TM 11-5895-1691-12

DRAFT

TECHNICAL MANUAL

OPERATOR AND UNIT MAINTENANCE MANUAL

Combat Service Support (CSS) Automated Information Systems Interface (CAISI)

Consisting of

OL-701/TYQ Processor Group, Signal Data
(CAISI Bridge Module (CBM))
NSN 5820-01-487-4020

OL-700/TYQ Processor Group, Signal Data
(CAISI Client Module (CCM))
NSN 5820-01-487-4023

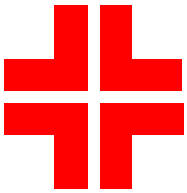
MK-2975/TYQ Accessory Kit, Electronic Equipment
(System Support Representative (SSR) Accessory Kit)
NSN 5999-01-487-2681

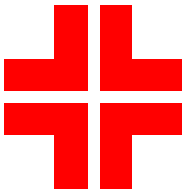
Distribution Statement C. Distribution authorized to the Department of Defense and DoD contractors only for official use or for administrative or operational purposes. This determination was made on 15 September 1997. Other requests for this document will be referred to Commander, US Army Communications-Electronics Command and Fort Monmouth, ATTN: AMSEL-LC-LEO-E-EQ-P, Fort Monmouth, New Jersey 07703-5007.

DESTRUCTION NOTICE

Destroy by any method that will prevent disclosure of contents or reconstruction of this document.

HEADQUARTERS, DEPARTMENT OF THE ARMY
1 AUGUST 2003





5 SAFETY STEPS TO FOLLOW IF SOMEONE IS THE VICTIM OF ELECTRICAL SHOCK:

1. DO NOT TRY TO PULL OR GRAB THE INDIVIDUAL.

2. IF POSSIBLE, TURN OFF THE ELECTRICAL POWER.

3. IF YOU CANNOT TURN OFF THE ELECTRICAL POWER, PUSH, PULL, OR LIFT THE PERSON TO SAFETY USING A DRY WOODEN POLE OR A DRY ROPE OR SOME OTHER NON CONDUCTING, INSULATED MATERIAL.

4. SEND FOR HELP AS SOON AS POSSIBLE.

5. AFTER THE INJURED PERSON IS FREE OF CONTACT WITH THE SOURCE OF ELECTRICAL SHOCK, MOVE THE PERSON A SHORT DISTANCE AWAY AND IMMEDIATELY START ARTIFICIAL RESUSCITATION.

NOTICE

This manual contains three types of notices: Warning, Caution, and Note. An explanation of each follows:

WARNING

Warning notices alert users to the possibility of immediate death or personal injury. Although damage to equipment may occur, the major concern is the probability of death or permanent injury if the warning notice is ignored.

CAUTION

Caution notices alert users to the possibility of damage to equipment from failure to follow procedures.

NOTE: A *Note, written in italics, provides general information concerning operations and procedures.*

WARNINGS

- Voltages as high as +56 Vdc can be encountered at the binding posts. Use extreme care when making connections as personal injury or death can result.

- Never work on electronic equipment unless there is another person nearby who is familiar with operation and hazards of the equipment and who is competent in administering first aid. When technicians are aided by users, they must be warned about dangerous areas. Whenever possible, the power supply to the equipment must be shut off before working on the equipment. Take particular care to ground every capacitor likely to hold a dangerous potential.

- Be careful not to contact high-voltage connections when installing or operating this equipment. Whenever the nature of the operation permits, keep one hand away from the equipment to reduce the hazard of current flowing through vital organs of the body.

- Do not be misled by the term low voltage. Potentials as low as 50 volts may cause death under adverse conditions.

WARNING

A hazardous condition exists during antenna erection and disassembly. Fatal injuries have been attributed to the pointed ends of the exposed antenna elements. Take the following precautions:

- Place a warning signal (Chem light, guard, or other signal) near the antenna elements during assembly, disassembly, or when the antenna elements are within reach, particularly at night,

- Remove the antenna elements if the antenna is lowered and unattended.

- Put on a helmet, safety glasses (NSN 4240-00-052-3776), and gloves before assembly and erection of the OE-254.

FIXED OPERATION WITH LONG RANGE ANTENNAS

WARNING

NEVER ERECT THESE LONG RANGE ANTENNAS
DIRECTLY UNDER POWER LINES

If you must erect these long range antennas near power lines, power line poles or towers, or buildings with overhead power line connections, never put the antenna closer than two times the antenna height from the base of the power line pole, tower, or building.

NEVER ATTEMPT TO ERECT ANY LONG RANGE
ANTENNA WITHOUT A FULL TEAM

Before erecting any long-range antenna, inspect all the parts making up the antenna kit. Do not erect the antenna if parts are missing or damaged.

Do as much of the assembly work as possible on the ground.

When erecting the antenna, allow only team personnel in the erection area.

Make sure the area for the anchors is firm. If the ground is marshy or sandy, get specific instructions from your crew chief or supervisor on how to reinforce the anchors.

When selecting locations for anchors, avoid traveled areas and roads. If you cannot avoid these areas, get specific instructions from your supervisor as to what clearance your guy wires and ropes must have over the traveled areas and road.

Clearly mark all guy wires and ropes, with the warning flags or signs supplied by your unit. In an emergency, use strips of white cloth as warning streamers.

If you suspect that power lines have made accidental contact with your antenna, stop operating, rope off the antenna area, and notify your superiors.

If the weather in your area can cause ice to form on your long-range antenna and its guy wires and ropes, add extra guys to support the system. Rope off the area and post it with warning signs, like “Beware of Falling Ice”.

Do not try to erect any antenna during an electrical storm.

Keep a sharp eye on your anchors and guy. Check them daily and immediately before and after bad weather.

UPS INSTALLATION SAFETY
CAUTION

- Do not allow UPS to be exposed to moisture, rain, dust, excessive heat or direct sunlight.
- Do not block the cooling vents on the side of the UPS.
- Position the UPS at least 6 inches from any monitors or floppy disks. Small magnetic fields present during backup operation can monitor interference or disrupt information on disks.
- Never plug a surge suppressor into any of the outlets; this will overload the UPS when operating from battery power.
- The UPS may be damaged if connected to a motor-powered AC generator with voltage and frequency output beyond nominal accepted ranges.

UPS BATTERY SAFETY
WARNING

- Batteries can present a risk of electrical shock and burn from high short-circuit current.
- Observe proper precautions.
- Do not dispose of the batteries in a fire.
- Do not open the UPS or the batteries.
- Do not short or bridge the battery terminals with any object.

UPS BATTERY SAFETY
CAUTION

- Batteries left discharged will suffer permanent loss of capacity.
- If the UPS is stored or not used for three months or longer, fully recharge the batteries by plugging the UPS into a live AC outlet, turning the Power Switch ON and letting the UPS charge for 4-6 hours.
- When the Power Switch is ON, the Battery Backup Protected/Surge Protected Outlets are energized from the internal battery, even when the unit is not plugged in.

CAUTION

This equipment contains parts and assemblies sensitive to electrostatic discharge (ESD). Use the following ESD precautionary procedures when touching, removing or inserting components:

ESD
CLASS 1
GENERAL HANDLING PROCEDURES FOR ESD ITEMS

- Always use wrist ground straps or manual grounding procedures.
- Keep ESD items in protective covering when not in use.
- Ground all electrical tools and test equipment.
- Periodically check continuity and resistance of grounding system.
- Handle ESD items only in protected areas.

MANUAL GROUNDING PROCEDURES

- Make sure equipment is powered down.
- Touch ground prior to removing ESD items.
- Touch package of replacement ESD item to ground before opening.
- Touch ground prior to inserting replacement ESD items.

ESD PROTECTIVE PACKAGING AND LABELING

- Always package ESD sensitive items in antistatic material and label with sensitive electronic symbol and caution statement.

CAUTION

Do not attempt to load any software or change any configuration on the CAISI notebook computer that is not part of the CAISI baseline or a change package officially released by Assistant Project Manager (APM), CAISI. Doing so will prevent the CAISI from functioning as designed.

LIST OF EFFECTIVE PAGES

INSERT LATEST CHANGED PAGES, DESTROY SUPERSEDED PAGES

NOTE: The portion of the text affected by the changes is indicated by a vertical line in the outer margins of the page. Changes to illustrations are indicated by miniature pointing hands. Changes to wiring diagrams are indicated by shaded areas.

Dates of issue for original and changed pages are:

Original.....0.....August 2003

TOTAL NUMBER OF PAGES IN THIS PUBLICATION IS 535
CONSISTING OF THE FOLLOWING:

Page No.	*Change No.
Title	0
a - f	0
A	0
B Blank	0
i - xxv	0
xxvi	0
1-1 - 1-27	0
1-28 Blank	0
2-1 - 2-48	0
2-49 – 2-199	0
2-200 Blank	0
3-1 - 3-91	0
3-92 Blank	0
4-1 – 4-2	0
A-1 - A-4	0
B-1 - B-8	0
C-1 - C-30	0
D-1 - D-2	0
E-1 – E-2	0
F-1 - F-22	0
G-1 - G-14	0
H-1 - H-9	0
H-10 Blank	0
I-1 - I-63	0
I-64 Blank	0
J-1 - J-26	0
Index-1 – Index-12	0 (Index)

THIS PAGE IS INTENTIONALLY LEFT BLANK

TECHNICAL MANUAL **HEADQUARTERS**
DEPARTMENT OF THE ARMY
No. 11-5895-1691-12 **WASHINGTON, D.C., 1 Aug 2003**

TECHNICAL MANUAL

OPERATOR AND UNIT MAINTENANCE MANUAL

COMBAT SERVICE SUPPORT (CSS) AUTOMATED INFORMATION SYSTEMS INTERFACE (CAISI)

Consisting of

OL-701/TYQ Processor Group, Signal Data
(CAISI Bridge Module (CBM))
NSN 5820-01-487-4020

OL-700/TYQ Processor Group, Signal Data
(CAISI Client Module (CCM))
NSN 5820-01-487-4023

MK-2975/TYQ Accessory Kit, Electronic Equipment
(System Support Representative (SSR) Accessory Kit)
NSN 5999-01-487-2681

REPORTING ERRORS AND RECOMMENDING IMPROVEMENTS

You can help improve this manual. If you find any mistakes, or if you know of a way to improve the procedures, please let us know. Mail or fax your letter, DA Form 2028 (Recommended Changes to Publications and Blank Forms), or DA Form 2028-2 located in the back of this manual directly to: Commander, US Army Communications-Electronics Command and Fort Monmouth, ATTN: AMSEL-LC-LEO-D-CS-CFO, Fort Monmouth, New Jersey 07703-5000. The fax number is 732-532-1413, DSN 992-1413. You may also e-mail your recommendations to: AMSEL-LC-LEO-PUBS-CHG@cecom3.monmouth.army.mil. A reply will be furnished direct to you.

TABLE OF CONTENTS

Section/Paragraph		Page
Chapter 1	**INTRODUCTION**	1-1
Section I	General Information	1-1
1.1	SCOPE	1-1
1.2	CONSOLIDATED INDEX OF ARMY PUBLICATIONS AND BLANK FORMS	1-1
1.3	MAINTENANCE FORMS, RECORDS, AND REPORTS	1-2
1.4	DESTRUCTION OF ARMY ELECTRONICS MATERIEL	1-2
1.5	PREPARATION FOR STORAGE	1-2
1.6	OFFICIAL NOMENCLATURE, NAMES, AND DESIGNATIONS	1-2
1.7	REPORTING EQUIPMENT IMPROVEMENT RECOMMENDATIONS (EIR)	1-3
1.8	WARRANTY INFORMATION	1-3
1.9	SAFETY, CARE, AND HANDLING	1-3
1.10	CORROSION PREVENTION AND CONTROL	1-4
1.11	SECURITY MEASURES FOR ELECTRONIC DATA	1-4
Section II	Equipment Description and Data	1-5
1.12	CAISI BACKGROUND/PURPOSE	1-5
1.12.1	CAISI Background	1-5
1.12.2	CAISI Purpose	1-6
1.12.3	System Design Requirements	1-8
1.13	CAISI BRIDGE MODULE (CBM)	1-9
1.14	CAISI CLIENT MODULE (CCM)	1-11
1.15	LEGACY SUPPORT ADAPTER (LSA)	1-12
1.16	SYSTEM SUPPORT REPRESENTATIVE (SSR) ACCESSORY KIT	1-13
1.17	ANTENNAS	1-16
1.18	CAISI EQUIPMENT DATA	1-18
1.18.1	Power Requirements And Physical Dimensions Data	1-18
1.18.2	Floor/Sub Floor Weight Capacity Requirements	1-21

Section/Paragraph		Page
Section III	Principles of Operation	1-22
1.19	CAISI ARCHITECTURE	1-22
1.19.1	CBM Architecture	1-24
1.19.2	CCM Architecture	1-26
1.19.3	LSA Architecture	1-27
Chapter 2	**OPERATION PROCEDURES**	**2-1**
Section I	Description and Use of Controls and Indicators	2-1
2.1	INTRODUCTION	2-1
2.2	CAISI BRIDGE MODULE (CBM)	2-1
2.3	WIRELESS BRIDGE	2-3
2.3.1	Power Injector for the Wireless Bridge	2-6
2.4	INLINE ENCRYPTOR	2-7
2.5	DSL BRIDGE	2-9
2.6	HUBS	2-12
2.7	UNINTERRUPTIBLE POWER SUPPLY (UPS)	2-14
2.8	CAISI CLIENT MODULE (CCM)	2-17
2.9	MULTI-CLIENT RADIO ADAPTER	2-18
2.10	LEGACY SUPPORT ADAPTER (LSA)	2-20
2.11	LINKSYS ROUTER	2-22
2.12	10Base-T TRANSCEIVER	2-25
Section II	Preventive Maintenance Checks and Services	2-27
2.13	INTRODUCTION	2-27
2.14	PMCS PROCEDURES	2-28
2.14.1	Routine Checks	2-28
2.14.2	Continuous Operations	2-29
2.14.3	Defects	2-29
2.14.4	Scheduling	2-29
2.14.5	PMCS Table	2-29

Section/Paragraph		Page
Section III	Operation Under Usual Conditions	2-49
2.15	CAISI COMPONENTS SETUP FOR OPERATION	2-49
2.15.1	CAISI in the MSE Environment	2-49
2.15.1.1	CAISI Root CBM	2-49
2.16	CAISI PREPARATION AND INITIATION	2-51
2.17	UNPACK THE CBM	2-52
2.17.1	Unpack the CBM Transit Case	2-54
2.17.2	Identify CBM Components	2-55
2.17.3	Inventory CBM Transit Case	2-67
2.17.4	Inspect CBM Components	2-67
2.18	SET UP THE CBM	2-68
2.18.1	Connect the Grounding Strap to the CBM	2-68
2.18.2	Connect the RF Cable to the Antenna and Bracket	2-69
2.18.3	Connect the Bracket to a Camouflage Pole and Erect the Antenna	2-71
2.18.4	Connect the RF Cable to the CBM Chassis	2-73
2.18.5	Connect the Power Cables to the CBM	2-74
2.18.6	Plug the UPS into 110VAC power	2-75
2.18.7	Connect Your Computers	2-75
2.18.8	Connect to the INE Device	2-76
2.19	INSTALLATION OF CBM IN SPECIAL CIRCUMSTANCES	2-77
2.19.1	DSL Bridge	2-77
2.19.2	Directional Panel Antenna	2-80
2.19.3	Long Antenna Cable using Barrel Connector	2-82
2.20	UNPACK THE CCM	2-83
2.20.1	Unpack the CCM Carrying Case	2-83
2.20.2	Identify CCM Components	2-84
2.20.3	Inventory CCM Carrying Case	2-88
2.20.4	Inspect CCM Components	2-89
2.21	SET UP THE CCM	2-89
2.21.1	Connect the Grounding Strap to the CCM	2-89
2.21.2	Connect the RF Cable to the Antenna and Bracket	2-89
2.21.3	Connect and Erect the Omni-Directional Antenna	2-89
2.21.4	Connect the RF Cable to the CCM Chassis	2-89
2.21.5	CCM Power Cable Connections	2-90

Section/Paragraph		Page
2.21.6	Connect Your Computers to the CCM	2-90
2.22	LSA	2-91
2.22.1	Unpack the LSA	2-91
2.22.2	Identify LSA Components	2-91
2.22.3	Inventory the LSA	2-92
2.22.4	Inspect LSA Components	2-92
2.23	UNPACK THE SSR ACCESSORY KIT	2-93
2.24	SSR TRANSIT CASE	2-93
2.24.1	Unpack the SSR Transit Case	2-95
2.24.2	Identify SSR Transit Case Components	2-97
2.24.3	Inventory SSR Transit Case	2-109
2.24.4	Inspect SSR Transit Case Components	2-111
2.25	SSR NOTEBOOK CASE	2-111
2.25.1	Unpack the SSR Notebook Case	2-112
2.25.2	Identify SSR Notebook Case Components	2-113
2.25.3	Inventory SSR Notebook Case	2-119
2.25.4	Inspect SSR Notebook Case Components	2-120
2.26	SSR ANTENNA CARRYING CASE	2-121
2.26.1	Unpack the SSR Antenna Carrying Case	2-121
2.26.2	Identify SSR Antenna Carrying Case Components	2-122
2.26.3	Inventory SSR Antenna Carrying Case	2-124
2.26.4	Inspect the SSR Antenna Carrying Case Components	2-124
2.27	SSR ANTENNA MAST CARRYING CASE	2-125
2.27.1	Unpack the SSR Antenna Mast Carrying Case	2-126
2.27.2	Identify SSR Antenna Mast Carrying Case Components	2-126
2.27.3	Inventory SSR Antenna Mast Carrying Case	2-127
2.27.4	Inspect the SSR Antenna Mast Carrying Case Components	2-128
2.28	SET UP THE ANTENNA MAST EQUIPMENT	2-129
2.28.1	Connect the RF Cable to the Omni-Directional Antenna and Bracket	2-129
2.28.2	Connect the RF Cable to the Directional Panel Antenna and Bracket	2-129
2.28.3	Connect Bracket to the Mast Section or Camouflage Pole	2-130
2.29	SET UP FOR ANTENNA MAST PROCEDURES	2-131
2.29.1	Positioning the Base Plate and Guy Stakes	2-131
2.29.2	Assembling the Antenna Mast	2-131

