in a deployed situation, the classification level of equipment or information may increase based on the mission it supports. It should be possible to predict increased sensitivity before deployment by studying intelligence assessments and OPORDs the organization is tasked to support.

Criticality

A-14. Criticality relates to the mission the system supports or the degree in which the mission depends on the system. Criticality normally increases during deployment because of support to higher level commands and operational mission requirements. The user must determine what effect loss or alteration of the system or data would have on other systems and missions.

Password Management

A-15. The ISSO manages passwords used for access control as specified in AR 380-19. Users will not have any control over choosing their password. If passwords are used to determine need-to-know, classify them at the highest level of information that can be accessed; otherwise, protect as For Official Use Only (FOUO).

Physical Security

A-16. Physical security requirements usually increase as the sensitivity, criticality, and threats increase. The ISSO must access the increased sensitivity, criticality, and threat, then determine appropriate security measures. Physical security is an important part of the overall computer security plan during deployed operations. It includes controlling access to the computers and establishing a secure perimeter for the deployed site.

TEMPEST

A-17. The ISSO must carefully review TEMPEST requirements for deployed operations. Systems deployed to a hostile threat area may require increased TEMPEST countermeasures to meet the requirements of a countermeasure assessment. Coordination with the organization's TEMPEST officer is essential before and during a deployment to determine TEMPEST requirements.

Emergency Destruction

A-18. Deployment to medium or high threat areas dictates developing emergency destruction procedures for software, firmware, magnetic media, hardware, and hard copy output. The ISSO must consider equipment used, information processed, and anticipated time available for destruction to develop the best destruction method.

Risk Analysis

A-19. Deployable systems require a risk analysis package. The ISSO conducts a risk analysis of the system to describe a baseline environment. This environment should describe the minimum protection required for each state of operation. The security features of the system must satisfy the security requirements for the most restrictive environment. The ISSO performs an informal risk analysis at each deployed site to determine unique or additional protection.

Plans

A-20. The ISSO should help to develop plans for deployable information systems. These plans must address unique deployed operating conditions, such as temperature and humidity variations, power fluctuations, and dust. Plans needed for deployment include a security plan and the continuity of operations plan (COOP). The COOP should include emergency destruction and declassification procedures, backup procedures, alternate power sources, partial or degraded systems operation, and approved methods of disposal. The security plan should include a description of the baseline environment, additional safeguards for varying threats, and minimum operating conditions.

Backup Requirements

A-21. The ISSO investigates and documents system requirements for a possible hostile and stressful environment. System requirements will vary with different deployments and information systems. The ISSO must consider the task being automated, the mission criticality, and the deployed environment. He must also consider human factors if a manual backup is expected. Procedures for operating the manual and automated system should be similar, so transitions can occur quickly from the automated to the manual mode.

REVIEW OF SECURITY VIOLATIONS

A-22. A review of security violations must occur on a regular basis. The review will include all previous violations. The reviewer attempts to determine if any trends or patterns can be identified which may be of concern. The results of this analysis shall be incorporated into the risk management program and also be factored into the security training program assessment.

ASSESSING THE SECURITY TRAINING PROGRAMS

A-23. Security training programs should be evaluated periodically IAW AR 380-19. A successful training program must emphasize security fundamentals and contemporary security issues related directly to information systems. Both the initial security training program and the recurring training program should be revised to reflect the ongoing risk management effort and security violations review. The training program will also be reviewed and revised following the reaccreditation of information systems.

OPSEC

A-24. OPSEC procedures are based on the need to deny the enemy information about friendly capabilities and intentions. Commanders–

- Implement OPSEC procedures in this SOP.
- Comply with existing unit OPSEC procedures and related security procedures addressed in this SOP.

PHYSICAL SECURITY

A-25. Hardware, software, documentation, and data will be protected to prevent unauthorized disclosure, destruction, denial of service, or modification. Physical security is one of the principal means used to protect against these threats. AR 190-13 and FM 19-30 provide specific guidance on physical security requirements. Physical security at each site is based on an analysis of regulatory requirements, mission criticality, sensitivity levels of the information being processed, security threats, and the vulnerability of information systems to the security threats.

STORAGE AND SHIPMENT

A-26. The user must purge all information systems components IAW applicable technical manuals before shipping or storage. The user will remove all classified material and store it in a General Services Administration (GSA)-approved security container.

A-27. Requirements for protection can increase during storage or shipment due to increased vulnerability. Increased threat and vulnerability considerations include special handling requirements during shipment. Considerations include whether the system components would ever be out of US control at any time during shipment, and if stored, what protection is provided at the storage location.

A-28. After all removable classified media is removed and nonremovable media is purged, information systems must be provided double barrier protection. Information systems components will normally be stored in locked military vehicles or communications shelters within a locked building or fenced motor pool.

A-29. The storage locations of information systems equipment are included on the staff duty officer or charge of quarters security checklists.

ADMINISTRATIVE MOVEMENT

A-30. Before any move, all information systems components must be accounted for and placed in a proper configuration for movement IAW applicable technical manuals. During administrative movements, if classified material is resident on information systems components, an authorized individual must guard them.

A-31. If transported by unauthorized personnel, the CCIs must be provided double barrier protection during transportation. This can be accomplished by securing the components to the shelter with a locking cable, then locking the shelter, or by dismounting the component and storing it in a separate locked container in the locked shelter.

A-32. After the move, all components must be accounted for.

TACTICAL MOVEMENT

A-33. Before any move, all information systems components must be accounted for and placed in a proper configuration for movement IAW applicable technical manuals.

A-34. During movement, information systems will be protected IAW the level of classified information stored in them. Personnel will execute emergency destruction plans when an ambush, enemy contact, or capture of information systems and components is imminent.

A-35. After completing the move, all information systems components must be accounted for.

GARRISON OPERATIONS

A-36. During garrison operations, information systems must be protected IAW the classification of the data and COMSEC key that is in use. When FOUO data and key material are used, the user can provide adequate security for the system. If classified data or key material is used, the site requires additional security measures of a secured perimeter and a guard limiting access to authorized personnel.

A-37. No personnel shall be granted access to information systems simply because they possess the requisite security clearance or because of their duty position. Commanders will determine whether a person's individual duties require access to information systems.

TACTICAL OPERATIONS

A-38. During tactical operations, information systems must be provided a secure site. Ideally, the site will have a perimeter fence and guards limiting access to authorized personnel. The minimum measure is an armed guard providing area security. System users must be aware of system security requirements at all times and provide at least the minimum security necessary. System users must enforce noise and light discipline in the site to minimize risk of compromise.

PERSONNEL SECURITY

A-39. Commanders, ISSOs, SAs/NAs, and users will enforce security procedures to limit access to unauthorized personnel.

A-40. Users will maintain positive control of information systems at all times. This includes restricting unauthorized personnel from observing the system's screen.

A-41. SAs/NAs and users will use access rosters and physical recognition to authorize access to information systems by other individuals.

MINIMUM CLEARANCE

A-42. All personnel operating C2/information systems WILL have a minimum of a SECRET security clearance.

NEED-TO-KNOW

A-43. The number of personnel cleared and granted access to the C2 networks will be kept to a minimum. No personnel will be granted access simply because they possess the requisite security clearance or because of their duty position. Commanders will determine whether a person's individual duties require access to the C2 network. Only authorized personnel should have access to the immediate areas where computers are operating.

A-44. Users will only have access to the information required to perform their assigned tasks, regardless of the user's security clearance. All commanders, assisted by their ISSOs, shall determine the maximum information access requirements of each user.

INITIAL TRAINING

A-45. All users are given initial security training. This training covers–

- Threats, vulnerabilities, and risks associated with the system.
- Reducing threats from malicious software.
- Prohibiting unauthorized software.
- Reducing the need for frequent backups.
- Reporting abnormal program behavior immediately.
- Information security objectives (what needs to be protected and why).
- Responsibilities associated with the system security.
- Information accessibility, handling, and storage considerations.
- Physical and environmental considerations necessary to protect the system.
- System data and access controls.
- Emergency and disaster plans.
- Authorized system configuration and associated configuration management requirements.

Ongoing Training

A-46. Security personnel will provide sustainment security training to users. Refresher training is conducted as needed. These updates should focus not only on those areas addressed in the initial security training, but also those areas that are discovered to be security risks based on the local risk assessment. Specific areas include–

- A review of security violations.
- New threats and associated countermeasures.
- Continuity of operations.
- Changes to security requirements.

A-47. All users, supervisors, and other personnel are trained to detect unauthorized or nonsecure procedures. Any person who detects or witnesses an unauthorized or nonsecure act will immediately notify the appropriate security personnel. This is true regardless of the rank of the person performing the nonsecure or unauthorized act or the rank of the person detecting the nonsecure or unauthorized act.

MAINTENANCE PERSONNEL

A-48. Maintenance personnel must be cleared to the highest classification level of data processed on the system. If this is not feasible, an individual with the required clearance and technical expertise will observe the maintenance personnel.

A-49. SAs/NAs will verify the security clearances of maintenance personnel before granting them access. The ISSO and the unit security manager will be notified BEFORE uncleared maintenance personnel are granted access or inadvertently gain access to classified information.

A-50. If components with classified information must be removed, the user will first purge the component. If the component cannot be purged, it will be stored in a GSA-approved security container until approved for release by the ISSO. Once cleared for release, maintenance personnel will be advised of the security classification and handling procedures of the classified material. Uncleared personnel will not remove classified components from the shelter.

INFORMATION SECURITY

A-51. Information security includes the measures taken to prevent disclosure, alteration, substitution, or destruction of data.

HANDLING CLASSIFIED MATERIAL AND INFORMATION

A-52. The guidelines for handling classified material and information are covered below.

A-53. All personnel will maintain positive control of all classified material for which they are responsible. Classified material will not be given to any individual who does not have the requisite security clearance and approved need-to-know.

A-54. Personnel carrying classified documents from the system's shelter to another location within the site perimeter must cover the material with a classified document cover sheet. Persons wishing to remove classified material from the site perimeter must wrap the material as directed by AR 380-5 and have DD Form 2501.

A-55. A system to provide accountability and control of classified material shall be established IAW AR 380-5. This system shall address creating, disseminating, and transferring classified information.

A-56. Handle and safeguard the printer ribbon IAW the classification of the material printed and AR 380-19.

MARKING PROCEDURES

A-57. All items being replaced or transported containing classified data will be marked IAW AR 380-19.

Removable Magnetic Media

A-58. All removable magnetic media shall bear external markings that clearly indicate the classification of the information.

A-59. SF 707 identifies removable media that contains information classified up to the SECRET level.

A-60. SF 710 identifies removable media that contains information that is unclassified.

A-61. SF 711 properly identifies the removable storage media. Use internal markings on files to indicate the classification and any special handling instructions. Mark in an obvious location all media used to store classified information. Mark the highest classification of data recorded on the media.

A-62. Personnel with a security clearance equal to or greater than the classification of the media shall only handle classified removable magnetic media.

Printed Material

A-63. C2 printer output will initially be controlled as SECRET material. As the operational situation permits, the material will be reviewed to determine the actual classification.

A-64. After manually reviewing printer output, it will be marked with the correct classification, classification source, and declassification date. As a reminder, this is not downgrading classified information, but only appropriately labeling.

Printer Ribbons and Toner Cartridges

A-65. Printer ribbons and toner cartridges will be marked with the same classification level as the material printed.

STORAGE PROCEDURES

A-66. All classified material will be stored in GSA-approved security containers when not in use by appropriately cleared personnel.

A-67. When one-drawer field safes are used to store classified material, the safe will be securely fastened to the shelter or guarded to prevent theft. Guards employed for this function only, and who do not otherwise have access to classified material, do not require a security clearance.

DESTROYING PRINTED MATERIAL

A-68. AR 380-5 provides guidance for destroying classified material associated with the TI. The secure-volume concept is the routine destruction of classified (paper) material originating from the printer. This concept stresses destroying at least 20 pieces of paper at a time. This results in an increased volume of residue. If necessary, add a sufficient number of unclassified pages to the classified document to arrive at the minimum 20-sheet page count.

A-69. If shredders are used for paper waste, ensure they are rated Class I (crosscut) or Class II (continuous strip).

A-70. When a shredder is not available, burning will destroy printed material. The fire must be carefully controlled to prevent burnt fragments that are still legible from being blown away. After all the material is burnt, wet and stir the ashes to destroy any legible burnt fragments.

A-71. Burning will destroy classified printer ribbons and floppy disks. When burning floppy disks, take precautions to avoid the toxic fumes that may be released.

A-72. Removing the platen and rollers and sanding the surfaces that contact the paper will destroy classified toner cartridges.

CLEARING, PURGING, DECLASSIFYING, AND DESTROYING ELECTRONIC AND MAGNETIC MEDIA

A-73. When information systems components are stored or left unattended, all classified information must be removed. Information systems components will have information stored in several locations.

A-74. The first is random access memory (RAM). RAM is very perishable and usually not accessible to the user once power has been removed. However, purge procedures addressed in this SOP must be followed to ensure classified data is removed.

A-75. The second location is components that have a permanent storage capability. The memory of these components is usually not affected by the removal of power. Procedures in this SOP must be followed to ensure classified data is properly protected.

A-76. Clearing of media means erasing or overwriting all information on the media, but without the totality and finality of purging. Removable media that has simply been cleared must continue to be controlled at their prior classification or sensitivity level.

A-77. Purging of media means to erase or overwrite totally and unequivocally any information stored on the media.

A-78. Declassifying of media refers to the administrative action taken after it has been purged. Declassify media for storage and shipment to reduce the amount of control and protection required. If the media contains classified software or data, copy it to removable media, if possible. If the ISSO cannot declassify the media, control and protect it as classified equipment.

A-79. Use overwrite procedures to purge classified data before storage or shipment. Once the data has been purged, the appropriate declassification authority must document the final decision to remove the classification from the media. Unless there is a hardware device that prohibits writing to the hard disk, classify and protect the hard disk at the highest classification processed until purged. Transferring classified information from hard disk to floppy, or deleting a file, does not purge the hard disk. It remains classified until purged. Information systems that have nonvolatile, non-removable semiconductor memory cannot be purged. If these systems have processed classified information, they must be protected as classified equipment.

Removable Hard Disk

A-80. Declassifying using the same procedures as with a fixed-hard disk.

Monitors

A-81. Inspect monitors for burned-in classified images on the screen before packing for deployment. If any part of the screen retains classified information, treat the monitor as classified and protect accordingly. Safeguard computer hardware while deployed to prevent alteration or damage to the equipment.

Hard Disks

A-82. Protect hard disks as classified if they are mounted on or are in systems that process classified information unless there is a hardware device that prohibits writing to the hard disk. Transfer of classified information from the hard disk to a floppy, or deleting a file, does not purge the hard disk. The disk is still classified and requires protection until purged.

RAM

A-83. The RAM of the FBCB2, tactical multinet gateway (TMG), NMT(B2), and NTDR RAM is considered classified. This RAM will be purged when the component has been properly powered down and all power has been removed. No additional on and/or off cycle is required. To purge the RAM from the printer, the user will turn the printer off, wait 60 seconds, turn the printer on, wait for its memory test to run, then turn it off.

Permanent Storage

A-84. Floppy diskettes cannot be purged. Due to their low cost, diskettes will be destroyed when no longer needed.

A-85. Using the C2P-NSM tools to overwrite every storage location on the disk will purge the FBCB2, NMT(B2), and lightweight computer unit (LCU) hard disks. Because some storage locations on disks with bad sectors cannot be overwritten, they cannot be purged; therefore, they must be treated and safeguarded as SECRET material. The system workstation hard and floppy disks must be removed from the workstation and stored in a GSA-approved security container or class B vault or guarded by an authorized individual. AR 380-5 contains specific storage sites for classified media.

A-86. The COMSEC key material stored in EPLRS with a very high-speed integrated circuit (EPLRS VHSIC) and the SINCGARS SIP equipment is cleared by using the zeroize key on the radio while the power is on.

COMPROMISE

A-87. Situations involving known or suspected loss of classified information will be investigated to determine their cause. Cost-effective corrective measures will be implemented to prevent recurrence.

A-88. Suspected or actual security incidents will be reported to the SA/NA and ISSO by the fastest means available.

