PNNL-13807

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Tradeoff Analysis for Combat Service Support Wireless Communications Alternatives

JR Burnette
CC Thibodeau
FL Greitzer

February 2002

Pacific Northwest
NATIONAL LABORATORY

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

This document was printed on recycled paper.
(9/2003)

PNNL-13807

Tradeoff Analysis for Combat Service Support Wireless Communications Alternatives

John R. Burnette
Christopher C. Thibodeau
Frank L. Greitzer

February 22, 2002

Prepared for
U.S. Army Logistics Integration Agency
under a Related Services Agreement
with the U.S. Department of Energy
Contract DE-AC06-76RLO 1830

Pacific Northwest National Laboratory
Operated for the U.S. Department of Energy
by Battelle Memorial Institute

Contents

Tradeoff Analysis for Combat Service Support Wireless Communications Alternatives

Executive Summary

The Combat Service Support (CSS) community has an urgent operational requirement to send data between Standard Army Management Information Systems (STAMIS) and Army Battle Command Systems. As the Army moves toward more mobile and agile forces and continued sustainment of numerous high-cost legacy STAMIS, the requirement for wireless connectivity and a wireless network to the CSS supporting organizations has become ever more critical. There are currently several Army communications initiatives underway to resolve this wireless connectivity issue. However, to fully appreciate and understand the value of these initiatives to the CSS community, a Tradeoff Analysis is needed to examine the various on-going Service wireless CSS communication initiatives and Commercial alternatives. The Army is faced with an immediate near-term wireless CSS communication connectivity issue, which must be resolved now. The present study seeks to identify and assess solutions.

The present study has identified the following issues that impede Interim Brigade Combat Team (IBCT) communication system integration:

- Legacy logistic STAMIS are difficult to configure for a network environment
- Existing tactical network support structure does not support unclassified data.
- Distance between the CRT and the Brigade Support Battalion (BSB) is typically outside the existing data communication range.
- The IBCT system architecture is unique and is evolving.

To enable the IBCT to send data between STAMIS systems and Army battle command systems, logistics communications systems are needed that meet the following "core" requirements:

1. Support a light force with a small footprint
2. Low density of technical support required
3. Supports split-basing and interim staging bases
4. Supports unclassified data network for the forward CRT
5. Support Unit Level Logistics System–Ground (ULLS-G) functionality in the CRT forward
6. CRT Communications work in all terrain conditions
7. CRT Communications system is integrated with other enablers

We refer to these as "core" requirements that any acceptable solution must satisfy. Additional factors that should be used to discriminate among possible alternative wireless communications architectures are bandwidth/transmission rates and transmission range. These requirements and performance factors were used as criteria in identifying gaps in

technology and to assess the potential for various technology options to fill these gaps in establishing a workable CSS Communication solution for the IBCT.

The following CSS wireless alternatives were examined as possible solutions for the IBCT CSS Communication problems:

Current Baseline. The CRT and its STAMIS systems will be located in the Brigade Support Area (BSA). If the CRT deploys forward, the STAMIS system will remain in the BSA. The CRT will provide updates to the ULLS-G system via FBCB2.

Option 1—SINCGARS (ASIP). Utilizes the Single Channel Ground and Airborne Radio System (SINCGARS) ASIP (Advanced SINCGARS Improvement Program) radios located in the brigade to transmit logistics data. This solution requires additional Windows OS computers, communication software, and a non-standard interface cable. It is not recommended as a primary means of communication because of its cumbersome configuration and slow transfer speed.

Option 2—Interim Wireless. Interim solution involving Wireless Combat Service Support Automated Information System Interface (CAISI), Near Term Digital Radio (NTDR), and an In-Line Network Encryption (INE) device (TACLANE). The combination of these systems would provide the logistician with near real time secure data processing without degrading the tactical command and control network. This would require reorganization of assets within the Combat Trains Command Post (CTCP) and would require the use of additional INEs.

Option 3—Cellular Satellite Communication. Utilize cellular satellite communications and replace the current legacy STAMIS communication software to enable connectivity with wireless technology. Satellite communications eliminates hand carrying of diskettes (sneaker nets) from the BSA and the CRT.

Option 4—3rd Generation Wireless Technology. Future Fix/Objective or long-term solution involving an upgrade to CAISI Wireless system and Code Division Multiple Access (CDMA) cellular technology. Third generation wireless technology achieves a 2.4 Mbs transmission rate, and CDMA cellular technology achieves a BSA range of 6-12 Km.

Option 1 provides wireless connectivity between the BSA and the CRT, but does not provide a complete solution since STAMIS limitations require sneaker net within the BSA and the CRT. Option 2 provides an interim wireless solution that eliminates sneaker net, but still suffers from terrain and distance limits. Option 3 provides cellular satellite communications that support data and voice and eliminate the terrain and distance constraints. Option 4 uses third generation wireless technology (digital cellular within the BSA and satellite between the BSA and CRT). Options 3 and 4 offer clear advantages and, though they are not being considered for IBCT-1 or IBCT-2, they should be considered for later IBCTs.

Tradeoff Analysis for Combat Service Support Wireless Communications Alternatives

1. Introduction

1.1 Problem and Background

The CSS community has an urgent operational requirement to send data between Standard Army Management Information Systems (STAMIS) and Army Battle Command Systems. As the Army moves toward more mobile and agile forces and continued sustainment of numerous high-cost legacy STAMIS systems, the requirement for wireless connectivity and a wireless network to the CSS supporting organizations has become ever more critical. Wireless connectivity is essential between the Warfighter's Army Battle Command Systems (ABCS) and the battalion and brigade level CSS organizations. Several Army communications initiatives are underway to resolve this wireless connectivity issue. However, to fully appreciate and understand the value of these initiatives to the Combat Service Support (CSS) community, a Tradeoff Analysis is needed to examine the various on-going Service wireless CSS communications initiatives and Commercial alternatives (e.g. Web-Enabled, Satellite, Cellular, or a Combination). The required study should identify the most feasible and cost effective immediate near-term wireless CSS communications alternatives, and provide a proposed "first-order" (high level) wireless CSS communications operational architecture that will support the vision of the Revolution in Military Logistics (RML), the Distribution Based Logistics System objectives, and the army transformation.

It should be noted that the communications technologies and future Army communication systems, such as the Warfighter Information Network-Tactical (WIN-T) currently under development, are expected to resolve the CSS assured communications issue in the mid-far term (5-10 years). However, the Army is faced with an immediate near-term wireless CSS communications connectivity issue, which must be resolved now. The Army's vision to reduce the logistics footprint cannot be achieved without this CSS connectivity.

The CSS Communications Tradeoff Analysis will yield the following benefits:

- The analysis fully supports and is essential to effectively executing the Army Strategic Logistics Plan (ASLP) and the Deputy Chief of Staff of Logistics (DCSLOG) RML, Distribution-Based Logistics System (DBLS), and Embedded Diagnostics and Prognostics Synchronization (EDAPS) initiatives that support the Army transformation in achieving the Objective Force.

- The First Order CSS Communication Operational Architecture will identify the potential resources required to establish a near term wireless CSS communication network for moving logistics information from the platform to the Weapon System Manager.

- The analysis will assist the Army to become more responsive, deployable, agile, versatile, survivable and sustainable.

1.2 Objectives

The CSS Communications Tradeoff Analysis has the following objectives, which are focused on the Interim Brigade Combat Team (IBCT):

1. **Identify, define** and clearly **delineate** wireless CSS communication connectivity **requirements** that are essential in developing an interim CSS wireless architecture.
2. **Identify and compare** currently available wireless communication technologies that could be implemented to solve the wireless connectivity issue between the Warfighter's Army Battle Command Systems (ABCS) and the battalion and brigade level CSS organizations.
3. **Evaluate** these wireless communication technologies to determine the **most feasible** and **cost effective** wireless communication connectivity solution for transmitting logistics information from the Platform to the Combat Service Support Control System (CSSCS), STAMIS systems and to the Weapon System Manager.
4. **Describe** a "First-Order" wireless CSS **operational communication architecture** that will **identify how** these wireless communication technologies could support the CSS community from the Platform to the Weapon System Manager **using best business practices**.
5. **Brief LIA on CSS Communications initiative at Ft. Lewis**. PNNL's Communication Task Force member at Ft. Lewis cell will provide near-term and mid-term briefing to LIA staff on the Ft. Lewis CSS Communications architecture and initiatives for the IBCT.
6. **Coordinate** this effort with ongoing **Logistics Command and Control Advanced Concept Technology Demonstration** (**LOGC2 ACTD) at CECOM** by collaborating with the LOGC2 ACTD Program Manager at CECOM.

2. IBCT Tactical Internet

2.1 Notional System Concept

The term Tactical Internet (TI) refers to both the physical communications network that provides the data backbone and the conceptual integrated combat zone information infrastructure. The TI is designed to electronically connect all users to critical Command and Control (C2) Systems and Situational Awareness (SA) architecture information. The TI is the integration of tactical radios and routers to form a voice and data network that transports C2 and SA data for tactical users. Principal TI equipment is shown in Figure 2-1. Current primary systems using TI are Force XXI Battle Command Brigade and Below (FBCB2) and Forward Area Air Defense Command and Control and Intelligence (FAADC2I). The TI extends existing digital communications from brigade headquarters to the foxhole. The TI is an integrated part of the Warfighter Information Network (WIN) providing digital communication to all echelons (Foxhole to Power Projection Sustaining Base). As the TI matures, plans are to provide digital transport services to all Battlefield Functional Areas (BFA). The TI uses JTA-A compliant protocols.

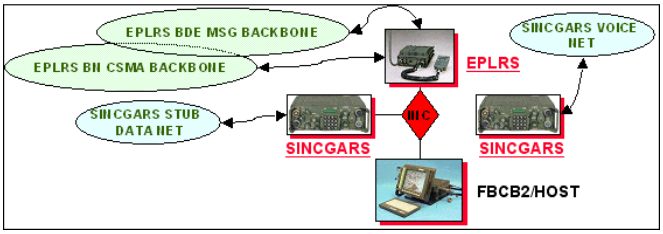
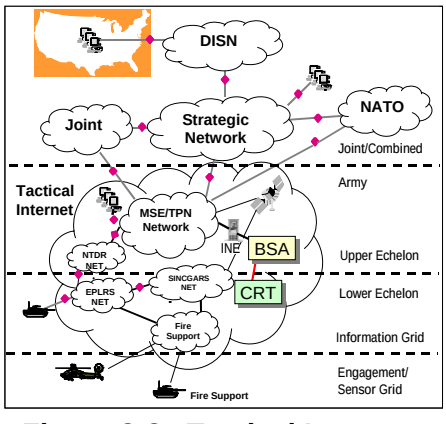


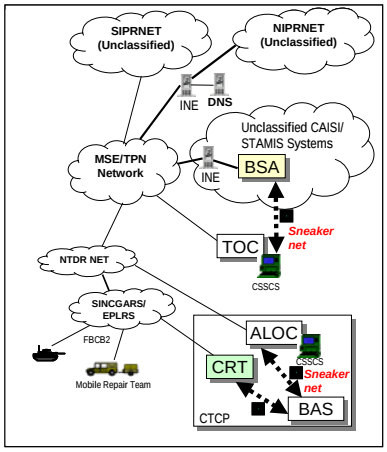
Figure 2-1 Principal Tactical Internet

The current notional concept of the TI includes several distinct layers, as shown in Figure 2-2. The top layer is made up of Mobile Subscriber Equipment (MSE) multi-channel satellite systems and existing tactical packet node (TPN) system. The MSE and TPN structure will transition to WIN-T as that program matures and is fielded. The lower TI is the communication support system for units found at the brigade, company and below level. Equipment such as FBCB2 computers, Enhanced Position Location Reporting Systems (EPLRS), and SINGCARS radios are networked to make up the lower TI structure.

The upper TI uses all available in-theater communications assets to enable the corps, division, brigade, and battalions to communicate and share information. The upper TI makes use of existing MSE and TPN components containing Asynchronous Transfer Mode (ATM) technologies, Near-Term Tactical Radio (NTDR), and multi channel secure satellite systems such as Secure Mobile Anti-jam Reliable Tactical Terminal (SMART-T) and the Tri-band Advanced Range Extension Terminal.



The lower half of the TI provides the C2 communications path for Brigade, Battalion and company level operations inside the theatre combat zone. The lower TI uses FBCB2 host computers and Appliqué and Embedded battle command (EBC) software. The communications path for the lower half of the TI is provided by EPLRS, NTDR and Single Channel Ground and Airborne Radio System (SINCGARS), with RS-232 interface. FBCB2 also provides the combat service support functionality for CSS situational awareness. The FBCB2 CSS functionality includes the following: logistics situational reports (LOGSITREP), personnel situation report (PERSITREP), supply point and field services status report, command tracked item list update message (CTIL-BRIL), task management suite (including call for support), and other reports. The FBCB2 also provides for limited free-text messages. Figure 2-3 shows the tactical Logistics Communication architecture for the IBCT.



As shown in Figure 2-3, the Combat Trains Command Post (CTCP) consists of the Administrative Logistics Operations Center (ALOC), the Combat Repair Team (CRT)

and the Battalion Aid Station (BAS). The CTCP is located 25-26 Km forward of the Brigade Support Area (BSA). All vehicles within the CRT are FBCB2 equipped. Equipment status reports are transmitted simultaneously to the CRT and the CSSCS system located within the Tactical Operations Center (TOC). In addition, the ALOC uses NTDR communications to transmit classified data to support the S1-S4 shop and the CSSCS workstation. The FBCB2 provides free text message capability across a classified network.

2.2 Current configuration of IBCT Tactical Internet

The IBCT Signal Company provides the strong C2 communications backbone required to support distributed operations within urban and complex terrain across potentially significant distances, as well as the linkages required for effective communications with division and higher echelons.