Section/Paragraph		Page
2.29.3	Erecting the Mast and Antenna	2-135
2.29.4	Connect the RF Cable to the CBM/CCM Chassis	2-136
2.30	OPERATING PROCEDURES	2-137
2.30.1	CAISI Components Requiring Configuration	2-137
2.30.2	SSR Notebook Setup and Configuration	2-138
2.30.2.1	Security Considerations for the CBM	2-139
2.30.2.2	Security Considerations for the CCM	2-140
2.30.3	Using the SSR Notebook	2-141
2.30.4	Using the SSR Notebook with the Wired NIC	2-143
2.30.5	Using the SSR Notebook with the Wireless NIC and Rabbit Ears Antenna	2-144
2.30.6	Using the SSR Notebook with the Wireless NIC and Large Antennas	2-145
2.31	CONFIGURE THE ROUTER	2-149
2.32	CONFIGURE THE CBM	2-150
2.32.1	Using the SSR Notebook to Configure the Wireless Bridge	2-150
2.32.1.1	Physical Connection of SSR Wireless Bridge for Configuration	2-153
2.32.1.2	Physical Connection of SSR Wireless Bridge for Operation	2-154
2.32.2	Configuring the Inline Encryptor	2-156
2.32.3	Configuring the DSL	2-156
2.33	CONFIGURE THE CCM	2-157
2.33.1	Using the SSR Notebook to Configure the Multi-Client Radio Adapter	2-157
2.33.1.1	Reset Multi-Client Radio Adapter	2-159
2.33.1.2	Physical Connection of SSR Multi-Client Radio Adapter for Configuration	2-160
2.33.1.3	Physical Connection of SSR Multi-Client Radio Adapter for Operation	2-161
2.33.2	Configuring the Inline Encryptor	2-162
2.34	10Base-T TRANSCEIVER CONNECTION	2-163
2.34.1	Connect SSR Wireless Bridge to the INE/NES	2-165
2.34.2	Connect SSR DSL Bridge to the INE/NES	2-167
2.35	STAMIS CONNECTIVITY TO CAISI	2-169
2.35.1	Connecting to CAISI Using 10Base-2	2-170
2.35.2	Connecting to CAISI Using 10Base-T	2-172
2.35.3	Connecting to CAISI Using the LSA	2-174
2.35.4	LSA Configuration	2-176

Section/Paragraph		Page
2.35.5	Monitoring Procedures	2-177
2.36	CAISI EQUIPMENT TEARDOWN	2-177
2.36.1	CBM Cable Disconnection Procedures	2-177
2.36.2	Disconnect the CBM Root Node from the INE	2-178
2.36.3	Disconnect STAMIS Users from the CBM	2-178
2.36.4	Disconnect CBM Connections	2-180
2.36.4.1	Disconnect UPS	2-180
2.36.4.2	Disconnect CBM Power Cables	2-180
2.36.4.3	Disconnect RF Cable from CBM Chassis	2-181
2.36.4.4	Teardown CBM Wireless RF Antenna	2-181
2.36.4.5	Disconnect RF Cable from the Antenna and Bracket	2-182
2.36.4.6	Disconnect CBM from Ground	2-183
2.36.4.7	Disconnect DSL or Directional Panel Antenna	2-183
2.37	CBM PACKUP PROCEDURES	2-185
2.37.1	Inventory CBM Transit Case	2-185
2.37.2	Packup CBM Transit Case	2-185
2.38	CCM DISCONNECTION PROCEDURES	2-187
2.38.1	Disconnect STAMIS Users from the CCM	2-187
2.38.2	Disconnect CCM Connections	2-187
2.38.2.1	Disconnect CCM Power Cables	2-187
2.38.2.2	Disconnect RF Cable from CCM Chassis	2-187
2.38.2.3	Teardown CCM Wireless RF Antenna	2-187
2.38.2.4	Disconnect RF Cable from the Antenna and Bracket	2-187
2.38.2.5	Disconnect CCM from Ground	2-187
2.39	CCM PACKUP PROCEDURES	2-188
2.39.1	Inventory CCM Carrying Case	2-188
2.39.2	Packup CCM Carrying Case	2-188
2.40	LSA DISCONNECTION PROCEDURES	2-189
2.40.1	Disconnect STAMIS Users from the LSA	2-189
2.40.2	Disconnect LSA Connections	2-189
2.41	LSA PACKUP PROCEDURES	2-189
2.41.1	Inventory LSA and Ancillary Components	2-189
2.41.2	Packup LSA	2-189
2.42	SSR ACCESSORY KIT PACKUP PROCEDURES	2-190
2.42.1	Teardown AB-1244B Antenna Mast	2-190

Section/Paragraph		Page
2.42.2	Disassemble the Whip Antenna and Bracket	2-191
2.42.3	Disassemble the Directional Panel Antenna	2-191
2.42.4	Disassemble the Antenna Mast Section	2-191
2.43	PACKUP SSR TRANSIT CASE PROCEDURES	2-192
2.43.1	Inventory SSR Transit Case	2-192
2.43.2	Packup SSR Transit Case	2-192
2.44	PACKUP SSR NOTEBOOK CASE PROCEDURES	2-195
2.44.1	Inventory SSR Notebook Case	2-195
2.44.2	Packup SSR Notebook Case	2-195
2.45	PACKUP SSR ANTENNA CARRYING CASE PROCEDURES	2-197
2.45.1	Disassemble Omni-Directional and Directional Panel Antennas	2-197
2.45.2	Inventory SSR Antenna Carrying Case Components	2-197
2.45.3	Packup SSR Antenna Carrying Case	2-198
2.46	PACKUP SSR ANTENNA MAST CARRYING CASE PROCEDURES	2-199
2.46.1	Teardown AB-1244B Antenna Mast	2-199
2.46.2	Inventory SSR Antenna Mast Carrying Case Components	2-200
2.46.3	Packup SSR Antenna Mast Carrying Case	2-200
Section IV	Operation Under Unusual Conditions	2-202
2.47	INTRODUCTION	2-202
2.47.1	Operation Under Extreme Heat or Desert Conditions	2-202
2.47.2	Operation Under Extreme Cold or Artic Conditions	2-202
2.47.3	Operation Under High Humidity or Tropical Conditions	2-202
Chapter 3	**OPERATOR MAINTENANCE INSTRUCTIONS**	**3-1**
Section I	Lubrication Instructions	3-1
3.1	LUBRICATION	3-1
Section II	Troubleshooting Procedures	3-1
3.2	OPERATOR TROUBLESHOOTING	3-1
3.3	DIAGNOSTIC FEATURES SUMMARY	3-1

Section/Paragraph		Page
3.3.1	Diagnostic LEDs	3-1
3.3.2	Audible Alarms	3-1
3.4	DIAGNOSTIC PROCEDURES	3-1
3.4.1	Troubleshooting Procedures	3-2
3.4.2	Individual Component Troubleshooting	3-3
3.5	TROUBLESHOOTING THE NETWORK	3-5
3.6	TROUBLESHOOTING THE SSR NOTEBOOK	3-19
3.7	TROUBLESHOOTING THE CBM	3-23
3.7.1	CBM General Troubleshooting Procedures	3-23
3.7.2	Troubleshooting the CBM Hubs	3-26
3.7.2.1	Troubleshooting CBM Inline Encryptor and Wireless Bridge	3-29
3.7.3	Troubleshooting CBM Antenna System	3-32
3.7.4	Troubleshooting the DSL Bridge	3-36
3.7.5	Troubleshooting the UPS	3-38
3.8	TROUBLESHOOTING THE CCM	3-40
3.8.1	CCM General Troubleshooting Procedures	3-40
3.8.2	Troubleshooting the CCM Hub	3-43
3.8.3	Troubleshooting CCM Encryptor and Multi-Client Radio Adapter	3-45
3.8.4	Troubleshooting CCM Antenna System	3-47
3.9	TROUBLESHOOTING THE LSA	3-51
3.9.1	Advance Troubleshooting for the LSA	3-52
3.10	TROUBLESHOOTING THE ROUTER	3-54
3.11	TROUBLESHOOTING THE 10BASE-T TRANSCEIVER	3-57
3.12	TROUBLESHOOTING THE AB-1244B ANTENNA MAST	3-58
3.13	TROUBLESHOOTING FLOWCHARTS	3-58
Section III	Operator Maintenance Procedures	3-78
3.14	MAINTENANCE	3-78
3.14.1	Introduction	3-78
3.14.2	Replacing Components within the CBM and CCM	3-91
Chapter 4	**UNIT MAINTENANCE INSTRUCTIONS**	**4-1**

Section/Paragraph		Page
Section I	Repair Parts, Tools, Special Tools, and Test, Measurement and Diagnostic Equipment (TMDE)	4-1
4.1	INTRODUCTION	4-1
4.2	COMMON TOOLS AND EQUIPMENT	4-1
4.3	SPECIAL TOOLS, TMDE, AND SUPPORT EQUIPMENT	4-1
4.4	REPAIR PARTS	4-1
Section II	Preventive Maintenance Checks and Services	4-1
4.5	PREVENTIVE MAINTENANCE CHECKS AND SERVICES	4-1
Section III	Troubleshooting	4-1
4.6	TROUBLESHOOTING	4-1
Section IV	Maintenance Procedures	4-1
4.7	MAINTENANCE PROCEDURES	4-1
Section V	Preparation for Storage or Shipment	4-2
4.8	INTRODUCTION	4-2
APPENDIX A	REFERENCES	A-1
APPENDIX B	MAINTENANCE ALLOCATION CHART (MAC)	B-1
APPENDIX C	COMPONENTS OF END ITEMS (COEI) AND BASIC ISSUE ITEMS (BII) LIST	C-1
APPENDIX D	ADDITIONAL AUTHORIZATION LIST (AAL)	D-1
APPENDIX E	EXPENDABLE AND DURABLE ITEMS LIST	E-1
APPENDIX F	CAISI SECURITY PROCEDURES	F-1
APPENDIX G	GLOSSARY/ACRONYM LIST	G-1

Section/Paragraph		Page
APPENDIX H	SAFE GROUNDING OF COMMUNICATIONS-ELECTRONICS EQUIPMENT IN THE FIELD	H-1
APPENDIX I	CAISI PLANNING	I-1
APPENDIX J	QUICK REFERENCE GUIDE AND INVENTORY CARDS	J-1
INDEX		Index-1

LIST OF FIGURES

FIGURE NUMBER	NAME	PAGE
1-1	Standard CAISI Node Architecture	1-7
1-2	CAISI System Architecture	1-8
1-3	CAISI Bridge Module (CBM) Front View	1-9
1-4	CBM Rear View	1-10
1-5	CAISI Client Module (CCM) Front View	1-11
1-6	CCM Rear View	1-12
1-7	CAISI Legacy Support Adapter – Lantronix MSS-100	1-12
1-8	System Support Representative (SSR) Accessory Kit	1-13
1-9	Duplicate Items of Equipment in SSR Accessory Kit	1-14
1-10	One-of-a-Kind (Unique) Items in SSR Accessory Kit	1-15
1-11	Directional/Omni-Directional Pattern	1-16
1-12	Antenna Specifications	1-17
1-13	CAISI Architecture	1-22
1-14	CAISI System Architecture	1-23
1-15	CBM Architecture	1-24
1-16	CBM Employment	1-25
1-17	CCM Architecture	1-26
1-18	CCM Employment	1-27
1-19	LSA Architecture	1-27
2-1	CBM Front View Components	2-1
2-2	CBM Rear View	2-1
2-3	Wireless Bridge Rear Panel	2-3
2-4	Wireless Bridge Rear Panel LEDs	2-4
2-5	Wireless Bridge Top Panel LEDs	2-4
2-6	Power Injector Connections and LED	2-6
2-7	Inline Encryptor Front View	2-7
2-8	Inline Encryptor Rear View	2-8
2-9	DSL Bridge Front View	2-9
2-10	DSL Bridge Rear View	2-10
2-11	Rate Configuration Switch	2-11
2-12	Hub Front View	2-12
2-13	Hub Rear View	2-12

FIGURE NUMBER	NAME	PAGE
2-14	UPS LEDs	2-14
2-15	CCM Front View	2-17
2-16	CCM Rear View	2-17
2-17	Multi-Client Radio Adapter Rear Panel	2-18
2-18	Multi-Client Radio Adapter Rear Panel LEDs	2-19
2-19	Multi-Client Radio Adapter Top Panel LEDs	2-19
2-20	LSA (MSS-100)	2-20
2-21	LSA (MSS-100) Front Panel	2-20
2-22	LSA (MSS-100) Rear Panel	2-20
2-23	LSA LEDs	2-21
2-24	Linksys Router Rear View	2-22
2-25	Linksys Router LEDs	2-23
2-26	10Base-T Transceiver Controls and Indicators	2-25
2-27	10Base-T Transceiver LEDs	2-26
2-28	CAISI Connectivity	2-50
2-29	CBM Transit Case Overview	2-52
2-30	CBM Transit Case	2-54
2-31	CBM Transit Case - Main Compartment	2-54
2-32	CBM Transit Case - Top Compartment (Lid Section)	2-55
2-33	CBM Chassis Sections	2-56
2-34	Wireless Bridge Deployment	2-58
2-35	Normal DSL Bridge Employment	2-59
2-36	CAISI Components MDI/MDI-X	2-66
2-37	Grounding Strap Connected to CBM	2-68
2-38	Grounding Strap Connected to the Ground	2-68
2-39	“7 in” Antenna Bracket	2-69
2-40	Thread Whip Antenna Through U-Bolts	2-69
2-41	Connecting the Antenna to the Bracket	2-70
2-42	Provide Strain Relief	2-70
2-43	Connecting the Whip Antenna	2-70
2-44	Connecting the Antenna to the Mast	2-71
2-45	Good Mast Placement – Example 1	2-72
2-46	Good Mast Placement – Example 2	2-72
2-47	RF Cable Entering Shelter	2-73
2-48	Cable Loop Inside Shelter	2-73

FIGURE NUMBER	NAME	PAGE
2-49	Antenna Cable Connection	2-74
2-50	CBM Power Connections	2-74
2-51	UPS Power Connections	2-74
2-52	UPS Power Connections On/Off Switch	2-75
2-53	Connect STAMIS Computers to CBM	2-76
2-54	Hub LEDs after Connection of STAMIS	2-76
2-55	Connecting to the INE with RG-58 Cable	2-76
2-56	Terminator and “T” Connector	2-77
2-57	Stripped Wire	2-78
2-58	Stripped Wire – Split Ends	2-78
2-59	Field Wire Connected to CBM Chassis	2-78
2-60	Field Wire Connected to DSL	2-79
2-61	Change the Data Transmission Rate (Speed) on DSL	2-79
2-62	Connecting the Panel Antenna	2-80
2-63	Connect Guy Ropes to Antenna Bracket	2-81
2-64	Barrel Connector	2-82
2-65	CCM Carrying Case	2-83
2-66	CCM Chassis Sections	2-84
2-67	Grounding the CCM	2-89
2-68	CCM Power Cord Connection	2-90
2-69	Connect STAMIS Computers to CCM	2-90
2-70	SSR Transit Case Overview	2-93
2-71	SSR Transit Case	2-95
2-72	SSR Transit Case – Main Compartment (with Encryptors)	2-96
2-73	SSR Transit Case – Main Compartment (without Encryptors)	2-97
2-74	Wireless Bridge Cabling	2-98
2-75	DSL Cabling	2-99
2-76	10Base-T Transceiver Used at the INE/NES using Wireless Bridge or DSL	2-102
2-77	SSR Transit Case – Top Compartment	2-104
2-78	SSR Notebook Case	2-111
2-79	SSR Notebook Case Latch	2-112
2-80	Rabbit Ears Antenna	2-114
2-81	Rabbit Ears Antenna and Wireless NIC	2-114
2-82	Wireless NIC Antenna Adapter Cables	2-115

FIGURE NUMBER	NAME	PAGE
2-83	SSR Antenna Carrying Case	2-121
2-84	SSR Antenna Carrying Case and Components	2-121
2-85	SSR Antenna Mast Carrying Case	2-125
2-86	Antenna Mast Sections	2-126
2-87	Antenna Mast Kit	2-127
2-88	Connecting the Panel Antenna – “7x7” and “14x14”	2-130
2-89	Ground Anchor/Pivot Clevis Attachment	2-131
2-90	Positioning the Guy Stakes	2-132
2-91	Attaching Guy Hooks to Guy Plate	2-132
2-92	Attaching Guy Loops to Ground Anchor	2-133
2-93	Attaching Guy Loops to Side and Back Guy Stakes	2-133
2-94	Pulling Guy Rope Tight	2-134
2-95	Securing Guy with Snubber Lock	2-134
2-96	Strain Clamp Closed	2-134
2-97	Erecting the Antenna Mast	2-136
2-98	Antenna Site with Inadequate Distance Between Power Lines and Antenna Mast	2-136
2-99	CAISI Components Requiring Configuration	2-137
2-100	Wired NIC and Wireless NIC	2-141
2-101	Notebook Connections	2-142
2-102	Wired NIC	2-143
2-103	SSR Notebook with Wireless NIC and Rabbit Ears Antenna	2-144
2-104	Rabbit Ears Antenna and Wireless NIC	2-144
2-105	Wireless Client Encryption	2-145
2-106	Antenna Adapter Cables, Right Angle Adapter and Barrel Connector	2-145
2-107	RPTNC and N Connectors	2-146
2-108	Wireless NIC Antenna Adapters	2-146
2-109	Permanent Connection of Large Antenna to SSR Notebook	2-147
2-110	Temporary Connection of Large Antenna to SSR Notebook	2-148
2-111	Router Configuration Ports	2-149
2-112	Connect 4-inch Whip Antenna to CBM	2-152
2-113	Connect Right-Angle Adapter and 40-inch Whip Antenna to CBM	2-152
2-114	Wireless Bridge Serial Connection	2-153
2-115	Connect Antenna to SSR Wireless Bridge	2-153
2-116	SSR Wireless Bridge, Power Supply and Power Injector	2-154

FIGURE NUMBER	NAME	PAGE
2-117	SSR Wireless Bridge and Inline Encryptor Connections	2-155
2-118	Inline Encryptor Console Configuration	2-156
2-119	Connect 4-inch Whip Antenna to CCM	2-158
2-120	Connect Right-Angle Adapter and 24-inch Whip Antenna to CCM	2-158
2-121	Connect Antenna to SSR Multi-Client Radio Adapter	2-160
2-122	SSR Multi-Client Radio Adapter and Inline Encryptor Connections	2-162
2-123	10Base-T Transceiver	2-163
2-124	10Base-T Transceiver Used at the NES	2-164
2-125	Connect to INE Using SSR Wireless Bridge Components	2-165
2-126	Connect to INE Using DSL Components	2-167
2-127	Connect Network Capable STAMIS to CAISI	2-169
2-128	Non-Network Capable STAMIS via Null Modem	2-170
2-129	RG-58 Cable Connection with Terminator	2-171
2-130	Connecting an Additional Hub	2-173
2-131	LSA Components	2-174
2-132	LSA with Null Modem and Cat-5 Cable	2-174
2-133	CAISI LSA Connection with Null Modem Cable	2-175
2-134	LSA Schematic View	2-175
2-135	CAISI Notebook Direct Configuration of LSA	2-176
2-136	Disconnect CBM from the INE	2-178
2-137	Disconnect RG-58 and T-Connectors	2-179
2-138	Disconnect LSA Cables	2-179
2-139	Turn off UPS / Disconnect CBM Power Cables	2-180
2-140	Disconnect CBM Power Cables from CBM Chassis	2-180
2-141	Disconnect RF Cable from CBM Chassis	2-181
2-142	Disconnect RF Antenna from Bracket	2-181
2-143	Disconnect Whip Antenna	2-182
2-144	Disassemble Whip Antenna from Bracket	2-182
2-145	Disconnect Grounding Strap from CBM and the Ground	2-183
2-146	Disconnect DSL Bridge	2-183
2-147	Teardown Directional “Panel” Antenna	2-184
2-148	Remove Guy Ropes from Directional Panel	2-184
2-149	CBM Transit Case	2-185
2-150	CBM Transit Case – Main Compartment	2-186
2-151	CBM Transit Case – Top Compartment (Lid Section)	2-186