A-89. Incidents that may signal the beginning or presence of a possible security incident include–

- Unexplained output received at a terminal or from a printer.
- Extraneous data.
- Abnormal system responses.
- Any indication of media manipulation, modification, or corruption of files and data.

A-90. The ISSO will report security incidents not directly attributed to administrative error (such as system penetration, malicious acts by an operator, and so on) within five days, through the chain of command, to the Commander, United States Army Intelligence and Security Command (INSCOM), ATTN: IAOPS-CI-TO, Fort Belvoir, VA 22060-5370.

EMERGENCY DESTRUCTION PROCEDURES

A-91. Every effort should be made to prevent loss or compromise of the data processed by automated equipment.

A-92. When C2 or information systems equipment is subject to imminent danger or capture, the following actions will take place:

- Zeroize COMSEC material and destroy SOI, authentication codebooks, and any other hard-copy classified material.
- Purge the system workstation computer RAM and printer.
- Destroy equipment in the following order:
  - COMSEC devices.
  - Hard disks.
  - Floppy disks.
  - AN/UYK-86 computer.
- Destroy all information systems components to deny the enemy any use of the information or equipment.

- Disassemble and destroy the hardware, as much as possible, and burn it using petroleum, oils, and lubricants. If tools are not available, thermite grenades will be ignited directly over equipment, as needed.
- Integrate the emergency destruction requirements into the unit's tactical SOP and overall priority of the unit's destruction plan.
- Conduct dry runs and/or practices on a periodic basis.

COMSEC

A-93. The quality of information shared on the network is everyone's responsibility beginning at the user level. COMSEC includes clearances and most importantly the need-to-know. The G6/S6 and the ISSO are responsible to the commander for COMSEC IAW AR 380-19.

COMSEC EQUIPMENT AND KEY LISTS

A-94. The equipment used in ABCS uses many concepts and systems for generating, distributing, and managing electronic COMSEC keys. ABCS ensures the integrity and security of communications up to the SECRET level. ABCS considers the security of COMSEC material used by existing training material and unit SOPs regarding COMSEC handling.

A-95. Access to classified COMSEC material may be granted to US citizens whose duties require access. Security clearance requirements for persons granted access is determined by the classification level of the material to be accessed.

A-96. The G6/S6 will ensure COMSEC is–

- Distributed and implemented on a timely basis.
- Properly reported when lost or compromised.
- Properly disposed of or destroyed.
- Documented after destruction.

ELECTRONIC EMANATIONS

A-97. Compromising emanations are unintentional intelligence-bearing signals. If intercepted or analyzed, these signals will disclose unclassified sensitive and classified information transmitted, received, handled, or otherwise processed by information systems. Users will–

- Maintain and operate information systems.
- Check terminal cables periodically to ensure connections are in place.
- Report and have repaired any damaged equipment.

LAN

A-98. Data transmissions over a LAN must be protected in the same manner as transmissions over a radio. If the entire LAN resides within the confines of a physical control zone (PCZ), unencrypted transmissions over the LAN are considered protected.

A-99. When a LAN does not reside entirely within a PCZ, the LAN must be made a protected distribution system (PDS). Commanders may approve a PDS in a tactical environment. Under battlefield conditions, commanders may delegate this authority to company commanders. AR 380-19 discusses the use of a PDS.

A-100. The G6/S6 will verify that all LAN cables are properly tagged IAW unit SOPs.

SOFTWARE SECURITY

A-101. Software security depends on the prompt identification and resolution of all software errors. All software errors, no matter how insignificant, shall be reported so they may be investigated and corrected.

SOFTWARE ERRORS

A-102. AR 380-19 requires that information systems software be rigorously tested before approved for use. Despite the extensive testing efforts made before fielding, some software errors will undoubtedly occur. These errors, which may compromise security, must be properly addressed to preserve the protection provided by the software suite.

A-103. All users are responsible for promptly reporting software errors and abnormal or unusual system responses to the SA/NA, ISSO, or other point of contact (POC) IAW with unit SOP.

A-104. The following guidelines will protect software during storage and shipment from loss, damage, or alteration.

- Classification of the software determines the protection required.
- Software is stored away from high-voltage and magnetic material.
- Ship classified software separate from hardware using an approved storage container.
- Software contains proper internal and external security markings.
- Software receives the same level of protection in deployed operations and the home environment.
- Backup copies will have the same level of protection as the original.

VIRUSES

A-105. Computer viruses are rarely distributed with authorized system software. However, personal software has a much higher probability of contamination since it is not as tightly controlled. Entertainment programs and programs on electronic bulletin boards are ideal carriers for viruses and Trojan horses, since they are frequently copied and widely distributed. Programs of this nature WILL NOT be loaded on the computers.

UNAUTHORIZED SOFTWARE

A-106. The delivered software, as identified in the ABCS generic accreditation, has been authorized for use on ABCS after extensive testing and evaluation. The authorized software suite is an integral part of the ABCS security plan. Users are encouraged to make full use of the features and capabilities provided in these programs to accomplish their assigned tasks to preclude unauthorized actions.

A-107. Data files may be transferred between workstations on removable media IAW operating and security procedures to update necessary operating data.

A-108. Users WILL NOT load additional software programs other than authorized updated revisions.

A-109. AR 710-2 requires original copies of all software, regardless of value, to be issued and accounted for through normal hand-receipt procedures. Unit commanders will ensure that the software suite issued with each workstation is properly accounted for and hand receipted. The G6/S6 or ISSOs will ensure the compliance of copyrighted software licensing restrictions.

SOFTWARE MODIFICATIONS

A-110. Modification or alteration of the ABCS software is strictly prohibited. Only formally released software revisions or modifications shall be installed.

SOFTWARE INTEGRITY

A-111. The procedures set forth in this SOP are only effective if the integrity of the ABCS software is maintained. The G6/S6 or ISSO is responsible for the integrity of the ABCS software suite.

SYSTEM AUDIT PROCEDURES

A-112. Systems operating in the systems high mode of operation will ensure all persons having access to the system are held accountable for their actions. In the ABCS environment, this is accomplished through an audit trail. Because the ABCS software does not provide an automated audit trail of all security-related events, this tracking is done manually. Therefore, it is necessary for users to maintain a manual record of all security-related events.

A-113. As a minimum, an audit log will be reviewed daily for security implications. If the tactical situation does not permit the daily review of the audit log, commanders may authorize the review of the audit log weekly. Audit trail information will be maintained for 30 days.

CONFIGURATION CONTROL

A-114. The configuration of ABCS shall be strictly controlled. Proper configuration management practices play a significant role in preserving system security and in assuring continued performance.

A-115. Unit personnel will conduct regular inventories of information systems components. In addition to regular inventories, periodic inspections shall be conducted to verify the hardware configuration has not been altered. Each piece of hardware shall be visually inspected for signs of unauthorized modification or tampering.

A-116. An accurate accounting of all hardware shall be maintained throughout the system's life. This inventory shall reflect any authorized equipment replacements, upgrades, modifications, and additions that take place.

HARDWARE SECURITY

A-117. Hardware security depends on the prompt identification and resolution of all hardware errors. All hardware errors, no matter how insignificant, will be reported so they can be investigated and corrected.

HARDWARE MALFUNCTIONS

A-118. Although the hardware is thoroughly tested before fielding, some malfunctions will undoubtedly occur. It is important that these malfunctions be identified and corrected as quickly as possible. Malfunctioning hardware may undermine procedural or automated security features and make ABCS susceptible to unauthorized access attempts.

A-119. All users are responsible for identifying and reporting any equipment malfunctions so appropriate corrective action can be taken. Users can quickly resolve most equipment malfunctions that are caused by user errors.

A-120. Users identify most equipment malfunctions when they fail to receive the equipment response anticipated by an initiated action. Normally, after several unsuccessful attempts, the user will begin to look for an explanation of the equipment malfunction. The user will verify–

- The power is available to the device in question and cables are connected.
- All data is correct and has been properly input and the proper procedures were used.
- The built-in-test (BIT) is monitored during system initialization.
- Any equipment malfunction that affects the security.
- Local maintenance is conducted IAW the appropriate technical manuals and unit SOP.

EQUIPMENT INSTALLATION

A-121. The security of the system depends on the installation of the hardware suite. It is critical to the security and operation of the system that components are kept in their proper installation configuration.

SECURITY BRIEFING

A-122. AR 380-19 states that all users, supervisors, and managers of information systems receive initial and periodic training in automation security. This briefing fulfills the training requirements of AR 380-19. All personnel will read or will be briefed on this information. They will also acknowledge receipt of the briefing with their signature.

PURPOSE OF AUTOMATION SECURITY

A-123. ABCS and other information systems operate in the active Army, Army Reserve, and National Guard processing classified and unclassified sensitive information. These systems are vulnerable to computer hackers, hostile intelligence agents, thieves, and individuals with malicious intent. The rapid increase in information systems has made security a major issue concerning the safeguarding of systems and, most important, the data they process. The US Army Information Systems Security Program defines various threats to our information systems and applies countermeasures. The program protects against–

- Espionage.
- Compromise or unauthorized manipulation of classified and unclassified sensitive information.
- Unintentional loss or malicious destruction of data files.
- Malicious or unintentional damage to, or destruction of, hardware and software.
- Theft of hardware and software.
- Unauthorized use of software that may contain malicious programs (computer viruses, logic bombs).
- Unauthorized personal use of the equipment.
- Natural disasters.

PERSONAL RESPONSIBILITY

A-124. Users, supervisors, and managers must adhere to prescribed security policies and procedures. These are divided into three areas: procedural, data, and physical security, which constitute the minimum for operating the system.

PROCEDURAL SECURITY

A-125. Procedural security dictates how to operate and maintain the system. Users, supervisors, and managers will–

- Have a minimum of a SECRET security clearance and approved need-to-know.
- Obtain an information systems briefing from their ISSO or designated representative.
- Ensure the equipment and processing environment is maintained with care (for example, used properly and kept clean).

- Operate the equipment IAW operator's manuals and posted security instructions.
- Ensure that personal copies of software are not used on government equipment.
- Ensure that no additional equipment is attached to the network without the knowledge and permission of the ISSO. Attaching additional equipment will require additional accreditation.
- Protect against disaster (always have backup copies of programs ready to go).
- Protect unattended workstations.
- Protect against viruses (never load unauthorized or personal software onto any workstation).
- Report immediately any suspected computer misuse or abuse to the ISSO.

DATA SECURITY

A-126. Always protect classified and unclassified sensitive information. Sensitive and mission critical information requires protection from disclosure, alteration, and loss. Classified data products must be safeguarded (processed and stored) IAW AR 380-5. Users, supervisors, and managers will–

- Protect data storage media (secure removable media and equipment that contain fixed media).
- Not attempt unauthorized access to any data on any ABCS equipment or network.
- Label disks with the contents of the data stored on them (classified and unclassified) and the name of the application program.
  - Handle disks carefully to avoid damage.
  - Do not write on a disk with pencil or pen. (The correct procedure for labeling a disk is to write the classification and identification data on the label and then attach the label to the disk.)
- Label disks used for classified data with the highest classification of the information contained on the disk. (Use SF labels for SECRET and unclassified, when appropriate.)
- Store classified and unclassified disks in jackets that have been correctly labeled.
- Mark classified data output products at the top and bottom of the page with the proper classification and required caveats IAW AR 380-5.
- Verify that all output (hard copy, files, and media) are marked with the proper classification.

- Dispose of waste containing classified information as classified waste (for example, burn or shred).
- Not allow any person outside the organization to access information unless the person has a SECRET security clearance and a need-to-know.
- Store classified and sensitive data products in authorized security containers IAW AR 380-5.

PHYSICAL SECURITY

A-127. Physical security limits access to the processing environment and provides security for hardware, software, and the data it processes. Users, supervisors, and managers will–

- Protect data processing areas (recognize people who do not belong in the area).
- Limit access to those who are authorized to use, service, and repair the equipment.
- Lock doors to offices, rooms, vehicles, and motor pools that house information systems during nonduty hours.
- Restrict access to areas where classified information is being processed.
- Ensure that hardware and software are hand receipted by serial numbers to users, sections, or office chiefs. Hardware and software must have an accountability chain back to the property book officer.
- Challenge persons carrying components out of an office, building, motor pool, or net control station (they may be in the process of stealing).
- Not allow storage media, on which classified and/or unclassified sensitive data or applications has resided, to leave controlled channels until it has been declassified.

PERSONAL LIABILITY

A-128. Users, supervisors, and managers must know the Federal law provides for punishment of up to a $100,000 fine and one year in jail for the first offense of anyone who–

- Knowingly accesses a computer without authorization or exceeds authorized access and obtains information which requires protection against unauthorized disclosures.
- Intentionally accesses government-owned computers without authorization and alters, damages, or destroys information or prevents authorized use of the computer.

A-129. The offense is for the access and not necessarily disclosure.

ACKNOWLEDGMENT

A-130. Users, supervisors, and managers will acknowledge, by signature, that they have read and understood the above instructions. The ISSO or SA/NA (briefer) must answer any questions regarding these instructions before signing. Persons who refuse to acknowledge the briefing will not be allowed to operate in the network. All persons receiving this briefing will be given a signed personal file copy for future reference.

USER: _____RANK: _____DATE: _____

ISSO: _____RANK: _____DATE: _____

TECHNICAL VULNERABILITIES

A-131. This section describes policies and procedures for reporting technical vulnerabilities (for example, contamination and intrusions and/or attempted intrusions).

A-132. A technical vulnerability is a hardware, firmware, communication, or software weakness that is not documented in the system's literature. It leaves a computer processing system open for potential exploitation, either externally or internally, resulting in a security risk.

A-133. Some technical vulnerabilities include–

- The use of software commands which unexpectedly disable protection features.
- The failure of the hardware to separate individual processes or to protect security relevant protective mechanisms from unauthorized access or modification.
- A communications channel which allows two cooperating processes to transfer information such that the transmission violates the system's overall security policy.

RESPONSIBILITIES

A-134. The ISSM–

- Serves as the commander's representative on ISS.
- Maintains a technical threat database on technical vulnerabilities, such as contamination and intrusion attack methodologies, and provides this information to individuals on a need-to-know basis.
- Provides security training to educate users about the threats of technical vulnerabilities. This ensures the users are aware of defensive strategies, which may be taken to control and minimize threats and to advise users of reporting requirements under Federal statute and Army directives.

A-135. The ISSO–

- Reports any security incidents and technical vulnerabilities to the higher headquarters ISSO or ISSM.
- Implements automation security training to include technical vulnerability reporting.
- Provides support to the ISSM and to the INSCOM, as necessary.

A-136. Users will–

- Comply with AR 380-19 and the unit SOP.
- Immediately report any suspected or actual security violations, such as contamination, intrusions and/or attempted intrusions, and other technical vulnerabilities, upon their detection, to their SA/NA or ISSO.

POLICIES

A-137. All computer contamination, intrusions and/or attempted intrusions and other technical vulnerabilities will be reported immediately upon their detection to the SA/NA or ISSO.

A-138. As a minimum, all information on technical vulnerabilities will be classified at the CONFIDENTIAL level. Individuals reporting such information must use a secure means of transmission and ensure that the recipients of the transmitted information have the proper security clearance and need-to-know. If the individual reporting the information does not have access to a STU-III security phone (or other COMSEC device), the ISSO or ISSM should be notified in person, or by mail, regarding the technical vulnerability information.

A-139. All technical vulnerabilities will be reported IAW AR 380-19.

A-140. IAW AR 380-19, vendors may be provided with the technical details of vulnerabilities. Within contractual limitations, the prime contractor is responsible for taking corrective actions and for establishing procedures that will eliminate identified technical vulnerabilities.

A-141. Same day reporting to the INSCOM is required for actual intrusions, virus attacks, or other events which would likely affect or apply to other sites.

PROCEDURES

A-142. Audit trail records are an essential element of detecting a technical vulnerability. Information systems components will be audited IAW the standards of AR 380-19 and the unit SOP.

A-143. Users will report suspicious activities to their SAs/NAs or ISSOs for a determination on whether a security incident or technical vulnerability has occurred and what action must be taken. Suspicious activities include–

- Successful and unsuccessful connections from external interfaces that do not normally establish connections to the network.
- Alert messages, which indicate that users have attempted to execute or obtain privileges that they have not been granted.
- Unauthorized use of the network.