The communications system within the IBCT is founded on a TI consisting of EPLRS, SINCGARS, NTDR, and routers. The TI provides secure, jam resistant, on the move, non-line of sight, long range, data communications for multiple subnets while operating in a frequency-constrained environment. Internal IBCT communications systems support stationary and on the move distribution of data across the tactical communications network two echelons up and two echelons down (to include: adjacent, joint and allied units). The communication system links with a selectable set of external information and Reconnaissance Surveillance Target Acquisition (RSTA) platforms, adjacent, supported, and supporting units according to mission needs and Theater/National architectures. International communications interoperability is required and essential.

The IBCT communications system and network are open and modular in construction. This open architecture facilitates future growth/modification to the internal network system. The open architecture also facilitates the addition or deletion of many different types of communication devices (to include Joint/Combined and Coalition systems) into the internal network. This flexibility is the foundation that allows the IBCT to exchange information with Joint, Combined and Coalition forces.

Dispersed operations require the IBCT's C2 support network to rely upon several means of range extension to maintain information connectivity within the IBCT. Tactical satellite assets provide responsive, high bandwidth voice, video and data support to the IBCT's command elements. At the Commander's direction, TACSAT (Tactical Communications Satellite) can provide intra-IBCT "enclave" connectivity, as required. TI range extension provides maneuver and RSTA C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) network support across complex terrain via airborne platforms such as the Airborne Communications Node (CAN) and Tactical Unmanned Airborne Vehicle (TUAV). The IBCT maintains TI retransmission (RETRANS) assets to support operations from within secured locations to realize economies in force protection. If required, these assets provide critical range extension capability in the event of failure or absence of airborne platforms. Finally, the preferred IBCT radio systems execute multi-point relay of data.

In essence, each member of individual data networks serve as a RETRANS means to transfer C4ISR data across the combat zone.

2.3 Issues

Some of the issues associated with the IBCT TI are doctrinal support of the unclassified infrastructure, limited technical support for the unclassified infrastructure, and lack of unclassified infrastructure for the combat zone.

Classified-to-unclassified interface. The current Tactical C4ISR architecture was designed to support a secret and higher infrastructure. The current STAMIS family of applications is not certified to run at the secret level, and the higher echelon systems that STAMIS has to communicate with are also unclassified. Currently, there does not exist a seamless automated process to move unclassified logistic data to and from the classified network. Technology does exist that can be configured and certified to pass this type of information between networks (e.g., secure GateGuard is a remote automatic digital network, or AUTODIN, terminal, which operates on desktop and laptop personal computers). However, this technology requires a heavy system administration overhead. Finally, because there is no plan to upgrade STAMIS security requirements, actual transfer of information between networks will continue to be done by means of manual re-keying or hand-carrying of diskette (sneaker net).

Limited technical staff to support unclassified network infrastructure. To make STAMIS work in the tactical environment, several fixes have been put into place but are not supported by official doctrine. The Logistic community has procured several quick initiatives to place into service an interim unclassified network infrastructure with minimal organization support structure. For example, the Combat Service Support Automated Information System Interface (CAISI) unclassified network infrastructure introduced additional support items such as the NES (Network Encryption System), an unclassified DNS (Domain Name Server). The burden of supporting these systems for the IBCT falls on the S6 (Communications Staff Officer).

Lack of unclassified infrastructure for the combat zone. Predominantly, forward elements such as the CRT and Mobile Repair Team have only classified communications. The only way to transmit the unclassified logistics information from the CRT is via clear text messages, voice transmissions, or sneaker net to the unclassified CAISI/STAMIS systems located within the BSA.

3. IBCT Logistics Information System Distribution and Supporting Communications

3.1 Notional System Concept

This section provides an overview of the IBCT Organizational and Operational (O&O) concept, as described in Chapter 10 of the IBCT O&O Plan *[2]*.

BSB Mission Description
The Brigade Support Battalion (BSB) provides centrally managed, distribution-based combat service support (CSS) to the Interim Brigade Combat Team (IBCT) to sustain its operational employment in joint contingencies. The BSB executes a unique, execution-focused concept of support that is fully integrated with the Brigade concept of operations and scheme of maneuver. In accordance with its focus on execution, BSB support operations are characterized by continuous adaptation and creative tailoring, based on unit operational tempos, commander-designated priorities for support, and the frequently changing requirements of the combat zone. Through centralized management and CSS situational understanding, the BSB combines unit level distribution and area supply points to insure that services and supplies are delivered where, and as they are needed. This coordination allows the IBCT to synchronize logistical rhythm with the battle rhythm. Logistical flexibility and dynamic tasking of BSB support elements typify BSB operations. The unit's effectiveness depends on continuous integration of operational and logistical planning; employment of the latest advances in CSS command and control; enhanced CSS situational understanding; information fusion; and considerable scaling and augmentation to accomplish its mission. This scaling and augmentation may be provided through joint, multinational, host nation, or commercial sources.

Operationally, the IBCT is doctrinally portrayed to fight under a division. The IBCT can also fight under the direct control of a corps headquarters, within a joint or combined command. As such, the BSB will normally be connected to a higher echelon level of CSS, either directly or through reach (or reachback) operations. Reachback is the electronic ability to exploit resources that are not located with the deployed unit, thus enhancing the operational agility of the unit by improving its access to timely and relevant information *[3]*. Reachback linkages of the BSB are referred to as "echelons above brigade" (EAB), and include, as appropriate, any organization from which the BSB would gain the next higher level of CSS support.

The BSB is the base organization from which CSS force packages are tailored for each contingency. It is strategically, operationally, and tactically mobile and focused on the sustainment demands dictated by each specific contingency. It is capable of both providing a smaller element of itself to support a single battalion task force, and receiving a combat service support company (CSSC) to supplement the CSS capability for the IBCT. CSS is structured to optimize the use of CSS resources (through CSS situational understanding and the IBCT common operating picture) and minimize the operational and CSS footprint in the area of operations. Maximizing internal lift capabilities and

exploiting the commonality of combat and support vehicles and their systems will enhance logistics support and reduce both deployment and sustainment requirements

IBCT CSS Roles & Responsibilities

To achieve collaborated and coordinated operations between maneuver and CSS, it is important that an operational framework of roles and responsibilities exits throughout the IBCT. The following is a list of Brigade Combat Team (BCT) organizations and their key roles and responsibilities:

- BCT S1 & Section—provides personnel accounting, casualty reporting, medical platoon management, and advice to the BCT Commander on personnel issues.
- BCT S4 & Section—serves as BCT Commander's principal logistics planner.
- BCT S3 & Section—collaborates with BCT S4 and BSB SPO during MDMP to determine COA CSS supportability and feasibility, selects/manages supply routes, air routes, medevac routes, and terrain for logistics operations.
- BCT Surgeon—focal point of all medical care within the BCT.
- BSB Cdr—principle logistics operator for the IBCT.
- BSB SPO & Section—establishes daily logistics plan and synchronization matrix, planning both current and future logistics operations; advises BSB CDR on requirements and available assets; resolves logistical support problems; manages CSSCS.
- BSB S4 & Section—Area Support Planner for BSA, BSB Logistics Planner.
- BSB S1 & Section—principle Personnel Services planner to the BSB Commander.
- HDC Company Commander—focal point of all sustainment distribution within the BCT.
- FMC Company Commander—focal point of all maintenance within the BCT; executes the BCT and BSB Commanders' maintenance plan; provides area support within the BSA.
- BSMC Company Commander--provides area medical support to the BSA.
- Battalion/Squadron S4 & Section—principle CSS planner to the battalion commander.
- Battalion/Squadron S3 & Section—collaborates with Bn/Sqdn S4, BCT S4 and BSB SPO to synchronize CSS and maneuver operations; selects/manages supply routes, air routes, medevac routes, and terrain for logistics operations within battalion/squadron AO.
- Battalion S1 & Section—principal personnel services planner to the Bn Cdr
- Battalion/Squadron HHC/HHT/HSB Cdrs—responsible for Bn/Sqdn TOC life support mission.
- Battalion HHC Xos--functions as the battalion maintenance officer (BMO) under the supervision of the Bn/Sqdn S4.
- Bn/Sqdn HHC/HHT/HSB 1SGs— Company level "CSS Manager" responsible for the health and welfare of soldiers; facilitates area support to all elements in the Battalion Area; assists in coordination for sustainment support and delivery to separates and to platoons

- Unit (Line Co) 1SGs— Company level "CSS Manager" responsible for the health and welfare of soldiers; directs and supervises sustainment deliveries to platoons; maintains visibility over unit log status.
- Company/Troop/Battery Supply Sergeants—coordinates company supply functions.
- Platoon Sergeants—typically, the data point of entry for all platoon CSS information; initiates requests for supplies and manages the receipt and transfer of supplies for his platoon.
- Squad Leaders—identifies and forwards squad requirements to Platoon Sergeant.

Concept of Support Operations

The BSB executes a unique, execution-focused concept of support that is fully integrated with the Brigade concept of operations and scheme of maneuver. Combat service support is performed as far forward as possible, given the tactical situation. Other considerations—beyond Mission, Enemy, Terrain, Troops, Time, Civilians (METT-TC)—include distance and volume of sustainment required.

The BSB commander is the BCT commander's senior logistician and serves as the single CSS operator for support to the IBCT. His battle staff monitors and manages sustainment operations through an array of digital information systems and other technological innovations. Superior situational understanding, provided by such systems as Global Combat Support System – Army (GCSS-A), Combat Service Support Control System [CSSCS], Force XXI Battle Command Brigade and Below [FBCB2], and Movement Tracking System [MTS] permits CSS commanders and staff to actively anticipate BCT support requirements throughout operations.

Communication linkages between STAMIS systems represent important enablers of the IBCT mission. To facilitate rapid and efficient transfer of information, STAMIS systems located both inside and outside of the BSA must be able to send and receive data electronically. For example, the Combat Repair Teams (CRT) and the Battalion Aid Stations (BAS) that are located forward in the Combat Trains Command Post (CTCP) must be able to send and receive data from other BCT organizations located in the BSA. CSS elements will have a common relevant operating picture of the battlefield and its sustainment requirements provided by FBCB2 and CSSCS, which will enable CSS commanders and battle staffs to anticipate, plan and execute support requirements and maximize battlefield distribution. This will require CSS units to have early and continuous access to robust communications networks such as the Warfighter Information Network, that enable them to review and pass information from support elements to theater or continental US providers.

The fundamental principles supporting this concept are:

- *Execution-centric Support*. Execution-centric support encompasses the intent to provide CSS support that can be continuously adapted to IBCT and sub-unit operations even *as they are being executed*, while simultaneously building combat power for the next battle.
- *Anticipatory Logistics*. Anticipatory logistics expands the concept of execution-focused support beyond the current or immediate sustainment requirements to include

the anticipation of requirements that can be predicted and planned with accuracy. Anticipatory logistics can be based on several factors including: operational plans and orders; demand history; prognostics and diagnostics; advanced planning and scheduling; operational experience; BCT usage rates; and fleet management.

- *Unity of Command and Control*. The principle of unity of command is combined with unity of effort to insure positive, effective command and control of CSS operations within the IBCT.
- *Centralized Management*. CSS assets within IBCT units are designed to minimize CSS deployment requirements and in-theater infrastructure. Given that design parameter and the likelihood that the IBCT will be operating in a non-contiguous combat zone over a large AO, the BSB centrally manages its resources and operations in order to maximize the support that can be provided in accordance with the BCT commander's priorities. As a result, most services and support are provided without dedicating BSB resources to specific units. (Typical exceptions to this rule are the maintenance combat repair teams (CRT) and the medical support structure.)
- *Area Support*: The key principle behind area support requires that the "separate" units, which are operating within a battalion area, but are not organic to that battalion, receive their sustainment and maintenance from local higher headquarters. Under the area support concept, the BSB will typically deliver sustainment to all units operating within a particular geographical area at the same time in order to optimize delivery. Additionally, maintenance CRTs will typically support all units within their geographical area in accordance with the priorities and time, personnel and equipment available.
- *Distribution Based Logistics*. Distribution-based logistics leverages information, force structure designs, technological enablers, and command and control relationships achieve the capability of delivering the "right stuff, at the right time, to the right location." This ability, combined with increased speed of movement and responsiveness throughout the system, will allow the Army to eliminate large "just-in-case" stockpiles that were relied upon in the past. However, distribution-based logistics does not eliminate the need for or the use of stockpiled inventory. Distribution-based logistics uses anticipation and visibility of the inventory moving through the distribution pipeline, in effect making the distribution pipeline into another warehouse, to limit, but not eliminate, stockpiled inventories.
- *Unit Level Distribution*. The BSB will provide the distribution of supplies and services to company, troop and battery level. Generally, distribution to infantry battalions is provided to company/team level. Distribution to other units will be executed on an area support basis and will normally occur at the same time as the parent battalion under the current task organization of units. Typically, distribution points are established for a specified period of time and a single point will serve several different units and/or serve as a materiel collection point.
- *Tactical Tailoring/Dynamic Support*. CSS operations are continuously adjusted through routine, tactical tailoring of BSB support assets, appropriately task-organized on a temporary basis to meet the current or projected near-term sustainment requirements. For example, a typical distribution day may include distribution to a battalion level distribution point for one customer cluster, to company/battery level

for another customer cluster and all the way to platoon/team level for a third cluster, while the fourth cluster receives no delivery that particular day.