FIGURE NUMBER	NAME	PAGE
2-152	Disconnect CCM Power Cables	2-187
2-153	CCM Carrying Case	2-188
2-154	Disconnect LSA Connections	2-189
2-155	Tearing Down the Antenna Mast	2-190
2-156	SSR Transit Case	2-192
2-157	SSR Transit Case – Main Compartment	2-193
2-158	SSR Transit Case – Top Compartment (Lid Section)	2-194
2-159	SSR Notebook Case	2-195
2-160	Unlatch SSR Notebook Case	2-195
2-161	SSR Notebook Case – Main Compartment	2-196
2-162	SSR Antenna Carrying Case	2-197
2-163	SSR Antenna Carrying Case and Components	2-198
2-164	Schematic Layout of SSR Antenna Carrying Case	2-199
2-165	SSR Antenna Mast Carrying Case and Components	2-199
2-166	Mast Sections	2-200
2-167	Antenna Mast Kit	2-201
3-1	Troubleshoot Antenna, Ethernet, Coaxial and Power Cables	3-7
3-2	Troubleshoot Antenna & Cable Connectors	3-8
3-3	Omni-Directional Whip Antenna Gain	3-9
3-4	Omni-Directional Whip Elevation Difference	3-9
3-5	Directional Panel Gain	3-10
3-6	Wireless NIC and MMCX to N (F) Adapter Cable	3-10
3-7	5-4-3 Rule	3-13
3-8	RJ-45 Connector	3-15
3-9	Crimp Strain Relief	3-16
3-10	Straight-Through (EIA 568-B/568-A) Cabling	3-17
3-11	Crossover (EIA 568-B) Cabling	3-17
3-12	Wireless NIC, Rabbit-Ears Antenna and SSR Notebook	3-21
3-13	Troubleshoot the CBM	3-23
3-14	Wireless Bridge Rear Panel	3-23
3-15	Wireless Bridge Top Panel	3-24
3-16	Inline Encryptor LEDs	3-25
3-17	DSL Bridge LEDs	3-25
3-18	Hub LEDs	3-26

FIGURE NUMBER	NAME	PAGE
3-19	Troubleshoot Omni-Directional Antenna	3-32
3-20	Troubleshoot Directional Antenna	3-32
3-21	Testing 4”, 24” or 40” Whip Antenna	3-33
3-22	Troubleshoot Lightning Arrestor in CBM	3-34
3-23	MMCX to RPTNC and 12-inch RF Antenna Cable	3-35
3-24	Troubleshoot 12” RF Antenna Cable in CBM	3-36
3-25	DSL Bridge Front View	3-36
3-26	DSL Bridge Speed Setting	3-37
3-27	Troubleshoot the CCM	3-40
3-28	Multi-Client Radio Adapter Rear Panel	3-41
3-29	Multi-Client Radio Adapter Top Panel	3-41
3-30	Inline Encryptor LEDs	3-42
3-31	Hub LEDs	3-42
3-32	Troubleshoot Omni-Directional Antenna	3-47
3-33	Testing 4”, 24” or 40” Whip Antenna	3-48
3-34	Troubleshoot CCM Lightning Arrestor and RF Antenna Cable	3-49
3-35	Troubleshoot Lightning Arrestor in CCM	3-49
3-36	MMCX to RPTNC and 12-inch RF Antenna Cable	3-50
3-37	Troubleshoot 12” RF Antenna Cable in CCM	3-50
3-38	LSA LEDs	3-51
3-39	Router LEDs	3-54
3-40	10Base-T Transceiver LEDs	3-57
3-41	Troubleshooting the Network Flowchart	3-60
3-42	CAISI Installation – CBM Flowchart	3-61
3-43	CAISI Installation – LSA Flowchart	3-62
3-44	CAISI PMCS Flowchart	3-63
3-45	Troubleshooting Components Flowchart	3-64
3-46	Troubleshooting Hardware Components Flowchart	3-65
3-47	Troubleshooting SSR Notebook Flowchart	3-66
3-48	Troubleshooting Wireless Bridge Flowchart	3-67
3-49	Troubleshooting Inline Encryptor Flowchart	3-68
3-50	Troubleshooting DSL Bridge Flowchart	3-69
3-51	Troubleshooting the Hub(s) Flowchart	3-70
3-52	Troubleshooting the UPS Flowchart	3-71
3-53	Troubleshooting Multi-Client Radio Adapter Flowchart	3-72

FIGURE NUMBER	NAME	PAGE
3-54	Troubleshooting LSA (MSS-100) Flowchart	3-73
3-55	Troubleshooting Linksys Router Flowchart	3-74
3-56	Troubleshooting 10Base-T Transceiver Flowchart	3-75
3-57	Troubleshooting CAISI Maintenance Support Flowchart	3-76
3-58	CAISI Maintenance Support	3-77
3-59	CAISI Maintenance Concept	3-78
C-1	CBM Components of End Item	C-18
C-2	CBM Chassis Components of End Item	C-19
C-3	CBM Transit Case – Main Compartment	C-19
C-4	CBM Transit Case – Top Compartment (Lid Section)	C-19
C-5	CCM Components of End Item	C-20
C-6	CCM Carrying Case – Compartments	C-20
C-7	CCM Chassis Components of End Item	C-21
C-8	LSA Components of End Item	C-22
C-9	SSR Transit Case Components	C-23
C-9b	SSR Transit Case Components – continued	C-24
C-10	SSR Transit Case – Main Compartment	C-25
C-11	SSR Transit Case – Top Compartment (Lid Section)	C-25
C-12	SSR Notebook Case Components	C-26
C-13	SSR Notebook Case – Main Compartment	C-27
C-14	SSR Antenna Carrying Case Components	C-28
C-15	SSR Antenna Carrying Case Layout	C-28
C-16	SSR Antenna Mast Carrying Case	C-29
C-17	Antenna Mast Sections	C-29
C-18	Antenna Mast Kit	C-30
F-1	Priority for Destruction Chart	F-12
F-2	DoD Warning Banner	F-16
F-3	Tactical CAISI LAN Architecture	F-22
H-1	Single-Section Ground Rod	H-2
H-2	Multiple-Section Ground Rod	H-2
H-3	Proper Cleaning of Ground Rod	H-3
H-4	Proper Method to Drive a Ground Rod	H-3

FIGURE NUMBER	NAME	PAGE
H-5	Proper Method to Connect Ground Strap to Ground Rod	H-4
H-6	Substitute Method for Ground Strap Binding	H-4
H-7	Complete Earth-Ground System	H-5
H-8	Improving Soil Connectivity with Salt and Water	H-5
H-9	Examples of Good Ground Connections to Buried Objects	H-6
H-10	Desert Ground System	H-7
H-11	Streambed Grounding System	H-7
H-12	Possible Ground Rod Layouts to Improve Ground	H-8
H-13	Prevent Lightning Flashover by Grounding	H-9
I-1	The Local Area Network (LAN)	I-2
I-2	The Wide Area Network (WAN)	I-4
I-3	IP Address vs. House Address	I-6
I-4	IP Address	I-7
I-5	Bridges vs. Routers	I-10
I-6	Wireless Communication Modes	1-13
I-7	Wireless Communications with Multiple Access Points	1-14
I-8	Wireless Bridges Connecting LAN Segments	1-15
I-9	Wireless Bridges Connecting LAN Segments and Clients	1-15
I-10	CAISI Connectivity	I-17
I-11	Normal DSL Bridge Employment	I-19
I-12	Using DSL Bridges with Field Wire	I-19
I-13	DSL and Field Wire Solution – Remote Command Post Operations	I-20
I-14	DSL and Field Wire Solution – Down the Hill Operations	I-20
I-15	Using Wireless Bridge with Directional Panel Antennas	I-23
I-16	Using the Router	I-24
I-17	Segmented Network Addresses	I-25
I-18	Router Between Two CBMs	I-26
I-19	Router Connected to a Bridge (Wireless or DSL)	I-27
I-20	Router Between CBM and Bridge	I-29
I-21	CAISI External Router Architecture	I-31
I-22	CAISI Security Device Architecture	I-33
I-23	Air Fortress Remote Client Employment	I-33
I-24	NES Gateway	I-34
I-25	CAISI System Architecture	I-36

FIGURE NUMBER	NAME	PAGE
I-26	Logistics Support Area	I-38
I-27	Line of Sight Factors	I-40
I-28	Antenna Gain	I-42
I-29	Compensating for Elevation Differences	I-43
I-30	CAISI in a DSA or other Larger Logistics Support Area	I-44
I-31	CAISI in a BSA and TFSA	I-45
I-32	Using the NTDR to Extend the CAISI	I-46
I-33	Using Multiple SSIDs for Segmentation	I-48
I-34	Multiple Root Radios	I-50
I-35	Adding an Additional Hub Components	I-55
I-36	Connection of Hubs via CAT-5 Straight-Through Cable	I-56
I-37	Daisy-Chain Technique	I-57
I-38	Connection of Hubs via CAT-5 Crossover Cable/RG-58 Cable	I-57
I-39	Garrison LAN Connectivity	I-59

LIST OF TABLES

TABLE NUMBER	NAME	PAGE
1-1	CAISI Nomenclature Cross Reference List	1-2
1-2	Planning Ranges for Antennas	1-16
1-3	Location of Antenna and Antenna Ancillary Components	1-17
1-4	CBM Equipment Characteristics	1-18
1-5	CCM Equipment Characteristics	1-19
1-6	LSA Equipment Characteristics	1-19
1-7	SSR Accessory Kit Equipment Characteristics	1-20
1-8	SSR Notebook Case Characteristics	1-21
2-1	CBM Components	2-2
2-2	Wireless Bridge Rear Panel Controls and Indicators	2-3
2-3	Wireless Bridge Rear Panel LEDs	2-4
2-4	Wireless Bridge Top Panel LEDs	2-4
2-5	Wireless Bridge Top Panel LEDs Description	2-5
2-6	Power Injector Connections and LED	2-6
2-7	Inline Encryptor Front Panel LEDs	2-7
2-8	Inline Encryptor Rear Panel Controls and Indicators	2-8
2-9	DSL Bridge Front Panel LEDs	2-9
2-10	DSL Bridge Rear Panel Controls and Indicators	2-10
2-11	Transmission Data Rate	2-11
2-12	Hub Front Panel Controls and Indicators	2-12
2-13	Hub Rear Panel LEDs and Controls	2-13
2-14	UPS LEDs and Controls	2-14
2-15	CCM Components	2-17
2-16	Multi-Client Radio Adapter Rear Panel Controls and Indicators	2-18
2-17	Multi-Client Radio Adapter Rear Panel LEDs	2-19
2-18	LSA (MSS-100) Controls and Indicators	2-20
2-19	LSA (MSS-100) LEDs	2-21
2-20	Linksys Router Controls and Indicators	2-22
2-21	Linksys Router LEDs	2-23
2-22	10Base-T Transceiver Controls and Indicators	2-25
2-23	10Base-T Transceiver LEDs	2-26
2-24	User PMCS	2-31

TABLE NUMBER	NAME	PAGE
2-25	Organizational PMCS	2-37
2-26	CBM Transit Case – Compartments	2-52
2-27	CBM (Minimum Unpack Components)	2-53
2-28	CBM Chassis Components	2-56
2-29	CBM Chassis Components Description	2-57
2-30	CBM Components Description	2-62
2-31	Straight-Through/Crossover Cabling	2-65
2-32	CBM Inventory Checklist Card	2-67
2-33	CCM Carrying Case – Compartments	2-83
2-34	CCM Chassis Components	2-84
2-35	CCM Chassis Components Description	2-85
2-36	CCM Components Description	2-87
2-37	CCM Inventory Checklist Card	2-88
2-38	LSA Components Description	2-91
2-39	LSA Inventory Checklist Card	2-92
2-40	SSR Transit Case – Compartments	2-94
2-41	SSR Transit Case – Main Compartment	2-96
2-42	SSR Transit Case – Main Compartment Components Description	2-97
2-43	SSR Transit Case – Top Compartment	2-104
2-44	SSR Transit Case – Top Compartment Components Description	2-105
2-45	SSR Transit Case Inventory Checklist Card	2-109
2-46	SSR Notebook Case – Main Compartment	2-112
2-47	SSR Notebook Case Components Description	2-113
2-48	SSR Notebook Case Inventory Checklist Card	2-120
2-49	SSR Antenna Carrying Case Contents Layout	2-122
2-50	SSR Antenna Carrying Case Components Description	2-122
2-51	SSR Antenna Carrying Case Inventory Checklist Card	2-124
2-52	SSR Antenna Mast Carrying Case Inventory Checklist Card	2-128
2-53	CAISI Components Requiring Configuration	2-138
2-54	Cable Connections for SSR Wireless Bridge to the INE	2-164
2-55	Cable Connections for DSL Bridge to the INE	2-165
2-56	SSR Antenna Carrying Case Contents	2-195
2-57	Location of Antenna and Antenna Ancillary Components	2-198
3-1	CAISI Troubleshooting	3-4

TABLE NUMBER	NAME	PAGE
3-2	Straight-Through/Crossover Cabling	3-14
3-3	Pinout for 10Base-T/100Base-T Ethernet Connections	3-15
3-4	Notebook Computer Troubleshooting Procedures	3-22
3-5	CBM Hub LEDs Description	3-26
3-6	DSL Bridge LEDs Description	3-36
3-7	Common UPS Problems	3-38
3-8	CCM Hub LEDs Description	3-43
3-9	LSA LEDs Description	3-51
3-10	Router LEDs Description	3-54
3-11	10Base-T Transceiver LEDs Description	3-57
3-12	Flowchart Symbols	3-58
3-13	List of Troubleshooting Flowcharts	3-59
3-14	CAISI Maintenance Support	3-77
3-15	Forward Repair Activity (FRA) Addresses	3-87
B-1	Maintenance Allocation Chart (MAC) for the CAISI	B-6
B-2	Tool and Test Equipment Requirements for CAISI	B-7
B-3	Remarks for CAISI MAC	B-8
C-1	CAISI Components of End Item (COEI)	C-2
C-2	CAISI Basic Issue Items (BII) List	C-30
D-1	Additional Authorization List (AAL)	D-2
E-1	Expendable and Durable Items List	E-2
H-1	Ground Conductor for Various Soil Types and Qualities of Ground	H-1
I-1	IP Addresses for Network Classes	I-8
I-2	Networks Characterized by Physical Links	I-9
I-3	Location of Antenna and Antenna Ancillary Components	I-22
I-4	Cable Connections Between Router and Hub	I-26
I-5	Cable Connections Between Router and Wireless Bridge/DSL	I-28
I-6	Cable Connections for Router Between CBM and Wireless Bridge	I-29
I-7	Antenna Heights	I-41

TABLE NUMBER	NAME	PAGE
I-8	Planning Ranges for Antennas	I-43
I-9	Character-to-Hex Conversion	I-51
I-10	Special Circumstances	I-54
I-11	World-Wide Transmit Power Limitations	I-61

HOW TO USE THIS MANUAL

Target Audience. The Combat Service Support (CSS) Automated Information Systems Interface (CAISI) Technical Manual is designed for two audiences:

a. The primary target audience for this manual is the CAISI installer/maintainer, MOS 31U or MOS 74B, who will be responsible for unpacking, setting up, and monitoring the CAISI components during operation. This manual is formatted primarily to meet the installer/maintainer requirements.

b. Standard Army Management Information Systems (STAMIS) operators will have to connect to CAISI to transmit data. These users will focus on Paragraph 2.24, which addresses the various ways these users may connect their STAMIS devices to the CAISI.

Structure of this Manual. The manual contains the following four chapters:

- **Chapter 1 - INTRODUCTION**. Describes CAISI as a system and gives a detailed explanation of the individual components. Use this introduction to become familiar with the system and to learn about the basic function of each component.

- **Chapter 2 - OPERATING PROCEDURES**. Gives instructions and illustrations of the controls, indicators and connectors for each LRU of the CAISI. Provides a list of preventive maintenance checks and services and gives a schedule for their performance. This chapter also provides a detailed setup, turn on, turn off and tear down procedure for the CAISI and how to setup in different scenarios.

- **Chapter 3 - OPERATOR MAINTENANCE INSTRUCTIONS**. Provides operator instructions for troubleshooting and maintenance of the CAISI.

- **Chapter 4 - UNIT MAINTENANCE INSTRUCTIONS**. Provides organizational maintenance instructions for troubleshooting and correcting various malfunctions that may be encountered with the CAISI system and each of the line replaceable units (LRUs). Also contains instructions for packaging and storage.

- **APPENDIX A** - REFERENCES
- **APPENDIX B** - MAINTENANCE ALLOCATION CHART (MAC)
- **APPENDIX C** - COMPONENTS OF END ITEMS (COEI) AND BASIC ISSUE ITEMS (BII) LIST
- **APPENDIX D** - ADDITIONAL AUTHORIZATION LIST (AAL)
- **APPENDIX E** - EXPENDABLE AND DURABLE ITEMS LIST
- **APPENDIX F** - CAISI SECURITY PROCEDURES
- **APPENDIX G** - GLOSSARY/ACRONYM LIST
- **APPENDIX H** - SAFE GROUNDING OF COMMUNICATIONS – ELECTRONICS EQUIPMENT IN THE FIELD
- **APPENDIX I** - CAISI PLANNING
- **APPENDIX J** - QUICK REFERENCE GUIDE AND INVENTORY CARDS
- **INDEX**

Commands and Keystrokes. Throughout the manual are commands and keystrokes to be entered by the user when using the CAISI:

When a user is given a command to type, i.e. **test**, the information to be entered is presented in **bold**.

Any command key pressed by the user, i.e., ¿ **Enter** or **F1**, is also in **bold**.

Additional Information. The CAISI Team maintains a web site where users may obtain additional information concerning CAISI as well as additional documentation. The CAISI home page is located at: http://www.eis.army.mil/caisi/index.htm

Chapter 1

INTRODUCTION

Section I General Information

1.1 SCOPE

a. **Type of Manual**. This is an Operator and Unit Maintenance Technical Manual, which describes operation and support of the Combat Service Support (CSS) Automated Information Systems Interface (CAISI). It is designed for use by the installer/maintainer of the CAISI devices and to serve as a reference source for Standard Army Management Information Systems (STAMIS) users connecting to CAISI. This manual details both operation and user maintenance procedures for the CAISI modules. STAMIS-specific operating procedures such as connection with the CAISI devices and data transfer procedures are detailed in the STAMIS training documentation and the Standard Operating Procedures (SOPs).

b. **Model Number and Equipment Name**. The CAISI consists of the CAISI Bridge Module, (Part Number A3269821), the CAISI Client Module (A3269822), the Legacy Support Adapter (MSS 100-01), and the System Support Representative Accessory Kit, (A3269820).