A-144. If the vulnerability is a possible contamination, the component or system should be isolated from other components. Disconnect the system, if necessary.

A-145. The SA/NA, with assistance from the ISSO, will attempt to identify contamination symptoms which may be present based on a baseline of normal system operation.

A-146. Technical vulnerabilities will be reported immediately. Individuals will contact their SA/NA or ISSO for the initial reporting of the vulnerability. If the SA/NA or ISSO is not available, contact the ISSM.

A-147. The format for reporting a technical vulnerability will be IAW AR 380-19. The report should be thorough and detailed so the vulnerability can be demonstrated and researched.

A-148. All reports of technical vulnerabilities will be initially classified at least CONFIDENTIAL. The INSCOM, with the National Security Agency, determines if the report should be declassified to facilitate dissemination.

A-149. ISSOs will investigate the validity of all possible technical vulnerabilities, including contamination and intrusions and/or attempted intrusions.

A-150. ISSOs will coordinate technical recovery actions based on guidance from their ISSM and ISSPM and will submit interim and final reports on all vulnerability incidents.

A-151. If an ISS incident occurs because of a technical vulnerability, the security incident and the technical vulnerability can be combined on the same report IAW AR 380-19.

REPORTING

A-152. A report must contain general information. This includes–

- Report date.
- Person(s) contacted (include person's position, organization, mailing address, and telephone number).
- Hardware and software configuration, including the operating system (with release number) and any unique attributes, such as special security properties.
- Description of a technical vulnerability that includes–
  - A scenario that describes the specific conditions which demonstrate the weakness or design deficiency. The description should thoroughly describe the condition(s) so the deficiency can be demonstrated and researched with the given information.
  - A description of the specific impact or effect of the weakness or design deficiency in terms of denying service, altering information, and compromising data.

  - An indication of whether or not the vendor has been notified. The prime contractor may be provided with the technical details of vulnerabilities to take corrective actions within contractual limitations IAW AR 380-19. The vendor should not be provided with data regarding the specific sites concerned, methods of discovery, or information that could lead to increased site vulnerabilities without the written approval of the DAA.
  - A suggested correction. Any code or procedure that will reduce the impact or eliminate the defined technical vulnerability.
- System location, owner, network connections, system use, highest classification of data, and any other clarifying information. See Table A-1 for the security checklist contained in this SOP.

SECURITY CHECKLIST

A-153. Table A-1 is a security checklist that provides the information needed to ensure the unit is operating the equipment IAW AR 380-19 and unit SOP.

Table A-1. Security Checklist

Unit Identification: _____

Number of System Workstations: _____

Unit Location: _____

ISSO: _____

SA/NA: _____

Unit Security Manager's: _____

Name/Title: _____

Telephone: _____

Supervisor's Name/Title: _____

Telephone: _____

YES	NO	ACCESS
☐	☐	All personnel have a minimum of a SECRET security clearance.
☐	☐	Access rosters for all information systems. (Once the security clearance and the need-to-know are verified, access is granted.)
☐	☐	All systems connected to the LAN are properly accredited.
YES	**NO**	**AUDIT**
☐	☐	C2P tools are used to capture audit events.
☐	☐	Audit tools are reviewed for evidence of unauthorized access or tampering.
YES	**NO**	**CLEARING, PURGING, AND DECLASSIFYING ELECTRONIC MEDIA**
☐	☐	When left unattended, the information systems components must be placed in a purged, declassified state. All classified magnetic media is removed; workstation RAM is purged; and printer RAM is purged.
☐	☐	Floppy disks with classified information stored on them are always treated as classified and not used at the unclassified sensitive level. (Floppy disks can only be purged using a Type I or II Degausser.)

Table A-1. Security Checklist (Continued)

YES	NO	HARDWARE SECURITY
☐	☐	All information systems components are installed and maintained IAW applicable technical manuals.
☐	☐	All information systems component failures or malfunctions are documented and reported to the SA/NA or ISSO. (ISSOs will determine if the malfunctions should be reported as a technical vulnerability.)
☐	☐	Maintenance personnel have a SECRET security clearance.
☐	☐	Maintenance personnel with no SECRET security clearance and who do not access classified information during their operations are observed by an authorized individual with a SECRET security clearance, to ensure they perform no obvious unauthorized modifications.
☐	☐	Classified information systems components are not removed from the shelter by uncleared maintenance personnel.
YES	**NO**	**SOFTWARE SECURITY**
☐	☐	System workstation software errors or failures are documented and reported to the SA/NA or ISSO. (ISSOs will determine if software errors should be reported as a technical vulnerability.)
☐	☐	No unapproved modifications or alterations are made to the system workstation software.
YES	**NO**	**PHYSICAL SECURITY**
☐	☐	When unattended, the information systems components are secured with double barrier protection (for example, locked in a military vehicle or in a locked and secured motor pool).
☐	☐	Environment for operating information systems is authorized for processing SECRET material.
☐	☐	All components are maintained under the control of cleared, authorized users or supervisors.
☐	☐	Classified information, magnetic media, and other material are secured in a GSA-approved container, safe, or Class B vault when not under the direct control of an authorized individual.
☐	☐	All components are properly declassified before being left unattended.

Table A-1. Security Checklist (Continued)

YES	NO	PROCEDURAL SECURITY
☐	☐	ISSO is appointed.
☐	☐	Missions applications administrator assists SA/NA and ISSO in accomplishing security.
YES	**NO**	**PERSONNEL SECURITY**
☐	☐	Initial security training and awareness briefing for all workstation users and supervisors is given.
☐	☐	Periodic security and awareness training program is given.
☐	☐	All personnel who have access to the network have a minimum of a SECRET security clearance IAW AR 380-67.
YES	**NO**	**INFORMATION SECURITY**
☐	☐	All workstation removable magnetic media is clearly marked to indicate the classification of information stored on it (SF 707 or SF 710 label).
☐	☐	All workstation printer output is marked and safeguarded as SECRET until reviewed and marked accurately by an authorized individual.
☐	☐	Printer ribbons used by the workstation to print classified information are marked and stored with appropriate classification level.
☐	☐	All classified material, documents, removable magnetic media, printer output, and COMSEC material are secured in a GSA-approved container for securing classified material, a Class B vault, or guarded by an authorized individual.
YES	**NO**	**EMERGENCY DESTRUCTION**
☐	☐	Procedures to destroy workstations to prevent compromise of classified and unclassified sensitive information are in place.
☐	☐	Emergency destruction procedures are in place during tactical movements.
☐	☐	Emergency destruction procedures are periodically rehearsed.

Table A-1. Security Checklist (Continued)

YES	NO	TRANSPORTATION SECURITY
☐	☐	Procedures are in place to protect all components during tactical movements.
☐	☐	Procedures are in place to protect all components during administrative movements.
YES	**NO**	**MISCELLANEOUS**
☐	☐	AR 380-19 is on hand.
☐	☐	Unit SOP is on hand.
☐	☐	The command has conducted a local risk management review.
☐	☐	POC list for SA/NA, ISSO, and ISSM is on hand.

Appendix B

LAN Troubleshooting Guide

This appendix provides the user a guide for troubleshooting faults before contacting the G6/S6 for assistance.

PHYSICAL FAULT ISOLATION

B-1. Users are responsible for troubleshooting their information systems using diagnostic software and BIT equipment. The user will follow certain steps in determining fault isolation as hardware, network, or software related.

ROUTER-BASED ARCHITECTURE

B-2. LAN troubleshooting consists of isolating and repairing a LAN failure within the CP. With the tools provided, the SA/NA can find most LAN faults. Determining which devices on the LAN are reachable can easily identify most failures. Figure B-1 shows the router-based diagram. If a LAN monitoring device is connected at point DD and–

- Only devices 1 through 6 are reachable, then a fault exists in the LAN B segment between router 2 and router 3.
- All devices are visible except router 2 and devices 4 through 6, then either the LAN segment connecting router 2 to LAN B is bad or router 2 is not functioning.

B-3. Following this logic, physical LAN and device faults can be isolated quickly.

SWITCHED-BASED ARCHITECTURE

B-4. Fault isolation is a more difficult task. Figure B-2 shows the switch-based diagram. If a LAN monitoring device is connected at point FF and–

- Only devices 1 through 6 are reachable, then a fault exists in the central router switch 3 or switch 4 or any of the physical connections to these devices.
- All devices are visible except switch 2 and devices 4 through 6, then either the LAN segment connecting switch 2 to the LAN is bad, or the central router is not configured properly.

B-5. The SA/NA connects to these devices and tries to isolate the fault. In a switched-based architecture, the physical LAN and device faults can be isolated, but not as quickly.

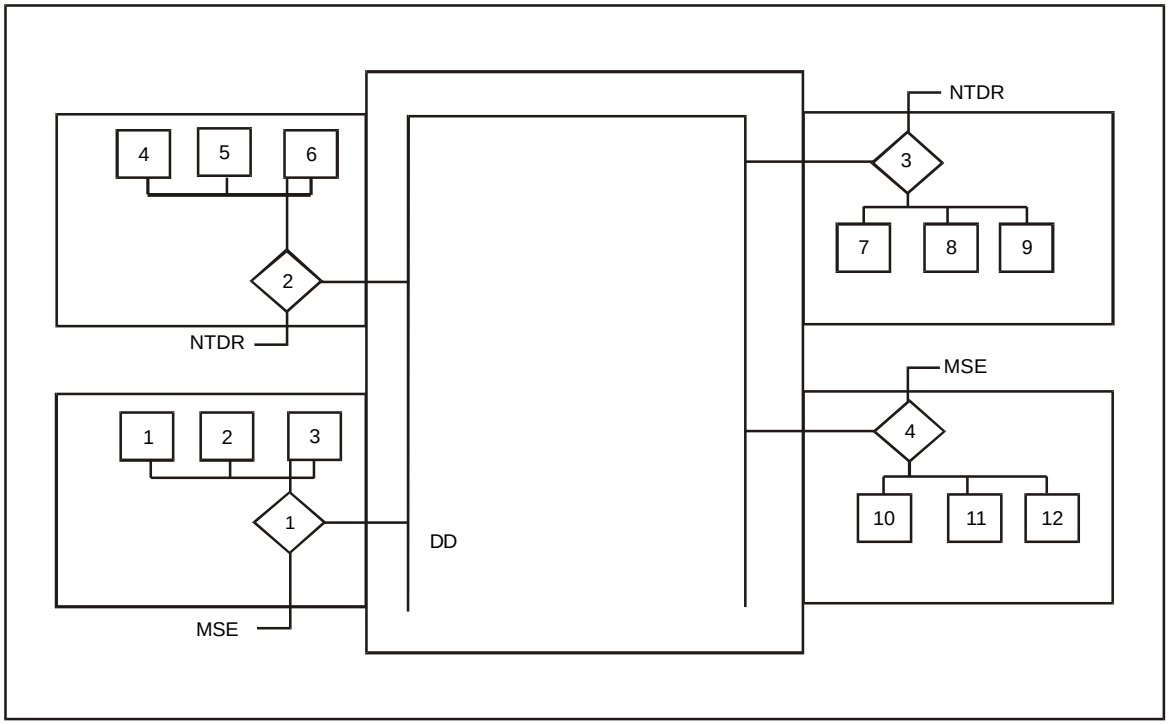

Figure B-1. Router-Based Architecture

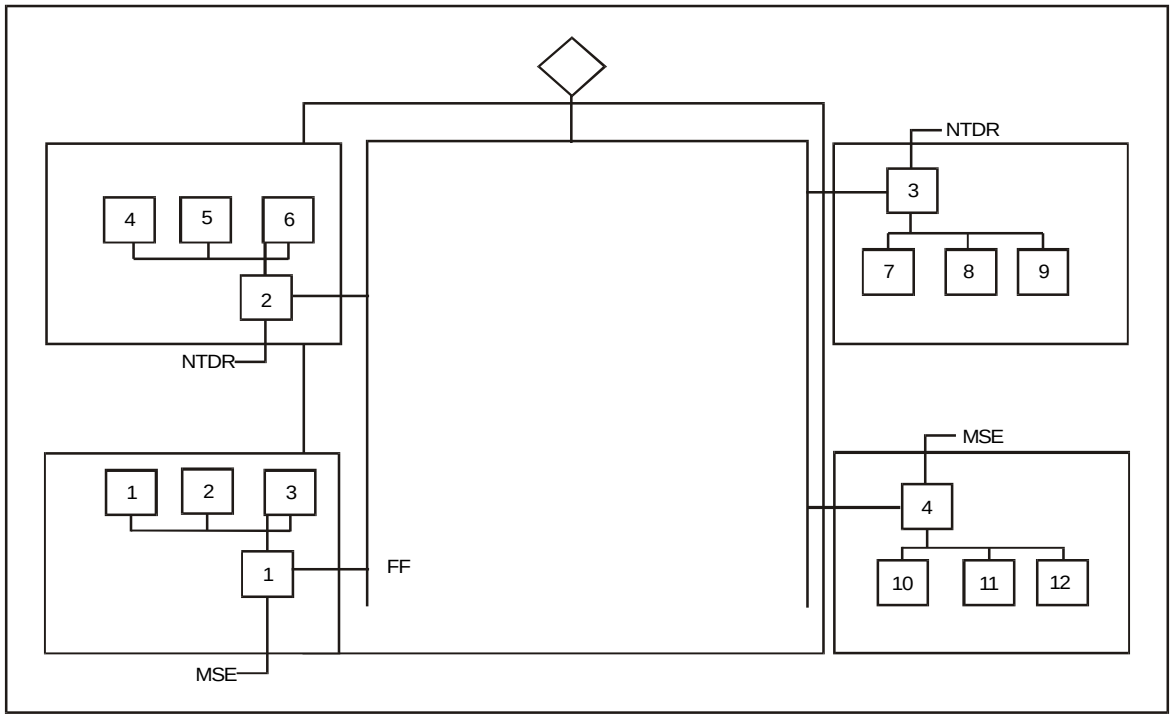

Figure B-2. Switched-Based Architecture

WORKSTATION FAILURES

B-6. If only one workstation is experiencing difficulty, the problem is probably a software failure on that machine. Further troubleshooting is required to verify the fault. Each workstation has maintenance and diagnostic (M&D) software installed for troubleshooting the systems software. Troubleshoot the system with the M&D software IAW the software section, the BFA users manual, or if needed, guidance from the G6/S6.

WAN FAILURES

B-7. If all the devices on the LAN can communicate locally but cannot send messages across the WAN, it is probably down. If the users identify this problem first, they should contact the SA/NA for network status. The SA/NA should check the current status of the network. If the WAN is down or is not accessible, the SA/NA should notify the users immediately. The C2 systems communicate outside of the TOC via the US message text format (USMTF) and/or VMF messages sent by the sendmail program. If the message cannot be delivered, sendmail places the message in a queue. The software is adversely affected as the sendmail queue fills with undeliverable messages.

INTERMITTENT PROBLEMS

B-8. Intermittent or sporadic LAN problems are usually caused by an improper LAN configuration, marginal piece of hardware, improper LAN grounding, or marginal WAN links. Since the problems are difficult to isolate, the maintainer should–

- Check the WAN status.
- Ensure no noise is being induced on the WE-16 X.25 connection by an improperly placed generator cable.
- Check the physical LAN for improper physical connections (such as branches, more than two terminators, LAN too long, or more than 30 devices connected.)

B-9. Improperly connected LANs may continue to function in a degraded mode, concealing the problem under certain conditions. Carefully examine the LAN for loose connections or damaged cables. Shake cables, if possible, to determine if the problem gets worse.

USER MAINTENANCE

B-10. The user of each system is responsible for performing preventive maintenance checks and services (PMCS) IAW applicable technical manuals. He is responsible for troubleshooting problems or failures before requesting assistance from the organizational maintainer. The tools identified below are available to assist the user during PMCS and troubleshooting.

B-11. Each system's software package includes an M&D program, which runs when the system is powered up. Figure B-3 shows startup troubleshooting procedures. These diagnostic routines identify failed components and/or open connections. When a failure is noted, the user troubleshoots IAW with instructions presented by the diagnostic program and IAW the appropriate technical manual.