- *Configured Loads*. The IBCT concept of support is based on distribution of unit-configured loads. The requirement to provide unit-configured loads will shift a significant portion of sustainment activities to units located outside the IBCT AO. Configured loads facilitate rapid replenishment and sustainment while simultaneously minimizing workload requirements within the IBCT. Successful implementation of configured loads requires situational awareness and the ability to make appropriate forecasts at various points on the planning time continuum. The intent of configured loads is to a) increase throughput, b) minimize handling, c) reduce footprint and d) physically speed the flow of supplies to the consumer.
- *Replace Forward Maintenance*. Repair and maintenance requirements within the BSB are based on the two-tiered maintenance concept. On-system tasks, those tasks that do not require disassembly of components off the system, will be performed forward in the combat zone as the supported unit's battle rhythm permits. A principle task of the CRTs is to assess and report maintenance requirements to the FMC. Normally, CRTs will perform battle damage assessment and repair (BDAR), and up to component and major assembly replacement in the forward area. Combat platforms and systems deemed unsuitable for repair forward will be recovered to the BSA for repair and may be replaced with "ready-to-fight" replacements.
- *Fusion of CSS and Operational Situational Understanding*. CSS situational understanding enables the BSB commander and staff to maintain visibility of current and projected requirements, to synchronize movement and material management, and to maintain integrated end-to-end visibility of transportation assets and supplies. GCSS-A, CSSCS, MTS, and FBCB2 are the battle command systems that will be fielded with the BSB (and other IBCT administrative and logistics elements) to insure effective CSS situational understanding. These systems enable CSS commanders and battle staffs to exercise centralized management, anticipate support requirements, and maximize battlefield distribution.
- *Synchronization of Battle Rhythm and Logistical Operations*. Support operations are fully integrated with the IBCT battle rhythm through integrated planning and oversight of ongoing operations. Logistical and operational planning occurs simultaneously rather than sequentially. Incrementally adjusting either the maneuver or logistics plan during its execution must be visible to all IBCT elements. The integration of battle rhythm and logistical operations may be enhanced significantly by the collocation of battalion/squadron CTCPs with or in proximity to the BSB HQ.
- *Reach Operations*. The BSB is organized to exploit capabilities external to the IBCT through reach operations. Reach operations include, but are not limited to external sources of information and intelligence, logistical planning and analysis conducted outside the AO, and telemedicine. The BSB exploits regionally available resources through joint, multinational, host nation, or contract sources for certain bulk supplies and services.

BSB Organization

The BSB consists of the headquarters and three companies: the Headquarters and Distribution Company (HDC), the Forward Maintenance Company (FMC), and the

Brigade Support Medical Company (BSMC); see Figure 3-1. Their fundamental capabilities are described below.

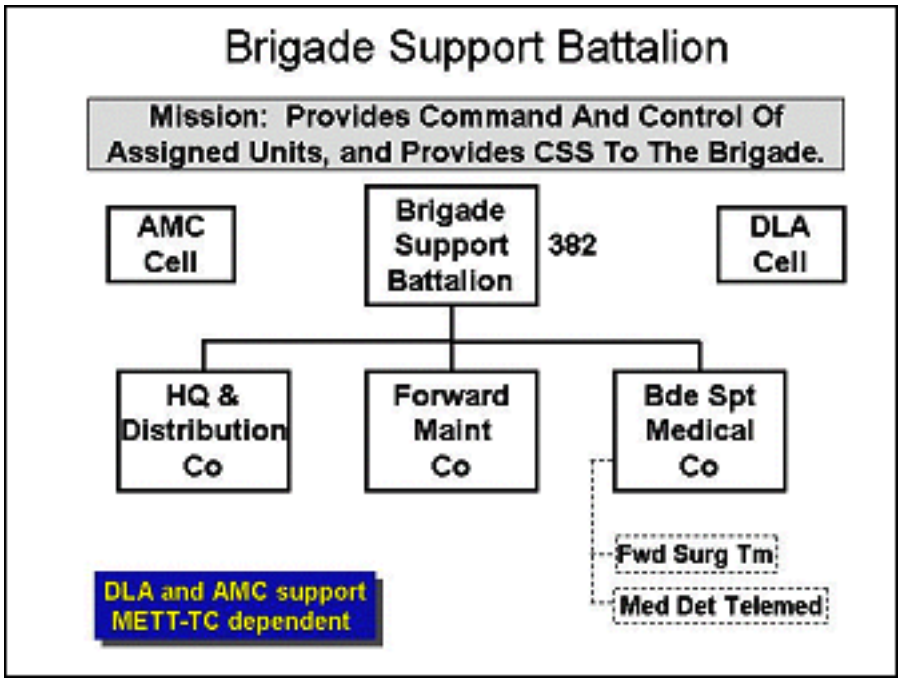


Figure 3-1. Brigade Support Battalion

The headquarters of the BSB provides command and control of the BSB's execution-based logistical operations IAW the commander's intent and the IBCT concept of operations. It includes a multi-functional staff organized on traditional doctrinal lines, but executing a set of staff procedures unique to the BSB and IBCT mission requirements. Organizing its efforts in accordance with sustainment priorities established by the IBCT commander, the BSB commander and staff operate on a 24-hour basis, adjusting and tailoring CSS support as required by METT-TC. Planning capabilities cover the doctrinal functions inherent within existing tactical logistical headquarters, although *planning/analytical support* in some areas is obtained through reach-back.

The HDC has the capability to provide 24-hour transportation support to the brigade. Overall, the HDC provides supply support for Class I (subsistence), Class II (organizational clothing and individual equipment), Class III (P) (packaged POL products); Class IV (barrier material only), Class V (ammunition, including bulk), Class VI (personal demand items), Class VII (major end items), and Class IX (repair parts) to the brigade.

The FMC provides maintenance support to units within the brigade through its combat repair teams (CRTs), automotive repair platoon and maintenance support platoon IAW the two-tiered system explained previously. Based on METT-TC, BCT OPTEMPO, and in keeping with the replace forward/fix rear doctrine, the preferred course of action is to perform maintenance, primarily consisting of LRU, component and major assembly

replacement as close to the supported customer as possible. Field maintenance within the BSA does not include services and will typically not include extended-duration repairs. Primary methods of returning systems to mission-capable status include component replacement through the use of combat spares, BDAR kits, controlled substitution/cannibalization, and end-item "ready-to-fight" replacements. The company is capable of performing primarily component and major assembly replacement repairs for artillery-specific equipment, power generation, wheeled/tracked vehicles, hull, engine and power trains, armament, ground support and engineer equipment, missile and electronics, basic sight assemblies, radios, and special electronic devices. Limited capability exists to repair computers (ABCS, STAMIS), radars and LRUs. The company also performs limited recovery and classification functions.

The BSMC provides level II combat health support (CHS) to those IBCT elements with organic medical support. The company provides, on an area basis, both level I and II CHS to units without organic CHS assets. Organic capabilities include treatment of wounds, injuries, and disease; ground evacuation; dental care; Class VIII resupply to medical platoons; blood management; patient holding services; mental health support; and reconstitution/regeneration of supported medical platoons. No organic aerial evacuation assets are present within the structure, but they will be employed when available through EAB. Preventive medicine (PVNTMED) services provided include field hygiene and sanitation oversight and coordination, deployment medical surveillance of disease and non-battle injury as well as environment hazards such as the presence and effects of NBC and toxic industrial material hazards.

3.2 Initial IBCT Implementation

The IBCT concept has created a force of highly mobile logisticians that rely heavily on STAMIS connectivity from its forward CRTs to the Brigade Support Battalion (BSB). The ability to effectively pass logistics information from these forward elements is essential in maintaining IBCT combat power and STAMIS system integrity. Identifying these requirements and providing short, mid, and long-term communications solutions is vital for combat zone and garrison logistics.

In November the IBCT identified that the brigade Combat Repair Teams would deploy forward of the BSA and therefore established the requirement to connect logistic automation systems using the tactical communications network. This requirement identified a shortfall in the communication systems architecture and presents a significant problem in the way the BSB supports the brigade.

Current Log STAMIS automation systems—e.g., Unit Level Logistics System (ULLS); Standard Army Maintenance System (SAMS); Standard Army Retail Supply System (SARSS)—operate independently with limited interface and no real time interoperability between systems. Because the current Information Exchange Requirement (IER) does not support STAMIS systems forward of the BSA the communication between these systems is normally reduced to sneaker nets.

3.3 Issues

Some of the issues associated with logistics connectivity are STAMIS locations, information flow between systems with different security classification, communication equipment availability, and bandwidth requirements.

Log STAMIS locations on the Battle Field. The CRT ULLS & SAMS equipment will be co-located in the battalion CTCPs, approximately 25 kilometers forward of the BSA. STAMIS equipment have been consolidated and downsized to laptops, which makes it easier for a single operator to move and operate forward of the BSA. All systems outside the capability of wireless CAISI (5-8 km) will have to use some type of non-standard disk transfer (FBCB2) to pass logistics information back and forth to forward logistics elements.

Support for systems operating at different classification levels. Although the Log STAMIS connectivity issues within the IBCT have been focused around the maintenance and supply systems (ULLS/SAMS)—which are unclassified—the brigade will eventually need to connect seamlessly to ULLS-4 and classified information sources such as CSSCS, SIDPERS (Standard Installation/Division Personnel System), and MC4 (Medical Communications for Combat Casualty Care). This will impact bandwidth requirements and will likely increase equipment authorizations. This also would require secure systems and infrastructure.

Communication Equipment Availability. Currently the brigade does not have the equipment authorized by the Modified Table of Organization and Equipment (MTOE) to create a seamless logistics communication system. Because the current O&O Plan was developed on the premise that GCSS-A would be available, the MTOE developers assumed the Log STAMIS systems would be co-located in the BSA. When GCSS-A was delayed and the IBCT decided to send the CRTs forward with STAMIS systems, they created an unanticipated gap in the communication architecture. Until the communication void is fixed and a seamless communication system is developed, the brigade will be forced to use slow, non-standard and outdated communication techniques: e.g., disk transfers, FBCB2 text messaging, and FM blast utilizing the Advanced SINCGARS Improvement Program (ASIP) radio. Appendix B discusses a proposed standard network communications protocol for STAMIS.

Bandwidth Requirements. Log STAMIS bandwidth requirements have not been quantified and will continue to expand as new systems are fielded. Based on recent discussions with POE STAMIS and DISC4, the Army has decided to wait until 2008 and the fielding of WIN-T to fix all log STAMIS bandwidth. Although WIN-T has the potential to fix the current logistics communication problem, no one agency has looked at the total requirements. All WIN-T requirements for log STAMIS are based on the optimistic deployment of GCSS-A and the supporting systems architecture. The risk associated with this approach is that initial deployment of WIN-T might not meet future STAMIS bandwidth requirements and the logistics community will be forced to operate its automation outside the digital battle space.

4. Current Wireless Network Communications Capabilities

Since the emergence of wireless network communications and computing in the mid-1990s, a steady stream of new technologies and initiatives have helped to boost public awareness about its potential—and about various gadgets associated with the technology. Like cellular telephones did for voice communications, wireless data communications will yield powerful benefits to users. To understand and evaluate the potential of wireless computing on a business enterprise, it is important to place the technology into perspective with respect to the business processes. Assessment of alternative technologies and architectures should be done within this context to determine which proposed solutions are best suited to the business processes that are in use (and for those processes that may be affected by the technology, how they will be affected).

Wireless connectivity offers the benefits of improved timeliness of information and increased ability to execute transactions that keep the business processes going without interruption. Challenges that continue to be associated with wireless technologies include limits of coverage, reliability of equipment, speed of communication, cost of implementation, and defining and/or meeting established standards for the equipment and communication protocols. Additional challenges concern the cost and resources/time required to enable legacy equipment/applications to support wireless communications. (For Army needs in particular, this applies to GCSS-A and STAMIS applications). As the technology advances and legacy applications are phased out and replaced by more wireless-capable applications, these challenges will gradually be overcome and wireless communications will emerge as a strategic, enabling technology.

Many types of wireless communications are in use today—and these architectures and devices are continually maturing. The purpose of this section is to describe the current state of wireless network communications technology and infrastructure. For the purpose of this report, wireless communications are listed as follows (see also Figure 4-1), and described more fully in subsequent subsections:

- Wide Area Networks (WAN) include both terrestrial and satellite networks. In the wireless world the more well-known cellular networks started with voice-to-voice communication, but with the introduction of Personal Communication Services (PCS) and other standard-based protocols, they are offering a wider range of services such as Email, two-way paging, and limited internet browsing capabilities for cellular phones and Personal Digital Assistants (PDAs).

- Local Area Networks (LAN) include fixed wireless efforts that connect local wireless LAN sites. This provides high-speed network connectivity for the mobile devices like PDAs and laptops.

- Personal Area Networks (PAN) are wireless services based on locations within short proximity of the vendor or device. Recently this area has gained momentum and support for standards such as Bluetooth *[4]*.

Type of Network	Wireless Generation	Connectivity/Protocol	Theoretical Throughput	Client Range
WAN	1G	GSM, AMPS	9.6 Kbps	5-8 Km
WAN	2G	CDPD, CDMA, TDMA	19.2 Kbps	6-12 Km
WAN	2.5G	GPRS, 1XRTT	100-150 Kbps	6-12 Km
WAN	3G	CDMA	384 Kbps	6-12 Km
LAN	--	Wired LAN	10-100 Mbps	300 m
LAN	--	802.11a	54 Mbps	100 m
LAN	--	802.11b	11 Mbps	100 m
PAN	--	Bluetooth	1-2 Mbps	10 m

Figure 4-1. Network Types, Standards, and Speeds

In Figure 4-1, the *Wireless Generation* is a function of speed and maturity of the technology. *Connectivity/Protocol* refers to the type of technology employed. *Theoretical Throughput* is the best-case attainable speed over the network, which is typically 1.5 to 2 times faster than what is observed in actual practice.

4.1 Wireless Wide Area Networks

First generation (1G) systems are analog cellular communications systems designed for voice transfer. The Advanced Mobile Phone Service (AMPS) is an example of 1G technology used in the US, operating in the 800 MHz range. Other examples were derived from AMPS, such as Total Access Communications System, which operates in the UK. Another 1G system is the Global System for Mobile Communications (GSM), which operates in the 800 MHz range.

