

**White Paper  
for: MTS Mobile  
Communications**

September 9

**2008**

---

This paper briefly describes how the MissionMobility LLC Data Communications Devices (MTS) provides the most reliable communications in the market today.

Getting time  
critical Data, Voice  
and Video when  
and where you  
need it

**Contents**

Purpose ..... 3

Mobile Transport Systems ..... 3

    The Baseband System ..... 3

    The Transmission System ..... 4

    Gateway ..... 5

The Data Communications Device (MTS) ..... 5

    MTS-INS Highlights ..... 7

        MTS-INS Technical Performance Measures ..... 7

        MTS-INS (RSU Module) ..... 8

        MTS-INS-SEN (Secure Network Module) ..... 11

## Purpose

Communications is the key to providing decision makers the information they need when they need it. Mobile, lightweight, easy to use, and reliable communication systems are essential to providing today's warfighter the data, voice, and video needed to make the most informed decisions possible. This paper briefly describes how the MissionMobility LLC Data Communications Devices (MTS) provides the most reliable communications in the market today.

## Mobile Communications Systems

Communications systems are often intended to extend classified and unclassified information from simple text to high definition video. The systems come packaged in many shapes and sizes from multiple transit cases requiring pallets for transport to small backpack systems that can be carried by one person. The requirements for this type of communication vary from systems that can be discretely carried into a location and quickly set up to push or pull data and quickly torn down and moved to systems residing in one location over an indefinite period, to systems inside aircraft, on ships, or in vehicles providing data while on-the-move and on-the-halt. They system is a system of systems generally comprised of a baseband system, a transmission system, and a gateway.