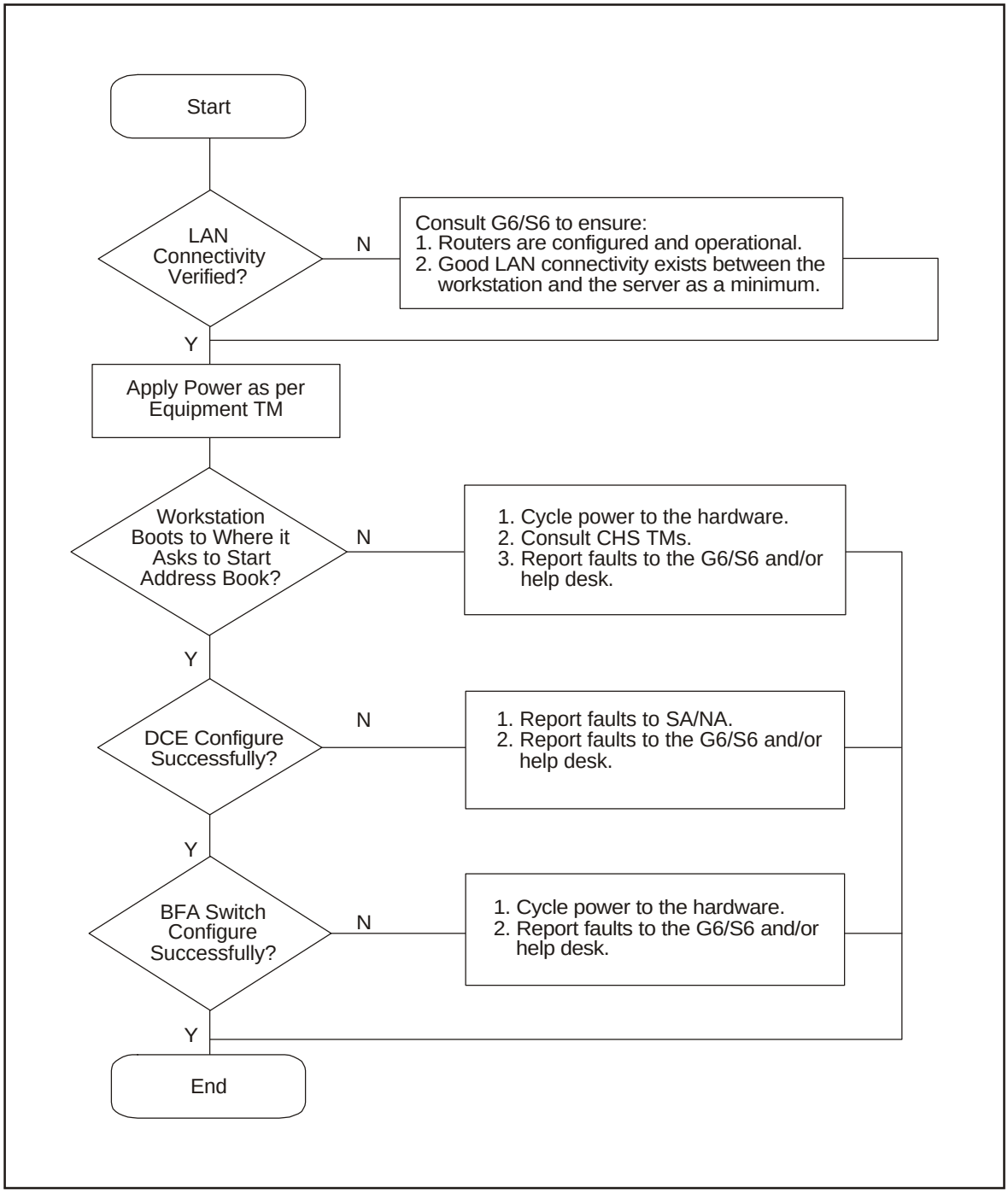

Figure B-3. Startup Troubleshooting Procedures

B-12. Each device has specific diagnostic procedures available when a failure is suspected. The user performs these procedures IAW the troubleshooting instructions in the technical manuals.

B-13. The technical manual contains troubleshooting instructions to be used when diagnostic procedures cannot run or fail to locate the problem.

HARDWARE (HOSTS) TROUBLESHOOTING

B-14. Users are responsible for troubleshooting hardware faults by using the appropriate technical manuals.

B-15. The user determines the information system to be nonoperational and notifies the mission applications administrator of a system failure. Using diagnostic software and BIT equipment, the user and mission applications administrator will try to determine whether the failure is hardware, network, or software related. For software related problems, the user will reload the software and return the system to operation. The user will replace LRUs and turn in failed LRUs through the forward support company. If the user cannot fix the problem or determines the problem to be a network/communication-related failure, he will contact the G6/S6 section.

NOTE: The user and the mission applications administrator will assist in the troubleshooting process and reloading of software.

UNIT-LEVEL MAINTENANCE

B-16. The user requests assistance from the G6/S6 section when he cannot diagnose or correct a problem with his device. The SA/NA is skilled in using M&D software and has the equipment needed to check cables and connectors for serviceability.

B-17. The G6/S6 will verify the status of the system by using troubleshooting procedures to identify the failure as a network, software, or hardware problem. When the troubleshooting is complete, the G6/S6 assists the user in restoring the system by reinstalling system/application software or by identifying the malfunctioning LRU. If the G6/S6 identifies the problem to be an unserviceable LRU and cannot repair it, the G6/S6 will turn the unserviceable LRU into the forward support company. If the problem is software related and reinstalling the application does not fix it, he will contact the supporting software subject matter expert.

SOFTWARE TROUBLESHOOTING

B-18. Generally, software is system specific and supported by each BFA. For example, the division artillery provides software support for AFATDS and the Military Intelligence Battalion provides software support for ASAS, and so on. The contractor or Army Communications-Electronics Command provides additional support. The user troubleshoots his software, but may require assistance from the G6/S6. Refer to Figure B-4 and the software manual for troubleshooting procedures.

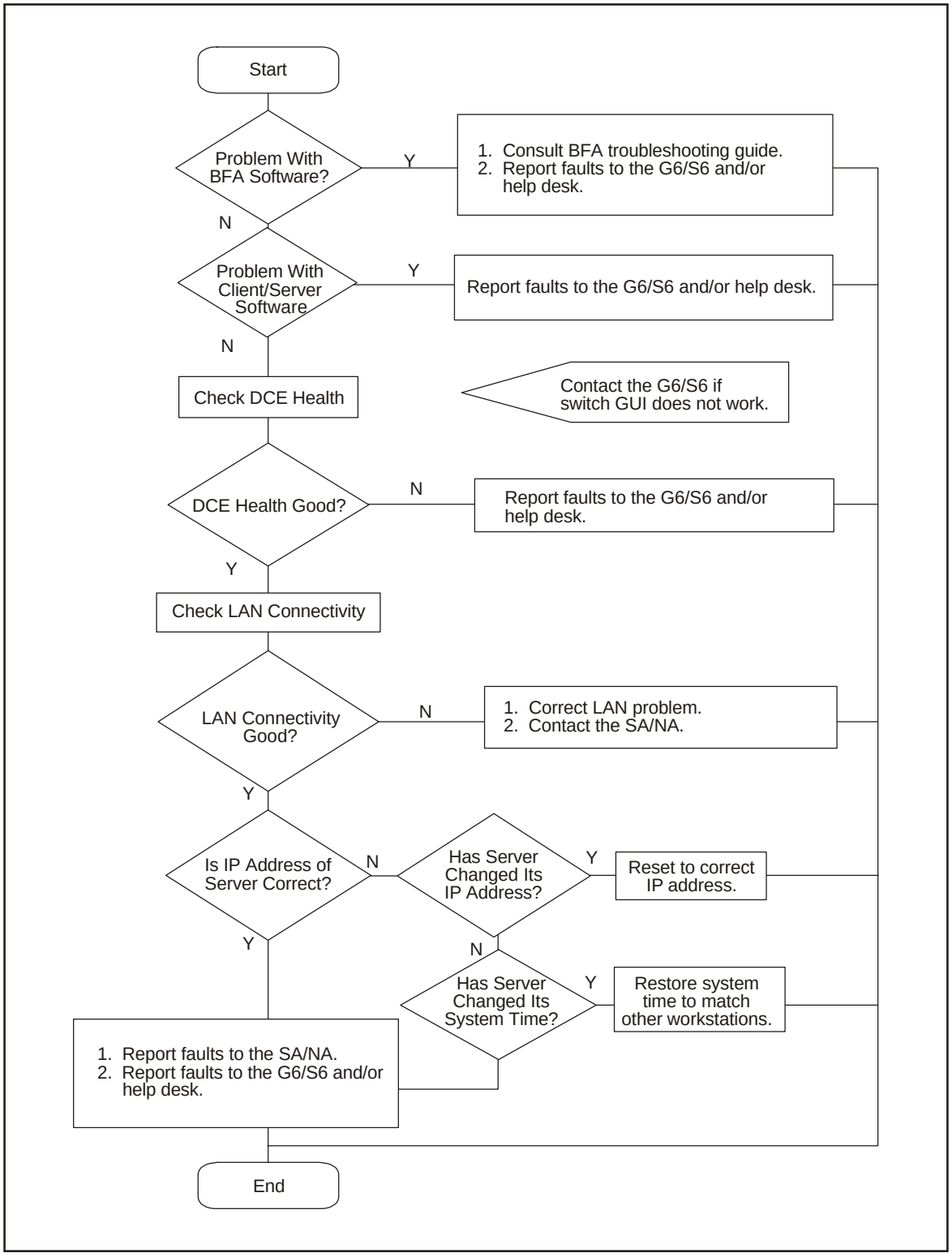

Figure B-4. Software Troubleshooting Procedures

NETWORK TROUBLESHOOTING

B-19. The potential for connectivity and performance problems is high, and the source of such problems is often elusive. Failures are characterized by certain symptoms. These symptoms may be general (such as clients being unable to access specific servers) or more specific (routes not in routing table). Each symptom can be traced to one or more problems or causes by using specific troubleshooting tools and techniques. Once identified, each problem can be remedied by implementing a solution consisting of a series of actions.

B-20. It is always easier to recover from a network failure if you are prepared ahead of time. Table B-1 gives a list of network preparation questions. To see if you are prepared for a network failure, answer the questions. If you can answer yes to these questions, your chances of recovering from a failure are improved.

Table B-1. Network Preparation Questions

QUESTION	YES	NO
Do you have an accurate physical and logical map of your internetwork?		
Does your organization or department have an up-to-date internetwork map?		
Does the map outline the physical location of all the network devices and how they are connected?		
Does the map give network addresses, network numbers, subnetworks, and so forth?		
Do you have a list of all network protocols implemented in your network?		
Do you have a list of network numbers, subnetworks, zones, areas, and so on that are associated with each implemented protocol?		
Do you know which protocols are being routed?		
Do you have a correct and up-to-date router configuration for each protocol?		
Do you know which protocols are being bridged?		
Are there any filters configured in any of these bridges, and do you have a copy of these configurations?		
Do you know all the points of contact to external networks, including any connections to the Internet?		
Do you know what routing protocol is being used for each external network connection?		
Do you have an established baseline for your network?		
Has your organization documented normal network behavior and performance so you can compare current problems with a baseline?		

GENERAL ETHERNET PROBLEMS

B-21. Table B-2 gives some general Ethernet problems and suggested solutions. These procedures will identify and correct some of the problems that a user may encounter.

Table B-2. Ethernet Troubleshooting

MEDIA PROBLEM	STEPS	SUGGESTED ACTIONS
Excessive Noise	Step 1	Use the show interfaces Ethernet EXEC command to determine the status of the routers Ethernet interfaces. The presence of many CRC errors but not many collisions is an indication of excessive noise.
	Step 2	Check cables for damage.
	Step 3	Look for badly spaced taps causing reflections.
	Step 4	If you are using 100BaseTX, make sure you are using category 5 cabling and not another type (such as category 3).
Excessive Collisions	Step 1	Use the show interfaces Ethernet command to check the rate of collisions. The total number of collisions with respect to the total number of output packets should be around 0.1 percent or less.
	Step 2	Use a TDR1 to find any nonterminated Ethernet cables.
	Step 3	Look for a jabbering transceiver attached to a host. (This may require a host-by-host inspection or using a protocol analyzer.)
Excessive Runt Frames		In a shared Ethernet environment, runt frames are almost always caused by collisions. If the collision rate is high, refer to the problem “Excessive Collisions” earlier in this table. If runt frames occur when collisions are not high or in a switched Ethernet environment, then they are the result of underruns or bad software on a network interface card. Use a protocol analyzer to try to determine the source address of the runt frames.
Late Collisions	Step 1	Use a protocol analyzer to check for late collisions. Late collisions should never occur in a properly designed Ethernet network. They usually occur when Ethernet cables are too long, or when there are too many repeaters in the network.
	Step 2	Check the diameter of the network and make sure it is within specifications.

Table B-2. Ethernet Troubleshooting (Continued)

MEDIA PROBLEM	STEPS	SUGGESTED ACTIONS
No Link Integrity on 10BaseT, 100BaseT4, or 100BaseTX	Step 1	Make sure you are not using 100BaseT4 when only two pairs of wire are available. 100BaseTX requires four pairs.
	Step 2	Check for 10BaseT, 100BaseT4, or 100BaseTX mismatch (for example, a card different than the port on a hub).
	Step 3	Determine whether there is a cross connect (for example, do not use straight through cables between a station and a hub).
	Step 4	Check for excessive noise (see the problem “Excessive Noise” earlier in this table.

Appendix C

Mobile Subscriber Equipment Support

This appendix gives a brief overview of the MSE systems and the range extension capabilities. See FM 11-55 for more information on MSE.

MSE ARCHITECTURE

C-1. As the commander maneuvers combat units, the MSE network deploys to support these elements. The direction of maneuver and the location of combat, combat support, and CSS units dictate the placement of communications units. MSE supports force subscribers at echelons from corps through battalion CPs. However, as the mission dictates, MSE will provide air defense artillery support to elements lower than battalion echelons.

C-2. The MSE network is a nodal switched voice and data communications system that is extended by a radiotelephone to provide area coverage. MSE is part of a three-tier communications network. It ties into the TRI-TAC tier supporting the EAC network at selected NCs. MSE also provides CNR users with an interface to the ACUS via the secure digital net radio interface unit (SDNRIU). This capability links SINCGARS users with telephone subscribers, which provides an added method of communication for maneuver units. Figure C-1 shows the architecture of the MSE network.

C-3. The standard five-division corps MSE network can serve up to 26,100 subscribers from battalion through corps. This includes–

- 8,200 digital nonsecure voice terminal (DNVT) subscribers.
- 1,900 mobile subscriber radiotelephone terminal (MSRT) subscribers.
- 16,000 data subscribers.

C-4. Figure C-2 shows the MSE architecture divided into three layers. The upper layer is the backbone structure that consists of interconnected NCs. The middle layer consists of LENs and SENs that provide CPs with network access. The bottom layer consists of static (wireline) and mobile subscribers. Up to 264 SENs and 9 LENs can deploy to support the corps. Typically, a SEN serves a brigade headquarters, separate battalion, or CP. Each of the 112 radio access units (RAUs) (13 in each division and 47 in the corps) support from 20 to 25 mobile subscribers.