In 1994 Sprint introduced what some say is the second generation of the cellular services PCS. This allows two-way 1900MHz digital voice, messaging and data services. Today cellular phones are rich with the features of this wireless service. From that time forward the US wireless industry has evolved into a ubiquitous presence in the commercial world. Wireless WAN services are not just about the cellular phone but have made their mark in the PDA market. Variations of GSM that operate in the 1800 and 1900 Mz ranges are considered to be 2G technology. 1800 MHz GSM, referred to as PCN 1800, is used primarily in Europe. 1900 MHz GSM is referred to as PCS 1900 and is used in the urban areas of the United States.

The newest models of cellular phone today are now capable of limited Internet browsing and e-commerce. Seven of the top ten cellular phones sold in the US are either e-mail or web browser capable. All phones produced by Kyocera, Sanyo, and Samsung are e-mail and web browser capable. The most common protocol used by these vendors is CDMA.

PDAs are now on the leading edge as these services expand their features. The Palm VII was introduced along with its Mobile Internet Kit, which allows them to connect to

palm.net services. Compaq has released their new iPAQ 3800 Series running Pocket PC 2002 with Pocket Internet Explorer, which allows for 128-bit support and features to store cookies in a similar fashion to a PC. The iPAQs are also Bluetooth Integrated. Other devices like the Blackberry can synchronize appointments, To Dos, and calendar events. This model will also enable limited encryption of Email and other information.

Today, second generation (2G) wireless computing is represented by Cellular Digital Packet Data (CDPD), Code Division Multiple Access (CDMA), and Time Division Multiple Access (TDMA) technologies. CDPD is in common use in the United States for wireless data transfer over existing cellular networks. CDMA is another 2G technology in use today in the United States; this standard allows for multiple transmissions to be carried simultaneously on a single wireless channel. TDMA is similar to CDMA, and provides increased bandwidth over digital cellular networks.

General Packet Radio System (GPRS) will provide packet switched data primarily for GSM based 2G networks. GPRS network elements consists of two main elements: SGSN (Service GPRS Support Node) and GGSN (Gateway GPRS Support Node). The GPRS is a new non-voice value added service that allows information to be sent and received across a mobile telephone network. It supplements today's Circuit Switched Data and Short Message Service.

Wireless WAN devices today and in the future will present some challenging obstacles to overcome. The lack of processing power limits some of the possibilities, such as advanced graphics for more enabled applications. The lower powered central processing units (CPUs) also play a role in limiting security features required by Virtual Private Networking (VPN), with its higher levels of encryption and authentication. These devices also have limited memory, commonly only several Megabytes, but up to 16 Mbytes are used for application and data storage. Small displays make Internet browsing challenging. But perhaps the most important limitations concern the amount of bandwidth and the latency associated with the wireless WAN infrastructure.

The 3G networks also use CDMA technologies, but in addition these must meet International Telecommunications Union specifications. Commercial deployment of 3G is likely to be delayed in the United States because the Department of Defense is using the wireless frequency bands allocated for 3G. There are also numerous competing 3G standards. Thus there is considerable uncertainty surrounding the deployment of the higher quality 3G WANs.

4.2 Wireless Local Area Networks

A wireless LAN is a data transmission system designed to use radio waves to provide network connectivity between two or more devices without the use of a wired cable infrastructure. There are several standards-based protocols used within this category, including HomeRF and 802.11b. The Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard was ratified in 1997 and specified a maximum data rate of

2Mbps. Adoption of this new technology was slow, and the IEEE recognized the need for higher data rates so the IEEE ratified the 802.11b standard. This allows for data rates up to 11Mbps at the unlicensed frequency of 2.4GHz. With the ratifying of the 802.11b standard the acceptance of wireless communication has boomed into the commercial world and products are readily available with cost decreasing. The HomeRF standard *[5]* also runs in the unlicensed frequency of 2.4GHz and data rates were recently allowed up to 10Mbps. Products for HomeRF are just starting to be delivered; therefore, the acceptance of this standard is yet to be seen. Most of these products are operating at 1.6 Mbps and are compliant with version 1.2. The Proxim Symphony products are compliant with version 2.0 and support 10Mbps speeds.

The 802.11b standard *[6]* defines two pieces of equipment: a wireless station, which usually consists of a PC with a wireless network interface card (NIC); and an access point that bridges communication from the wireless transmission media to a wired media. With these two types of equipment, the most common modes of operation are a wireless stations communicating with an access point, and two or more access points communicating directly. The wireless station / access point mode of operation is capable of 11Mbps at 150 meters in an open-air environment and approximately 40 meters in an office space environment with an omni-directional antenna. This mode will support upwards of 254 wireless stations all sharing the same 11Mbps. The direct access point to access point mode allows two or more wired networks to be bridged together with the wireless 802.11b technology. These access points running in bridging mode can reach upwards of 25 miles in an open-air environment with a line of site directional antennas. The distance limitations are derived by the amount of power allowed and the focus of the signal. An omni-directional antenna used when wireless stations are accessing it can only achieve relatively short distances, while a narrowly focused directional antenna in bridging mode can reach 25 miles. The access point can run both as an access point and a bridge at the same time, allowing wireless stations to communicate with other wireless stations on an adjacent access point.

The 802.11 standard defines the unlicensed frequency range for use of these devices at 2.4GHz. In the United States, this allows up to 11 channels; these devices use multiple channels to achieve the 11 Mbps maximum data rates. Several wireless media are used to accomplish communication Frequency-Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). Both of these wireless media shift their operating frequency to avoid interference and to make it harder to intercept the wireless signal. In the 2.4GHz range, only three access points can occupy a common air space using the 11 channels before they interfere with each other. If there are more than three access points in a single location, they will have some interference and will therefore not operate at the maximum 11Mbps.

4.3 Wireless Personal Area Networks

Wireless Personal Area Network (WPAN) specifications are for wireless connectivity with fixed, portable and moving devices within or entering a Personal Operating Space

(POS). A goal of the WPAN Group will be to achieve a level of interoperability, which could allow the transfer of data between a WPAN device and an 802.11 device. A POS is the space about a person or object that typically extends up to 10 meters in all directions and envelops the person whether stationary or in motion.

One protocol that is being used in the WPAN is Bluetooth. Designed as a short-distance networking protocol, Bluetooth connects disparate devices that traditionally have had wired connections, such as headset to telephone; digital still cameras; automotive accessories; medical devices; electronic payments at vending machines; and handheld computers and palmtop devices. Bluetooth is a standard set by Bluetooth Special Interest Group (SIG) whose founding members are Intel, Nokia, Ericsson, Toshiba, and IBM. Since setting this standard in 1988, the membership has grown to 2000+ Bluetooth SIG members and 1300+ adopters of Bluetooth. Bluetooth uses common unlicensed frequencies of the radio spectrum used by high-speed wireless local area networks and bar-code scanning devices. Currently, Bluetooth uses the 2.4GHz radio band, supports multipoint access, supports Personal Area Network (10-15 meters), and has data transfer speeds of 720 Kphs and 1 Mbps.

The direction for wireless PAN is for low complexity, low power consumption wireless connectivity to support interoperability among devices within or entering the POS. This includes devices that are carried, worn, or located near the body. Examples of devices, which can be networked, include Computers, PDAs or Handheld Personal Computers (HPCs), printers, microphones, speakers, headsets, bar code readers, sensors, displays, pagers, and cellular/ PCS phones. Representative examples are shown in Figure 4-2.

Wireless connectivity can be added easily to laptops using fairly standard technologies, typically PCMCIA (Peripheral Component Microchannel Interconnect Architecture) cards that are compatible with most machines. With hand-held devices, proprietary hardware often limits the network choices and makes the connectivity problem more complex. Cellular phones that support digital technology can support network connectivity; the wireless service provider for the phone provides the wireless Internet service.

Device	**Representative Manufacturers**
Laptop PC	Dell, Gateway, IBM, etc.
Tablet PC	Fujitsu, ViewSonic
Palm OS handheld	Palm, Handspring, Sony
Pocket PC handheld	HP, Compaq, Casio
Handheld PC handheld	HP, Casio, NEC, Sharp
Email Pagers	Motorola
SMS-enabled phones*	Ericsson, Motorola, Samsung, Nokia, etc.
WAP-enabled phones**	Ericsson, Motorola, Samsung, Nokia, etc.
Palm OS smartphones	Kyocera, Samsung, etc.

*SMS = Short Messaging Service (typically, delivering 160-character text message to digital phone)
**WAP = Wireless Application Protocol (provides optimized web access on digital wireless devices)

Figure 4-2. Mobile PAN Devices

4.4 Wireless Information Flow

There are two basic wireless architecture models: real-time and synchronized.

In the real-time access model, the mobile computing device can interact with information on the server only when a connection is available: the wireless device is connected to the network when the communication is desired; a query is sent to the server; the server locates the requested information and transmits it back to the device for viewing.

In the synchronized access model, the user can interact with the information on the device at any time, regardless of connection availability; and then synchronize with the server when possible. Synchronization middleware keeps information on the wireless device in sync with that on the server. This is also referred to as "store & forward" technology.

It is often assumed that wireless applications must always have real time access—a "thin client" model. This is not the case. In fact, synchronization, which has also been successfully applied to wired computing, is even more appropriate for many wireless applications. Synchronization ensures that even when they are away from wireless coverage cells, users are able to get the information they need and continue to transact business.

There are three basic connectivity models: wired, wireless WAN (ultimately 3G), and wireless LAN. It should not be assumed that any one of these models is always preferred over another. Indeed, a mixed model is almost always most appropriate and cost-effective—in which all of the connectivity options are exercised depending upon availability.

4.5 Security Implementation

The need for security has been prominent in recent months. Three types of security features are available in most commercial communication products today:

- The Service Set Identifier (SSID) or often called the network name.
- Wired Equivalent Privacy (WEP).
- Media Access Control (MAC) address filtering.

Most products require the SSID or network name be configured into all clients to make the association with an access point and function. This is simply a name associated with particular access point and would likely be the same if the wireless station roams between access points.

WEP enables the encryption of the communication between devices. WEP can be configured to use a 64-bit key or 128-bit key depending on the level of security desired. Recent discoveries have found vulnerabilities in the WEP protocol—for example, the initialization vector used as part of the encryption key is not a randomly generated number. These and other vulnerability issues are discussed further in Appendix C.

The third level of security is to filter MAC addresses of the wireless NIC. This address is a unique identifier assigned to every wireless NIC card. This form of security is secure but produces additional administrative overhead to update this filter list.

In using all three levels of security a wireless station would have to know the SSID or network name, the 128bit key, and also use a specific wireless NIC card with its MAC address configured into the access point.

Cisco, Microsoft, and other organizations have jointly initiated a promising security solution that uses a standards-based and open architecture approach to take full advantage of 802.11b security elements to provide the strongest level of security available and ensure effective security management from a central point of control.

Central to the security solution are the following elements:

- Extensible Authentication Protocol (EAP), an extension to Remote Access Dial-In User Service (RADIUS) that can enable wireless client adapters to communicate with RADIUS servers
- IEEE 802.1X, a proposed standard for controlled port access

When the security solution is in place, a wireless client that associates with an access point cannot gain access to the network until the user performs a network logon. When the user enters a username and password into a network logon dialog box or its equivalent, the client and a RADIUS server (or other authentication server) performs a mutual authentication, with the client authenticated by the supplied username and password. The RADIUS server and client then derive a client-specific WEP key to be used by the client for the current logon session. All sensitive information, such as the password, is protected from passive monitoring and other methods of attack. Nothing is transmitted over the air in the clear.

The sequence of events follows (see Figure 4-4):

1. A wireless client associates with an access point.
2. The access point blocks all attempts by the client to gain access to network resources until the client logs on to the network.
3. The user on the client supplies a username and password in a network logon dialog box or its equivalent.
4. Using 802.1X and EAP, the wireless client and a RADIUS server on the wired LAN perform a mutual authentication through the access point. One of several authentication methods or types can be used. With the Cisco authentication type, the

RADIUS server sends an authentication challenge to the client. The client uses a one-way hash of the user-supplied password to fashion a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. Once the RADIUS server authenticates the client, the process repeats in reverse, enabling the client to authenticate the RADIUS server.

5. When mutual authentication is successfully completed, the RADIUS server and the client determine a WEP key that is distinct to the client and provides the client with the appropriate level of network access, thereby approximating the level of security inherent in a wired switched segment to the individual desktop. The client loads this key and prepares to use it for the logon session. The RADIUS server sends the WEP key, called a session key, over the wired LAN to the access point. The access point encrypts its broadcast key with the session key and sends the encrypted key to the client, which uses the session key to decrypt it.
6. The client and access point activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session.

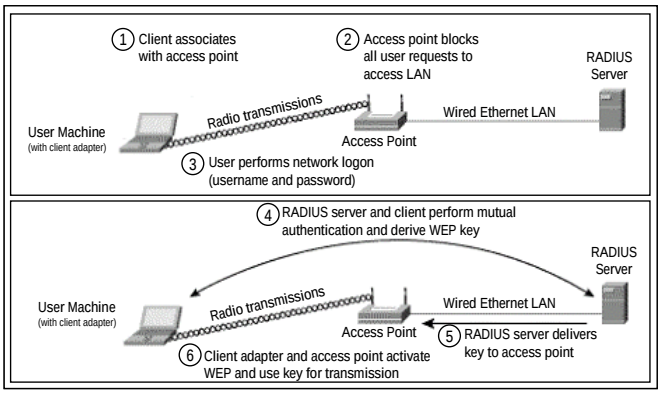


Figure 4-3. Centrally managed, standards-based security solution using EAP and

Support for EAP and 802.1X delivers on the promise of WEP, providing a centrally managed, standards-based, and open approach that addresses the limitations of standard 802.11 security. In addition, the EAP framework is extensible to wired networks, enabling an enterprise to use a single security architecture for every access method. It is likely that dozens of vendors will implement support for 802.1X and EAP in their wireless LAN products. Knowing the customer benefits of 802.1X, Cisco Systems supports the forthcoming standard today, offering a complete, end-to-end security solution that is fully compliant with 802.1X. The solution is available today when a site uses Cisco Aironet® wireless client adapters and access points and the Cisco Secure Access Control Server.