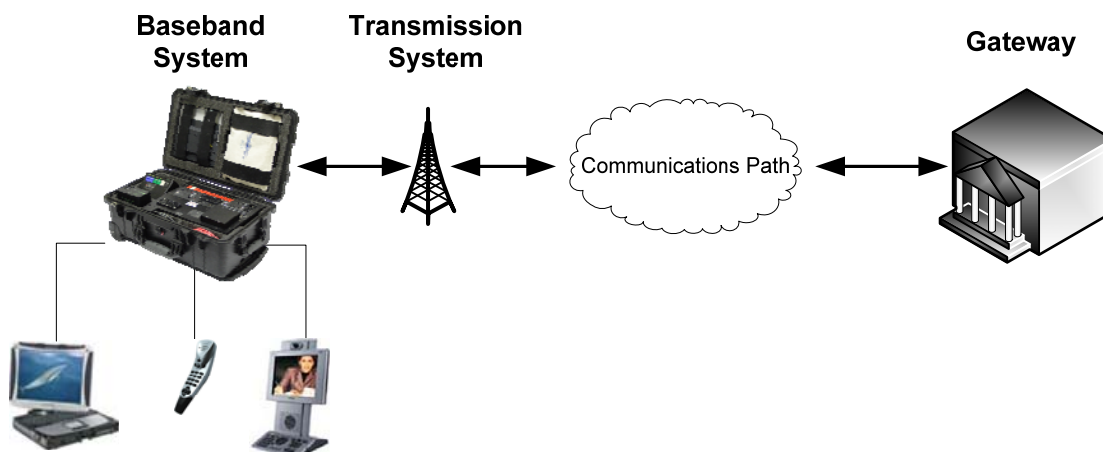


Figure 1: Mobile Communications Architecture

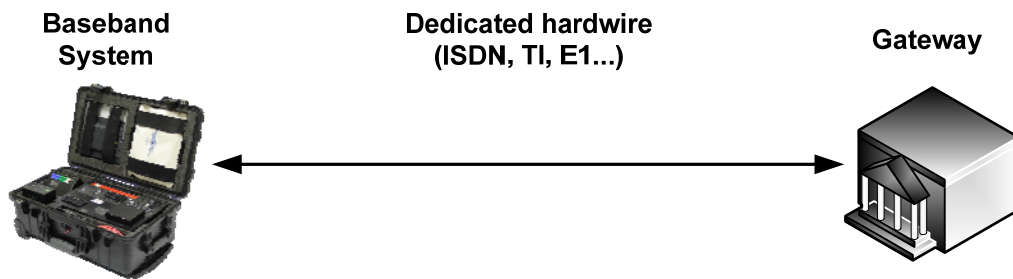
## The Baseband System

The baseband system is the key component of the communications package. The baseband system is the piece that handles the pushing and pulling of classified and unclassified data, voice, or video to and from the Gateway. In most recent communications systems this is being accomplished by placing Everything over Internet Protocol (EoIP). The baseband system connects to the transmission system for its Wide Area Network (WAN) connectivity to the gateway via an encrypted tunnel extending those services forward as if the operator were physically at the gateway. The operators connect their devices like laptops, VoIP telephones, and IP based VTC devices to the baseband system for Local Area Network (LAN) connectivity. In this scenario the operator can access their data (email, data bases...), voice

services, and VTC in the same manner they do while at the gateway. This helps reduce the training required for the operators to learn how to use their email and other services provided at the gateway. If the user devices like the laptops are from the gateway location, the users will not have to reconfigure their devices they simply plug in.

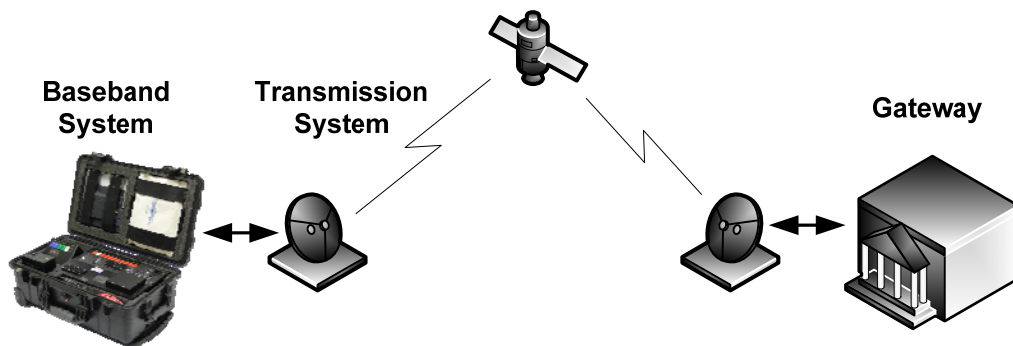
### ***The Transmission System***

The transmission system extends the classified and unclassified data, voice, and video from the baseband system via whatever transmission path is available in the region the system is operating in. These transmission systems can be hardware, line of site wireless, or satellite providing a wide range of throughput or bandwidth at a variety of costs and quality or performance. The transmission system can connect directly to the gateway via a dedicated data path or tunnel to the gateway via the public internet. Dedicated paths can be established using leased hardwire circuits from the baseband to the gateway, examples would be ISDN or T1 circuits from telephone providers, as shown in Figure2..



**Figure 2: Dedicated Hardware Connectivity**

Connectivity can be established via dedicated satellite circuits via point-to-point satellite service as shown in Figure 3. The point to point satellite could be a terminal located physically at the Gateway or terminal located at a commercial service provider with a dedicated hardwire connection between the service provider and the Gateway.



**Figure 3: Dedicated Satellite Connectivity**

Another method of reaching the gateway is through the public internet. Public Internet access can be established through many different ways including a hotel, cellular system via GSM or CDMA, 802.11

wireless hot spots, and different satellite services like KU and L band. The connectivity is established via the Advanced Encryption Standard (AES) 256B Virtual Private Network (VPN) tunnel from the baseband system to the gateway over the public internet. Figure 4 shows a high level picture where the transmission system represents the methods previously mentioned.