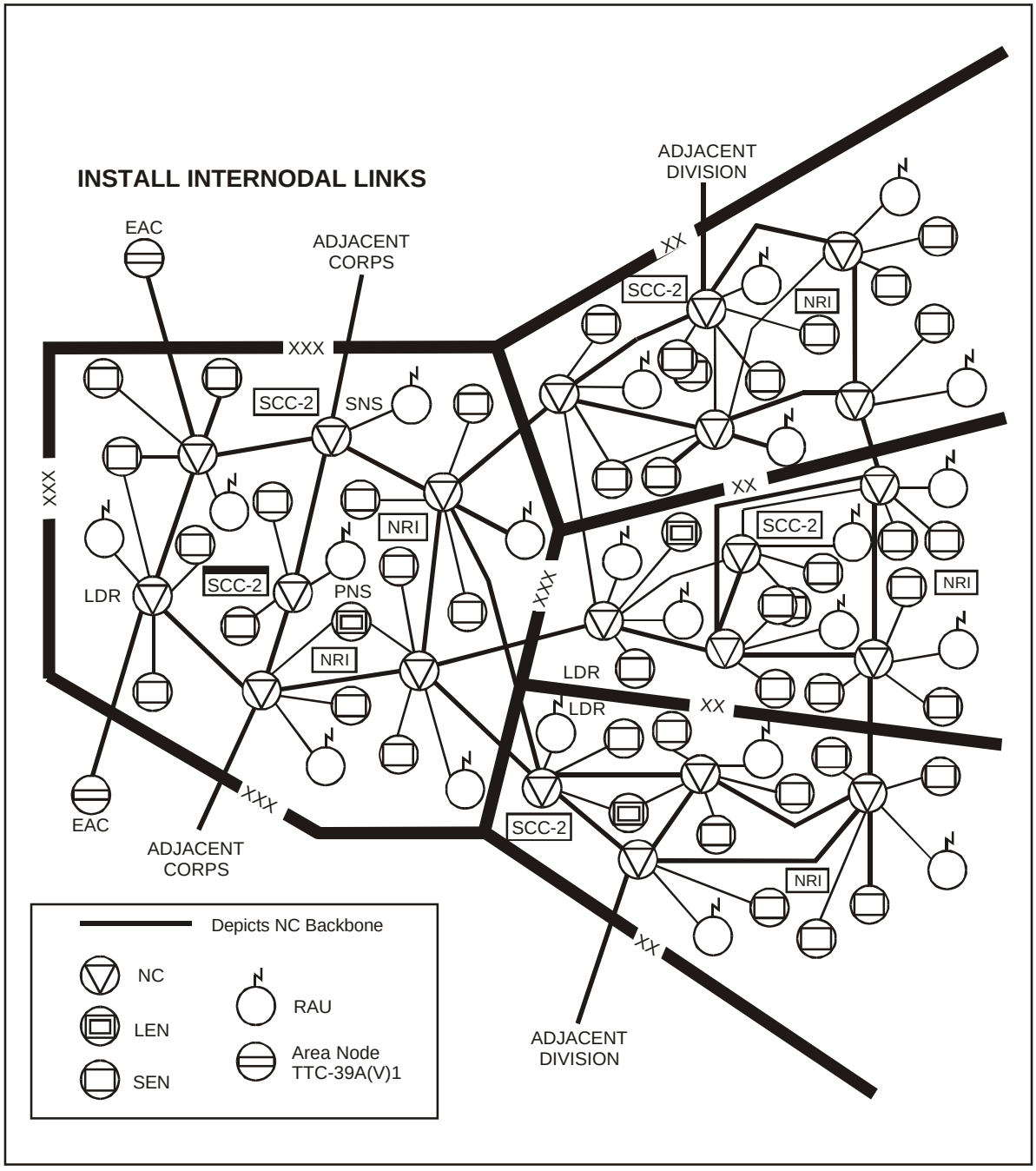

Figure C-1. MSE Network Architecture

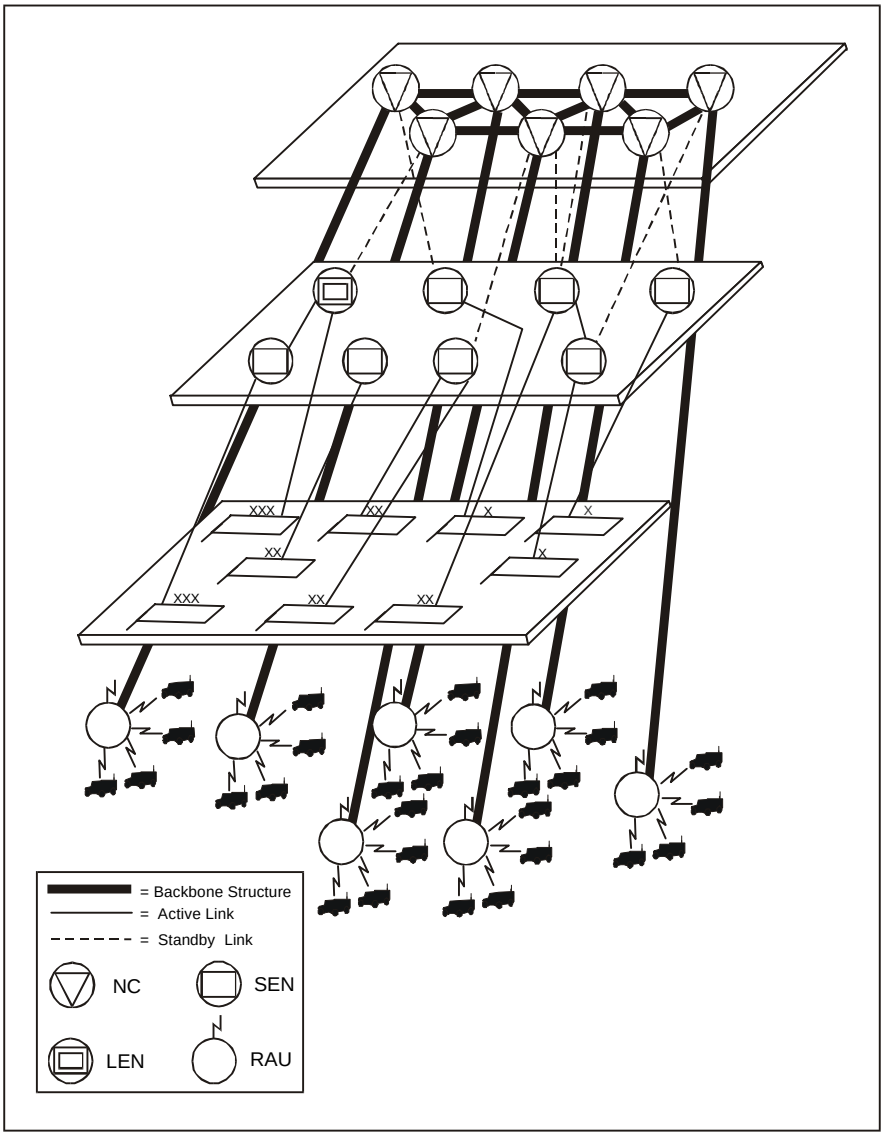

Figure C-2. MSE Architecture Layers

MSE TECHNIQUES

C-5. MSE is a digital telecommunications system, which provides tactical voice and data communications. MSE provides digital voice, data, and facsimile communications on an automatic, discrete address, fixed directory basis using flood search techniques. Flood search techniques initiate each call over multiple routes and establishes the connection over the optimum route based on current traffic within the network. This technique avoids heavily used routes, bypasses failed routes or nodes, and readily adapts to conditions of overload or blockage. Flood search routing ensures that trunks are not assigned and connected until after the called party has been located and an acknowledgment received.

EMPLOYMENT

C-6. MSE can support a corps of five divisions in an area of operations up to 15,000 square kilometers by a grid network. For a division, the MSE grid consists of four to six NCs that make up the backbone of the network. For the corps, the grid consists of 22 NCs. Throughout the maneuver area, subscribers connect to the SENs/LENs by radio or wire. These extension nodes serve as local call switching centers and provide access to the network by connecting to the node center switch (NCS) at the NC.

COMPONENTS

C-7. MSE has various integrated components to ensure mobile and static subscribers have voice, data, and facsimile capabilities. These capabilities support the subscribers' communications no matter where they are in the MSE grid network. MSE components include–

- NC.
- LEN.
- SEN.
- RAU.
- SCC-2.
- ISYSCON.
- LOS radio system (components of the switches).
- MSRT.
- Subscriber terminals.
- Force entry switch (FES).

NC

C-8. NCs provide key switching, traffic control, and access points for MSE. After determining the coverage area, NCs are allocated to establish a corps MSE grid network. NCs are primarily linked by LOS radios to provide communications throughout the system via the NCS. TACSAT and tropospheric scatter (tropo) are connected to the NCs by cable. If one NC is disabled, the system automatically routes communications through another NC.

C-9. The NCS serves as an access point for LENs, SENs, RAUs, SCC-2s, and ISYSCON. The NCS is the hub of the MSE node and provides network interface for subscriber access elements. Figure C-3 shows internodal connectivity. It provides automatic subscriber finding features that allow permanent address assignment and removes the requirement of knowing where the subscriber is physically located. It is contained in three S-250 shelters: the switching group, the operations group, and the node management facility (NMF).

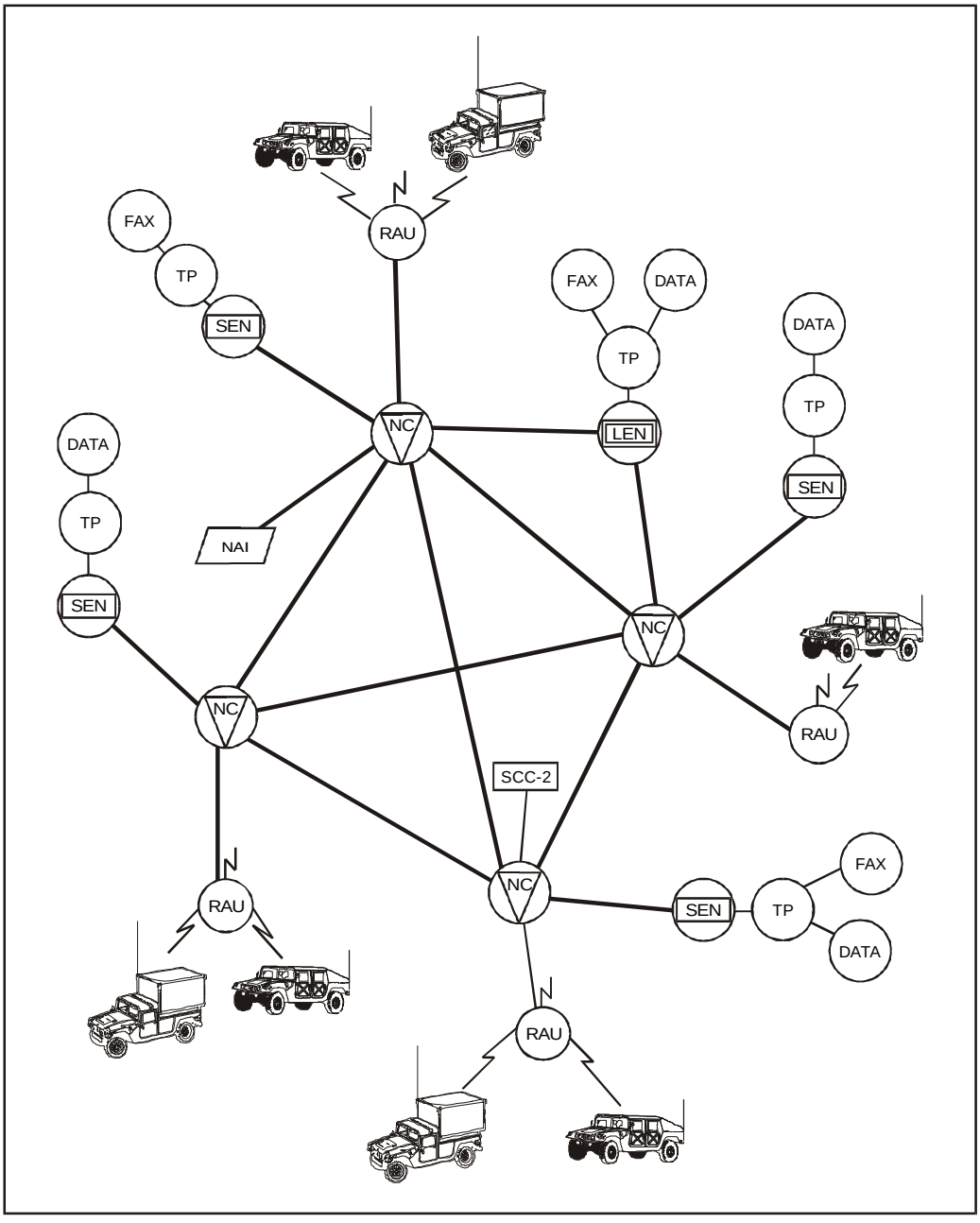

Figure C-3. Internodal Connectivity

LEN

C-10. The LEN provides wired communications for personnel at large CPs. A LEN enables up to 164 wired subscribers to communicate freely through the large extension node switch (LENS) using automatic flood search routing. Subscribers have access to the NCs and to the rest of MSE via LOS radios that connect to the LENS by cable or SHF radio systems.

C-11. The LENS provides automatic subscriber finding features that allow permanent subscriber address assignment. It also removes the requirement of knowing where the subscriber is physically located. It consists of two S-250 shelters containing a switching group and an operations group. The LENS is configured basically the same as the NCS. The differences include terminating trunks. The LEN is not a tandem switch because it is not used primarily as an intermediate switching point between other switching centers. The LENS supports flood search routing. The switching group provides the external interface, circuit switching, and associated functions. The operations group provides central processing and operator interface functions. Some LENSs enable CNR users to enter the MSE network and provide access to commercial networks.

SEN

C-12. The SEN supports the communications needs of smaller CPs. The AN/TTC-48(V)1 can support 26 wired subscribers and the (V)2 can support 41 subscribers. Users have access to NCs and to the rest of MSE via LOS radios that connect to the small extension node switch (SENS) by cable or SHF radio systems.

C-13. The SEN also provides automatic subscriber finding features when connected to an NCS or a LEN. These features allow permanent subscriber address assignment, and they remove the requirement of knowing where the subscriber is physically located. The SEN is in one S-250E shelter mounted on an M-1097 HMMWV. The SEN consists of switching, multiplexing, and COMSEC equipment. It is available in two versions: (V)1 and (V)2. Both versions provide two commercial office interfaces and a secure digital net radio interface (SDNRI) using the SDNRIU, KY-90. The SENS interfaces with the NCS and LENS directly via CX-11230A/G cable, LOS multichannel radio, or multichannel TACSAT.

RAU

C-14. The RAU picks up signals from the MSRT and sends them to the NCs. When a mobile user moves out of range of one RAU and into another, the telephone service automatically transfers to the next (new) and into the range of another RAU, thus providing automatic reaffiliation. Any subsequent calls will be placed through the system via the new RAU ensuring full and continuous functional affiliation throughout the area of operations.

C-15. The RAU, AN/TRC-191, is a fully automatic radio interface for MSRT subscribers. The RAU connects directly to the NC by cable or remotely via LOS radio. The local RAU provides radio coverage within the general area of the parent NCS by automatically establishing secure, full-duplex communications between the MSRT and the MSE network through the parent NCS. Figure C-4 shows how the MSRT (AN/VRC-97) accesses the system through the RAU. MSRTs can receive or send voice, facsimile, or data traffic. The planning range between the MSRT and RAU is 15 kilometers (9.3 miles). Terrain and weather will affect the actual range.