The above description is one proprietary solution that addresses WEP security vulnerability. Other proprietary solutions exist, such as the wireless link layer security architecture offered by Fortress Technologies (AirFortress) and a VPN tunneling solution architecture offered by NetScreen.

4.6 Issues

Issues concerning use of wireless technology include security, commercial viability and competing standards, and support for multiple clients.

Security. All computer systems and communications channels face security threats that can compromise systems, the services provided by the systems, and/or the data stored on or transmitted between systems. WEP is not immune to these threats and contains several inherent weaknesses.

The foundation of WEP is a stream cipher algorithm. A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender performs an Exclusive Or (XOR) operation on the key stream with the plaintext to produce ciphertext. The receiver has a copy of the same key, and uses it to generate identical key stream. XORing the key stream with the ciphertext yields the original plaintext. This mode of operation makes stream ciphers vulnerable to several attacks. If an attacker flips a bit in the ciphertext, then upon decryption, the corresponding bit in the plaintext will be flipped. Also, if an eavesdropper intercepts two ciphertexts encrypted with the same key stream, it is possible to obtain the XOR of the two plaintexts. Knowledge of this XOR can enable statistical attacks to recover the plaintexts. The statistical attacks become increasingly practical as more ciphertexts that use the same key stream are known. Once one of the plaintexts becomes known, it is trivial to recover all of the others.

WEP was never intended to provide more protection than a physically protected LAN environment. Since most LAN's are physically protected from external access, WEP was designed for equivalency protection from casual eavesdropping. WEP was never intended to be a complete security solution. Like wired LANs, a wireless network needs to be augmented with additional security mechanisms (e.g., end-to-end encryptions, virtual private networks, etc.), as appropriate to the requirements of the user organization.

Finally, the standard on which WEP is based is not as stringent as it needs to be. It will be sometime yet until the standard is modified, balloting is complete, and new protection mechanisms work their way into commercial products. However, the message is clear that the standard will change and new products will provide increased protection.

For a more detailed review of these issues and possible safeguards, refer to Appendix C.

Commercial viability and competing standards. Wireless communication using the 802.11b standard is gaining acceptance with the commercial market. Products are becoming more user-friendly and the price to install and operate is decreasing. Product compatibility is improving but it is recommended to stay with one vendor's suite of solutions to guarantee 100% compatibility of features. Improved data rates are expected with the ratification of the IEEE 802.11a standard. This new standard specifies a frequency range at 5.4GHz, which allows for a maximum of 54Mbps throughput. Devices are expected to be shipping with this capability within the year.

Support for multiple clients. The support for the 802.11b standard is developing rapidly. Depending on the vendor, there is support for all Windows clients, Macintosh, Linux, Palm and other devices that have a PC Card Type II slot.

5. Summary of Requirements and Issues

To summarize, the previous sections of this report reviewed the existing IBCT O&O plan with regard to identifying requirements and impediments to achieving optimal CSS information flow. The study seeks to identify short-term solutions to fill existing gaps or to recommend modifications to O&O plan to overcome communications issues. Any proposed short-term plans must provide for integration and transition into the operational architecture.

5.1 Unique IBCT "Core" Requirements

To date, the following unique requirements have been identified for the IBCT:

1. Light force, small footprint requirement
2. Low density of technical support due to elimination of CSSAMO organization for the IBCT
3. Introduction of the concept of split basing and Interim Staging Bases (ISB)
4. No existing unclassified date network support for the CRT forward.
5. ULLS-G function required in the CRT forward
6. Requirement for a communications path from the CRT to work in all terrain conditions
7. Requirement for the CRT communications system to be integrated with other enablers.

We will refer to these as core requirements in the sense that any solution must satisfy these requirements in order to be acceptable. Additional factors that may be used to discriminate among possible alternative wireless communications architectures are discussed in Section 5.3.

5.2 Issues Identified In the Draft Interim Report

The Draft Interim Report *[1]* identified the following impediments or issues for the IBCT:

- Doctrinally the Tactical Internet (TI) is classified as secret and all log STAMIS traffic has been identified as Sensitive but Unclassified (SBU). This limits the transmission of log data to local area intranets and disk transfers.
- There is no seamless process for moving information from unclassified systems to classified systems on the battlefield.
- There are no unclassified communications pipes from the CRT to BSA.
- Originally the capacity on the ULLS-G platform in the CRT did not support multiple line item input. *{PNNL identified this problem and followed through in facilitating a solution: software changes have been made to eliminate the problem}.*
- The IBCT technical support staff has strong concerns about their ability to continue to support the growing unclassified network structure and computer devices that are being fielded.

During the past 12-18 months the IBCT has deliberated with TRADOC to define and resolve the issue of logistics connectivity and doctrine. PNNL has continued to work with the IBCT to describe possible solutions and chart out courses for their implementation. There has been only modest progress in overcoming these challenges. As a result of the recommendations in the PNNL Draft Interim Report *[1]* and continued follow-on efforts to assist the brigade by defining alternatives and assessing solutions, the following incremental improvements have been accomplished:

- The IBCT successfully transmitted data utilizing the Advanced SINCGARS (ASIP) radio. This is a very slow and unreliable system that requires additional equipment, personnel, and non-standard cabling.
- PNNL assisted in coordination and setup of the CAISI wireless system and its subsequent implementation as the means of transmitting daily log STAMIS data.
- PNNL supported the IBCT in utilizing the Electronic Technical Manual Interface (ETM-I). ETM-I software automates the mechanic fault and requisitioning data and wirelessly transmits it to the STAMIS. ETM-I saves time and decreases clerical error.

As a result of these accomplishments, the previous baseline logistics communications architecture that was described in the Draft Interim Report *[1]* has changed from one based on the legacy CAISI design (shown below in Figure 5-1) to one based on the new wireless CAISI. This new baseline architecture is shown in Figure 5-2.

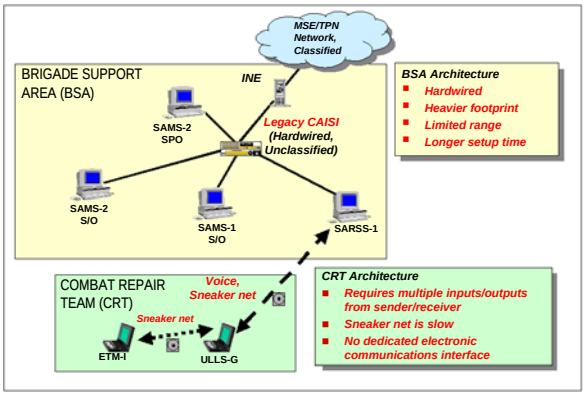


Figure 5-1. Previous IBCT Logistics

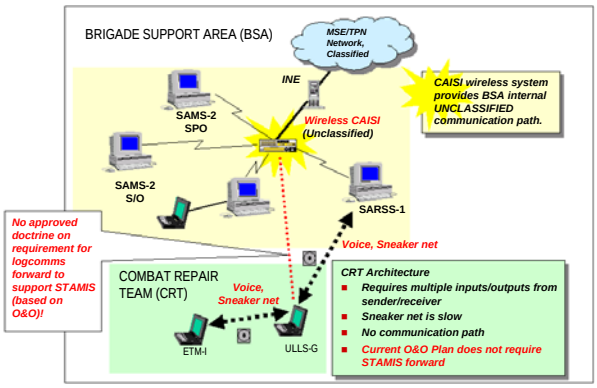


Figure 5-2. Current Baseline IBCT

5.3 Remaining IBCT CSS Wireless Communications Issues

The current baseline, depicted in Figure 5-2, provides an unclassified network infrastructure in support of logistics systems that utilizes the wireless CAISI and network-enabled STAMIS. The CRT and its STAMIS systems will be located in the BSA. The following issues are identified (those shown in *italics* have been added since the Draft Interim Report):

<u>Planning and Doctrine-Related Issues</u>

- Current doctrine does not support unclassified network infrastructure. The Tactical Internet (TI) is classified as secret and all log STAMIS traffic has been identified as Sensitive but Unclassified (SBU). This limits the transmission of log data to local area intranets and disk transfers.
- The IBCT technical support staff has strong concerns about their ability to continue to support the growing unclassified network structure and computer devices that are being fielded.
- TRADOC staff has been unwilling to change the systems architecture in support of log STAMIS initiatives. Initiatives have been denied for the present; and IBCT1 and IBCT2 have been directed to work within the current baseline. System architecture changes are being considered to support IBCT-3 and IBCT-4.
- *Currently, the O&O plan does not support the ULLS-G or SAMS systems forward with the CRT. If the CRT deploys forward, the STAMIS system will remain in the BSA. The CRT will provide updates to the ULLS-G system via free-text messages in FBCB2. In addition to manual entry of the FBCB2 free-text message at the CRT, this requires manual re-keying of the FBCB2 message at the BSA to transfer it back to STAMIS.*
- *There is a need for overall systems integration oversight as new wireless systems (such as ETM-I, DPMCS, MC4) emerge. At some point there may be a risk that the current architecture will be unable to scale up appropriately to accommodate additional wireless devices.*

Technical Issues and Additional Performance Factors

Technical Issues:

- There is no seamless process for moving information from unclassified systems to classified systems on the battlefield.
- There is not an unclassified network infrastructure to pass logistics data back from the CRT to the STAMIS systems located within the BSA
- *There is a need to define emerging requirements for hand held logistics devices—possible fielding to support ETM-I, PMCS, MC4, and STAMIS (locations, number of devices, number of wireless clients required).*

Additional Performance Factors:

- *Bandwidth and transmission rates are significant factors in choosing among potential wireless communications options.*
- *Transmission range limitations represent another significant factor to be considered in evaluating possible wireless communications options.*

The following section examines alternative options to overcome *technical* issues toward meeting the IBCT core requirements.

6. IBCT Logistics Communications Options

As described in the previous section, there are a number of issues and impediments preventing the IBCT from meeting its logistics communications needs. Principal among these are: The current unclassified network infrastructure in support of logistics systems is provided by wireless CAISI and network-enabled STAMIS systems (see Figure 5-2). Currently, the O&O plan **does not** support the ULLS-G or SAMS systems forward with the CRT. There is no unclassified network infrastructure to pass logistics data back from the CRT to the STAMIS systems located within the BSA.

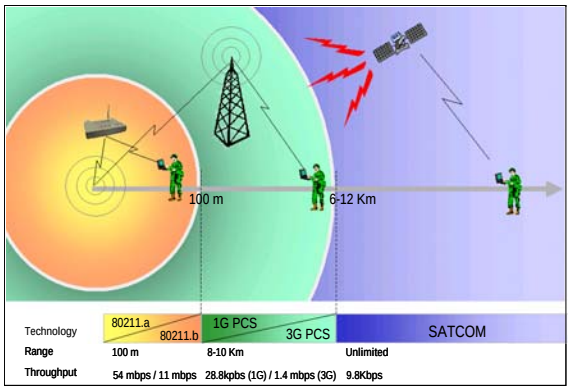


Figure 6-1. Communication

The current logistics communications baseline supports the light force with a small footprint, requires a low density of technical support, and supports split basing and Interim Staging Bases. However, communication gaps remain and sneaker net is required because of lack of seamless wireless connectivity. The communication technologies that may be applied to provide solutions to the logistics communications issues and requirements are illustrated in Figure 6-1. As can be seen from the figure, there are trade-offs between range and throughput for the various technology solutions.

This section describes near term architectures that enable the IBCT to function with current assets and some recommended upgrades that will enable the IBCT Logistic Community to meet its communications needs.

The following alternatives are considered:

Option 1—SINCGARS (ASIP). Utilizes the Single Channel Ground and Airborne Radio System (SINCGARS) ASIP (Advanced SINCGARS Improvement Program) radios located in the brigade to transmit logistics data. This solution was tested and evaluated by the brigade at Yakima Training Center in April 2001. The ASIP data transfer was very slow and unreliable; and limited in distance and terrain. It requires additional Windows OS computers, communication software, and a non-standard

interface cable. This is not recommended as a primary means of communication because of its cumbersome configuration and slow transfer speed.

Option 2—Interim Wireless. Interim solution involving Wireless Combat Service Support Automated Information System Interface (CAISI), Near Term Digital Radio (NTDR), and an In-Line Network Encryption (INE) device (TACLANE). The combination of these systems would provide the logistician with near real time secure data processing without degrading the tactical command and control network. This would require reorganization of assets within the Combat Trains Command Post (CTCP) and would require the use of additional INEs.

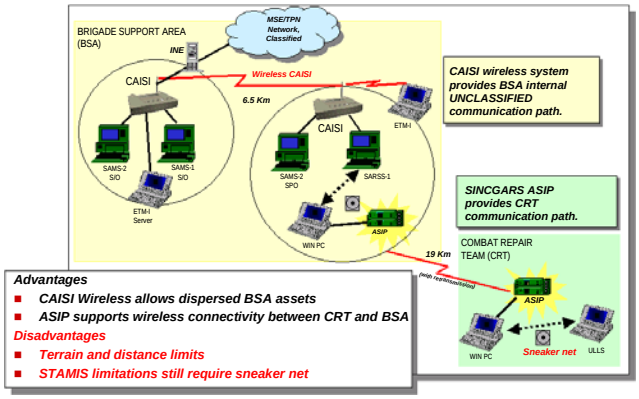
Option 3—Cellular Satellite Communication. Utilize cellular satellite communications and replace the current legacy STAMIS communication software to enable connectivity with wireless technology. Satellite communications eliminates sneaker nets from the BSA and the CRT.

Option 4—3rd Generation Wireless Technology. Future Fix/Objective or long-term solution involving an upgrade to CAISI Wireless system and Code Division Multiple Access (CDMA) cellular technology. Third generation wireless technology achieves a 2.4 Mbs transmission rate, and CDMA cellular technology achieves a BSA range of 6-12 Km.