CAISI is comprised of various combinations of CAISI Bridge Modules (CBM), CAISI Client Modules (CCM), Legacy Support Adapters (LSA) and System Support Representative (SSR) Accessory Kit to accommodate different unit needs. **At a minimum, two CBMs will be issued**. Depending on the size and mission of the unit, some may receive more or fewer CBMs and CCMs. The number of components to be issued to a unit will be listed in the Table of Organization and Equipment (TOE).

c. **Purpose of Equipment**. The CAISI provides the capability to battlefield CSS automation devices to electronically exchange information via both tactical and commercial networks with other CSS automation devices (primarily other STAMIS), as well as automation devices within the sustaining base. Most STAMIS do not possess the hardware or software capability to pass data through the Tactical Packet Network (TPN) element of Mobile Subscriber Equipment (MSE). The CAISI device provides an interface for these STAMIS devices to allow access to the TPN

1.2 CONSOLIDATED INDEX OF ARMY PUBLICATIONS AND BLANK FORMS

Refer to the latest issue of DA PAM 25-30 to determine whether there are new editions, changes, or additional publications pertaining to the equipment.

1.3 MAINTENANCE FORMS, RECORDS, AND REPORTS

a. *Reports of Maintenance and Unsatisfactory Equipment*. Department of the Army (DA) forms and procedures used for equipment maintenance will be those prescribed by DA PAM 738-750, as contained in The Army Maintenance Management Update.

b. *Reporting of Item and Packaging Discrepancies*. Fill out and forward SF 364 [Report of Discrepancy (ROD)] as prescribed in AR 735-11-2.

c. *Transportation Discrepancy Report*. Fill out and forward SF 361 [Transportation Discrepancy Report (TDR)] as prescribed in AR 55-38.

1.4 DESTRUCTION OF ARMY ELECTRONICS MATERIEL

Destruction of Army electronics materiel to prevent enemy use shall be in accordance with TM 750-244-2.

1.5 PREPARATION FOR STORAGE

Administrative storage of equipment issued to and used by the Army will have Preventive Maintenance Checks and Services (PMCS) performed before being stored. Place items in administrative storage for short periods of time when a shortage of operator or maintenance resources exist. Keep appropriate maintenance records during storage. When removing the items from administrative storage, perform PMCS to ensure operational readiness. Inside storage is preferred for items selected for administrative storage. If inside storage is not available, use trucks, vans or other containers.

1.6 OFFICIAL NOMENCLATURE, NAMES, AND DESIGNATIONS

Shortened nomenclature is used in this manual to make procedures easier to read. Table 1-1 is a cross reference between the shortened nomenclature and the official nomenclature.

Table 1-1 CAISI Nomenclature Cross Reference List

Common Name	Acronym	Official Name	Part #	NSN
CAISI Bridge Module	CBM	Processor, Communications Gateway OL-701/TYQ	A3269821	5895-01-487-4020 Z53098
CAISI Client Module	CCM	Processor, Bridge OL-700/TYQ	A3269822	5895-01-487-4023 Z53096
Legacy Support Adapter	LSA	Interface Unit, ADP	MSS100-01	7025-01-487-4021
SSR Accessory Kit		Accessory Kit, Electronics Equipment MK-2975/TYQ	A3269820	5999-01-487-2681 Z00057

1.7 REPORTING EQUIPMENT IMPROVEMENT RECOMMENDATIONS (EIR)

If your equipment needs improvement, let us know. Send us an EIR. You, the user, are the only one who can tell us what you don't like with your equipment. Let us know why you are not satisfied with the design or performance. Put it on an SF 368 (Product Quality Deficiency Report). Mail it to Commander, US Army Communications-Electronics Command and Fort Monmouth, ATTN: AMSEL-LC-LEO-D-CS-CFO, Fort Monmouth, New Jersey 07703-5000. We'll send you a reply.

1.8 WARRANTY INFORMATION

Warranty Service will be acquired at the depot level and will not involve unit intervention. The unit level personnel using the CAISI may perform only limited troubleshooting on the CAISI components. Performing software diagnostics is primarily the responsibility of System Support Representative (SSR) personnel, who should be contacted when a problem arises. These personnel, as well as the software help desk may, during telephonic consultation, "talk" the user through diagnostic procedures in an attempt to diagnose the problem. Customer Assistance Office (CAO) phone numbers, FAX numbers and E-mail address are:

Comm: 804-734-1051
DSN: 687-1051
FAX Comm: 804-734-2947
FAX DSN: 687-2947
E-mail: cao@lee-dns2.army.mil

Users experiencing a problem with the CAISI components should never hesitate to contact SSR personnel or their designated next higher level of support. See Chapter 3 of this manual for further information.

1.9 SAFETY, CARE AND HANDLING

To prevent personal injury and damage to equipment, obey the following general rules and precautions.

- Familiarize yourself with the **CAUTIONS** and **WARNINGS** posted throughout this manual
- All Transit Cases for the CAISI require a two-person lift and carry.
- Turn off all power before starting any removal task.
- Do not touch connections, terminals, or pins with tools, bare hands, or a dirty cloth. Tools will damage the connections. Dirt or sweat will cause corrosion.

- Whenever possible, use an anti-static ground strap to ground your body to discharge static electricity. A static discharge to an electrical component can destroy internal circuits and possibly cause personal injury.

- Know where the emergency safety equipment and first aid kits are located. Read the instructions on the fire extinguisher label.

1.10 CORROSION PREVENTION AND CONTROL

Corrosion Prevention and Control (CPC) of Army Material is a continuing concern. It is important that any corrosion problems with these items be reported so that the problem can be corrected and improvements can be made to prevent the problem in future items. While corrosion is typically associated with the rusting of metals, it can also include deterioration of other materials, such as rubber and plastic. Unusual cracking, softening, swelling, or breaking of these materials may be a corrosion problem. If a corrosion problem is identified, it can be reported using SF 368 (Product Quality Deficiency Report). Use of key words such as “corrosion”, “rust”, “deterioration”, or “cracking” will ensure that the information is identified as a CPC problem. The form should be submitted to Commander, U.S. Army Communications-Electronics Command and Fort Monmouth, ATTN: AMSEL-LC-LEO-D-CS-CFO, Fort Monmouth, NJ 07703-5000.

1.11 SECURITY MEASURES FOR ELECTRONIC DATA

Security measures described in AR 380-19 shall be followed to control access to classified electronic data. Procedures described in the unit security Standard Operating Procedure (SOP) should be followed when electronic media are removed from the CAISI. See Appendix F for CAISI-specific security procedures.

Section II Equipment Description and Data

1.12 CAISI BACKGROUND/PURPOSE

1.12.1 CAISI Background

The background for the development of CAISI wireless system is the following:

1. One of the Lessons learned in Desert Shield/Storm was the inability of deployed Combat Service Support (CSS) computers to effectively exchange electronic data in a tactical environment.

2. CSS automation systems had no capability to access the Tactical Packet Network (TPN).

3. CSS units resorted to "Sneaker Net", a slow and resource intensive means of data transfer in which floppy disks were physically carried between computers.

4. An immediate corrective action was developed to ensure Legacy STAMIS connectivity to the Mobile Subscriber Equipment (MSE) TPN CSS Battle Field Mission Area. CAISI has three versions:

   a. CAISI Near Term Fix (NTF) - was developed, however its design was cumbersome.

   b. CAISI Mid-Term (MT) – was designed to correct the shortcomings of the CAISI NTF. After its development, several of its hardware and software components became obsolete requiring the development of the current system.

   c. CAISI wireless - The new configuration of CAISI incorporates commercial off-the-shelf (COTS) wireless technology and eliminates the need for much of the cabling and wiring required for connectivity to the CAISI MT.

The wireless CAISI is designed with three primary hardware modules and one kit:

1. CAISI Bridge Module (CBM).
2. CAISI Client Module (CCM).
3. Legacy Support Adapter (LSA).
4. System Support Representative (SSR) Accessory Kit.

In order to accommodate differing unit needs, a CAISI is comprised of various combinations of the above modules.

1.12.2 CAISI Purpose

The purpose of CAISI remains to provide a capability to battlefield Combat Service Support (CSS) automation devices to electronically exchange information via both tactical and commercial networks with other CSS automation devices. The CSS automation devices includes Standard Army Management Information Systems (STAMIS), as well as mail-enabled or web-enabled clients performing CSS functions or owned by CSS units.

The CAISI operates primarily in a tactical deployed environment, but may also be operated at the installation. Home station (installation) operation is authorized and encouraged for training purposes and to enhance the readiness posture of the unit in day-to-day operations.

CAISI provides Local Area Networks (LAN) for CSS computers.

1. When deployed, CAISI is part of a larger Army network that includes other voice and data communications - communications over radios as well as transmissions over data cables.

2. Other elements within the CAISI network include the Unclassified Packet Network (UCPN), which, interfaces with the Tactical Packet Network (TPN), a component of the Mobile Subscriber Equipment (MSE and Tri-services Tactical (TRI-TAC)) Communications Systems.

The CAISI provides a secure local network for CSS operations within logistics support areas. The STAMIS and CSS clients connect to the CAISI which in turn connects through the Signal backbone to the other deployed support areas and to the support base.

The standard CAISI node architecture is illustrated in Figure 1-1. Depending on the size and mission of the unit, some may receive more or fewer CBMs and CCMs. The number of components to be issued to a unit will be listed in the Tables of Organization and Equipment (TOE).

The CAISI is a fully meshed, but structured network. Clients connect to bridges. Bridges connect to multiple other bridges. And one bridge connects to the Signal unit for connection to other CAISI networks.

For long-haul communications, CAISI interfaces with the MSE. MSE will provide an isolated path through the TPN for the STAMIS and CSS clients to exchange information with other deployed STAMIS and CSS clients. Because these circuits are encrypted, transmission of sensitive but unclassified (SBU) data is authorized.

CAISI Node

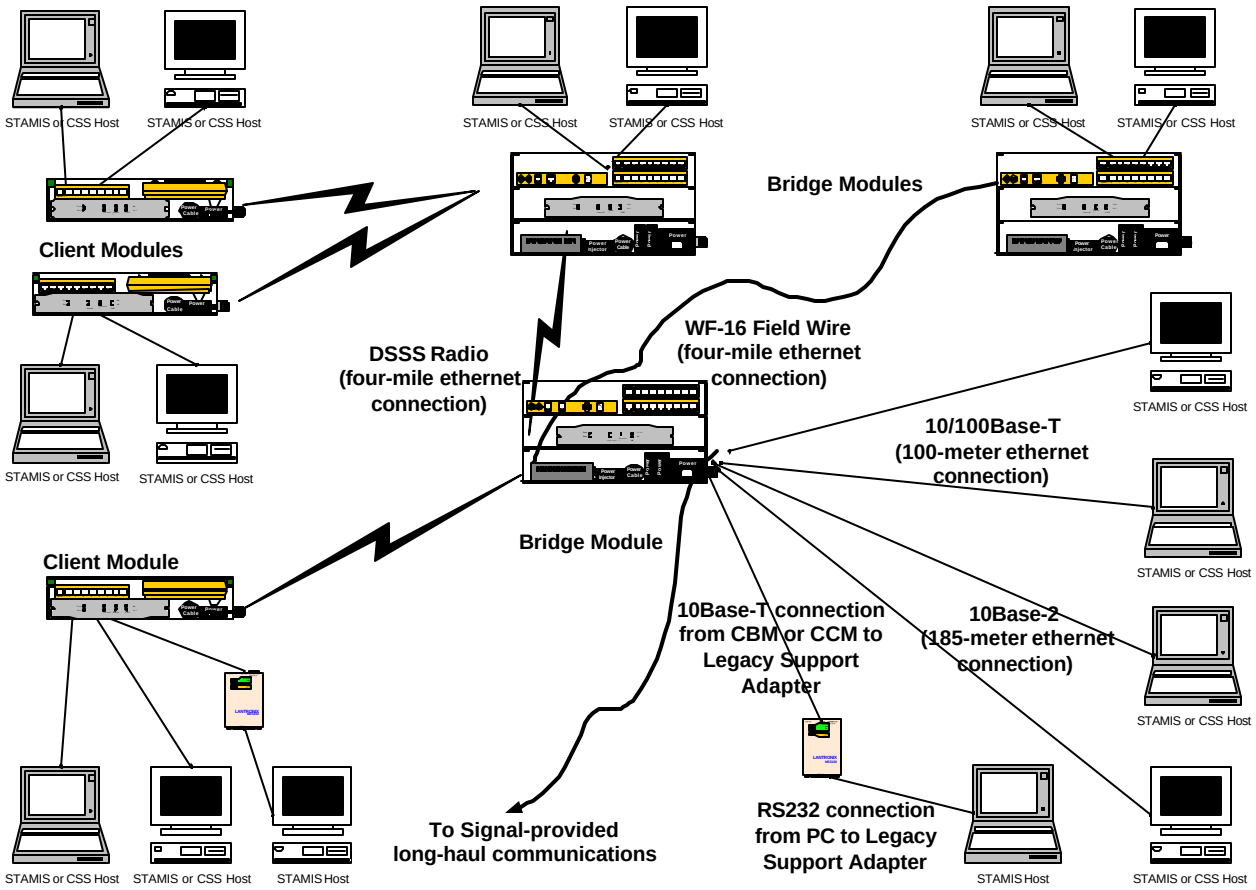


Figure 1-1 Standard CAISI Node Architecture

Additionally, the tactical network is usually connected through a "reach-back" node to support access to the installation network, the Non-classified Internet Protocol Router Network (NIPRNET) portion of the military network (MILNET), and the Internet. Although SBU STAMIS-to-STAMIS exchanges via installation networks and the NIPRNET are authorized, ***special caution must be taken to ensure that unencrypted SBU data is not passed over the Internet.***

The overall system architecture is shown on Figure 1-2.

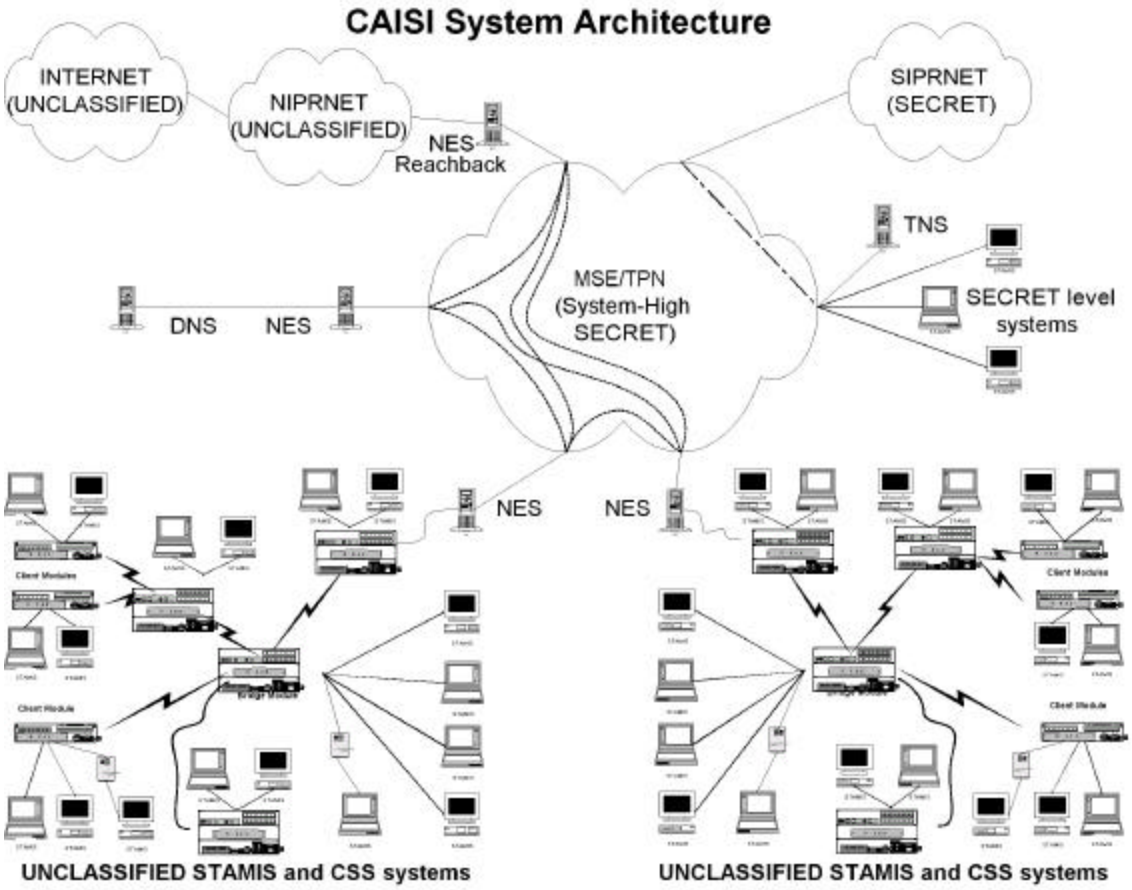


Figure 1-2 CAISI System Architecture

1.12.3 System Design Requirements

The CAISI system was developed to perform each of the following functions with 95 percent of the time with 100 percent accuracy:

1. Facilitate the exchange of data between CSS automation devices.

2. Provide a back up power source Uninterruptible Power Supply (UPS), which allows an automatic or manual shutdown process and an orderly restart with no loss of data if power is lost.

3. Allow for system set up/teardown to be accomplished within 30 minutes.

4. Provide on-line help functions, configuration management and diagnostic tools to the user as required by the system design to assist in troubleshooting the CAISI.

1.13 CAISI BRIDGE MODULE (CBM)

The CBM is the heart of the CAISI wireless. The CBM chassis contains:

1.	A wireless bridge (radio), power supply and power injector	Requires software configuration
2.	A synchronous Digital Subscriber Line (DSL) modem with power supply	Requires hardware configuration
3.	Inline encryptor	Requires software configuration
4.	Two 9-port 10Base-T hubs and power supplies.	Requires no configuration
5.	Lightning arrestor and grounding stud.	