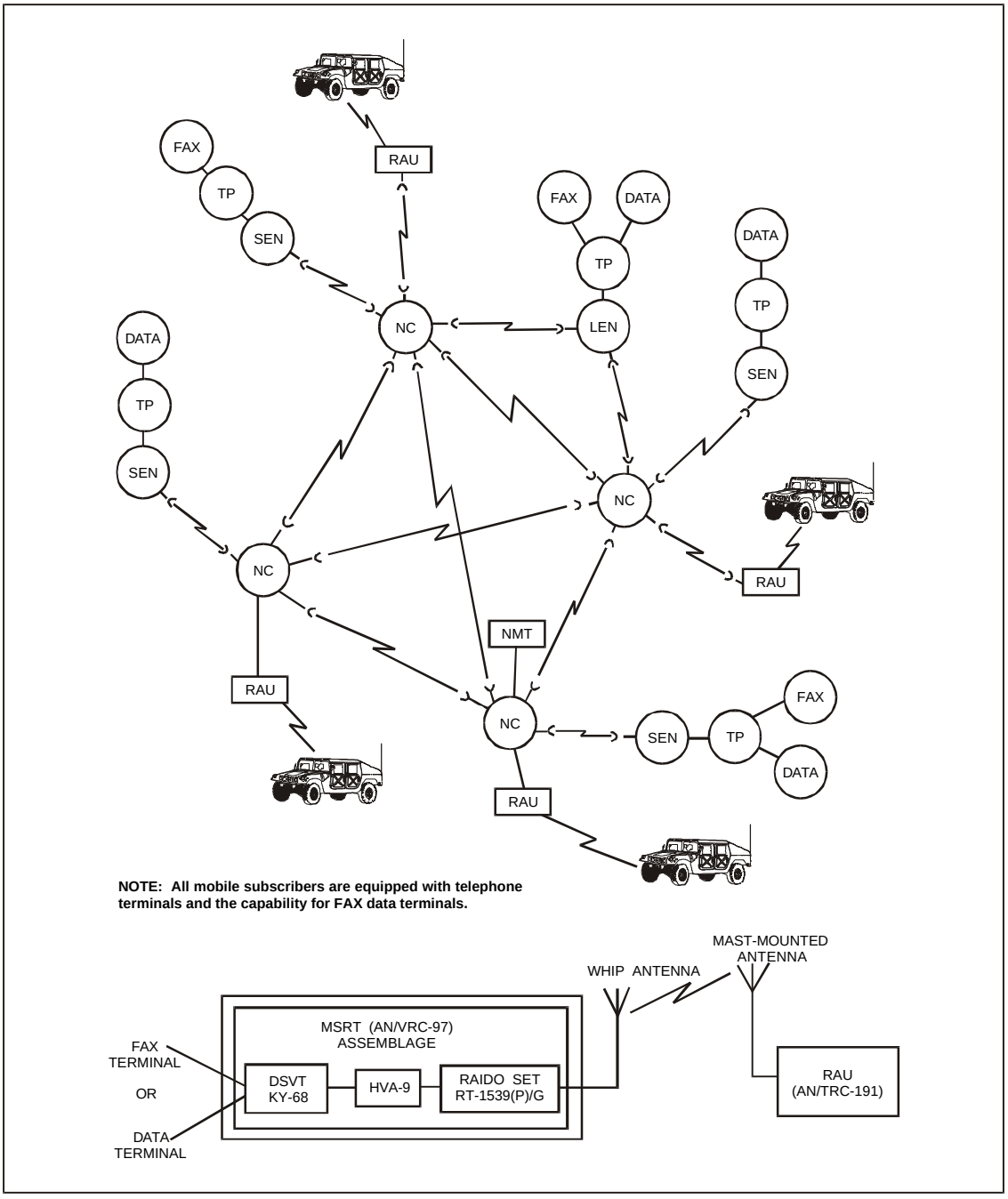

Figure C-4. Mobile Subscriber Interface

C-16. RAUs are used in local and remote configurations. However, it does not mean both RAUs cannot be remoted; it depends on the availability of an LOS assemblage. Because RAUs constantly emit marker beacons declaring availability to affiliated MSRTs, those RAUs closest to the forward edge of the battle area must use EP techniques to mask the emitter from the opposing force.

C-17. Deployment of the LOS assemblages must be considered to minimize the radio signature of the node. As an internodal link, the LOS(V)3 can deploy on hills up to 400 meters from the node via CX-11230A/G cable. If the distance exceeds 400 meters, the SHF radio link can be used up to 10 kilometers (Figure C-5). SHF radio distribution to the NCs and LOS assemblages allows for remoting 50 percent of the radio links.

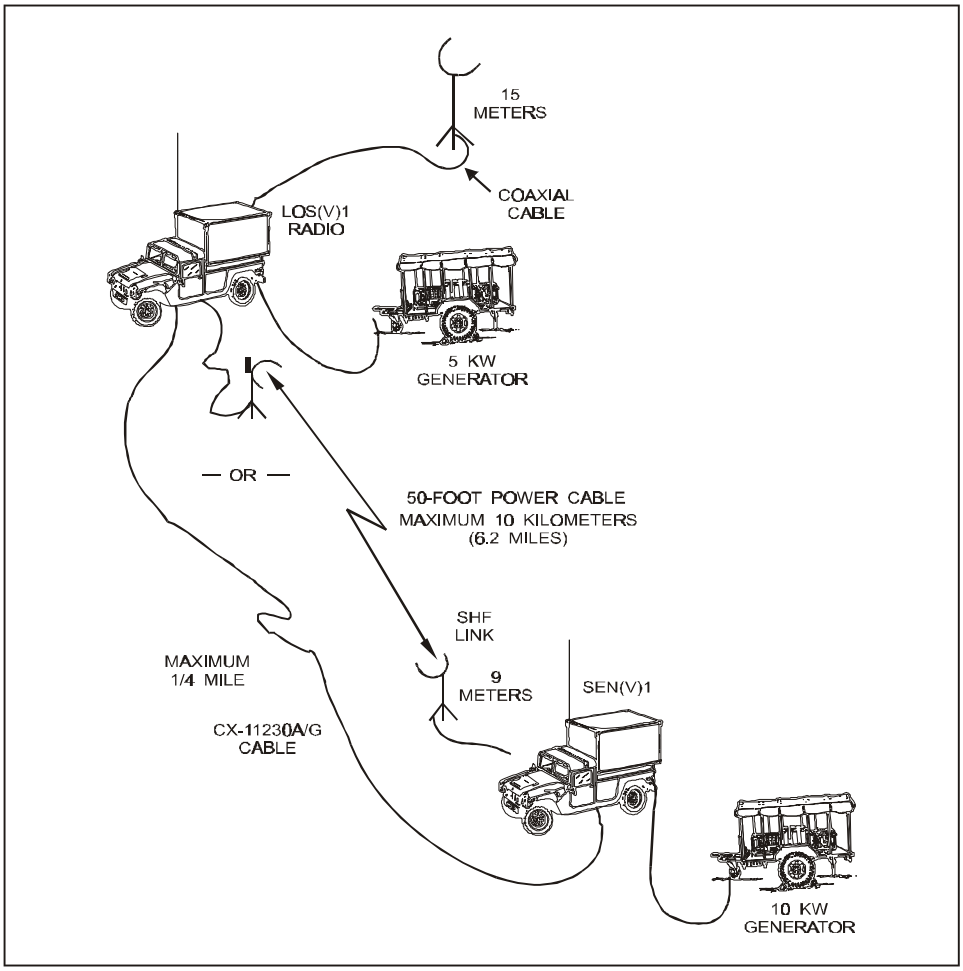

Figure C-5. SHF Radio Link

SCC-2

C-18. The existing MSE SYSCON capability is the SCC-2, AN/TYQ-46(V). It monitors, manages, and configures the MSE network (voice and data) for optimum communications.

C-19. The SCC-2 is an integrated, computerized communications control system that provides automated, near-real-time system control to support planning, configuring, reconfiguring, and monitoring the operation and movement of MSE assets. The SCC-2 normally connects to an NCS or LENS using CX-11230A/G pulse code modulation cable.

C-20. The SCC-2 comes in two versions: (V)1 and (V)2. Version 1 at corps consists of three shelters: one technical and two management/planning shelters. Version 2 is a stand-alone workstation for the corps area and support signal battalions. The SCC-2 at division consists of two shelters: one technical and one management/planning.

C-21. The technical shelter contains a network management center workstation and a technical workstation that provides a near-real-time graphic display of the MSE network. The network management center monitors and controls the TPN. The primary function of the technical workstation is to monitor and assign management functions. The network planners working inside the management/planning shelter complete the following functions:

- Deployment management.
- SCC-2 supervision and management.
- Boundaries management.
- COMSEC key management.
- Very high frequency (VHF) management.
- UHF/SHF management.
- Subscriber database management.
- Message management.

C-22. The management/planning shelter houses two system management workstations. These workstations provide a near-real-time graphic display of the MSE network and the automated tools necessary to create and change databases required for MSE operations.

C-23. The network planning tool (NPT) with its planning and management functions supports the SCC-2. The NPT provides improved NPE and operational automated information management capabilities. The enhanced NPE and operational functions of the NPT include–

- Environmental parameters.
- Digitized mapping.
- Radio/antenna system engineering.
- Terrain analysis profiling.
- System asset placement.
- Frequency assignment management (VHF, UHF, SHF).
- Team information.
- One-on-one interference analysis.
- Electronic warfare threat analysis.
- Subscriber list management.
- Word processing program.
- Spreadsheet program.
- E-mail program.
- Packet network monitoring.

C-24. The SCC-2 includes the following functional software tools:

- NPE for MSE assets.
- Battlefield spectrum management.
- MSE WAN management.
- System administration.
- E-mail.

ISYSCON

C-25. The ISYSCON is a suite of hardware and software giving the G6 and staff the automation capability to engineer, plan, and operate all communications systems including MSE. It enables the commander to interact with ABCS by exchanging common battle command information with the force commander and his staff and by exchanging communications information with maneuver force signal officers. The ISYSCON uses common hardware and software (CHS) for its workstations. ISYSCON provides the tools to perform the information management process by automating the following functions:

- Network planning and engineering (NPE).
- WAN management.
- Mission plan management.
- Battlefield spectrum management.
- COMSEC management.
- System administration.
- LAN management.

C-26. The ISYSCON program will field the system in a variety of configurations. The ISYSCON(V)1 will consist of two servers, four workstations, and ten remotes. The ISYSCON(V)1 will reside at the corps signal brigade and the division signal battalions. The ISYSCON(V)2 will consist of two servers, two workstations, and five remotes. The ISYSCON(V)2 will reside at the corps area signal battalion. The ISYSCON(V)1 will replace the SCC-2.

LOS RADIO SYSTEM

C-27. The LOS radio system consists of versatile links that connect all NCs in a grid network and provides automatic switched services to all wire and mobile subscribers. This radio grid delivers wireless communications to areas covering thousands of square kilometers. The LOS radio system, AN/TRC-190(V), has four versions.

C-28. The AN/TRC-190(V)1 is an LOS multichannel radio terminal. It provides point-to-point UHF radio links using the AN/GRC-226(P) radio set between various nodes of the MSE system. If the AN/TRC-190(V)1 has an AN/GRC-224(P) radio set installed, it can provide a short-range and a point-to-point SHF radio link. The SHF radio functions as a short-range, down-the-hill (DTH) radio providing a low signature connection between the sheltered CP site and the more exposed LOS terminal site. Each radio link supports a single, full-duplex, group-level connection and a single digital voice orderwire

(DVOW) channel. The (V)1 is equipped with one AB-1339 mast with Band I and Band III antennas. The planning range of the UHF radio is 40 kilometers (28 miles). The (V)1 typically deploys with the SENS or remote RAU.

C-29. The AN/TRC-190(V)2 is an LOS multichannel radio terminal. It provides point-to-point UHF radio links using the AN/GRC-226(P) radio set between various nodes of the MSE system. If the AN/TRC-190(V)2 has an AN/GRC-224(P) radio set installed, it can provide a short-range and a point-to-point SHF radio link. The SHF radio set operates in tandem with the primary UHF radio link. Each radio link supports a single, full-duplex, group-level connection and a single DVOW channel. The (V)2 is equipped with two AN/GRC-226(P) radio sets (one on-line and one spare) and one AB-1339 mast with Band I and Band III antennas. The planning range of the UHF radio is 40 kilometers (28 miles). The (V)2 typically deploys as an analog interface to North Atlantic Treaty Organization (NATO) forces.

C-30. The AN/TRC-190(V)3 is an LOS multichannel radio terminal. It provides point-to-point UHF radio links using the AN/GRC-226(P) radio set between various nodes of the MSE system. If the AN/TRC-190(V)3 has an AN/GRC-224(P) radio set installed, it can provide a short-range and a point-to-point SHF radio link. The SHF radio set operates in tandem with the primary UHF radio link. The SHF radio functions as a short-range radio link providing connectivity for CPs. Each radio link supports a single, full-duplex, group-level connection and a single DVOW channel. The (V)3 is equipped with four AN/GRC-226(P) radio sets (two on-line and one spare) and three AB-1339 masts with two Band I and two Band III antennas. The planning range of the UHF radio is 40 kilometers (28 miles). The (V)3 typically deploys with the NCS and is a radio relay.

C-31. The AN/TRC-190(V)4 is an LOS multichannel radio terminal. It provides point-to-point UHF radio links using the AN/GRC-226(P) radio set between various nodes of the MSE system. Each radio link supports a single, full-duplex, group-level connection and a single DVOW channel. If the AN/TRC-190(V)4 has an AN/GRC-224(P) radio set installed, it can provide a short-range, DTH, and a point-to-point SHF radio link. The (V)4 is equipped with two AN/GRC-226(P) radio sets (two on-line) and two AB-1339 masts with Band I and Band III antennas. The planning range of the UHF radio is 40 kilometers (28 miles). The (V)4 typically deploys with the LENS.

MSRT

C-32. MSE network users gain mobile access using the MSRT (AN/VRC-97) through the RAU by affiliating onto the network. MSRTs can receive or send voice, facsimile, or data traffic. The planning range between the MSRT and RAU is 15 kilometers (9.3 miles). Terrain and weather will affect the actual range.

SUBSCRIBER TERMINALS

C-33. MSE users initiate and end all communications by using subscriber terminals. The terminals are described below.

C-34. The DNVT, TA-1035/U, provides voice and data access to the MSE network. Its features include–

- Handset.
- Keypad.
- Digital transmission (16 kilobits per second (kbps)).
- Four wire with data port to interface with computer/facsimile (FAX).
- Compatibility with other terminals.

C-35. The digital subscriber voice terminal (DSVT), KY-68, provides secure access to MSE for all mobile or fixed subscribers. It functions closely to the DNVT, and its features are the same.

C-36. The FAX terminal, AN/UXC-7, transmits critical information such as overlays, diagrams, and handwritten messages over the system in seconds. Ruggedized versions are usable with both DNVTs and DSVTs. Its features include–

- Digital transmission (16 kbps).
- Black and white copy with eight shades of gray.
- Standard issue paper usage.
- Embedded memory with burst transmission.
- NATO interoperable.

FES

C-37. The FES combines the essential functions of the NCS/LEN/NMF shelters and a RAU in one shelter. The FES combined with an LOS AN/TRC-198 comprises the CCP. The connections between the FES and the LOS are by cable since no SHF is supplied. The FES has packet switch capability, but it has no gateway function. Therefore, it has no direct connections to adjacent corps or EAC. The FES can be operator-controlled outside the shelter by a dismountable node management facility (DNMF) remote terminal.

C-38. The FES provides full flood search capability via the downsize routing subsystem, an SHF interface capability, and a DSVT in the truck. The line termination unit provides modem/multiplex functions for the local subscriber interface and is equipped with a rear terminal board to permit direct connections instead of the J-1077.

C-39. The LOS AN/TRC-198 is similar to an LOS(V)3, except that the LOS AN/TRC-198 UHF radios operate on three separate link connections to the FES (no multiplex) and all links operate on either band.

MSE RANGE EXTENSION

C-40. The corps signal brigade has a range extension company that allows the grid network to flex with the dynamics of rapidly changing tactical operations. Range-extension packages are organic to this company and deploy according to METT-TC needs. The range extension company has one TACSAT platoon and four tropo platoons. Range-extension packages have two transmission media forms: TACSAT and light tropo. Both are vehicular mounted, air transportable, and have multichannel capability. Satellite availability determines the TACSAT range. The tropo range is about 160.9 kilometers (100 miles).

BASIC ASYNCHRONOUS TRANSFER MODE (ATM) TECHNOLOGY

C-41. ATM technology provides a highly efficient communications system for high-speed data switching. This capability transmits voice, video, and data in a single communication link. Figure C-6 shows the basic ATM switch technology. The system can also transmit still photography, images, and graphics.