6.1 Option 1: SINCGARS (ASIP)

A proposed immediate fix for the IBCT is to utilize the CAISI wireless system to provide an unclassified network infrastructure to support legacy STAMIS systems within the BSA. To support the transmission of STAMIS information from the CRT, it is proposed that the IBCT CRT make use of the SINCGARS (ASIP) FM radio. The ASIP would transfer CRT STAMIS data over the current FM network.

This solution provides a 1200 baud transmission rate and a CRT to BSA range of 19.5 Km. This architecture is depicted in Figure 6-2.



Advantages:

- Eliminates the requirement for disk transfer (sneaker net) from the CRT to the BSA.
- Supports light force, small footprint requirement
- Supports limited split basing and Interim Staging Bases (limited frequencies available to SINCGARS limits the number of data nets to support interim staging bases)
- Provides limited support of unclassified data transfer from the CRT forward (because of low data rates)
- Provides limited support of ULLS-G function in the CRT forward (sneaker net still required in BSA and CRT)
- Provides limited support of STAMIS communications path from CRT in all terrain conditions (severe terrains limit SINCGARS transmission distances and require increased number of relay stations).

Disadvantages:

- Data transfer is very slow, unreliable
- Requires increased density of technical support
- Sneaker net is still required within BSA and within CRT to accommodate data transfer between ASIP and STAMIS systems
- CRT communications systems are not integrated with other enablers. Feasibility of integrating with other enablers is *low* because of low data transmission rates and the difficulty of establishing a seamless connection between the enabler and WIN-PC.

6.2 Option 2: Interim Wireless

This interim solution, illustrated in Figure 6-3, involves the wireless CAISI, NTDR, and an INE device (TACLANE or NES). The combination of these systems provides the logistician with near real time secure data processing without degrading the tactical command and control network. This requires some reorganization of assets within the Combat Trains Command Post (CTCP) and some additional INEs. It is currently being considered for incorporation into the systems architecture for IBCT-3 and IBCT-4.

This solution provides a transmission rate of 11 mbps and a CRT to BSA range of 5-8 Km, constrained by line-of-sight/terrain limitations.

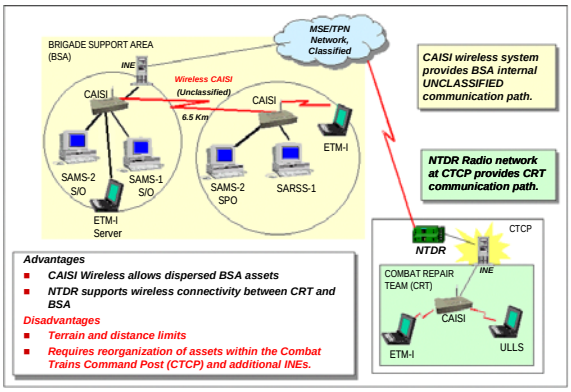


Figure 6-3. Option 2--Interim

Advantages:

- Supports light force, small footprint requirement
- Requires a lower density of technical support
- Supports split basing and Interim Staging Bases by allowing the STAMIS system to work in dispersed locations
- Supports unclassified data network for the CRT forward by tunneling unclassified data via the INE device through the classified tactical network
- Supports ULLS-G function in the CRT forward by providing a communication path to its support assets (SARSS and SAMS)
- Supports CRT communications path in the same terrain conditions that the Tactical Internet is able to support
- Integrates CRT communications system with other enablers
- Processes data at near real time; updates command /control systems more frequently
- Eliminates the risk of lost data, people, and equipment

Disadvantages:

- Utilizes command and control communication pipeline
- Requires more equipment (INE).

6.3 Option 3: Cellular Satellite Communication

Several new communications initiatives use 2nd and 3rd generation wireless communications technology. This technology provides for both voice and data throughput support speeds of up to 2.4 mbps. To fully support these systems, an upgraded ULLS-G type of application is needed to overcome lower bandwidth access speeds. This problem should be fixed with future ULLS-G changes that will provide the option to convert the ULLS software to Windows 2000.

Satellite communications (SATCOM) address the communications requirements for the diverse locations of the CRT in all kinds of terrains. Current SATCOM voice/data handset supports a data throughput in the range of 14.4 kbs.

Option 3 (Figure 6-4) uses SATCOM phones to transmit ULLS-G type information from the CRT via satellite to the BSA. This eliminates the sneaker net between the CRT and the BSA, eliminates the SINCGARS ASIP device, and provides terrain independent communications for the CRT. However, for the unclassified, higher density BSA communications, SATCOM is an expensive alternative.

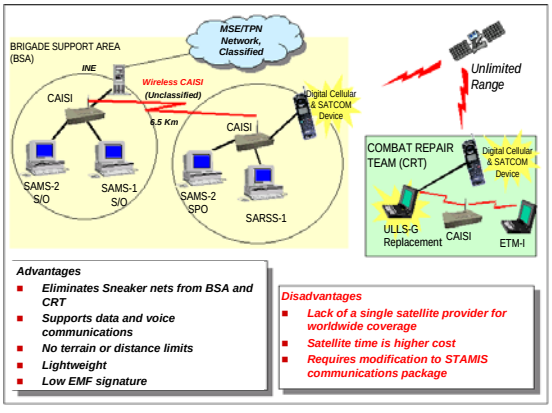
This option provides a transmission rate of 9.8 kbps uplink, 14.4 kbps downlink. The CRT to BSA range is unlimited in ideal circumstances, but practically limited by geographic constraints and availability of cellular access.

Advantages:

- Eliminates disk transfer from forward deployed CRT
- Supports light force, small footprint requirement
- Supports split basing and Interim Staging Bases by allowing the STAMIS system to work in dispersed locations
- Supports unclassified data network from the CRT to BSA with its own dedicated communication path
- Supports ULLS-G function in the CRT forward by providing a communication path to its support assets (SARSS and SAMS)
- Provides CRT communications path in all terrain conditions. Satellite communications not normally hindered by terrain features
- Processes data at near real time and updates command and control systems more frequently
- Eliminates the risk of lost data, people, and equipment

Disadvantages:

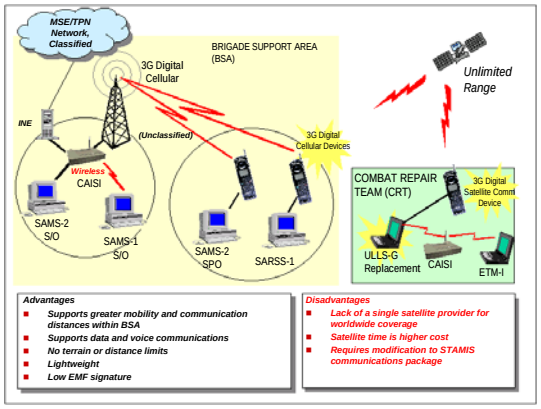
- Requires ULLS-G upgrade
- Cellular satellite communications have not been fully integrated with existing CRT logistics systems enablers. Feasibility of integration with other enablers is *high* because of the ability of satellite communications systems to support standard network protocols. (A feasibility demonstration is planned for December 2001).
- SATCOM is expensive
- There is not currently a single satellite communications system with worldwide coverage.



6.4 Option 4: 3rd Generation Wireless Technology

Option 4 incorporates the 3rd-generation cellular communications systems that would utilize the same SATCOM data/voice handset used in option 3, but also includes an upgrade to existing LAN wireless technology from CAISI wireless to CDMA cellular. This achieves a 6-12 km BSA range. Option 4 is represented in Figure 6-5.

Notionally, a CRT operating outside the BSA 6-12 km range would use a satellite link to transmit log information back to the BSA. When operating within the 6-12 km range, the CRT SATCOM voice/data handset would automatically transmit the log information via the cellular network instead. Within the BSA, the cellular network would support unclassified network access at up to 2.4 mbs.



Advantages:

- Eliminates disk transfer from forward deployed CRT
- Supports light force, small footprint requirement
- Supports split basing and Interim Staging Bases by allowing the STAMIS system to work in dispersed locations
- Supports unclassified data network for the CRT forward by tunneling unclassified data via the INE device through the classified tactical network
- Supports ULLS-G function in the CRT forward by providing a communication path to its support assets (SARSS and SAMS)
- Supports CRT communications path in the same terrain conditions that the Tactical Internet is able to support
- Processes data at near real time; updates command/control systems more frequently
- Eliminates the risk of lost data, people, and equipment.

Disadvantages:

- Requires ULLS-G upgrade
- Cellular satellite communications have not been fully integrated with existing CRT logistics systems enablers. Feasibility of integration with other enablers is *high* because of the ability of satellite communications systems to support standard network protocols.

- SATCOM is expensive
- Currently there is no single satellite communications system with world-wide coverage.

7. Conclusions

The results of the Tradeoff Analysis are summarized in Table 7-1. The ability of the various architectures to satisfy the core requirements is summarized in the top part of the table. Options that do not satisfy one or more of these core requirements represent unacceptable solutions. Options that satisfy all of the core requirements should be further evaluated according to their capability in achieving the additional performance factors, shown in the lower portion of the table.

Table 7-1. IBCT Requirements Supported by CSS Communications Options

	Options				
Core Requirements	Current Baseline	(1) SINCGARS	(2) Interim Wireless	(3) Cellular SATCOM	(4) 3G Wireless
1. Supports light force with small footprint?	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
2. Requires low density of technical support (CSSAMO eliminated)?	**Yes**	No	**Yes**	**Yes**	**Yes**
3. Supports split basing and Interim Staging Bases (ISB)?	Yes (Limited)	Yes (Limited)	**Yes**	**Yes**	**Yes**
4. Supports unclassified data network for the CRT forward?	No	Yes (Limited)	**Yes**	**Yes**	**Yes**
5. Supports ULLS-G function in the CRT forward?	Yes Limited	Yes Limited	**Yes**	**Yes**	**Yes**
6. Provides a STAMIS communications path from the CRT to work in all terrain conditions?	No	Yes (Limited)	**Yes**	**Yes**	**Yes**
7. Feasibility of integrating CRT communications system with other enablers.	Low	Low	**High (already integrated)**	**High**	**High**

Additional Factors	Current Baseline	(1) SINCGARS	(2) Interim Wireless	(3) Cellular SATCOM	(4) 3G Wireless
Bandwidth/Transmission Rate	Sneaker Net	1200 baud	11 mbps	9.8/14.4 kbps	**2.4 mbps**
CRT to BSA Range/Limits	Sneaker Net	19.5 Km	5-8 Km Line of Sight	Unlimited*	**Unlimited**

As is evident from Table 7-1, the Interim Wireless solution, the Cellular SATCOM solution, and the 3G Wireless solution (Options 2, 3, and 4, respectively) each satisfy all

of the core requirements; but they may be discriminated according to the additional performance factors.

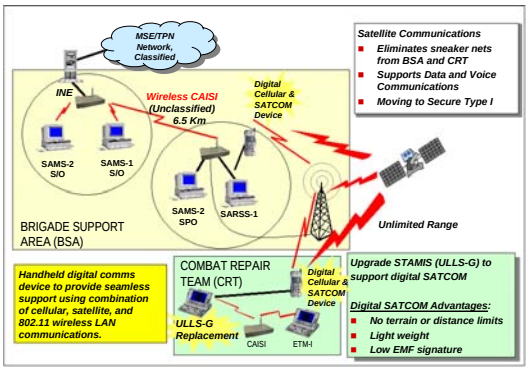


Figure 7-1. Vision for "smart"

PNNL continues to support the IBCT in developing optimized configurations to implement immediate fixes to the baseline architecture using existing assets of the IBCT. Thus, the current baseline, shown in the second column, already represents an improvement over the situation as described in our draft Interim Report *[1]*. Option 1 (SINCGARS; third column in the above table) represents a substantial improvement over the current baseline, but still requires sneaker net and still suffers from terrain limitations. The Interim Wireless solution (Option 2; fourth column in the above table) represents the first step along the path toward the objective solution in which all of the requirements are met. This architecture provides near real time secure data processing without degrading the tactical command and control network, but it will require some reorganization of assets within the Combat Trains Command Post (CTCP) and some additional INEs. This option also has some distance limitations (CAISI wireless communication limited to 6.5 km within the BSA). This solution is being considered for incorporation into the systems architecture for IBCT-3 and IBCT-4. Option 3 (Cellular Satellite Communications) eliminates the terrain and range limitations of Option 2. However, for the unclassified, higher density BSA communications, SATCOM is an expensive alternative. Option 4 incorporates the 3rd-generation cellular communications systems that would utilize the same SATCOM data/voice handset used in Option 3, but also includes an upgrade to existing LAN wireless technology from CAISI wireless to CDMA cellular. This achieves a 6-12 km BSA range.

Options 3 and 4 are clearly preferred and should be considered for IBCT-3 and IBCT-4. Currently, several tests have been conducted using QualComm's deployable PCS system. Other tests are scheduled in the near future to test the viability of using their deployable PCS system to transmit logistics data. Use of 3G cellular communications systems is also being evaluated as part of the WIN-T architecture.