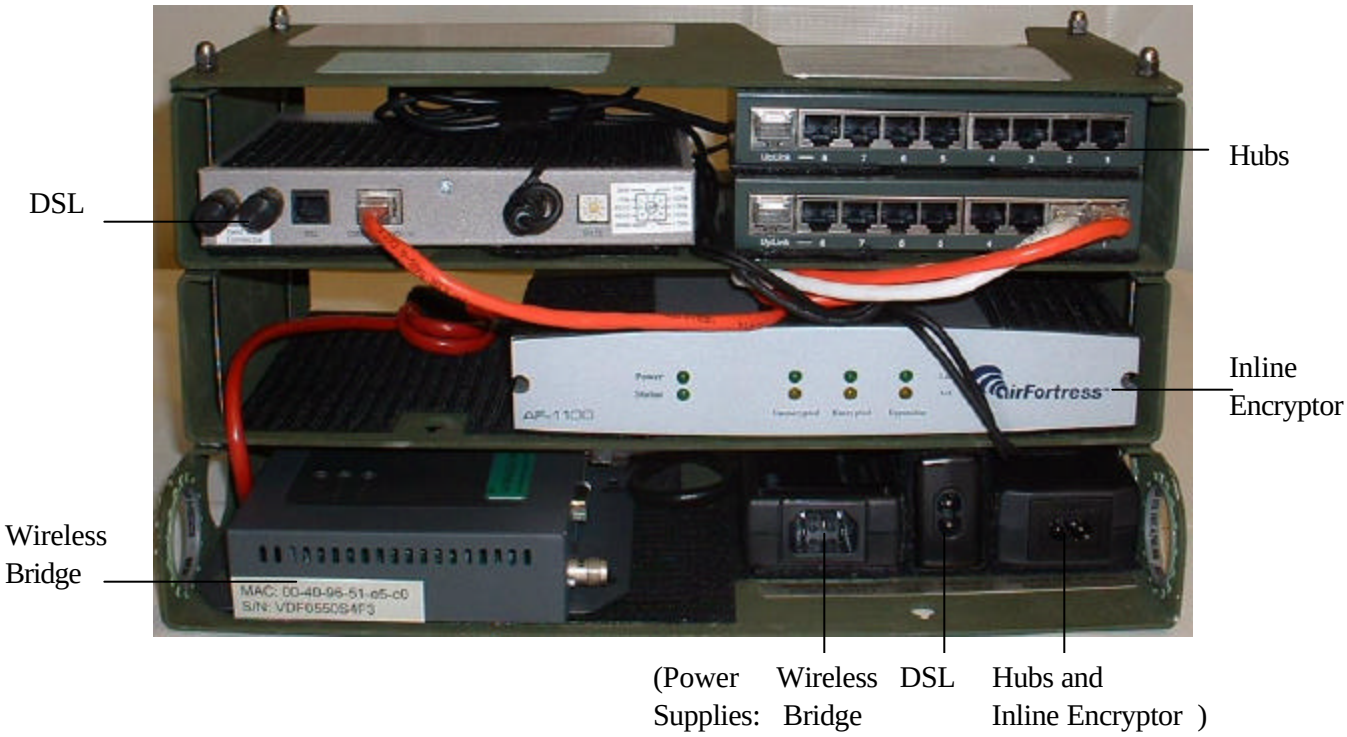


Figure 1-3 CAISI Bridge Module (CBM) Front View

All CBM components are mounted in a green aluminum chassis that is open in the front and back to provide access to equipment mounted inside and to allow for airflow. The components are mounted in the chassis with Velcro to make it easy for maintenance personnel to replace any that malfunction.

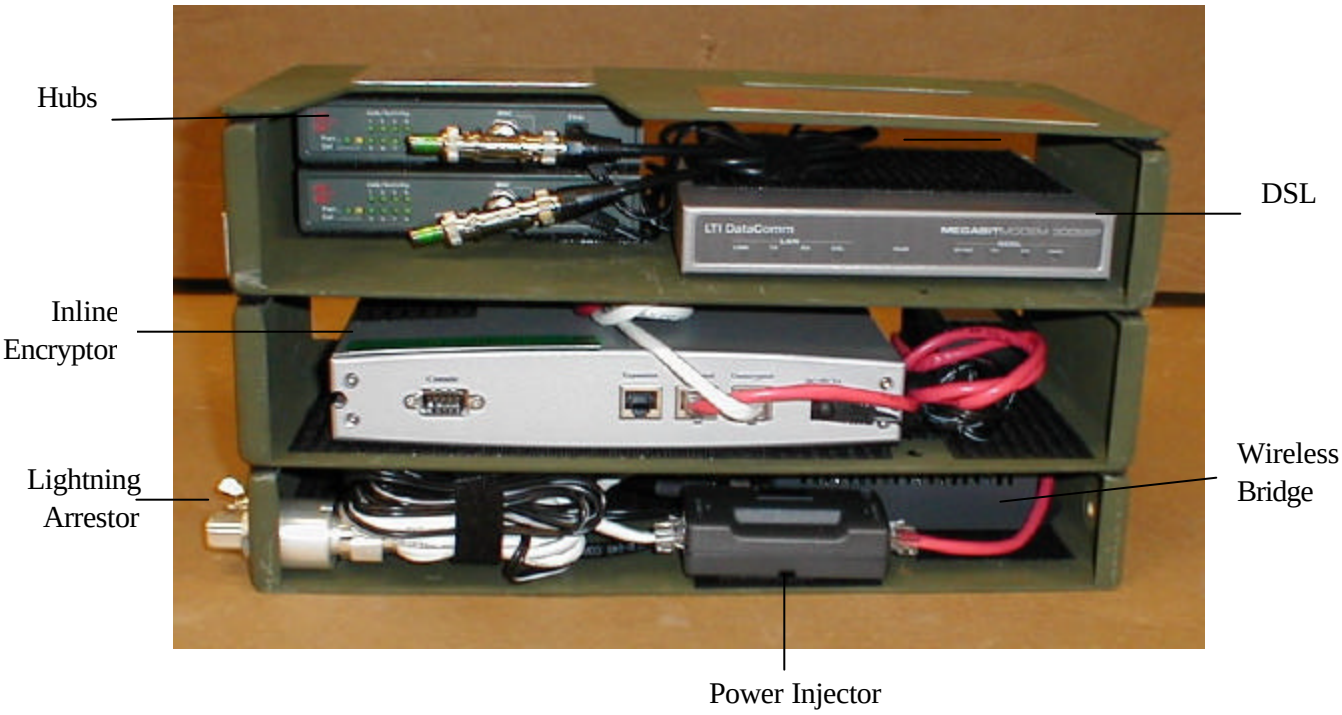


Figure 1-4 CBM Rear View

At least two CBMs are fielded with each CAISI. Each provides connectivity for STAMIS users and serves as "relays" for other CBMs in the network, passing data through the radios to the final (STAMIS) destination in the network.

One CBM will be designated the central, or "**root**" CBM:

1. This "root" node controls the LAN for that field site, sets parameters for and directs traffic amongst other radios in the network.

2. The root node serves as the central distribution point that extends the network within the logistics support area.

   a. Each CBM connects, directly or indirectly back to the root.

   b. The root node in turn connects to the MSE Small Extension Node (SEN) or Brigade Subscriber Node (BSN) provided by the Signal unit to interconnect the various field sites.

   c. This connection to the MSE allows the users that are connected throughout the CBM network, access to the TPN. This connection will be made to the In-Line Network Encryption (INE) device located with the MSE.

The radios use 128-bit encryption to provide secure data transmission. These encryption keys will be set as part of initial configuration. The wired equivalent privacy (WEP) built into the CAISI wireless equipment is not approved by the National Institute of Standards and Technology (NIST). It represents a very real risk of interception by hostile forces. Therefore, CAISI includes an inline encryptor to protect traffic within the CAISI network. They are certified by the NIST, in accordance with the Federal Information Processing Standards Publication (FIPS Pub) 140-1 and DoD policies.

Each CBM is packed in a ruggedized transit case that also contains antennas, antenna cables, brackets, grounding straps, an uninterruptible power supply (UPS), and support material.

1.14 CAISI CLIENT MODULE (CCM)

The CCM is the distant-end extension for the CBM. In other words, the CCMs extend the network out beyond the range of the CBMs. Each CCM supports a single work center – eight workstations located in a single vehicle, tent or collection of vehicles and tents under a common camouflage net.

CCM Chassis is made up of the following components:

1.	Multi-Client Radio Adapter	Requires software configuration
2.	Inline Encryptor	Requires software configuration
3.	One 9-port 10Base-T Hub	Requires no configuration
4.	Power supply with three leads to power the radio, encryptor and hub	
5.	Lightning arrestor and grounding stud	

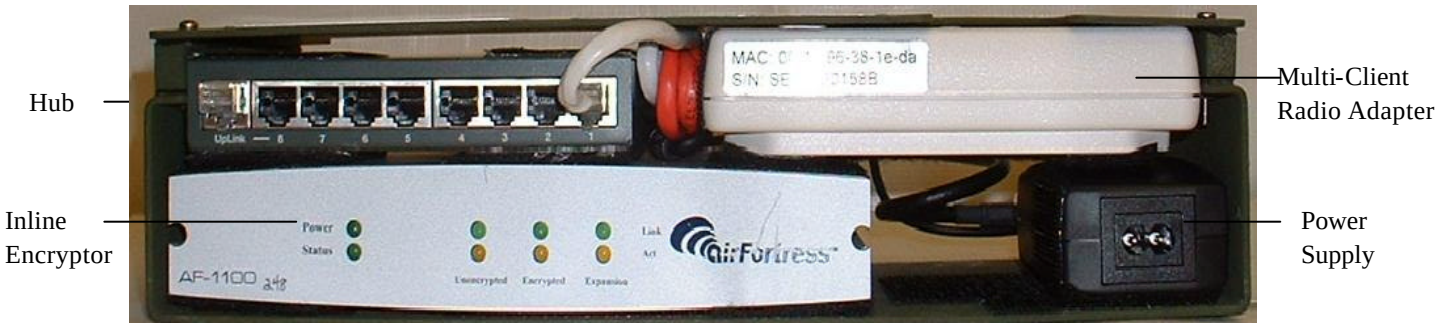


Figure 1-5 CAISI Client Module (CCM) Front View

Figure 1-6 CCM Rear View

CCMs only work when connected by radio to a CBM, usually the CBM closest physically to that CCM. The radios handle this connection automatically. The CCM hub will support up to eight users connecting to the network.

Number of CCMs issued with the CAISI is determined by the units needs. CCMs are stored in a soft-sided case, along with antennas, cables, and brackets.

CCM components are mounted in a green aluminum chassis that is open in front and back to provide access to equipment mounted inside and to allow for airflow. Refer to Figures 1-5 and 1-6.

1.15 LEGACY SUPPORT ADAPTER (LSA)

Many STAMIS computers are prevented, due to either hardware or software limitations, from making a connection from a Network Interface Card (NIC) to a 10Base-T or 10Base-2 hub such as the ones contained in the CBMs and CCMs. The CAISI LSA MSS-100 provides a virtual circuit from one host computer's serial port to another, over the 10Base-T network.

The LSA makes it easy to network-enable any device with a serial interface. It is connected to the STAMIS computer's serial port and then to one of the ports in the hubs on either the CBM or CCM.

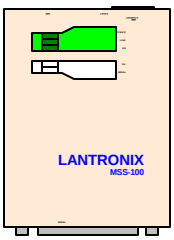


Figure 1-7 CAISI Legacy Support Adapter – Lantronix MSS-100

The LSA consists of the following components:

1. LSA MSS-100 Requires software configuration
2. Null Modem cable
3. White straight-through Ethernet cable
4. Power adapter and cable for LSA

1.16 SYSTEM SUPPORT REPRESENTATIVE (SSR) ACCESSORY KIT

Figure 1-8 System Support Representative (SSR) Accessory Kit

The SSR Accessory Kit contains equipment primarily required for module component configuration. This equipment is either duplicate items from the CBM/CCM or unique components for use in special circumstances. It will be issued to the CSSAMO, S-6, or those personnel performing SSR duties for the CAISI.

The SSR Accessory Kit is packaged in four containers: one transit case, one notebook case, one antenna carrying case and one AB-1244B antenna mast carrying case.

1. **Transit Case** – contains duplicate items of equipment in the CBMs/CCMs and stand-alone supplementary equipment (one of a kind).

2. **Notebook Case** – contains the notebook and assortment of NICs, adapters and cables.

3. **Antenna Carrying Case** – contains large panel antennas, brackets and cables.

4. **Antenna Mast Carrying Case** – contains the AB-1244B antenna mast section and the antenna mast kit.

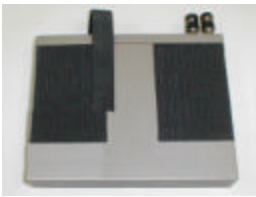
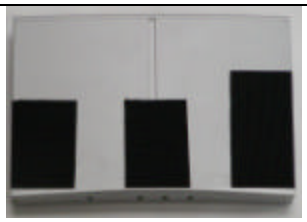
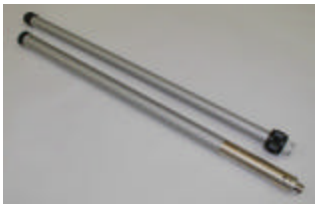
1. Wireless Bridge	 2. Digital Subscriber Line	3. Multi-client Radio Adapter
4. Two nine port Hubs	5. UPS	 6. Inline Encryptor (Qty 2)
 7. 40-in Break-apart Whip Antenna (Qty 2)		

Figure 1-9 Duplicate Items of Equipment in SSR Accessory Kit

Most components are duplicates of equipment in the CBMs and CCMs.

1. Wireless Bridge
2. Digital Subscriber Line (DSL)
3. Multi-client Radio Adapter
4. Two nine port hubs
5. UPS
6. Two Inline Encryptors
7. Two 40-in Break-apart Whip Antenna

The duplicate items can be used as stand-alone supplementary equipment or loaned to CBM or CCM operators to extend the capabilities of their equipment. Each piece of equipment will be discussed in more detail in Paragraphs 2.24 – 2.27.

A few of the items appear only in the SSR Accessory Kit. The one-of-a-kind (unique) items can be used as stand-alone supplementary equipment or loaned to CBM or CCM operators for use with their equipment. Each piece of equipment will be discussed in more detail in Paragraphs 2.24 – 2.27.

Amongst these supplementary items are:

1. A notebook for configuring and monitoring components and supplementary items.

2. A router, which acts as a firewall and divides the local area network into "public" and "private" segments.

3. The 10BaseT transceiver is provided in case you need to connect a 10Base-T device to the Network Encryption System (NES).

4. Various antenna components are also included in addition to the "14x14" directional panel. These are intended to supplement or temporarily replace CBM or CCM antenna systems or components when the standard antenna items issued with those modules will not suffice or awaiting replacement.

5. Various adapters for troubleshooting the CAISI network. (Not shown)

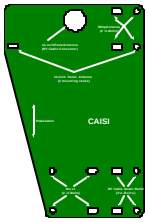
1. Notebook	2. Router	3. 10Base-T Transceiver
4a. 14x14 inch Panel Antenna	 4b. 14-inch Panel Antenna Bracket	4c. 50-ft. RF Antenna Cable

Figure 1-10 One-of-a-Kind (Unique) Items in SSR Accessory Kit

1.17 ANTENNAS

RF antennas are provided with each CBM and CCM. As we discussed, there are two basic types:

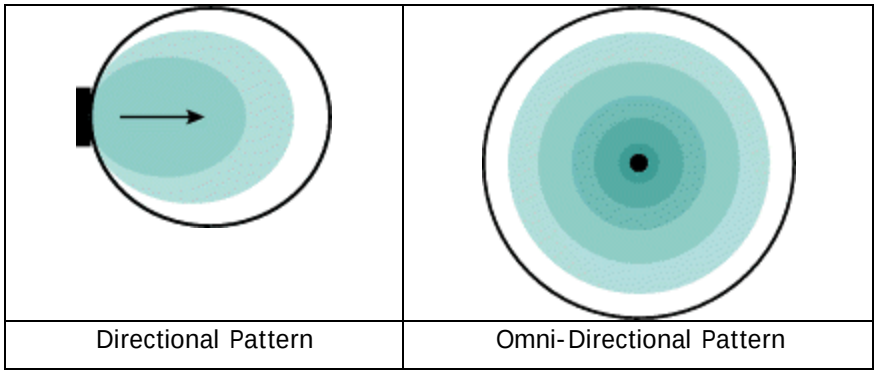


Figure 1-11 Directional/Omni-Directional Pattern

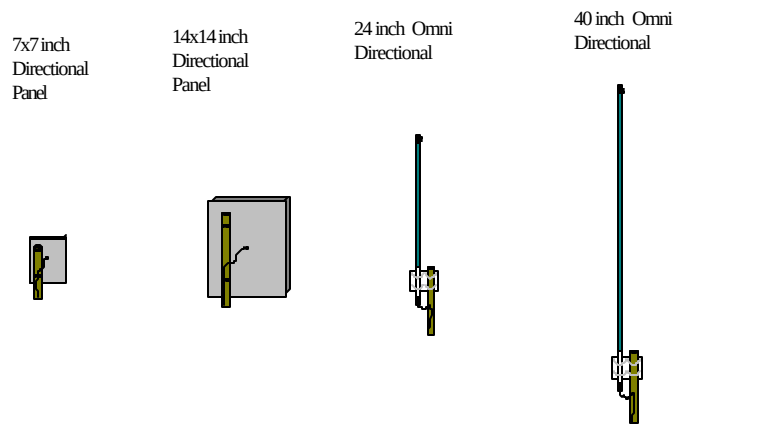
1. **Directional "Panel" antennas** - come in many different styles and shapes. An antenna does not offer any added power to the signal, but simply redirects the energy it received from the transmitter. By redirecting this energy, it has the effect of providing more energy in one direction, and less energy in all other directions. As the gain of a directional antenna increases, the angle of radiation usually decreases, providing a greater coverage distance, but with a reduced coverage angle.

2. **Omni-Directional Antennas** – designed to provide a 360 degree radiation pattern. This type of antenna is used when coverage in all directions from the antenna is required.

Table 1-2 Planning Ranges for Antennas

CCM, 24-inch whip, 35-foot cable, 13-foot mast (top of the camouflage net)	¼ mile
CBM, 40-inch whip, 25-foot cable, 13-foot mast (top of the camouflage net)	½ mile
CBM, 7-inch panel, 25-foot cable, 13-foot mast (top of the camouflage net)	½ mile
CBM, 40-inch whip, 35-foot cable, 19-foot mast (well above the camouflage)	1 mile
CBM, 7-inch panel, 35-foot cable, 19-foot mast (well above the camouflage)	1 mile
CBM, 40-inch whip, 50-foot cable, 30-foot mast (from the SSR kit)	2 miles
CBM, 7-inch panel, 50-foot cable, 30-foot mast (from the SSR kit)	2 miles
CBM, 14-inch panel, 50-foot cable, 30-foot mast (from the SSR kit)	4 miles

These RF antennas in conjunction with the wireless bridges enable wireless Local Area Network (LAN) data communication throughout the Logistics Support Area. Each antenna has different heights and decibel (dBi) ratings, which are shown in Figure 1-47.