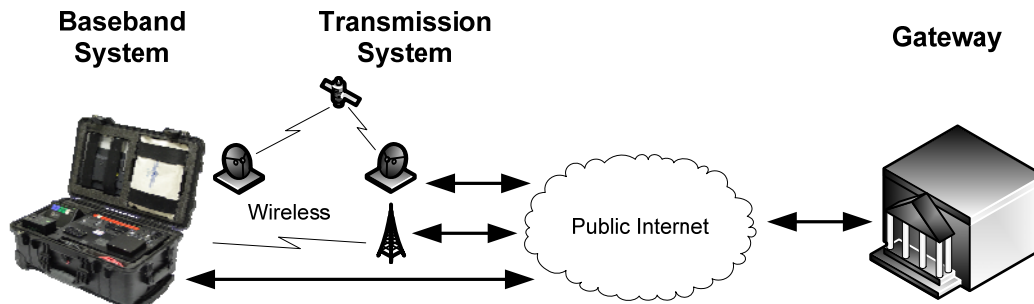


Figure 4: Public Internet Connectivity

## Gateway

The gateway is the location the requested services or data networks originate. Some examples of a gateway would be a headquarters the operators originate from or an entry point form a government provided gateway like a DISA step site. The Headquarters access point would provide connectivity to the network and domain the operators originate from to extending their existing email, databases, telephone, and VTC services. The users would operate as they do at their desk. A government provided gateway would provide those services like access to the global NIPRNET and SIPRNET but does not provide direct connectivity to the existing headquarters services.

## The Modular Transport Suite (MTS)

The MTS's are scalable mobile Multi-Network Communications packages that securely and simultaneously extend garrison classified networks, unclassified networks, video, and telephone capabilities worldwide via multiple transmission paths.

The MTS-INS is comprised of the Network Module (WAN/NIPR) and INS module (SIPRNET), Thrane & Thrane BGAN 500 terminal, and a MILSTD rechargeable battery. Housing of the primary equipment of the MTS-INS is within a customized, and lightweight, rugged case, backpack, or a customer defined package. Figure 5 shows an example of a commercial airline carry on size packaging for the MTS-INS and Figure 6 shows systems architecture.