As mentioned earlier in this report (the end of section 4.4), best practices would suggest that all communications connectivity models (wired, wireless WAN/ultimately 3G, and wireless LAN) should be employed in a mixed-mode architecture. All of the connectivity options may be exercised depending upon availability. This vision for logistics communications is illustrated in Figure 7-1 (vision of mixed-mode, flexible architecture)

and Figure 7-2 (vision of logistics information flow). Thus, in-garrison communications can be supported via wired LAN when operators have access to networked systems and wireless WAN modes may be used for operations within 300-400 feet of 80211.b equipment. CAISI wireless equipment and handheld devices may be used to download detailed maintenance information from crew/mechanic computers (or PDAs) as well as the "rich data stream" available from onboard embedded diagnostic/prognostic systems. For operations in the field, 80211.b wireless systems such as CAISI and PDAs (e.g., DPMCS) may be used to acquire logistics/health status data from onboard computers – e.g., during preventive maintenance checks and services or fuel resupply. When operations extend to the 5-11 km range, 3G cellular communications may be used to transmit maintenance reports and high-level platform health status (e.g., LOGSITREP). Conceivably, 3G cellular technology has sufficient bandwidth to allow even the "rich data stream" to be captured this way, directly from onboard embedded diagnostics/prognostics systems. For operations that are beyond the range of cellular communications, satellite communications offer the ultimate solution. Because bandwidth constraints may limit the amount of logistics data that can be transmitted via satellite, it is possible that this type of communication will be limited to high level LOGSITREP data. Downloading of the rich data stream, more useful for maintenance scheduling and life cycle analyses, would be done routinely at opportune times during inspections, resupply, refueling, etc. In any case, high-level (LOGSITREP) data should always be available in near real time via the tactical logistics communications supported by FBCB2.

Ideally, the determination of which communications modes to use at any time would be accomplished automatically, transparent to the users. This will require "smart" communication devices that will support 802.11b, 3G cellular, and SATCOM modes, and that will have the capability to switch autonomously among them based on such factors as signal strength, availability, etc

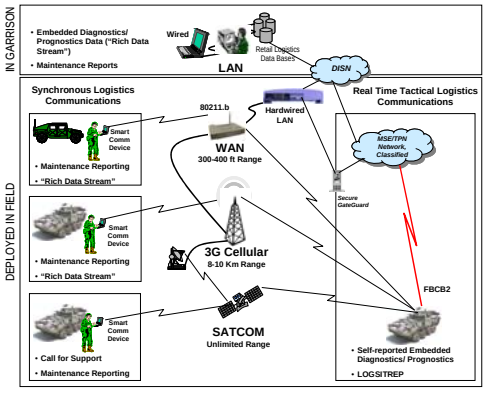


Figure 7-2 "Smart" mixed-

Finally, it is noted that these conclusions are considered to have an "interim" status due to the evolving nature of the IBCT O&O and the ongoing integration of various enabling technologies. The final results of this study must await validation with other stakeholders, assessment of integration potential with the WIN-T architecture, possible

compatibility with the GCSS-A, and assessment of additional advanced technology demonstrations.

Figure 7-2. Information flow in "smart"

8. Recommendations

The following areas for further study represent a summary of our current recommendations, based upon the preceding analysis:

- Investigate alternatives to ULLS-G that support low-bandwidth communication
- Integrate the various enablers to use a common communication backbone (e.g., ETM-I to use CAISI wireless)
- Optimize location of STAMIS systems within the CRT and BSA
- Continue to examine STAMIS connectivity issues. Current direction is to use FTP (File Transfer Protocol) to support connectivity with CAISI wireless, rather than the previous method using the Legacy Support Adapter and Blast protocol. There are currently two alternative solutions for implementing the FTP link with CAISI (offered by Ft. Hood and Ft. Stewart)
- Determine the most effective interface between classified and unclassified networks for the transfer of logistics information between CSSCS systems and log STAMIS systems
- Continue to explore mid-term communications architecture solutions to encompass the full suite of future logistics communications devices, tools and technologies (specifically, Qualcomm's wireless DPMCS, the wireless ETM-I implementation, the new wireless CAISI, and Qualcomm's deployable PCS).
- Examine active synchronization performance of wireless handheld devices (PDAs) with laptop computers, as envisioned for mid-term and future transfer of CSS data from platforms to platoon leaders in the field
- Continue coordination with CECOM, CASCOM, TRADOC, the LIA, and the IBCT to ensure effective transition of enablers and new technologies for CSS communications

9. Reference Notes

[1] Interim Project Report prepared for the US Army Logistics Integration Agency (draft version of the present document). Burnette, J.R., Allen, L.W., Thibodeau, C.C., Dische, S.T., and Greitzer, F.L., *Tradeoff Analysis for Combat Service Support Wireless Communications Alternatives: Interim Report.* Pacific Northwest National Laboratory, June 2001. The present document updates and supercedes the June 2001 draft.

[2] IBCT Organizational and Operational Plan, 30 June 2000. http://www.lewis.army.mil/transformation

[3] Neal, MAJ John M. US Army, "A Look at Reachback." Military Review, September-October 2000, pp. 39-43. Paper may be downloaded as .pdf from http://www-cgsc.army.mil/milrev/English/SepOct00/pdf/nea.pdf

[4] Bluetooth wireless technology is a worldwide specification for a small-form factor, low-cost radio solution that provides links between mobile computers, mobile phones, other portable handheld devices, and connectivity to the Internet. The specification is developed, published and promoted by the Bluetooth Special Interest Group (SIG). Internet reference: http://www.bluetooth.com/

[5] Internet reference for HomeRF standard: http://www.homerf.org/data/tech/homerfbroadband_whitepaper.pdf

[6] Internet reference for 80211.b standard: http://www.ieee.org (this information requires payment to be viewed).

APPENDIX A: Acronym List

ABCS	Army Battle Command Systems
ALOC	Administrative Logistics Operations Center
AMPS	Advanced Mobile Phone Service
ASIP	Advanced SINCGARS Improvement Program
ASLP	Army Strategic Logistics Plan
ATM	Asynchronous Transfer Mode
AUTODIN	Automatic Digital Network
BAS	Battalion Aid Station
BCT	Brigade Combat Team
BDAR	Battle Damage Assessment and Repair
BFA	Battlefield Functional Areas
BSA	Brigade Support Area
BSB	Brigade Support Battalion
BSMC	Brigade Support Medical Company
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAISI	Combat Service Support Automated Information System Interface
CAN	Airborne Communications Node
CDMA	Code Division Multiple Access
CDPD	Cellular digital Packet Data
CECOM	US Army Communications-Electronics Command
CHS	Combat Health Support
CPU	Central Processing Unit
CRT	Combat Repair Team
CSS	Combat Service Support
CSSCS	Combat Service Support Control System
CTCP	Combat Trains Command Post
CTIL-BRIL	Command tracked item list update message
D	Digital
DBLS	Distribution-Based Logistics System
DCSLOG	Deputy Chief of Staff of Logistics
DNS	Domain Name Server
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EBC	Embedded battle command
EPLRS	Enhanced Position Location Reporting Systems
FAADC2I	Force XXI Battle Command Brigade and Below
FHSS	Frequency-Hopping Spread Spectrum
FMC	Forward Maintenance Company
GCSS-A	Global Combat Support System–Army

GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HDC	Headquarters and Distribution Company
HPCs	Handheld Personal Computers
IBCT	Interim Brigade Combat Team
IEEE	Institute of Electrical and Electronics Engineers
IER	Information Exchange Requirement
INE	In-Line Network Encryption
ISB	Interim Staging Bases
LAN	Local Area Network
LIA	Logistics Integration Agency
LOGC2 ACTD	Logistics Command and Control Advanced Concept Technology Demonstration
LOGSITREP	Logistics situational reports
MAC	Media Access Control
MC4	Medical Communications for Combat Casualty Care
METT-TC	Mission, Enemy, Terrain, Troops, Time, Civilians
MSE	Mobile Subscriber Equipment
MTOE	Modified Table of Organization and Equipment
MTS	Maneuver Tracking System
NES	Network Encryption System
NIC	network interface card
NTDR	Near Term Digital Radio
PAN	Personal Area Networks
PCS	Personal Communication Services
PCMCIA	Peripheral Component Microchannel Interconnect Architecture
PDAs	Personal Digital Assistants
PERSITREP	Personnel situation report
PNNL	Pacific Northwest National Laboratory
POS	Personal Operating Space
RADIUS	Remote Access Dial-In User Service
RETRANS	Re-Transmission
RML	Revolution in Military Logistics
RS-232	Recommended Standard 232 (IEEE computer serial interface)
RSTA	Reconnaissance Surveillance Target Acquisition
SA	Situational Awareness
SAMS	Standard Army Maintenance System
SARSS	Standard Army Retail Supply System
SATCOM	Satellite communications
SGSN	Service GPRS Support Node
SIDPERS	Standard Installation/Division Personnel System
SINCGARS	Single Channel Ground and Airborne Radio System
SMART-T	Secure Mobile Anti-jam Reliable Tactical Terminal
SSID	Service Set Identifier
STAMIS	Standard Army Management Information Systems

TACSAT	Tactical Communications Satellite
TDMA	Time Division Multiple Access
TI	Tactical Internet
TOC	Tactical Operations Center
TPN	Tactical packet node
TUAV	Tactical Unmanned Airborne Vehicle
ULLS	Unit Level Logistics System
ULLS-G	Unit Level Logistics System-Ground
V	Voice
VPN	Virtual Private Networking
WAN	Wide Area Networks
WEP	Wired Equivalent Privacy
WIN	Warfighter Information Network
WIN-T	Warfighter Information Network-Tactical
WPAN	Wireless Personal Area Network
WSSPR	Weapon Systems Support Platform-based Readiness
XOR	Exclusive Or
1G	First generation
2G	Second generation
3G	Third generation

APPENDIX B: Standard Network Configuration for STAMIS

Problem

Legacy STAMIS file transfer options have restricted the ability of the IBCT to operate on the modern digital battlefield. The majority of the operating systems and hardware configurations do not have the ability to use the newer networking technologies present in the IBCT. The Army does not plan to upgrade the current STAMIS configuration until the deployment of Global Combat Support System–Army (GCSS-A). This makes operating within the current IBCT systems architecture almost impossible.

In our experience with the IBCT, the support personnel are able to set up current wireless communication technology (e.g., 802.11b) and get the network to communicate effectively, but there have been serious challenges in getting STAMIS to operate within this architecture. *The source of the problem is that it is difficult and time consuming to configure legacy STAMIS equipment to support standard network interface cards.*

Background

Current communication configuration: In order to establish communications, most units use a Point-to-Point Protocol (PPP) most commonly called "blast." Blast PPP establishes the communication link by passing a set of packets to configure and test the data link. Once established, Blast sends a set of packets that must be processed in sequence to be authenticated. Drawbacks of this method are:

- Blast requires that the communication link be continuously operational and dedicated to the specific transmission.
- Any interruption in the communication link requires a complete retransmission of the file.
- The Blast configuration requires an additional device (Legacy Support Adapter/LSA) to convert serial communications from STAMIS to a network IP interface.

FTP Interim Solution: Recently the IBCT acquired hardware and software from PEO STAMIS that utilizes standard File Transfers Protocols (FTP) to connect to CAISI wireless. FTP will allow the STAMIS systems to operate within a standard network and extend the communication capabilities into the Tactical Internet. The FTP solution will provide the following advantages:

- FTP is a more robust communications protocol with inherent error-checking capability
- FTP does not tie up the network interface (allows multiple simultaneous transactions over the same connection)
- FTP is supported by more modern, wireless communications systems
- FTP eliminates the requirement for a LSA device; it uses a standard network (Ethernet) card in the STAMIS equipment.

At present, there are multiple proposed procedures for configuring the FTP solution for STAMIS applications (e.g., procedures for implementing the FTP link are available from Fort Lee and from Ft. Stewart). While these procedures yield the same result, they are not standardized within or between STAMIS applications. Further, there are no plans to implement the FTP process into any legacy Software Change Packages (SCP). Lacking organizational support, the burden of making necessary STAMIS configuration changes reverts to operational units with limited resources. Therefore, we have observed (at the IBCT) piecemeal conversion to a STAMIS standard network configuration. Because of the inconsistencies and potential for errors and incompatibilities, operators tend to revert to traditional manual modes of information transfer (sneaker net).

There is a need to standardize the various proposed procedures for converting standalone STAMIS systems to be network capable and to support FTP.

Objective

The objective is to further define and assess the efficacy of the FTP interim solution in meeting IBCT communication requirements. The goal is to develop a single, standardized procedure for configuring all STAMIS equipment (SAMS, ULLS, etc.) that will be supported and promoted by the Army (in SCPs).

Recommended Approach

The following tasks are required to achieve this objective:

1. Collect/survey procedures that are in use for configuring STAMIS to support FTP.
2. Consolidate procedures based on best practices.
3. Develop a single, authoritative document that standardizes the procedure across all STAMIS applications.
4. Provide necessary supporting documentation for operators in the field.

Work with IBCT in facilitating the adoption of the proposed standard (it should be implemented using the SCP process).

APPENDIX C: Wireless Communications Vulnerabilities

Introduction

Local Area Network (LAN) standards are developed by the IEEE 802 LAN/MAN Standards Committee, which develops Local Area Network standards and Metropolitan Area Network standards. The most widely used standards are for the Ethernet family: Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs. An individual Working Group provides the focus for each area.

The IEEE 802.11 standard specifies the requirements for implementing wireless Local Area Network. There are three prevailing IEEE 802.11 specifications. IEEE 802.11 was ratified in 1997 and supports a data rate of 2 Mbits/second. IEEE 802.11b specifies rates up to 11 Mbits/second and was ratified in 1999. IEEE 802.11a operates at data rates up to 54 Mbits/second and is the emerging high-speed option. Part of the specification is the Wired Equivalent Privacy (WEP) protocol that is designed to protect the link layer traffic from eavesdropping and other attacks.

Security Threats

All computer systems and communications channels face security threats that can compromise systems, the services provided by the systems, and/or the data stored on or transmitted between systems. The most common threats are:

- Denial of service
- Interception
- Manipulation
- Masquerading
- Repudiation

Denial of service occurs when an adversary causes a system or a network to become unavailable to legitimate users or causes services to be interrupted or delayed. Overloading the target system often causes denial of service. Consequences can range from a measurable reduction in performance to the complete failure of the system. A wireless example would be using an external signal to jam the wireless channel. There is little that can be done to keep a serious adversary from mounting a denial of service attack.