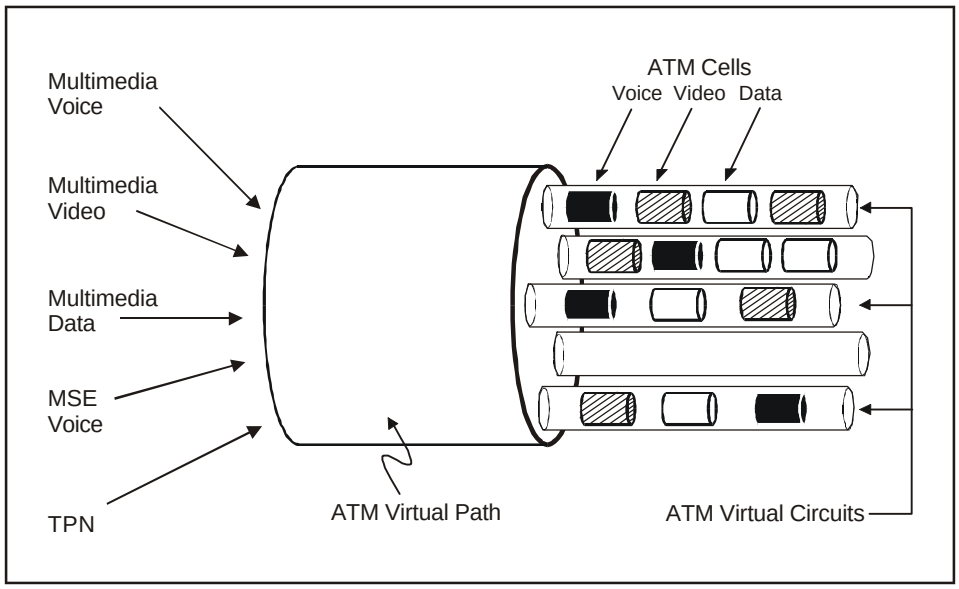

Figure C-6. ATM Switch Technology

C-42. The ATM basic technology concept involves using a virtual path identifier and a virtual circuit identifier. These identifiers are used for ATM address assignment. The path identifier directs the data to the correct receiver, and the circuit identifier identifies the different cell streams within a transmission. Virtual circuits are one-way ATM connections from source to destination, which means that two connections are required for full-duplex (two-way) communications.

HIGH-SPEED MULTIPLEXER (HSMUX) CARD

C-43. The HSMUX card enhances the capabilities of the communications modem (CM) and can terminate data rates higher than 512 kbps. The HSMUX provides up to four additional ports within a standard digital transmission group. Depending on the configuration, these ports can provide up to four synchronous data circuit-terminating equipment (DCE) RS-422 (balanced) serial data links at 64, 128, or 256 kbps. Figure C-7 shows the HSMUX SEN configuration.

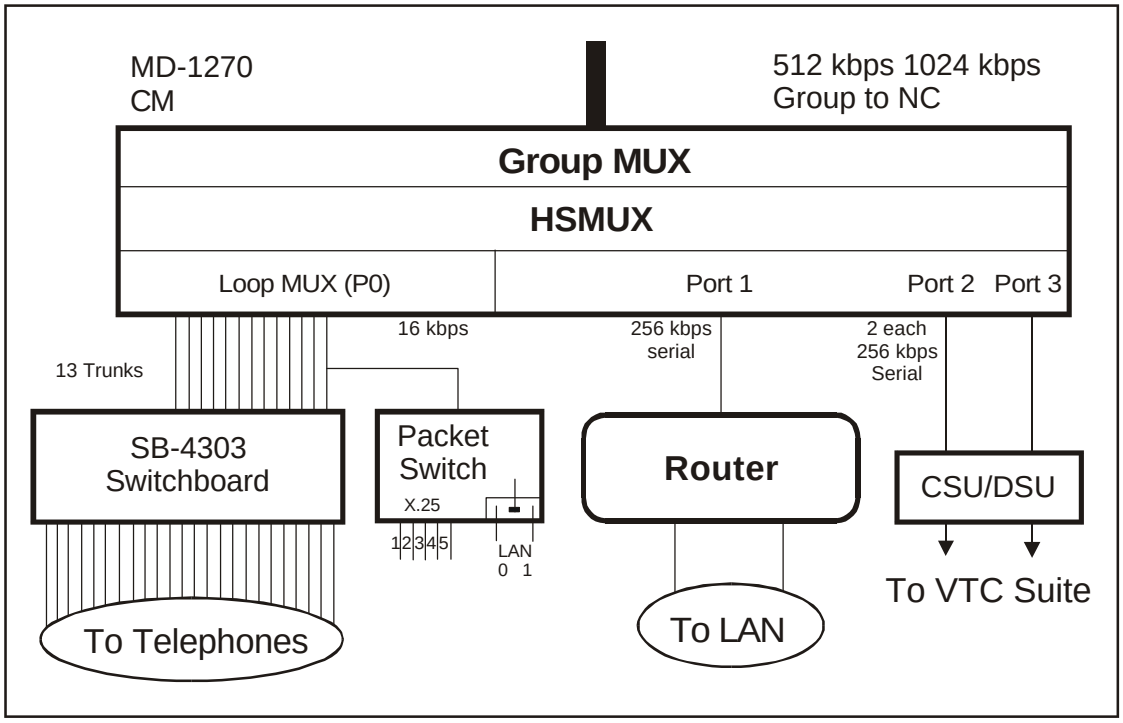

Figure C-7. HSMUX SEN Configuration

C-44. The HSMUX performs an inverse multiplexer function by taking the aggregate port rate (256 kbps) of each serial data circuit (router) and breaks it into individual 16 or 32 kbps channels on the digital transmission group. Figure C-8 shows the inverse multiplexer.

C-45. The HSMUX card replaces the A10 multiplexer/demultiplexer card in the CM, and it provides four additional serial ports. The back plane of the A10 card is not wired for access outside the CM. The individual Diphase Loop Modem-A (DLPMA) card provides access to the patch panel for the original SEN trunks. A high-speed balanced interface card (HSBIC) provides access to the new high-speed ports without modifying the CM or the line terminating unit. The HSBIC replaces one of the DLPMA cards in the CM. The HSBIC terminates two of the four HSMUX ports and extends them to the patch panel instead of the four voice trunks. These serial circuits are then patched over to the line side of the patch panel so the circuit can be extended over 26-pair to a J-Box. Figure C-9 shows the HSMUX/HSBIC SEN signal flow.

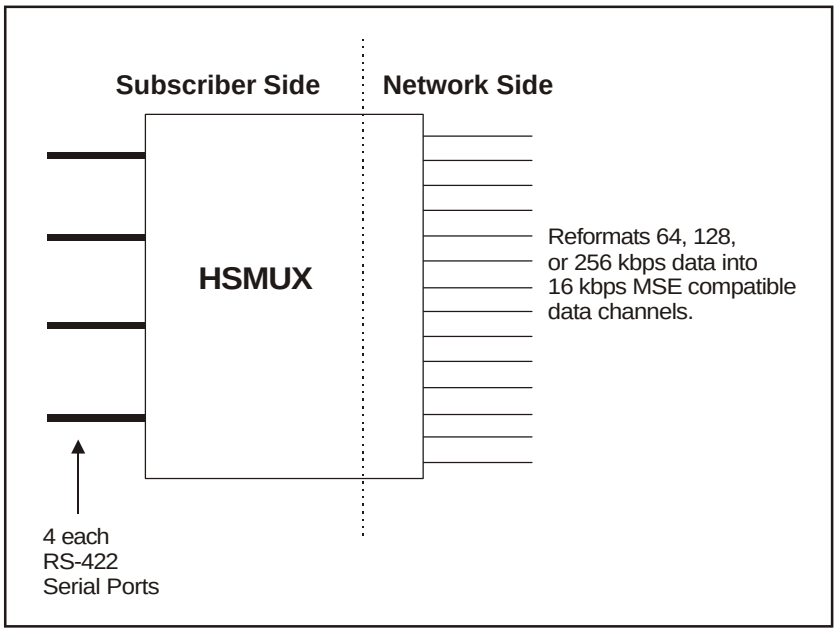

Figure C-8. Inverse Multiplexer

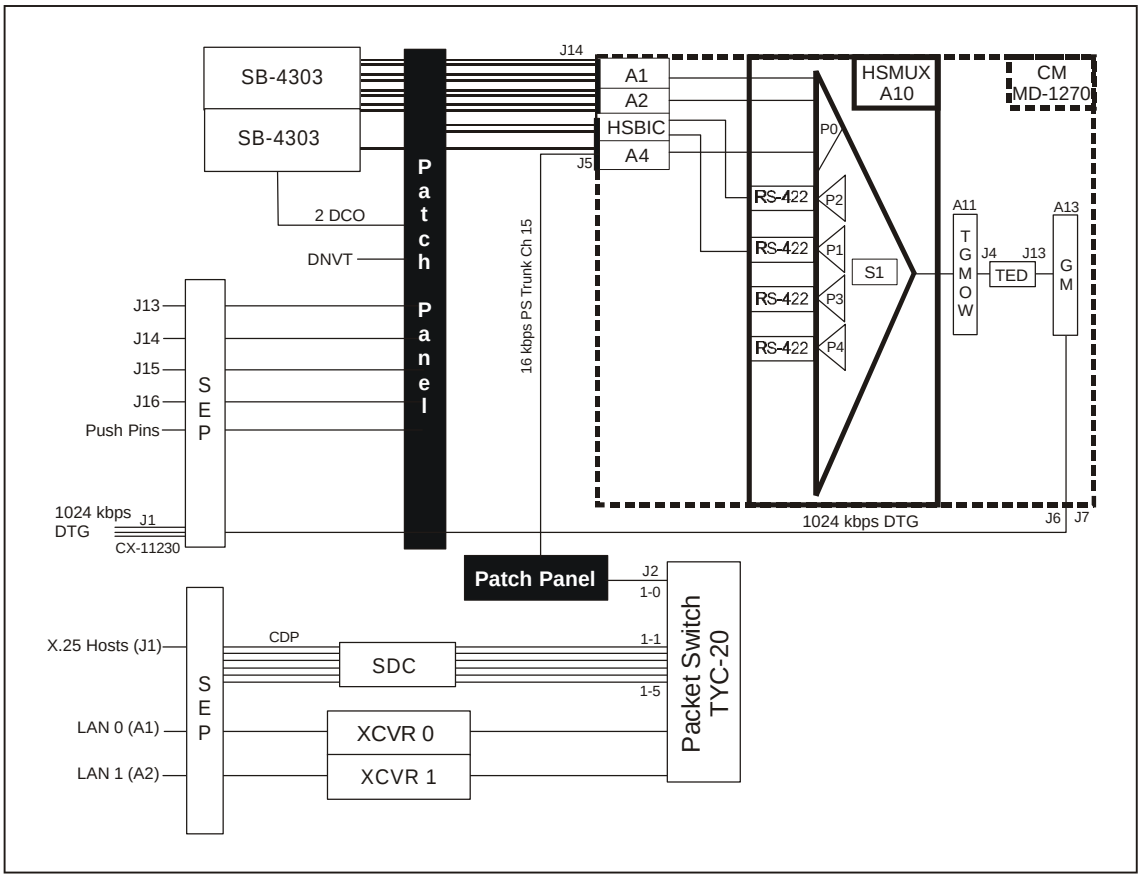

Figure C-9. HSMUX/HSBIC SEN Signal Flow

C-46. The HSMUX enhancement provides standard MSE connectivity and two high-speed ports that terminate in a router and a channel service unit/data service unit used for serial video teleconferencing. The router and the service units are safeguarded by a universal power supply. This power supply provides battery backup and acts as a direct current inverter, drawing power off the vehicle's 24-volt electrical system. Figure C-10 shows the enhanced SEN configuration signal flow.

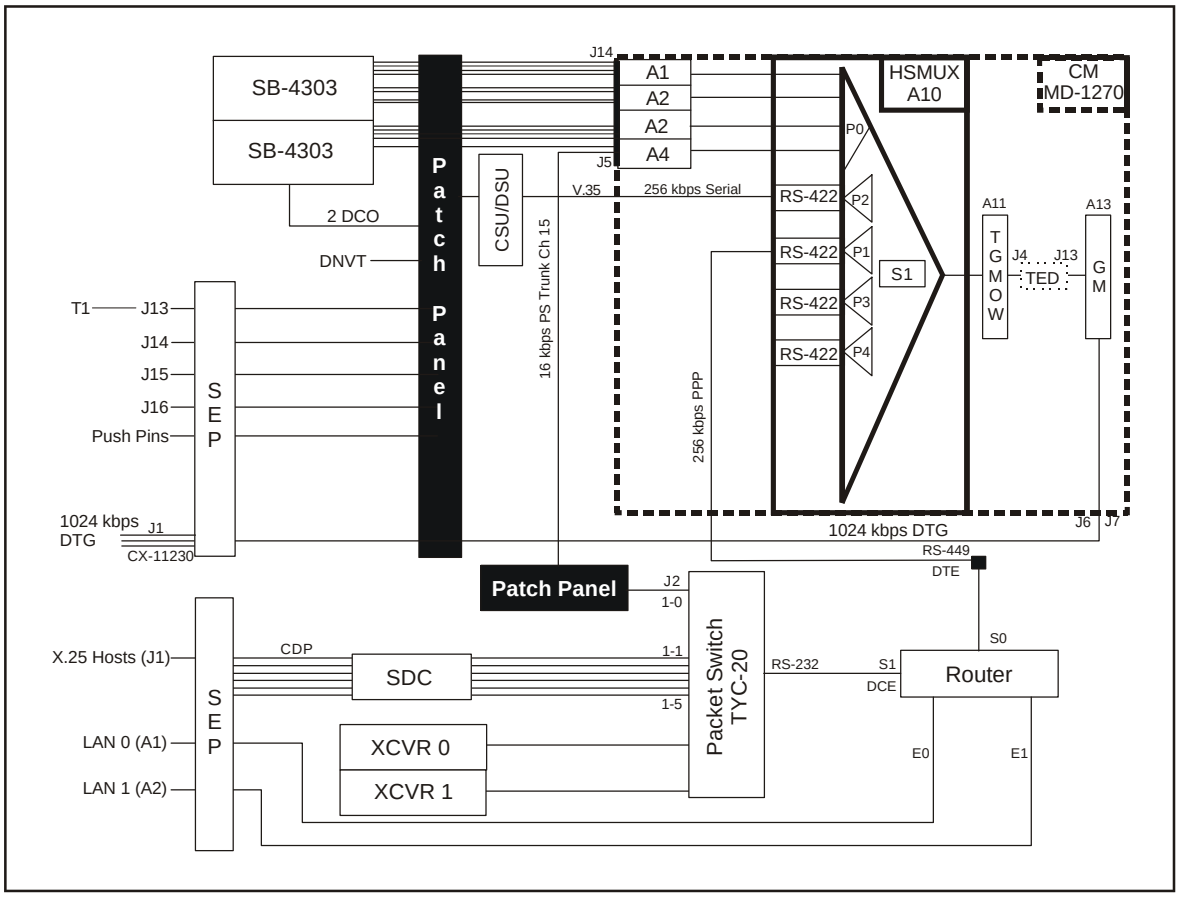

Figure C-10. Enhanced SEN Configuration/Signal Flow

Appendix D

Training and Automation Support

This appendix covers training requirements for personnel who operate and maintain information systems in a tactical LAN. It provides supervisory personnel with an understanding of the training system enabling them to effectively plan, execute, and supervise training. There is no single institution responsible for training personnel on operating information systems. This appendix provides supervisory personnel with an understanding of how the logistics system supports automation equipment for combat readiness. Detailed information on maintaining specific items can be found in appropriate technical manuals and unit SOPs. Maintenance and supply support for the SICPS shelters and communications equipment will follow the normal Army maintenance patterns.

TRAINING CONCEPT

D-1. Commanders, principal staff officers, and supervisors use information systems to support their decision-making process. They require familiarization training to understand what the BFA and its components can do to support them in performing their primary functions. They plan and supervise its use in training and combat. They require detailed training on BFA information and communications systems.

D-2. Users can be staff officers, NCOs, and soldiers who use information systems and their components as an integral part of their duties. They require detailed training on system-specific software operation, hardware operation, maintenance, and troubleshooting.

D-3. Maintainers provide M&D services for information systems and their components. These personnel require training in operating common diagnostic software (using electronic diagnostic equipment) and training on the maintenance concept.

NEW EQUIPMENT TRAINING (NET)

D-4. A team of soldiers/trainers provides NET to units when new equipment is fielded or when a major hardware or software change occurs. Developers may form mobile training teams (MTTs) to support sustainment training or hardware or software upgrade training. MTTs may present training to all target audiences, or may orient on one, two, or three specific audiences depending on the purpose of the training.

INSTITUTIONAL TRAINING

D-5. Institutional training incorporates training into existing or newly developed programs.

D-6. Personnel in field artillery, air defense artillery, military intelligence, and signal operations receive training on operating and maintaining information systems. The following courses provide this institutional training.