ANTENNA	7x7 Directional Panel	14x14 Directional Panel	24 in Omni-Directional	40 in Break-apart Omni-Directional
GAIN	12 dBi	18 dBi	9 dBi	12 dBi
LENGTH w/MAST	30 feet, 3 in	30 feet, 7 in	32 feet, 2 in	33 feet, 4 in

Figure 1-12 Antenna Specifications

Table 1-3 Location of Antenna and Antenna Ancillary Components

Location	**Antenna/Ancillary Component**
CBM	40-inch Whip break-away antenna (omni-directional)
	7-inch Directional Panel antenna
	7-inch Antenna bracket
	25-ft RF antenna cable
	35-ft RF antenna cable
CCM	24-inch Whip antenna
	7-inch Antenna bracket
	35-ft RF antenna cable
SSR Transit Case	40-inch Whip break-away antenna (omni-directional) (Qty 2) 4-inch Whip antenna (Qty 2)
SSR Antenna Carrying Case	14-inch Directional Panel antenna (Qty 2)
	7-inch Antenna bracket (Qty 2)
	14-inch Antenna bracket (Qty 2)
	50-ft RF antenna cable (Qty 4)

1.18 CAISI EQUIPMENT DATA

1.18.1 Power Requirements and Physical Dimensions Data

1. **CAISI Bridge Module**

Table 1-4 CBM Equipment Characteristics

Equipment Type	Physical Dimensions				Electrical Requirements	
	Weight (Lbs)	Height (in)	Width (in)	Depth (in)	Volts	Current (Amps)
Transit Case (empty)	15	24	15	15		
Equipment Chassis	3	4	14	8.5		
Cisco Aironet BR352 wireless bridge	1.5	1.9	7.8	5.9	48 VDC	1.0 A
External Power Supply and Power Injector for wireless bridge	1	2	4	6	100-240 VAC 50/60 Hz	0.5 A
ADC PairGain Megabit Modem 300SBP DSL bridge	1.4	1.2	6.9	5.5	5 VDC	1.0 A
External power supply for DSL bridge	1	1	2	3	100-240 VAC 50/60 Hz	0.2 A
AirFortress 1100 Inline Encryptor	3	1.6	9	6	5 VDC	3.0 A
2 Microhubs (8 10Base-T ports, 1 10Base-2 port)	1	1	6.5	3	5 VDC	1.0 A
External power supply for hubs and encryptor (one supply for all)	1	1-1/4	2	4	100-240 VAC	1.0 A
UPS	10	2-5/8	11	4-1/2	120 VAC 50-60 Hz	up to 12 A
Antennas, Cables and Brackets	8					
CBM TOTALS:	46	24	15	15	120 VAC 50-60 Hz	up to 12 A

NOTE: *The transport case dimensions include the externally mounted tote handle and wheels.*

2. CAISI Client Module

Table 1-5 CCM Equipment Characteristics

Equipment Type	Physical Dimensions				Electrical Requirements	
	Weight (Lbs)	Height (in)	Width (in)	Depth (in)	Volts	Current (Amps)
Carrying Case (empty)	1	6	24	9		
Equipment Chassis	2	2	14	8.5		
Cisco Aironet WGB-352 Wireless Multi-client Adapter	1	1.9	4	5.5	12 VDC	0.6 A
AirFortress 1100 Inline Encryptor	3	1.6	9	6	5 VDC	3.0 A
MicroHub (8 10Base-T ports, 1 10Base-2 port)	1	1	6.5	3	5 VDC	1.0 A
External power supply for radio, encryptor and hub (one supply for all)	1	1-1/4	2	4	100-240 VAC	1.0 A
Antenna, Cable and Bracket	4					
CCM TOTALS:	13	26	5	8	120 VAC 50-60 Hz	Up to 12 A

NOTE: *The Carrying Case is fabricated of vinyl-covered canvas.*

3. Legacy Support Adapter

Table 1-6 LSA Equipment Characteristics

Equipment Type	Physical Dimensions				Electrical Requirements	
	Weight (Lbs)	Height (in)	Width (in)	Depth (in)	Volts	Current (Amps)
Lantronix MSS-100 (8 per CAISI)	< 1#	1”	2.5”	3.5”	5 VDC	1 A
External Power Supply for MSS-100	< 1#	2”	2”	5”	110-240 VAC 50-60 Hz	.15 A
LSA TOTALS:	2	3	4.5	4.0		

NOTE: *The LSA requires a third-party switched DC power supplies. It comes with 110 or 220-volt wall-transformer style power supply which must be replaced with a multi-voltage desktop style power supplies.*

***Dimensions shown above are for the replacement switched power supplies.*

4. **System Support Representative (SSR) Accessory Kit**.

Table 1-7 SSR Accessory Kit Equipment Characteristics

Equipment Type	Physical Dimensions				Electrical Requirements	
	Weight (Lbs)	Height (in)	Width (in)	Depth (in)	Volts	Current (Amps)
Transit Case (empty)	15	24	15	15		
BR-352 Wireless Bridge with external power supply	1.5	1.31	6.25	6.42	100-240 VAC to 48 VDC	.125
WGB-352 Wireless Multi-Client Radio Adapter	<1	1.45	6.30	4.72	5 VDC	1.5
MM-300SBP DSL Bridge with external power supply	1.4	1.25	6.75	5.5	100-240 VAC to 5 VDC	1.0 A
AirFortress 1100 Inline Encryptor (Qty 2)	3	1.6	9	6	5 VDC	3.0 A
Micro Hub (Qty 2)	1.25	1	5.5	3	5 VDC	.8
BEFSR81 Internal Router with external power supply	1.1	1.8	9.3	5.6	100-240 VAC to 5 VDC	6A
Power Supplies, 1 lead (Qty 5)	.25				100-240VAC to 5 VDC	3 amp 5V
Power Supplies, 3 lead (Qty 2)	.5				100-240VAC to 5 VDC	6 amp 5V
Ancillary Items	7					
Transit Case Totals	46	24	15	15		
Antenna Carrying Case (Including 2 large panel antennas and four 50-foot cables)	25	16	16	12		
Antenna Mast Carrying Case (including Antenna Mast Kit)	30	40	9	6		
SSR TOTALS:	120	27.4	32.8	29.7		

NOTE: *The Antenna Carrying Case is fabricated at Tobyhanna Army Depot. The Antenna Mast Carrying Case will be purchased with the mast kit or fabricated at Tobyhanna Army Depot if desired by the Assistant Project Manager.*

Table 1-8 SSR Notebook Case Characteristics

Equipment Type	Physical Dimensions				Electrical Requirements	
	Weight (Lbs)	Height (in)	Width (in)	Depth (in)	Volts	Current (Amps)
Transit Case (empty)	20	8	19	15		
MITAC 7020 or 7251 Notebook Computer with external power supply	8	1.6	12.2	10.4	100-240 VAC 50-60 Hz	0.5 A
Power Supplies, 1 lead	.25				100-240VAC to 5 VDC	3 amp 5V
Ancillary Items	15					
Notebook Case Totals	38					

1.18.2 Floor/Sub Floor Weight Capacity Requirements. CAISI components can and should be placed on any sturdy table, desk, or workbench. The compact size of the individual components minimizes weight capacity requirements.

Section III Principles of Operation

1.19 CAISI ARCHITECTURE

CAISI is comprised of various combinations of CBMs, CCMs, LSAs and SSR Accessory Kits.

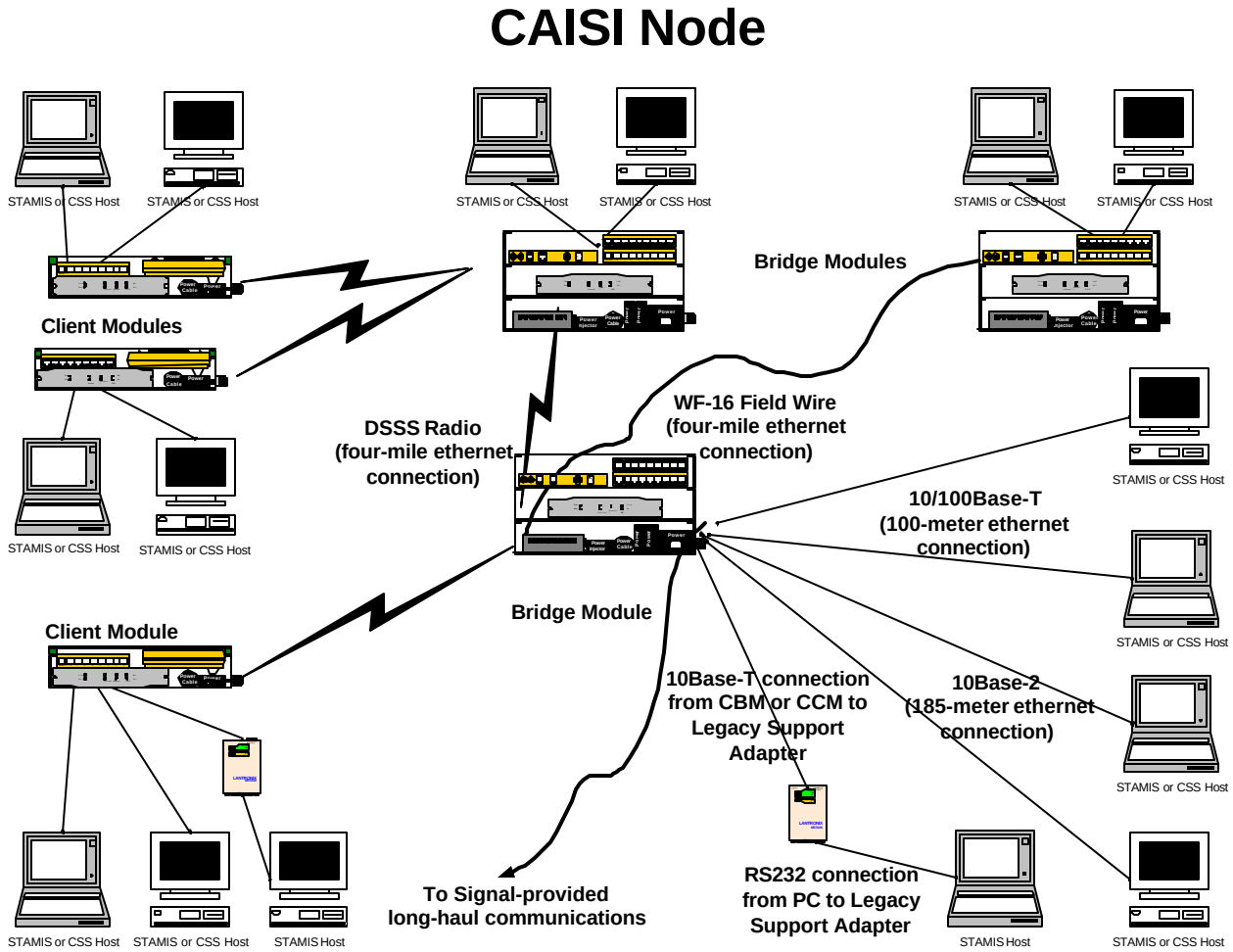


Figure 1-13 CAISI Architecture

Specific information on the connectivity of the wireless CAISI is in Paragraph 2.15.1.1.

How does everything fit together? It's kind of like that old song: "The head bone's connected to the neck bone"...

1. STAMIS applications that require CAISI VEE support are connected to LSAs.
2. LSAs are in turn connected to CCMs or CBMs.
3. CSS computers and STAMIS applications that do not require VEE support connect directly to CCMs or CBMs.

4. CCMs communicate to CBMs.

5. CBMs communicate to other CBMs.

6. The CBM root node is connected to the INE device, which in turn connects to the MSE.

7. MSE is connected to the installation network or the NIPRNET. The NIPRNET is connected to the Internet.

NOTE: *CAISI provides local communications.* ***Only****.*

The Signal unit provides all of the long-haul, inter-site communications.

The NES, TACLANE, and MSE belong to the Signal unit not the CAISI. Network services, such as DNS, are also provided by Signal.

Figure 1-14 shows the overall system architecture.

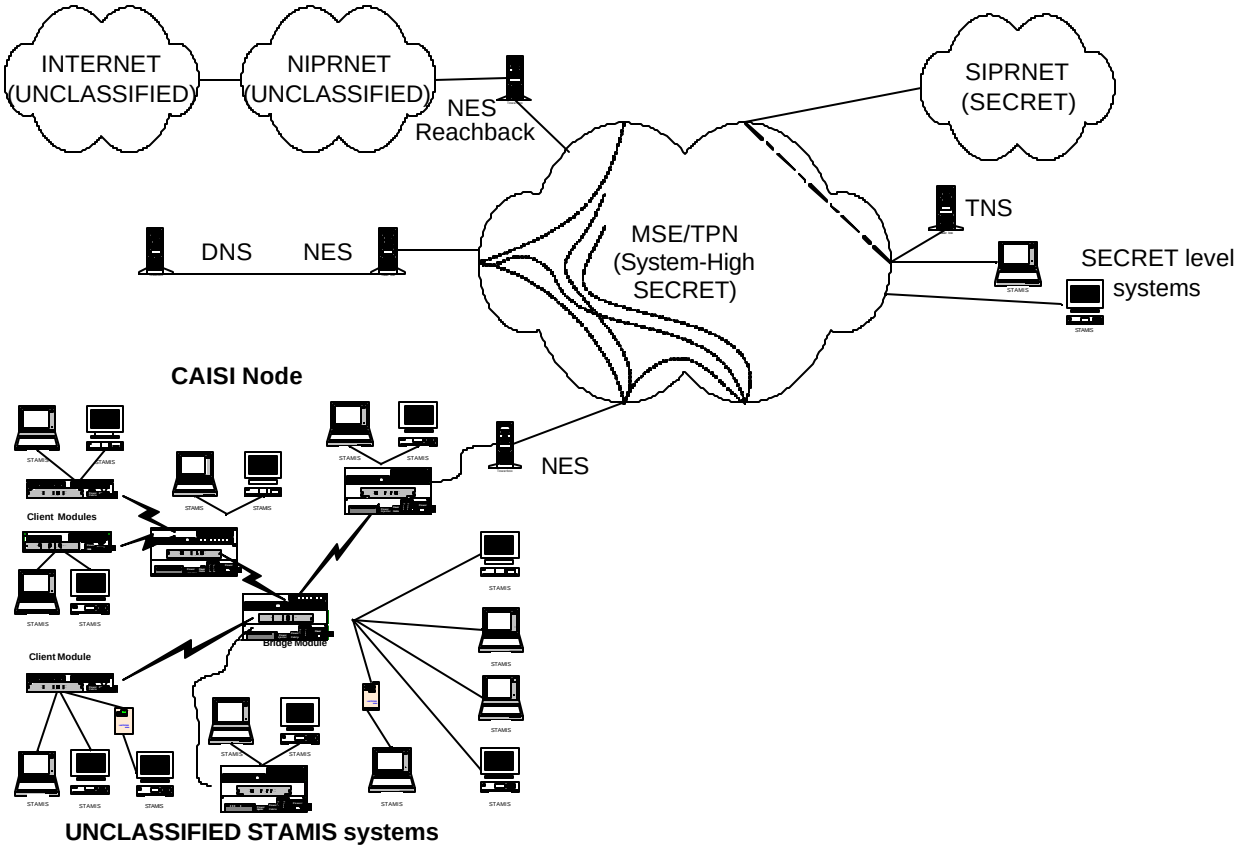


Figure 1-14 CAISI System Architecture

1.19.1 CBM Architecture

The CBM has five major components (DSL, two hubs, Inline Encryptor and Wireless Bridge) and they are all interconnected. The connections within the Bridge Module are shown on Figure 1-15.

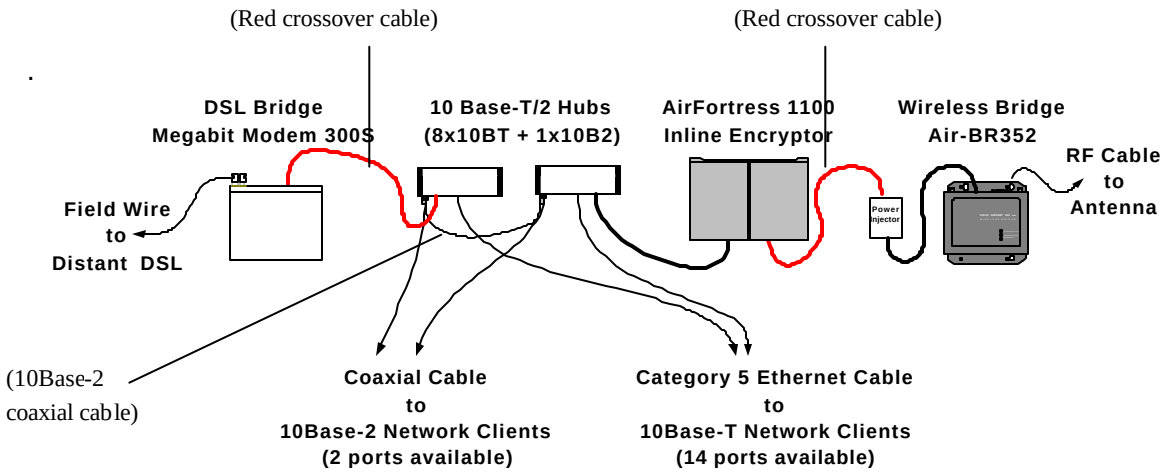


Figure 1-15 CBM Architecture

1. A red category-5 (CAT-5) Ethernet crossover cable runs from the DSL Bridge to one of 10Base-T ports on a hub.

2. The hubs are connected together with a short 10Base-2 coaxial cable with a "T" connector and 50-ohm terminator on each end to the BNC ports on the back of the hubs. (10Base-2 legacy computer cables can be connected in place of the terminators).

3. A white straight-through CAT-5 Ethernet cable runs from a 10Base-T port of a hub (same hub or different hub) to the "Internal/Unencrypted" port on the inline encryptor.

NOTE: *The standard for the CBM connections is to use the bottom hub – port 1 to the DSL (red crossover cable) and port 2 for the inline encryptor (white straight-through cable). These ports were designated so that the cables can be kept out of the way as much as possible. Any of the ports on either hub can be used.*

4. A red crossover CAT-5 cable runs from the "External/Encrypted" port of the inline encryptor to the "Network" port on the power injector of the wireless bridge.

5. A white straight-through Ethernet cable runs from the "AP/Bridge" port on the power injector to the "Inline Power Ethernet" port on the back of the bridge.

The remaining fourteen 10Base-T ports are available to the users.

When installed, the CBM looks like Figure 1-16.

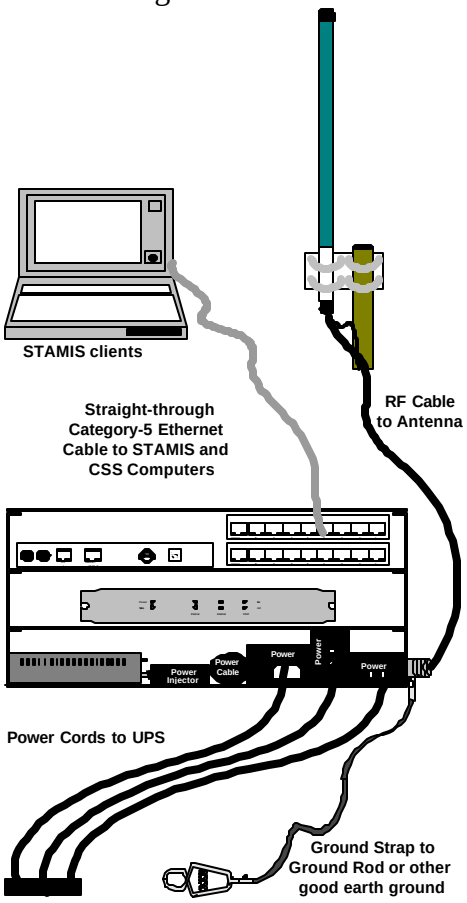


Figure 1-16 CBM Employment

1.19.2 CCM Architecture

The CCM has three major components and they are all interconnected. The connections within the Client Module are shown on Figure 1-17.