Figure 5: Example MTS-INS Package

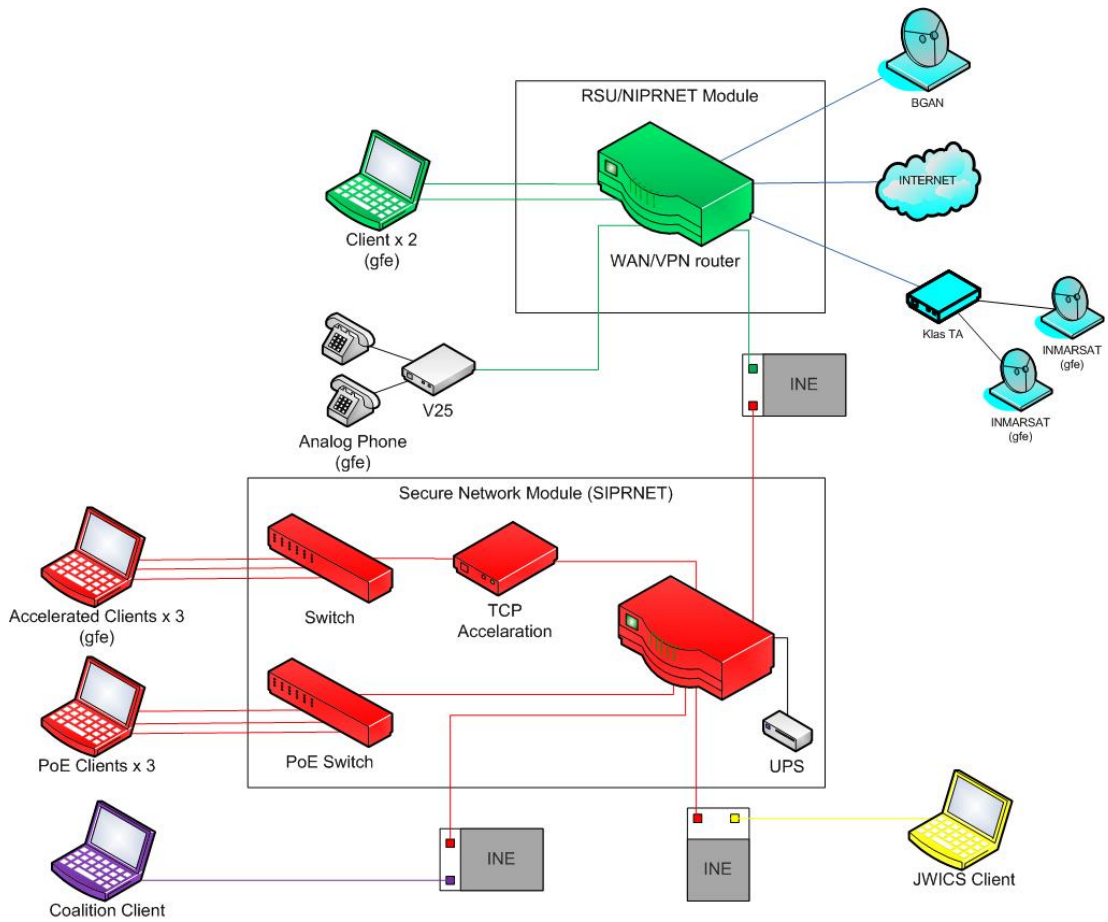


Figure 6: MTS-INS Example Systems Architecture

## ***MTS-INS Highlights***

- The MTS-INS extends the classified and unclassified enclaves of a customer's existing base network
- User retains access to the network using their credentials accessing their base email, web and network shares throughout the deployment
- The MTS-INS has redundant WAN connections allowing for automatic fail-over if primary WAN connection fails with no loss of connection
- The MTS-INS uses enterprise level 3200 series router designed by CISCO for integration into communications packages to equal the hardware standards of the base network domain. This extends to the life of the entire system by making it robust and future upgradable. The 3200 series routers are designed to scale up or down by using standards based hardware platforms, they are not office routers removed from their plastic covers. Using standards based modular router allows for applying DISA STIG's, Advanced QoS and future growth without having to replace the entire system
- FIPS 140-1 and FIPS 140-2 compliant VPN
- Power over Ethernet (PoE) devices such as IEEE 80211.3af compliant VoSIP phones and PoE switches or VTC devices
- The MTS-INS provides 2 ea un-accelerated RJ-45 ports enabling the extension of alternate networks such as JWICs or a Coalition network
- Encryption devices can be powered from the MTS-INS providing uninterrupted power in the event of loss of AC power
- The MTS-INS uses a wide range of single phase AC power (96 to 264 VAC at 47 to 440 Hz) and various DC sources (12 to 36 VDC).
- The MTS-INS can continue to operate for 90 minutes via a MIL-STD rechargeable battery in the event of loss of AC power
- The MTS-INS is equipped with surge and brown-out protection
- The MTS-INS supports two DC inputs including the battery input. This allows the MTS to connect to an external source like vehicle power and still maintain UPS capability. **If the DC source is above 12V the internal battery will charge.**
- The MTS-INS power supply provides power to 4 external components such as BGAN terminals, external switches, and external routers

## **MTS-INS Technical Performance Measures**

The MTS-INS has been designed to operate in multiple environments and can be packaged in cases allowing for compliance with military standards for shipping. Each component is removable allowing for multiple packaging options to include commercial airline carry on, backpack, and commercial airline checkable depending upon the end users requirements.

The calculated environmental specifications for operational use are provided in Table 1 below. Please note the temperature, humidity, and altitude are based on metrics provided by the vendors of the COTS components. Dataline has taken measures to ensure the proper cooling and has options to harden these components even further.