- The Basic Noncommissioned Officers Course (BNCOC) provides BFACS related training to junior NCOs.
- The Advanced Noncommissioned Officers Course (ANCOC) prepares graduates for supervising users and LAN management techniques.
- The Battle Staff Noncommissioned Officers' Course provides training on using information systems to students assigned to battle staff positions.
- The Warrant Officers' Course provides instruction on skill-pertinent BFACS.
- The Signal Officer Basic Course (SOBC) incorporates familiarization training.
- The Signal Officer Advanced Course (SOAC) prepares graduates to use information systems at the user level when performing their duties as staff officers and commanders.
- The Combined Arms and Services Staff School (CAS3) provides training on information systems as a staff integration tool.
- The Command and General Staff College (CGSC) provides training on using information systems to conduct combat operations as a combined arms team at division and corps level. Aspects of joint and combined operations (to include interconnection of information systems) are addressed.

EMBEDDED TRAINING

D-7. Embedded training (ET) supports individual skill development and sustainment training in the institutional and unit sustainment training environments. ET includes a capability to link one or several information systems to a local or remote simulation system to support collective training. ET incorporates performance support systems. These systems provide—

- A means to track individual user proficiency and automatically modify the amount of assistance which the system provides during operation or training.
- A context sensitive help feature, which, upon request, provides information on system operation, tailored to the process or function being performed.
- Mini tutorials that are more extensive than a help screen. This feature provides a short and context sensitive lesson aimed at helping the student negotiate complex functions.

- Courseware that is the conventional training portion of ET. It provides interactive, scenario-based instruction on all or a part of the operational software.
- Technical and field manuals via electronic media. This feature enables the user to call up a reference to a tactical or technical problem without leaving the keyboard.

UNIT SUSTAINMENT TRAINING

D-8. The unit must provide sustainment training to ensure individual skills do not decay, and collective proficiency is attained to support mission accomplishment. The G6/S6 section provides the technical expertise with the training. A unit's sustainment training program should include—

- A user training program on hardware and software for staff officers, NCOs, and soldiers.
- Maintainer training for unit maintainers and support maintenance personnel.
- Training for WAN, LAN, and BFA supervisors.
- FLC collective training at the sub unit level and for the entire unit.

OPERATOR MAINTENANCE

D-9. Each user performs PMCS as specified in the appropriate technical manuals. He also troubleshoots problems or failures before requesting assistance from the SA/NA. Each system's software package includes a diagnostic program, which runs when the system is powered up. These diagnostic routines identify failed components and/or open connections. The equipment technical manual contains troubleshooting instructions to be used when diagnostic procedures cannot run or fail to locate the problem.

UNIT-LEVEL MAINTANCE

D-10. The user requests assistance from the unit-level maintainer when he cannot diagnose a problem on his system. The maintainer is skilled in using M&D software and has the equipment needed to check cables and connectors for serviceability. When the maintainer isolates the item (a computer component or cable) which cannot be restored to operation, he prepares it for turn-in to DS maintenance.

DS MAINTENANCE

D-11. The DS maintenance facility receives the failed item and issues a replacement item to the maintainer. DS maintenance personnel install, inspect, test, and perform DS and GS maintenance on a number of assemblages. These include computers, COTS hardware, and associated equipment. The DS facility either repairs or evacuates the failed item to a supporting maintenance facility for repair. When repaired, the item is returned to the supply room.

NOTE: If the equipment is under a manufacture's warranty, it is returned to the manufacture.

D-12. The Army supply system provides support for automated devices. Repair parts stockage is limited because only minimal repairs are performed at the unit level. Self-service supply centers may stock consumables.

Glossary

A2C2	Army Airspace Command and Control
ABCS	Army Battle Command and Control System
ACUS	Area Common-User System
AD	air defense
ADA	air defense artillery
ADDS	Army Data Distribution System
AFATDS	Advanced Field Artillery Tactical Data System
AMD	air and missile defense
AMDPCS	Air And Missile Defense Planning Control System
ANCOC	Advanced Noncommissioned Officer Course
AR	Army Regulation
ASAS	All Source Analysis System
ATCCS	Army Tactical Command and Control System
ATM	asynchronous transfer mode
ATTN	attention
AUI	attachment unit interface
AUTODIN	automatic digital network
AWG	American wire gage
BADD	Battlefield Awareness Data Distribution
BDCST	Broadcast
bde	brigade
BFA	Battlefield Functional Area
BFACS	Battlefield Functional Area Control System
BIT	built-in-test
bn	battalion
BNC	Bayonet Neill Concelman [Electronics] (connector used with coaxial cable. Named after inventor.)
BNCOC	Basic Noncommissioned Officer Course
BSA	battalion/brigade support area
BVTC	battlefield video teleconferencing

C2	command and control
C2P	command and control protect
C2P-NSM	command and control protect-network security management
CAS3	Combined Arms and Services Staff School
CCI	controlled cryptographic item
cdr	commander
CGCS	Command and General Staff College
Ch	channel
chem	chemical
CHS	common hardware and software
CM	communications modem
CNR	combat net radio
co	company
CofS	Chief of Staff
COMSEC	communications security
CONUS	continental United States
COOP	Continuity of Operations Plan
COTS	commercial-off-the-shelf
CP	command post
CS	combat support
CSMA/CD	carrier sense multiple access/collision detect
CSS	combat service support
CSSAMO	combat service support automation officer
CSSCS	Combat Service Support Control System
CSU	channel service unit
CSU	channel service unit
DA	Department of the Army
DAA	designated accreditation authority
DAMMS-R	Department of the Army Movement Management System-Redesign
DCE	data circuit-terminating equipment
DCO	dial central office
DD	Department of Defense Form
DDN	defense data network
DII	defense information infrastructure

DISA	Defense Information Systems Agency
DISCOM	division support command
DISN	Defense Information Systems Network
div	division
DIVARTY	division artillery
DIX	refers to the Digital, Intel, Xerox companies
DLPMA	diphase loop modem-A
DMS	Defense Messaging System
DNMF	dismountable node management facility
DNVT	digital nonsecure voice terminal
DOD	Department of Defense
DS	direct support
DSCS	Defense Satellite Communications System
DSSCS	Defense Special Security Communications System
DSU	data service unit
DSVT	digital subscriber voice terminal
DTCU	division transportable unit
DTG	digital transmission group
DTH	down-the-hill
DVOW	digital voice orderwire
EAC	echelons above corps
ECB	echelons corps and below
e-mail	electronic mail
EMI	electromagnetic interference
Engr	engineer
EO	engagement operations
EP	electronic protect
EPLRS	Enhanced Position Location Reporting System
ET	embedded training
FAX	facsimile
FBCB2	Force XXI Battle Command - Brigade and Below
FES	force entry switch
FLC	force-level control
FM	field manual

FO	fiber optic
FOUO	For Official Use Only
FS	fire support
FSCT	fire support computer terminal
FSE	fire support element
G3	Assistant Chief of Staff, G3 (Operations and Plans)
G6	Assistant Chief of Staff, G6 (Signal Officer)
GBS	global broadcast service
GCCS-A	Global Command and Control System-Army
GCSS-A	Global Combat Support System-Army
GM	group modem
GS	general support
GSA	General Services Administration
GUI	graphic user interface
HCU	high-capacity computer unit
HF	high frequency
HMMWV	high mobility multipurpose wheeled vehicle
HQ	headquarters
HSBIC	high-speed balanced interface card
HSDL	high-speed data link
HSMUX	high-speed multiplexer
IAW	in accordance with
IEEE	Institute of Electrical and Electronic Engineers
IMETS	Integrated Meteorological System
INC	Internet controller
INSCOM	United States Army Intelligence and Security Command
IP	Internet protocol
ISS	Information Systems Security
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISSPM	Information Systems Security Program Manager
ISYSCON	integrated system control
JCS	Joint Chiefs of Staff
JTDR	joint tactical data radio

JTIDS	Joint Tactical Information Distribution System
JTRS	Joint Tactical Radio System
kbps	kilobits per second
kW	kilowatt(s)
LAN	local area network
LCU	lightweight computer unit
ldr	leader
LEN	large extension node
LENS	large extension node switch
LNO	liaison officer
LOS	line-of-sight
LRU	line replaceable unit
LTU	line terminating unit
M&D	maintenance and diagnostic
MAC	media access control
MAU	media access unit
mbps	megabits per second
MCS	Maneuver Control System
METT-TC	mission, enemy, terrain, troops, time, and civilian consideration
MILSATCOM	military satellite communications
MILSTAR	military strategic and tactical relay
MMC	materiel management center
MSE	mobile subscriber equipment
MSRT	mobile subscriber radiotelephone terminal
MTOE	modification table of organization and equipment
MTT	mobile training team
mux	multiplex/multiplexer
mvr	maneuver
NA	network administrator
NAI	net radio interface
NATO	North Atlantic Treaty Organization
NC	node center
NCO	noncommissioned officer
NCOIC	noncommissioned officer in charge

NCS	node center switch
NET	new equipment training
NIC	network interface card
NIPRNET	Nonclassified Internet Protocol Router Network
NMF	node management facility
NMT	network management tool
NMT(B2)	network management tool (brigade and below)
No	number
NPE	networking, planning, and engineering
NPT	network planning tool
NRI	net radio interface
NSA	National Security Agency
NSO	Network Security Officer
NTDR	near-term data radio
OC3	optical carrier (level 3) [SONET data rate of 155.52 mbps which is 3 STS-1 or OC1 levels.]
ohm	unit of resistance
OPLAN	operation plan
OPORD	operation order
ops	operations
OPSEC	operations security
OSI RM	open systems interconnect reference model
OSPF	open shortest-path first
PC	personal computer
PCZ	physical control zone
PDS	protected distribution system
PLL	prescribed load list
plt	platoon
PMCS	preventive maintenance checks and services
PNS	primary node switch
POC	point of contact
PS	packet switch
PTR	problem trouble record (or report)
RAM	random access memory

RAU radio access unit
RBM received broadcast manager
S2 Intelligence Officer (US Army)
S3 Operations and Training Officer (US Army)
S4 Supply Officer (US Army)
S6 Signal Officer (US Army)
SA system administrator
SAAS Standard Army Ammunition System
SAMS Standard Army Maintenance System
SARSS Standard Army Retail Supply System
SB switchboard
SCC-2 system control center-2
SCI special category information
SDC signal data converter
SDNRI secure digital net radio interface
SDNRIU secure digital net radio interface unit
SEN small extension node
SENS small extension node switch
SEP signal entry panel
Seq sequence
SF standard form
SHF super high frequency
SICPS Standard Integrated Command Post System
SIDPERS-3 Standard Installation/Division Personnel System-3
SINCGARS Single-Channel Ground and Airborne Radio System
SIP System Improvement Program
SNS secondary node switch
SOAC Signal Officer Advanced Course
SOBC Signal Officer Basic Course
SOI signal operation instructions
SOP standing operating procedures
SPBS-R Standard Property Book System-Redesign
SSA Supply Support Activity
STAMIS Standard Army Management Information System

STP	shielded-twisted pair
SU	situational understanding
SYSCON	system control
TACSAT	tactical satellite
TAMMIS	Theater Army Medical Management Information System
TAPDB	Total Army Personnel Database
TB	technical bulletin
TBD	to be determined
TCU	transportable computer unit
TED	trunk encryption device
TEMPEST	transient electromagnetic pulse emanations standard
TGMOW	transmission group modem and orderwire
TI	tactical Internet
TIP	tent interface panel
TM	technical manual
TMG	tactical multinet gateway
TOC	tactical operations center
TOE	table(s) of organization and equipment
TP	telephone
TPN	tactical packet network
TRI-TAC	Tri-Services Tactical Communications
tropo	tropospheric scatter
TS	TOP SECRET
UHF	ultra high frequency
ULLS	unit-level logistics system
ULLS-A	unit-level logistics system-aviation
ULLS-G	unit-level logistics system-ground
ULLS-S4	unit-level logistics system-S4
US	United States (of America)
USMTF	United States Message Text Format
UTP	unshielded-twisted pair
VA	Virginia
VHF	very high frequency
VHSIC	very high-speed integrated circuit

VMF	variable message format
WAN	wide area network
WWW	World Wide Web
XCVR	transceiver

Bibliography

AR 25-1. *The Army Information Resources Management Program*. 25 March 1997.

AR 190-13. *The Army Physical Security Program*. 30 September 1993.

AR 350-41. *Training in Units.* 19 March 1993.

AR 380-5. *Department of the Army Information Security Program*. 25 February 1988.

AR 380-19. *Information Systems Security*. 27 February 1998.

AR 380-67. *The Department of the Army Personnel Security Program*. 09 September 1988.

AR 381-14. *(S) Technical Surveillance Countermeasures (TSCM) (U).* 03 October 1986.

AR 381-19. *Intelligence Dissemination and Production Support.* 16 February 1988.

AR 710-2. *Inventory Management Supply Policy Below the Wholesale Level.* 31 October 1997.

DA Form 2028. *Recommended Changes to Publications and Blank Forms.* 01 February 1974.

DA Form 4569. *Requisition Code Sheet (only available in electronic media).* July 1996

DA Pam 350-40. *Army Modernization Training Plans for New and Displaced Equipment*. 17 August 1989.

DD Form 2501. *Courier Authorization Card*. March 1988.

FM 1-100. *Army Aviation Operations.* 21 February 1997.

FM 1-111. *Aviation Brigades.* 27 October 1997.

FM 1-112. *Attack Helicopter Operations.* 02 April 1997.

FM 3-101. *Chemical Staffs and Units.* 19 November 1993.

FM 5-100. *Engineer Operations.* 27 February 1996.

FM 6-20-30. *Tactics, Techniques, and Procedures for Fire Support for Corps and Division Operations.* 18 October 1989.

FM 6-20-40. *Tactics, Techniques, and Procedures for Fire Support for Brigade Operations (Heavy).* 05 January 1990.

FM 6-20-50. *Tactics, Techniques, and Procedures for Fire Support for Brigade Operations (Light).* 05 January 1990.

FM 7-20. *The Infantry Battalion*. 06 April 1992.

FM 7-30. *The Infantry Brigade.* 03 October 1995.

FM 11-32. *Combat Net Radio Operations.* 15 October 1990.

FM 11-43. *The Signal Leader's Guide.* 12 June 1995.

FM 11-50. *Combat Communications within the Division (Heavy and Light).* 04 April 1991.

FM 11-55. *Mobile Subscriber Equipment (MSE) Operations.* 22 June 1999.

FM 17-95. *Cavalry Operations.* 24 December 1996.

FM 19-30. *Physical Security.* 01 March 1979.

FM 25-100. *Training the Force.* 15 November 1988.

FM 34-10. *Division Intelligence and Electronics Warfare Operations.* 25 November 1986.

FM 34-25. *Corps Intelligence and Electronic Warfare Operations.* 30 September 1987.

FM 44-64. *SHORAD Battalion and Battery Operations.* 05 June 1997.

FM 44-100. *US Army Air Defense Operations.* 15 June 1995.

FM 63-2. *Division Support Command, Armored, Infantry, and Mechanized Infantry Divisions.* 20 May 1991.

FM 63-21. *Main Support Battalion.* 07 August 1990.

FM 63-3. *Corps Support Command.* 30 September 1993.

FM 71-2. *The Tank and Mechanized Infantry Battalion Task Force (reprinted w/basic incl C1, 17 August 1994).* 24 September 1988.

FM 71-3. *The Armored and Mechanized Infantry Brigade.* 08 January 1996.

FM 71-100. *Division Operations.* 28 August 1996.

FM 90-13. *River-Crossing Operations {MCWP 3-17.1}.* 26 January 1998.

FM 100-5. *Operations.* 14 June 1993.

FM 100-6. *Information Operations.* 27 August 1996.

FM 100-10. *Combat Service Support.* 03 October 1995.

FM 100-15. *Corps Operations.* 29 October 1996.

FM 100-103. *Army Airspace Command and Control in a Combat Zone.* 07 October 1987.

FM 101-5. *Staff Organization and Operations.* 31 May 1997.

SF Form 707. *SECRET Label for ADP Media.* January 1987.

SF Form 710. *Unclassified Label for ADP Media.* January 1987.

SF Form 711. *Data Descriptor Label for ADP Media.* January 1987.

Index

FM 24-7
8 OCTOBER 1999

By Order of the Secretary of the Army:

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Official:

JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army
9924402

DISTRIBUTION:

Active Army, Army National Guard, and U.S. Army Reserve: To be distributed in accordance with the initial distribution number 115439, requirements for FM 24-7.

PIN: 077514-000