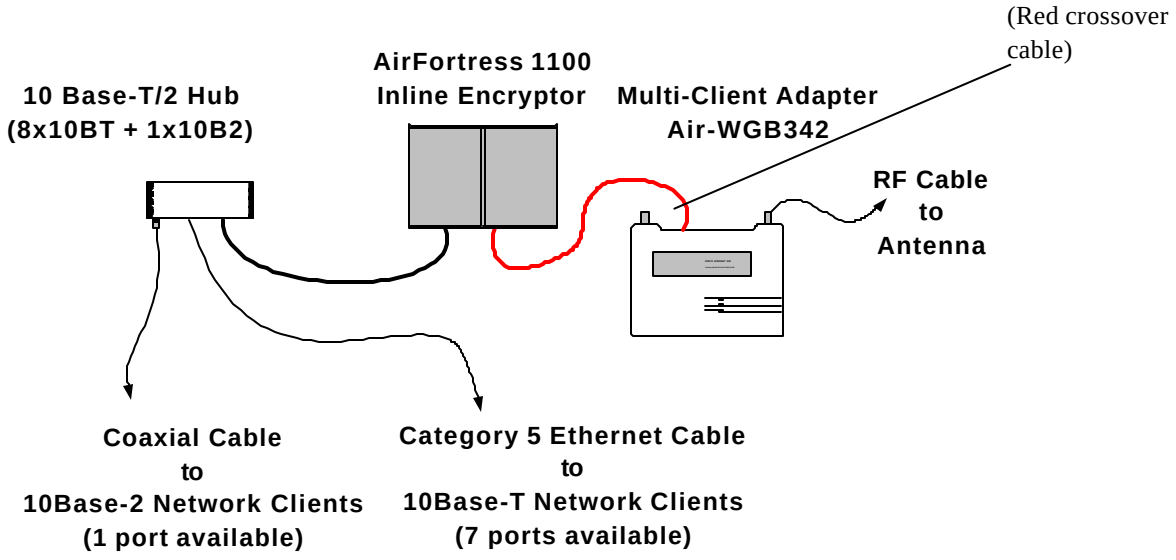


Figure 1-17 CCM Architecture

1. A white straight-through CAT-5 Ethernet cable runs from port 1 on the hub to the "Internal/Unencrypted" port on the inline encryptor. (Any port 1 – 7 could be used, the standard for CAISI is port 1).

2. A red crossover CAT-5 Ethernet cable runs from the "External/Encrypted" port of the inline encryptor to Ethernet port on the Multi-Client Radio Adapter.

A "T" connector and two coaxial terminators come installed on the BNC connector on the back of the hub.

The remaining seven 10Base-T ports are available to the users.

When installed, the CCM looks like Figure 1-18.

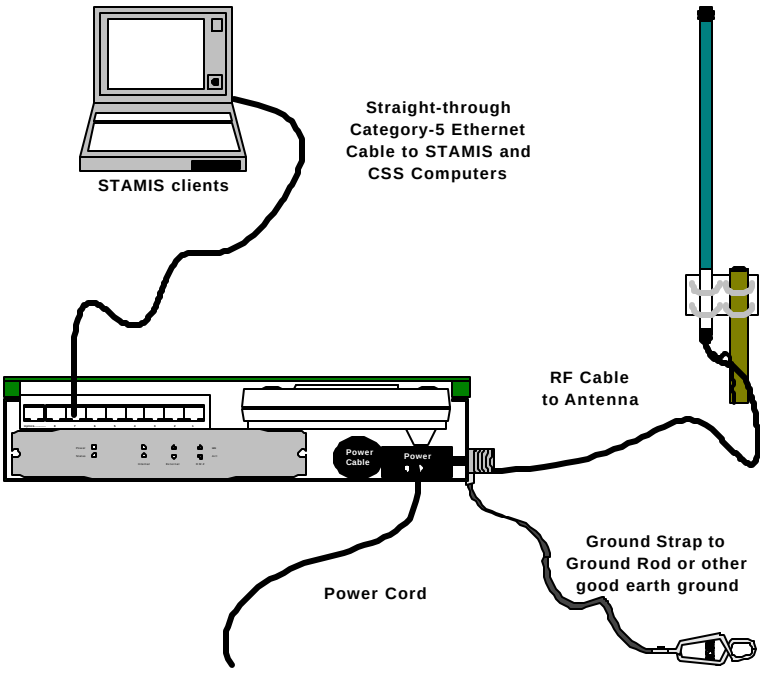


Figure 1-18 CCM Employment

1.19.3 LSA Architecture. The MSS-100 provides a multi-protocol support over a 10/100Base-T network. It is programmed using the CAISI Virtual End to End (VEE) software.

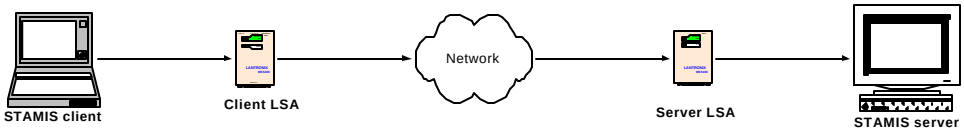


Figure 1-19 LSA Architecture

Figure 1-19 illustrates the LSA architecture. The serial port of a STAMIS client is connected to an LSA. The LSA connects to another LSA via the network. The second LSA is connected to the serial port of the STAMIS server. The STAMIS systems serial ports are interconnected as if by a single physical cable.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 2

OPERATING PROCEDURES

Section I Description and Use of Controls and Indicators

2.1 INTRODUCTION

This section illustrates and describes the operator controls, indicators, and connectors for the components of the CAISI.

2.2 CAISI BRIDGE MODULE (CBM)

It is essential to look at both the front and the rear of the CBM.

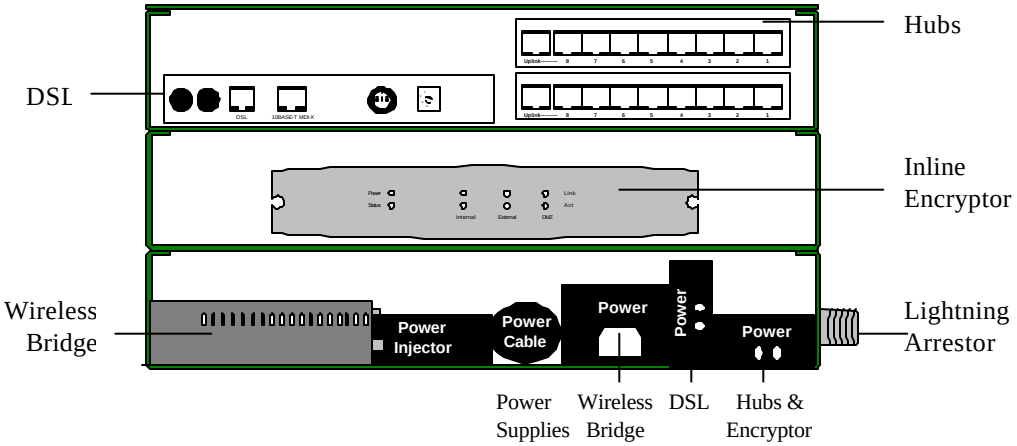


Figure 2-1 CBM Front View

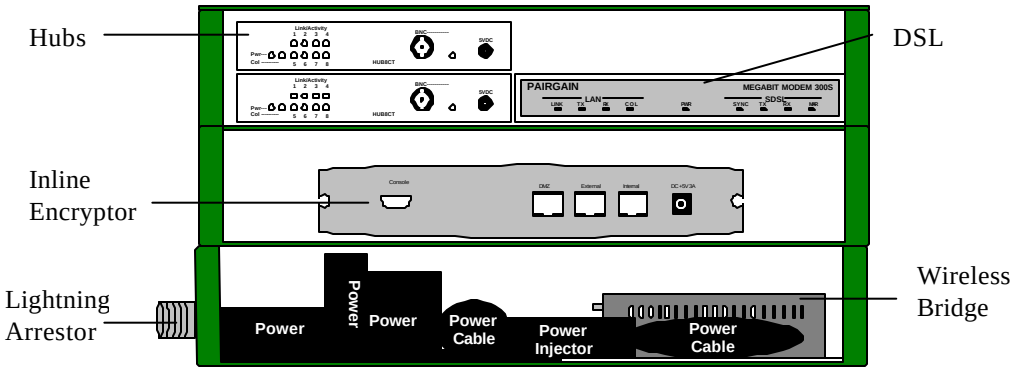


Figure 2-2 CBM Rear View

CBM Front and Rear view will be discussed by the individual components – Wireless Bridge, Paragraph 2.3, Inline Encryptor, Paragraph 2.4, DSL Bridge, Paragraph 2.5, and the hubs, Paragraph 2.6.

Table 2-1 CBM Components

COMPONENT	FUNCTION
Wireless Bridge	CISCO Aironet Wireless Bridge BR-352
DSL	ADC PairGain 300SBP synchronous DSL modem
Hubs	Addtron or Farallon 9-port hubs
Inline Encryptor	AirFortress 1100 Security Device – protects radio transmissions
Lightning Arrestor	The RF cable from the antenna connects here.
Grounding Strap Connection	(Not Shown). Connection (ground stud) for the grounding strap is located next to the antenna cable connection. Consists of the ground stud, wing nut and washer.
Hubs & Encryptor Power Connector	A two-prong power cord connects here for the encryptor and hubs.
DSL Power Connector	A two-prong power cord connects here for the DSL modem (if used).
Wireless Bridge Power Connector	A three-prong power cord for the wireless bridge connects here **NOTE***: Name of each power connector is permanently etched onto the chassis itself.*

2.3 WIRELESS BRIDGE

The Wireless Bridge in the CBM is a Cisco Aironet BR-352. The Wireless Bridge overview will be discussed in 2 sections – rear and top panels.

Figure 2-3 Wireless Bridge Rear Panel

Table 2-2 Wireless Bridge Rear Panel Controls and Indicators

KEY	CONTROL / INDICATOR	TYPE	FUNCTION
1.	LEFT		Left Antenna Connection. Not used with CAISI.
2.	SERIAL PORT	DB 9-pin	Used to connect wireless bridge to a notebook using a serial cable, (9-pin male to 9-pin female straight through cable (Blue cable)). This connection is required for initial configuration of the wireless bridge. After the configuration is completed, this cable may be removed until additional configuration is required.
3.	INLINE POWER ETHERNET	RJ-45 / CAT-5	Used to connect wireless bridge to the power injector using CAT-5 cable (twisted pair). (shown in more detail in Figure 2-4). **CAUTION:** The power injector is designed for Cisco Aironet 350 series Access Points **only**. Using the power injector with other Ethernet devices can damage the equipment.
4.	RIGHT/PRIMARY		Primary antenna connection. In CBM – it is connected to the built-in lightning arrestor with a 12-in RF antenna cable.

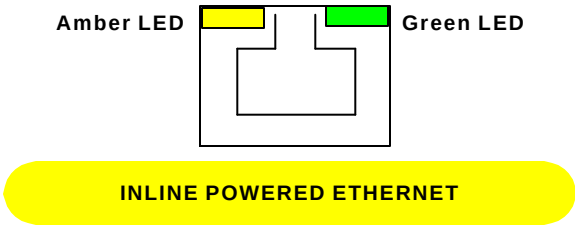


Figure 2-4 Wireless Bridge Rear Panel LEDs

Table 2-3 Wireless Bridge Rear Panel LEDs

KEY	CONTROL / INDICATOR	FUNCTION
1.	Amber LED	Blinks to indicate traffic
2.	Green LED	Should be solid green, to indicate the link to the encryptor.

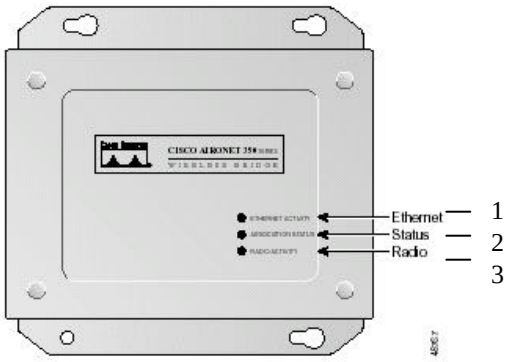


Figure 2-5 Wireless Bridge Top Panel LEDs

Table 2-4 Wireless Bridge Top Panel LEDs

KEY	CONTROL / INDICATOR	FUNCTION
1.	ETHERNET ACTIVITY	Ethernet Traffic - Used to indicate infrastructure traffic activity. The light is normally off, but will blink green whenever a packet is received or transmitted over the Ethernet interface.
2.	ASSOCIATION STATUS	Association Status - Used to show operational status. Shows solid green when the bridge has accepted a radio association. (Bridge is in contact with at least one other radio). Blinking green indicates that the bridge is operating normally but is not associated with any wireless devices.
3.	RADIO ACTIVITY	Radio Traffic - Used to indicate radio traffic activity. The light is normally off, but will blink green whenever a packet is received or transmitted over the radio.

When the wireless bridge is initially powered up, all three LEDs will flash amber, red and then green, in sequence. If a power-on test fails, the status indicator will go solid red and the unit will stop functioning. See Table 2-5 for a detailed explanation of the Top Panel LEDs.

Table 2-5 Wireless Bridge Top Panel LEDs Description

TYPE	INDICATOR DISPLAY			DESCRIPTION
	ETHERNET	STATUS	RADIO	
Association Status		Steady Green		At least one wireless client device is associated with the unit.
		Blinking Green		No client devices are associated; check the unit's SSID and WEP settings
Operational		Steady Green	Blinking Green	Transmitting/Receiving radio packets
	Blinking Green	Steady Green		Transmitting/Receiving Radio packets
		Steady Green	Blinking Amber	Maximum Retries or buffer full occurred on the radio The access point with which the bridge is communicating may be overloaded, or radio reception may be poor.
Error/Warning	Blinking Amber	Steady Green		Transmit/Receive errors
			Blinking Red	Ethernet cable is disconnected
		Blinking Amber		General Warning, check the logs
Failure	Steady Red	Steady Red	Steady Red	Firmware failure; disconnect power from the unit and reapply power
Firmware Upgrade		Steady Red		Unit is loading new firmware

2.3.1 Power Injector for the Wireless Bridge.

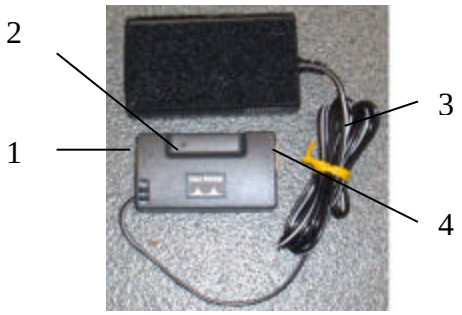


Figure 2-6 Power Injector Connections and LED

Table 2-6 Power Injector Connections and LED

KEY	CONTROL / INDICATOR	FUNCTION
1.	TO NETWORK	Network Port - The network connection passes through the injector and picks up 48-volts DC to power the bridge. Network port is used to connect the injector to the inline encryptor. A red crossover cable runs from the "External/Encrypted" port on the encryptor to the "Network" port on the injector.
NOTE: *When the wireless bridge needs to be reset or rebooted, disconnecting this cable and connecting it again will reset the bridge just like pulling the power cord to bridge.*		
2.	Power/Bridge Connection LED	LED serves two purposes: When lit amber, indicates power is being received to injector itself. When lit solid green, indicates the connection at the AP/Bridge port is good.
3.	Power	Power for the injector
4.	TO AP/BRIDGE	AP/Bridge Port - Connects the injector to the bridge. A white straight-through Ethernet cable runs from the AP/Bridge port to the "Inline Power Ethernet Port" on the back of the bridge. **CAUTION:** Be careful not to connect network components to the "AP/Bridge" port. The voltage present on this port can damage equipment other than the bridges.

2.4 INLINE ENCRYPTOR

The Inline Encryptor has several LEDs that can be used for troubleshooting.

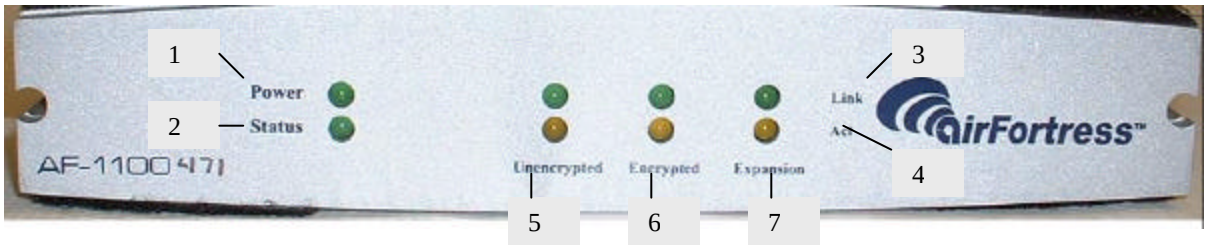


Figure 2-7 Inline Encryptor Front View

Table 2-7 Inline Encryptor Front Panel LEDs

KEY	CONTROL / INDICATOR	COLOR	FUNCTION
1.	Power	Green	When lit solid green indicates the encryptor is receiving power.
2.	Status	Amber	Blinks amber to indicate traffic on the LAN (Ethernet connection).
3.	Link	Green	When lit indicates that the ports are linked. It should remain solidly lit. (The top 3 LEDs).
4.	Act	Amber	Blinks to indicate traffic on the LAN (Ethernet connection). (The bottom 3 LEDs)
5.	Internal / Unencrypted (on future models – unencrypted)	Green / Amber	Top LED is the Link – should be lit solid green to indicate that the ports are linked. Bottom LED is the Act – should blink amber to indicate traffic on the ports.
6.	External / Encrypted (on future models – Encrypted)	Green / Amber	Top LED is the Link – should be lit solid green to indicate that the ports are linked. Bottom LED is the Act – should blink amber to indicate traffic on the ports.
7.	DMZ / Expansion	(on future models – Expansion)	DeMilitarized Zone. The DMZ LED should not be lit since the DMZ port is not used with CAISI.