Interception has more than one meaning. A user's identity can be intercepted leading to a later instance of masquerading. A data stream can be intercepted by an adversary for the purpose of disclosing otherwise private information. In either case, the adversary is attacking the confidentiality or privacy of the information that is intercepted. An example would be eavesdropping and capturing the wireless interchanges between a user device and the network access point. Since wireless systems use the radio band for transmission, a diligent adversary can intercept all transmissions. Therefore, some form of strong

authentication and encryption is necessary in order to keep the contents of intercepted signals from being disclosed.

Manipulation means that data have been inserted, deleted, or otherwise modified on a system or during transmission. This is an attack on the integrity of either the data transmission or on the data stored on a system. An example would be the insertion of a Trojan program or virus on a user device or into the network. Protection of access to the network is the most effective means of avoiding manipulation.

Masquerading refers to the act of an adversary posing as a legitimate user in order to gain access to a wireless network or a system served by the network. For example, a user with illegitimate access to a network authenticator could access the network. Strong authentication is required to avoid masquerade attacks.

Repudiation is when a user denies having performed an action on the network. Users might deny having sent a particular message or deny accessing the network and performing some action. Strong authentication of the user and integrity measures can minimize the possibility of repudiation.

Security Services and Vulnerabilities

The security function specified in IEEE 802.11 is Wired Equivalent Privacy (WEP). WEP provides two basic levels of security. Open System Authentication (OSA) is part of the standard, but provides little security. The second is shared-key authentication that provides the highest level of security available in WEP. Neglecting the OSA, the shared key model specifies a number of requirements intended to defeat or mitigate some of the threats mentioned earlier. Particular attention was paid to 1) authenticating users over an encrypted channel, 2) defeating an adversary's ability to eavesdrop on wireless transmissions in order to preserve confidentiality by encrypting the channel traffic, and 3) providing integrity assurance that a message was not modified in transit.

Open System Authentication. Open System Authentication (OSA) is an authentication method that depends on establishing a security association between any device attempting communication with the network and a network access point. The method blocks any access that is not associated with a valid Media Access Control (MAC) address. The MAC address is the unique 48-bit value identified on the MAC interface contained in each wireless interface card installed in a wireless user device. The access point maintains a list of valid addresses entered by the system administrator at the time a user is granted access to the network. If the MAC address offered is present in the access point list, access is granted; otherwise access is denied. This method has the following problems and vulnerabilities:

1. Maintaining a list of valid MAC addresses is a labor-intensive activity and adds significant cost to the administration of the network.
2. An individual with technical knowledge can spoof MAC addresses. While this might be discovered if two systems with the same MAC address attempt to

access the network, careful planning on the part of an adversary can often avoid using the network at the same time as the legitimate user.

Wired Equivalent Privacy (WEP). The foundation of WEP is based on the use of a stream cipher, RC4 encryption. The RC4 algorithm has three inputs, an initializing vector ***IV***, the random key, and the plaintext. The ***IV*** is input to ***E***, the RC4 encryption algorithm, along with the key. The algorithm generates a keystream output from ***E*** that is sent to the output box ***O***. The output box ***O*** shifts the keystream out, a byte at a time and each byte is combined with the plaintext ***P*** under the Exclusive OR function. The output of ***E*** is also fed back to the ***I*** stage which causes the keystream to vary as encryption proceeds.

Since ***IV*** must be known to the transmitter and receiver, it is sent to the receiver as an unencrypted part of the ciphertext stream. A straightforward logic function inserts ***IV*** into the ciphertext stream and recovers it from the stream for input to the ***I*** function at the receiving end. ***IV*** does not have to be secret since RC4's strength is derived from the algorithm and key, not ***IV***. However, the integrity of ***IV*** needs to be assured or decryption will not function properly.

The RC4 algorithm supports variable length keys. The two lengths most commonly used for wireless applications are 40 bits for export controlled systems and 128 bits for domestic application. Although most vendors advertise 128 encryption, the actual key length is 104 bits.

Key Management. The standard does not specify how keys are managed or distributed. It does provide for an externally populated globally shared array of 4 keys. In addition, it allows for an additional array that associates a unique key with each user station. Most existing implementations utilize a shared secret key to encrypt the link transmission between all users and the wireless network access point. All users and the access point know the key. Some access points allow for two channels such that the keys for each channel can be different. Devices assigned to one channel still share the secret key with other users assigned to that channel and the access point.

Integrity Assurance. The plaintext input pj string is composed of the original message M with a CRC32 checksum of the message appended to the end of the message. The purpose of the checksum is to provide the integrity service. At the receiver the ciphertext is decrypted, the CRC32 bit string is calculated on the original plaintext input string and compared to the CRC32 received. If the CRCs match then the original message is accepted as valid.

Vulnerabilities and Weaknesses

RC4 was developed in 1987 by Ron Rivest of MIT for RSA Data Security, Inc. Initially the algorithm was protected by RSA as a trade secret and not publicly disclosed. However, in 1994, the algorithm was anonymously posted to the Cypherpunk mailing list and it quickly spread to news and ftp sites around the world. Subsequent analysis indicates that RC4 is immune to linear and differential cryptanalysis, is very non-linear, and does not have short cycles. It is used in many commercial products.

Unfortunately, WEP is not a secure implementation of RC4 and violates several other cryptographic design and implementation principles, including issues of Interception, Keystream Reuse, and Integrity Assurance.

Interception. Many of the attacks depend on the ability of an adversary to intercept wireless traffic. Fundamentally, we know that any traffic transmitted by radio signal is subject to interception since it is a radio frequency broadcast. The IEEE 802.11 standard specifies three possible physical layers, Infrared (IR), Frequency Hopping Spread Spectrum (FHSS), and Direct Sequence Spread Spectrum (DSSS) and broadcasts in three frequency bands, 900 MHz, 2.4 GHz, and 5 GHz. Products in the field typically use DSSS and the 2.4 GHz band. Any device designed for service in the appropriate band of frequencies is readily capable of receiving all signals. It is a relatively easy matter to modify device drivers and/or flash memory to promiscuously monitor traffic. Consequently, it should be assumed that an adversary has access to intercepted signals.

Keystream Reuse. One of the well known attributes of stream ciphers operating in output feedback mode is that encrypting two messages under the same IV and key can reveal information about both messages to a cryptanalyst. In order to execute this attack the adversary would have to capture packets and compare IV values searching for collisions. A collision would allow analysis of a single packet. If the plaintext of one packet is known and is carefully selected, then the plaintext of the other packet would be revealed.

It is a relatively simple matter to get a known plaintext injected into the network by addressing a message to a mobile user. Monitoring transmissions is somewhat more difficult, but can be done with moderate effort. Once the key is revealed all transmissions using that key and IV are compromise. The process is simplified to a great extent if the ***IV*** is not changed every packet. The standard recommends, but does not require, the ***IV*** to be changed every packet.

Integrity Assurance. The standard specifies an integrity algorithm that operates on the original plaintext message to produce an Integrity Check Value (ICV). The original plaintext is concatenated with the IVC to form the plaintext to be encrypted. The IVC method specified in the standard is CRC-32. The IVC is a 32-bit field called the FCS field and is defined as the last 4 octets in the MAC frame. Since the CRC-32 function is a linear function that uses only addition and multiplication, it is possible to change one, or more, bits in the original plaintext and be able to predict the bits to change in the CRC-32 checksum such that the checksum remains valid when it is received. Integrity methods

that are cryptographically secure such as hash algorithms are non-linear functions that are not readily attacked. What this means is that it is possible to modify messages in transit without detection. This is probably not a concern as to the original message presented by the application for transmission. However, the checksum is performed over the entire MAC packet that includes higher-level protocol routing and port fields. If an adversary turns their attention to modification of the IP destination field, it is possible to re-direct traffic to an unintended destination under the control of the adversary.

Current Situation

Existing Products. In order to field a compatible implementation of the standard, vendors must implement all mandatory features of the standard. In some cases, like the use of CRC-32 for integrity, the standard is weak by design and needs to be changed. Until that happens, products will continue to be taken to market with known weaknesses. In other cases, stronger security measures are possible without violating the standard. Key management, for example, is a function that is external to the standard and can be implemented as a product developer sees fit. This creates the issue of interoperability limiting the selection of products for the organization that desires stronger protection, but most vendors do offer options that strengthen security.

IEEE Activities. There continues to be on-going development of the standard and a part of that development is stronger security measures. The chairman of the IEEE 802 committee has publicly responded to the threat and vulnerabilities raised by the U. C. Berkeley team. Some of his more important comments are paraphrased as follows:

1. WEP was never intended to provide more protection than a physically protected LAN environment. Since most LAN's are physically protected from external access, WEP was designed for equivalency protection from casual eavesdropping. WEP was never intended to be a complete security solution. Like wired LANs, a wireless network needs to be augmented with additional security mechanisms (e.g., end-to-end encryptions, virtual private networks, etc.), as appropriate to the requirements of the user organization.
2. The active attacks are not easy to mount. They are conceivable given enough time and resources, but may not yield enough value to an adversary to be worthwhile.
3. Since July 1999, task Group E of the standards committee has been working on extensions to the standard with the specific goal of strengthening the security of the standard. The enhancements currently being considered are intended to counter extremely sophisticated attacks, including those that have been recently reported in the press.

It will be sometime yet until the standard is modified, balloting is complete, and new protection mechanisms work their way into commercial products. However, the message is clear that the standard will change and new products will provide increased protection.

The U. C. Berkeley Paper. The Berkeley paper reveals that some attacks can be mounted with only a moderate effort while others are difficult and available only to a sophisticated

attacker with significant time and resources. In essence, the paper reports two significant weaknesses in wireless security:

1. The use of a shared key coupled with the use of a relatively short 24-bit Initialization Vector (IV) makes it possible with moderate effort to recover keys and decrypt encrypted communications. This also leads to more esoteric attacks, but they are harder to realize in practice.
2. The use of a CRC-32 checksum for integrity assurance instead of a cryptographically secure Message Authenticating Code places the integrity of messages at risk. This is not a generally a concern associated with the disclosure of the contents of applications messages, but it establishes the possibility of an IP re-direction vulnerability that could compromise the entire network. The effort in this case is still moderate and the threat cannot be realized remotely. It requires that the adversary have proximate access to the radio communications of the wireless network.

In their concluding remarks, the writers describe several countermeasures that can be implemented. In general, other authors who have written about wireless security also support these actions. They make the following recommendations:

1. As a first priority, the wireless network should be placed outside an organization's perimeter firewall as opposed to connecting behind the firewall.
2. For access between mobile stations attached to the wireless network and systems inside the firewall, they recommend the use of a Virtual Private Network.
3. The network should be configured to eliminate routes between the wireless network and the Internet. However, they do indicate that it may be desirable to allow visitors to access the Internet through the wireless network.
4. Finally, they recommend consideration of improvements in key management that results in every wireless station having its own encryption key and that the keys be changed frequently. Since this capability is external to the standard it does not affect compliance with the standard. However, it does increase the potential for interoperability failures and is likely to restrict product selection.

Conclusions and Recommendations

Based on the above discussion, and experience of PNNL in operating a pilot wireless network with a limited number of access points and stations since the middle of calendar year 2000, the following recommendations for network security are offered.

1. Provide a production network that is outside the existing firewall. Because this will be considered an insecure network, sensitive information will be prohibited from stations accessing the network.
2. Establish a Virtual Private Network. If staff need to connect back to the internal network behind the firewall, utilize a VPN tunnel that overcomes many of the problems with the WEP security measures provided on the wireless network.

In addition, several additional measures of protection may be provided:

1. Commercial access points from some vendors support more that one logical network that is implemented by a separate access point interface or transceiver card. This feature can be implemented such that visitors and assignees can be assigned to use one of the logical networks and staff can use the other network. This will permit use of separate sets of encryption keys for visitors.
2. The standard supports key schedules per logical network. Access points and clients can be individually configured *to transmit using any one* of the 4 shared keys, but can decrypt incoming traffic with any of the 4 keys. It is up to the network administrator to determine how many schedules to use for data transmission at the access points. Network administrators can rotate the transmit key used by the access points without affecting users directly. If only one key is used, then all stations on that schedule use the same key. It is advisable to use all four key schedules, so there will be a minimum of 4 different keys such that compromising one key will only compromise about 25% of the users. Key rotation in the access points also makes the attackers task more difficult by presenting network traffic with varying keys (i.e., users transmissions are spread among
3. Provide the capability for visitors to access the Internet from their wireless stations. Implement static routing so no routes to point to the firewall. Implement a second firewall outside the interior firewall and between the wireless LAN and the Internet. This firewall can be used to prevent external attacks on access points and wireless workstations using the network.
4. Those visitors and assignees that require access to information located behind the firewall will use a route that points to WebGate. WebGate is a web proxy server that can allow tightly restricted access to specific web pages following an authorization and approval process. Once granted, the user is securely authenticated, passes the request to WebGate, and WebGate satisfies the request in accordance with an authorization to view table. Connections to WebGate and webmail are encrypted also (i.e., https://), thus providing privacy even without WEP.

This Appendix was adapted from a document prepared in February 2001 by:
Robert E. Mahan
Pacific Northwest National Laboratory

Bibliography

_____, “Security of the WEP Algorithm,” available at http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Borisov, N, I. Goldberg, and D. Wagner, “Intercepting Mobile Communications: The Insecurity of 802.11,” draft, available at http://www.isaac.cs.berkeley.edu/isaac

Gillian, S., “Vulnerabilities within the Wireless Application Protocol,” August 31, 2000, available at http://www.sans.org/infosecFAQ/WAP.htm

Mitchell, G. L., “Wireless LANs – the Big New Security Risk,” May 5, 2000, available at http://www.sans.org/infodecFAQ/wireless/LAN.htm

Ross, B. J., “Containing the Wireless LAN Security Risk,” November 4, 2000, available at http://www.sans.org/infosecFAQ/wireless/wireless_LAN.htm

Wang, S., “Threats and Countermeasures in Wireless Networking,” December 20, 2000, available at http://www.sans.org/infosecFAQ/wireless/threats.htm