**Table 1** Technical Performance Measures

<b>Environmental Specifications</b>	<b>Min</b>	<b>Max</b>	<b>Notes</b>
Power			
Volts (VAC)	90	264	Single Phase 2 wire w/ground
Volts (VDC)	10	36	Single Phase 2 wire w/ground
Frequency Range (Hz)	40	440	Single Phase 2 wire w/ground
Input Current (Amps) @120VAC	0.9	1.0	SEN included KG250
Input Current (Amps) @240VAC	0.45	0.5	SEN included KG250
Operating Temperatures ( C )	-10	45	14 – 113 deg F Estimated*
Relative Humidity (%)	0	80	Estimated*
Operating Altitudes (ft)	Sea Level	10,000	Estimated*

\*NOTE: Values are vendor provided for the integrated COTS components

### **MTS-INS (NM Module)**

The NM Module will provide the connectivity to the WAN device providing network connectivity back to the garrison network as well as connectivity for the NIPRNET clients. The module will create an AES 256bit encrypted tunnel back to the base network extending NIPR, and creates the path for the SIPRNET Type 1 Encrypted tunnel. The parts list for the components internal to the module is shown in Table 1. The module will have:

1. 5 RJ45 Ethernet Ports with a recommended configuration
  - a. 2 WAN Ports
  - b. 2 Client Ports (supports NIPR Clients, Vocality, and JWICS extension)
  - c. 1 Option Port for the SIPRNET Module Connection
  - d. 1 Console port for the Cisco 3220 router
2. 2 Smart Serial connections for Serial WAN interfaces like the KLAS TA for ISDN or Serial Modem for serial based Ku satellite systems.
3. 1 Cisco 3200 series router allowing for DISA STIG's and Advanced QoS



Figure 7.1: MTS-INS RSU

Table 2 MTS-INS V4-RSU Physical Specifications

Parameter	Specification
Height	5.5"
Width	5.175"
Depth	4.25"
Weight	3 lbs

Table 3 MTS-INS V4-RSU Power Specifications

Parameter	Specification
DC Input	10 to 36 VDC

**Table 4 MTS-INS-RSU Interface Specifications**

<b>Interface</b>	<b>Specification</b>
WAN Port (blue)	Fast Ethernet (1)
Option Port (blue)	Fast Ethernet (1) for alternate WAN connection
BLACK KG Port (black)	Connection point (1) for Encryption (Black Side)
Unclassified (U-LAN) Ports (green)	RJ-45 connections (2) for laptops
Serial Port	Connection point for serial WAN like ISDN
Console Ports	Connection point for the 3230 Router management

**Table 5 MTS-INS V4-RSU Network Specifications**

<b>Network</b>	<b>Specification</b>
Router Operating System	Cisco IOS Advanced Enterprise 12.3.14T7
Router Central Processing Unit (CPU)	Motorola MPC8250 210 MHz
Router System Memory	128 MB DRAM
Router Flash Memory	32 MB Flash
IPSec Encryption	3DES, AES-128/192/256 (FIPS-140-2)
Analog Voice	Secure Relay and G.729 using Best Flow Signaling Protocol (BSP)
Tunneling	VPN, Dynamic Multipoint Virtual Private Network (DMVPN), Generic Routing Encapsulation (GRE), Multipoint Generic Routing Encapsulation (mGRE)
Firewall	Optional IOS Stateful Firewall (EAL 4+)
Intrusion Prevention Service (IPS)	Optional IOS IPS
Routing Types	Static, Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Routing Information Protocol (RIP)
Routing Standards	IPv4/IPv6
Traffic Types	Unicast, Multicast, Broadcast
Quality of Service	Differentiate Services Code Points (DSCP) based
Quality of Service Tools	Priority Queuing, Class Based Bandwidth Management, Traffic Shaping, Random Early Detection (RED)
Management (Router)	Secure Shell (SSH) (v1/v2), Standard Network Management Protocol (SNMP) v3 (Data Encryption Standard (DES) only), console

## **MTS-INS-SEN (Secure Network Module)**

The Secure Network Module extends the Garrison SIPRNET network via the Type 1 tunnel through the WAN Modules AES256bit encrypted tunnel. 3 accelerated client ports, 3 non-accelerated IEEE 802.3af Power Over Ethernet (POE) ports, and 2 non-accelerated client ports directly off the router. This configuration will allow the user to easily bypass the acceleration if it is interfering with system performance. The Module will include a Cisco 3200 series router providing advanced QoS for voice, video, and data prioritization as well as advanced configuration capabilities to support applications like Multicast. The parts list is shown in Table 2. This module will also be the master power module capable of one AC input and two DC inputs that can all be connected simultaneously to 3 separate sources. The power will auto roll over if any of the other sources fail. A visual indicator shows charge level of rechargeable battery. Surge protection is included in the system. This module can be secured with any form of high-speed encryption such as KG-250, KG-175, or SEC-NET-54 E.. The overall system will have:

1. 9 RJ45 10/100M Ethernet Ports
  - a. 1 Red port for connectivity to the INE
  - b. 3 accelerated client ports
  - c. 3 non-accelerated client ports with IEEE 802.3af POE
  - d. 2 non-accelerated client ports (directly off the router)
2. 3 Input power options (auto sensing and auto rollover)
  - a. 1 AC in (90 – 264VAC 40 – 440 HZ)
  - b. 2 DC in (10-36VDC)
    - i. 1 port will have the ability to Charge the UBI-2590 with AC or DC (12VDC or higher) input
3. Power Outputs
  - a. 1 12VDC that powers the WAN Module
  - b. 1 12VDC that can power the Vocality Module, BGAN terminal or other 12VDC capable devices
    - i. We will make cables with connectors as requested by the customer.
  - c. 1 5VDC capable of powering a KLAS TA or other 5VDC devices
    - i. We will make cables with connectors as requested by the customer.



Figure 8.2: MTS-INS SEN

Table 6 MTS-INS-SEN Physical Specifications

Parameter	Specification
Height	5.0"
Width	13.175"
Depth	9.125"
Weight (MTS-INS-SEN with KG-250)	21 lbs

Table 7 MTS-INS V4-SEN Power Specifications

Parameter	Specification
-----------	---------------

AC Input	96 to 264 VAC at 47 to 440 Hz
DC Input	10 to 36 VDC
AC Power Consumption (VA)	120 VA
AC Power Consumption (watts, PF 0.7)	84 watts
AC Current (120 VAC)	1 amps
AC Current (240 VAC)	0.5 amps
DC Power Consumption	84 watts
DC Current (12 VDC)	7 amps
DC Current (24 VDC)	3.5 amps
AC/DC Switching	Automatic (AC seeking)

**Table 8 MTS-INS V4-SEN Interface Specifications**

<b>Interface</b>	<b>Specification</b>
SBU Port (gray)	Fast Ethernet (1) provides connection from SEN to SBU
ALT Ports (red)	Fast Ethernet ports (2) allows additional network connectivity
Classified (C-LAN) Ports (red)	RJ-45 connections (3) for laptops
Classified (PoE) Ports (red)	RJ-45 connections (3) for PoE devices
RED Port (red)	Connection point (1) for KG-250 (Red Side)
BLACK Port (black)	Connection point (1) for KG-250 (Black Side)
Optional Serial Ports (no cost)	Connection points (2) for STE, Sectera, or OMNI
Console Ports	Connection points for future capability

**Table 3 MTS-INS V4-SEN Network Specifications**

<b>Network</b>	<b>Specification</b>
Router Operating System	Cisco IOS Advanced Enterprise 12.3.14T7
Router Central Processing Unit (CPU)	Motorola MPC8250 210 MHz
Router System Memory	128 MB DRAM
Router Flash Memory	32 MB Flash
PEP	AOS SkyPipe Eos
PEP CPU	Intel, XP 42x , 266 MHz
IPSec Encryption (optional)	3DES, AES-128/192/256 (FIPS-140-2)
Tunneling	VPN, DMVPN, GRE, mGRE
Firewall	Optional IOS Stateful Firewall (EAL 4+)
IPS	Optional IOS IPS
Routing Types	Static, BGP, EIGRP, OSPF, RIP
Routing Standards	IPv4
Traffic Types	Unicast, Multicast, Broadcast
Quality of Service	DSCP based
Quality of Service Tools	Priority Queuing, Class Based Bandwidth Management, Traffic Shaping, Random Drop Detection
Management (KG-250)	HTTPS (primary), console (limited)
Management (Router)	SSH (v1/v2), SNMP v3 (DES only), console
Management (PEP)	HTTPS (primary), SSH (limited)