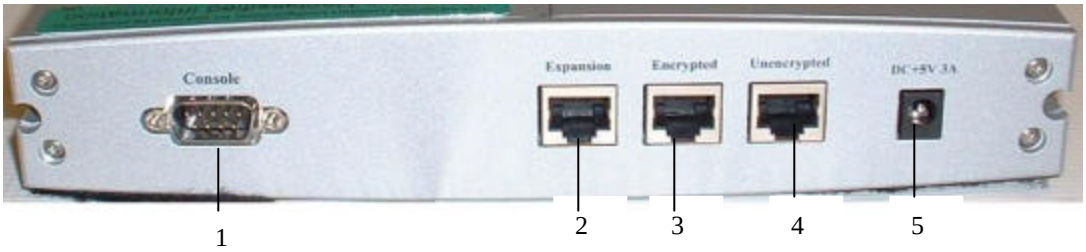


Figure 2-8 Inline Encryptor Rear View

Table 2-8 Inline Encryptor Rear Panel Controls and Indicators

KEY	CONTROL / INDICATOR	TYPE	FUNCTION
1.	Console	DB 9-pin	Serial Port - Used to connect inline encryptor to a notebook using a serial cable, (9-pin male to female straight through cable). This connection is required for initial configuration of the encryptor. After the configuration is completed, this cable may be removed until additional configuration is required.
2.	DMZ / Expansion port	RJ-45	CAISI does not use this port.
3.	External / Encrypted port	RJ-45	Used to connect Encryptor to the power injector of the wireless bridge. Use a red crossover cable to connect from the "External/Encrypted" port of the encryptor to the "Network" port on the power injector. **(Untrusted side)**
4.	Internal / Unencrypted port	RJ-45	Used to connect the Encryptor to a hub. Use a straight-through cable to connect from the "Internal/Unencrypted" port of the encryptor to any of the 10Base-T ports on the hub in the CBM. **(Trusted side)**
5.	DC+5V 3A	Plug	Power for the encryptor.

NOTE: *On future models of Inline Encryptor AF1100 – the DMZ will change to Expansion, External will change to Encrypted, and Internal will change to Unencrypted. Functionality will not change. Both are mentioned here since both versions are fielded.*

2.5 DSL BRIDGE

The DSL Bridge has several LEDs that can be used for troubleshooting, and are divided into the local area network - LAN (Ethernet) and the Single-pair Digital Subscriber Line - SDSL (network).

NOTE: *On future models of the DSL – the words PAIRGAIN will be replaced with LTI Datacomm. Functionality will not change. Both are mentioned here since both versions are fielded*

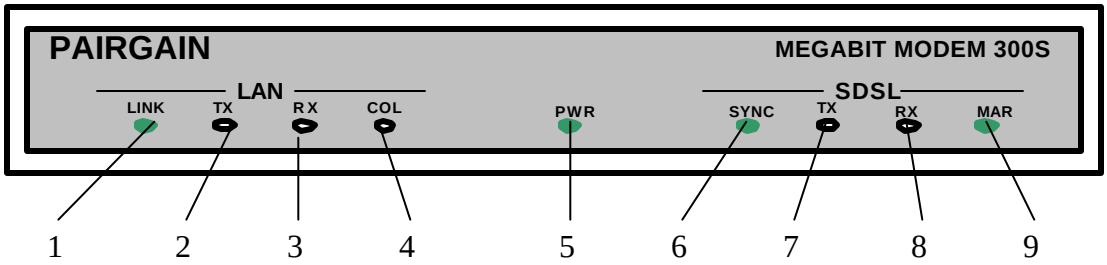


Figure 2-9 DSL Bridge Front View

Table 2-9 DSL Bridge Front Panel LEDs

KEY	CONTROL / INDICATOR	FUNCTION
LAN LEDs		
1.	LINK	When lit green indicates the link from the bridge to the hub is good. It should remain solidly lit.
2.	TX	Transmit. Blinks to indicate traffic on the LAN (Ethernet connection).
3.	RX	Receive. Blinks to indicate traffic on the LAN (Ethernet connection)
4.	COL	Collision. Will flicker to indicate data collisions on the network This is normal, but a solid lit LED indicates a problem.
5.	PWR	Power. When lit indicates the unit is receiving power.
SDSL LEDs		
6.	SYNC	Synchronized. Blinks green when the WF-16 (or other field wire) is first attached, solid lit when the connection is made to the destination bridge.
7.	TX	Transmit. Blinks green to indicate data traffic between the local and destination bridges.

Table 2-9 DSL Bridge Front Panel LEDs (Continued)

KEY	CONTROL / INDICATOR	FUNCTION
8.	RX	Receive. Blinks green to indicate data traffic between the local and destination bridges.
9.	MAR	Margin of Error. When lit green, indicates the local and destination modems have a strong enough signal to provide for a margin of error for reliable operations over time. On – margin is at or above the margin threshold. Off – margin is below the margin threshold.

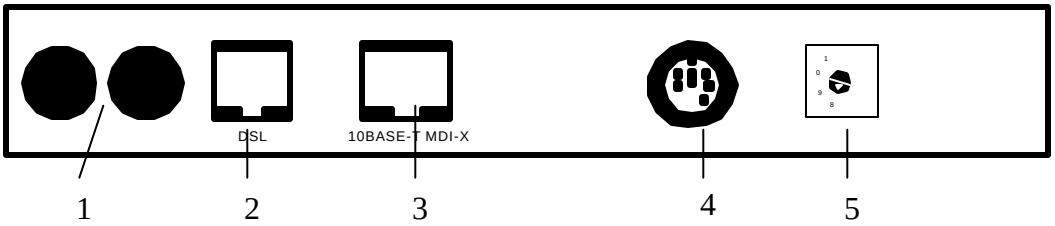


Figure 2-10 DSL Bridge Rear View

Table 2-10 DSL Bridge Rear Panel Controls and Indicators

KEY	CONTROL / INDICATOR	TYPE	FUNCTION
1.	Field Wire Connector	Spring	Binding Posts - Used to connect WF-16 field wire when using the DSL modem.
2.	DSL	RJ-11	DSL Port - Used to connect DSL modem to a 10Base-T port of a network hub or PC network card
3.	10Base-T MDI-X Port	RJ-45	Used to connect DSL modem to a SDSL interface
4.	POWER	Plug	Power for the DSL.
5.	RATE See Figure 2-11	Switch	Rate Configuration Switch - Controls the transmission data rate. Speed setting is normally set at 8; (2048k) The point end of the triangle points to the desired rate, not the screwdriver slit.

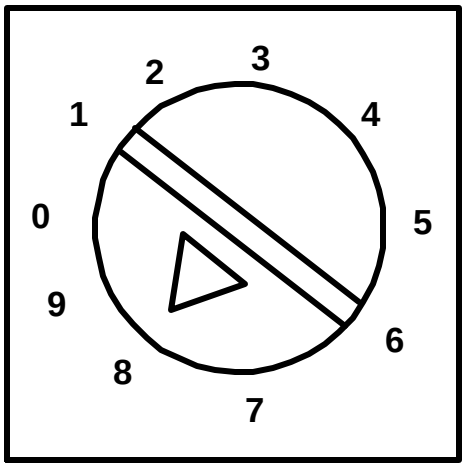


Figure 2-11 Rate Configuration Switch

* In near future we expect 9 to become 2300k and 0 to become "Rate adaptive". Setting 0 will be the standard, since it will allow the rate to automatically adjust itself to the fastest possible speed given the quality of the wire path.

NOTE: *Both ends of the connection must be on the same speed setting in order to connect*.

Table 2-11 Transmission Data Rate

1 = 128k	6 = 1536k
2 = 384k	7 = 1792k
3 = 768k	8 = 2048k **default**
4 = 1024k	9 = RSVD (reserved)
5 = 1280k	0 = RSVD (reserved)

2.6 HUBS

The hubs for the CBM and CCM are identical.

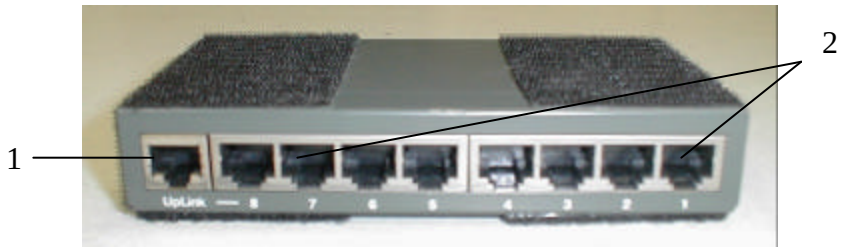


Figure 2-12 Hub Front View

Table 2-12 Hub Front Panel Controls and Indicators

KEY	CONTROL / INDICATOR	COLOR / TYPE	FUNCTION
1.	Uplink	RJ-45	Allow users to connect to a switch or a hub. Either the Uplink or port #8 can be used, but not at the same time.
2.	10Base-T ports	RJ-45	Used to connect STAMIS computers to connect to the CBM/CCM and therefore to the rest of the network. Ports 1 – 8.

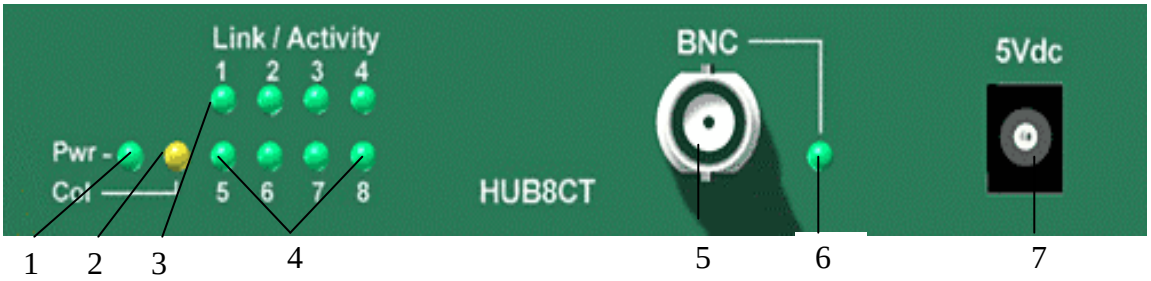


Figure 2-13 Hub Rear View

Table 2-13 Hub Rear Panel LEDs and Controls

KEY	CONTROL / INDICATOR	COLOR / TYPE	FUNCTION
1.	Pwr (Power)	Green	When lit, indicates the hub is getting power.
2.	Col (Collision)	Amber	Blinks occasionally to indicate collisions on the network. This is normal, but a solid lit Col LED indicates a problem.
3.	Link/Activity	Green	When lit, indicates the link from the hub to the bridge is good. Flickering lights indicate activity and a link on that port.
4.	Link/Activity 2 – 8	Green	When lit, each one indicates data traffic on that port.
5.	BNC	RG-58	BNC Connection - 10Base-2 connection; if not used, a T-connector and terminator is used. Method of daisy-chaining STAMIS devices together using the BNC connector. Up to 15 devices can be connected.
6.	BNC LED	Green	When a 10Base-2 connection is being used, to connect to a computer using RG-58 cable, this LED will be lit green.
7.	5Vdc	Plug	Power for the hub.

2.7 UNINTERRUPTIBLE POWER SUPPLY (UPS)

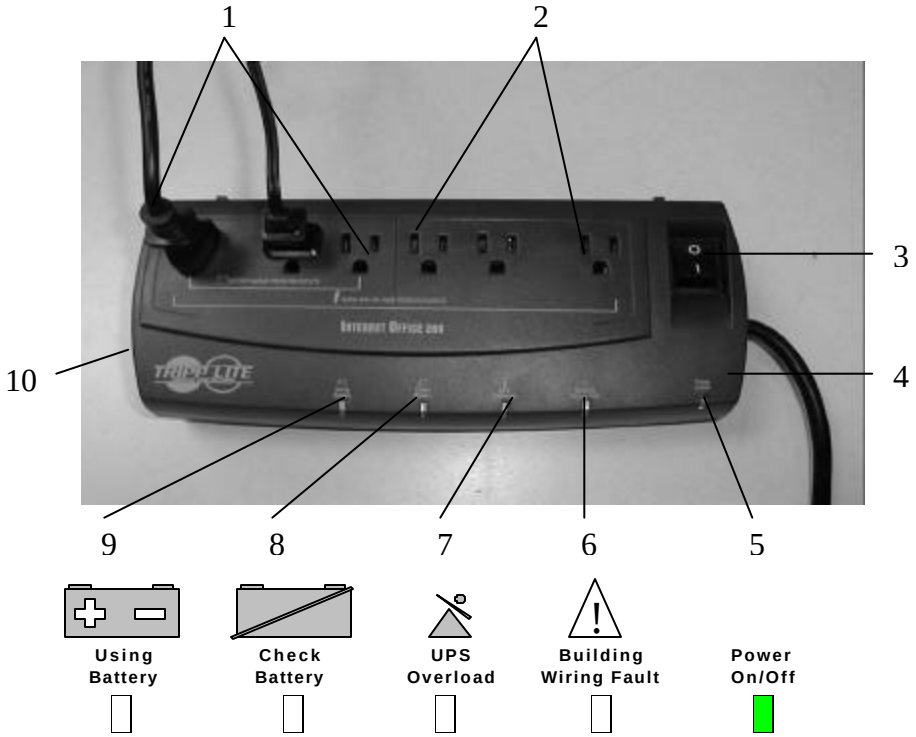


Figure 2-14 UPS LEDs

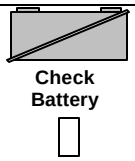
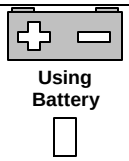
Table 2-14 UPS LEDs and Controls

KEY	CONTROL / INDICATOR	COLOR / TYPE	FUNCTION
1.	BATTERY BACKUP PROTECTED OUTLETS	Outlets	These 3 plug outlets provide both battery backup and surge protection. Plug the CAISI components into these outlets. If the power goes out, anything plugged into these three outlets will receive power so that a graceful shutdown can be completed or until power comes back on. **Backup time is 10 - 20 minutes.**
2.	SURGE AND LINE NOISE PROTECTED OUTLETS	Outlets	These 3 plug outlets only provide surge protection. Plug equipment that does not require battery backup during utility power failure into these outlets.

Table 2-14 UPS LEDs and Controls (Continued)

KEY	CONTROL / INDICATOR	COLOR / TYPE	FUNCTION
3.	Power On/Off Switch	Switch	The on/off switch is recessed to prevent accidental equipment turn-off while allowing convenient one-touch power control. "I" = ON and "O" = OFF. **NOTE:** *Even when switched OFF, the UPS maintains a battery charge whenever it is plugged in and utility voltage is present.* Alarm will sound if: the UPS detect either an undercharged battery or overloaded outlets when you turn the power switch ON. Follow instructions on Check Battery and UPS Overload LEDs
4.	Circuit Breaker	Breaker	Protects the equipment plugged into the 3 Surge Protected Outlets against short circuits and system overload. If the circuit breaker trips, unplug at least one piece of equipment from the Surge Protected Outlets and reset the breaker by pressing the button back into place.
5.	Power On/Off LED	Power On/Off	Is lit green when power is on. If on battery power, the LED will be orange.
6.	Building Wiring Fault	Building Wiring Fault	This LED instantly alerts you to faulty outlet wiring at your facility (either no ground circuit or a reversed polarity in the building wiring). This LED will detect most common wiring faults, but will not necessarily detect every possible type of fault. If it lights, consult a qualified electrician to examine your building wiring.
7.	UPS Overload LED	UPS Overload	When using battery power, this LED lights up when the 3 Battery Backup Protected/Surge Protected Outlets are overloaded (connected to equipment that exceeds 280VA/150 Watts). Alarm will Remain on until the overload is removed. Disconnect the equipment that does not require battery backup to eliminate the overload.

Table 2-14 UPS LEDs and Controls (Continued)

KEY	CONTROL / INDICATOR	COLOR / TYPE	FUNCTION
8.	Check Battery LED		This LED lights when the UPS detects a weak battery. If this indicator lights, follow this procedure: allow UPS to charge for 4 to 6 hours (leave it switched ON or OFF and plugged in). Test the battery by switching the UPS OFF and back ON again. If the Check Battery LED lights again, the battery **must** be replaced. Alarm will sound if the Check Battery indicator is lit. The alarm will sound for 10 seconds.
9.	Using Battery LED		This LED will light when the UPS is providing your equipment with battery power during a blackout or brownout, or during self-test when switch is turned ON. When this indicator lights, close any files you are working on, and shut down your computer. Then turn the UPS OFF to conserve the battery charge. When light is off, the UPS is constantly recharging the battery for later use. Alarm will sound if the utility power fails. Alarm will sound once every second. You should close your files and turn off your system immediately.
10.	RJ11/45 Telephone / Dataline Surge Suppressor Jack	RJ11 – RJ45 jack	Provide protection against surges on the telephone and data lines. CAISI does not use this option.

2.8 CAISI CLIENT MODULE (CCM)

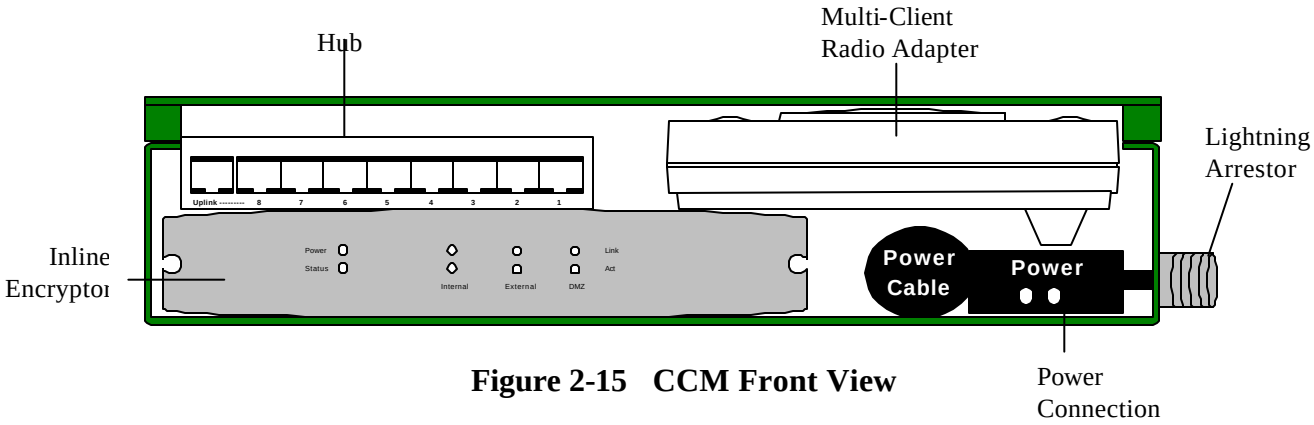


Figure 2-15 CCM Front View

Table 2-15 CCM Components

COMPONENT	FUNCTION
Hub	Addtron or Farallon 9-port hub
Multi-Client Radio Adapter	Cisco Workgroup Bridge (WGB-342/WGB-352)
Inline Encryptor	AirFortress 1100 – security device – protects radio transmissions
Lightning Arrestor	Antenna Cable Connection. The RF cable from the antenna connects here.
Grounding Strap Connection	(Not Shown). Connection (ground stud) for the grounding strap is located next to the lightning arrestor. Consists of the ground stud, wing nut and washer.
Power Connection	Power cord is for the hub, inline encryptor and the multi-client radio adapter.

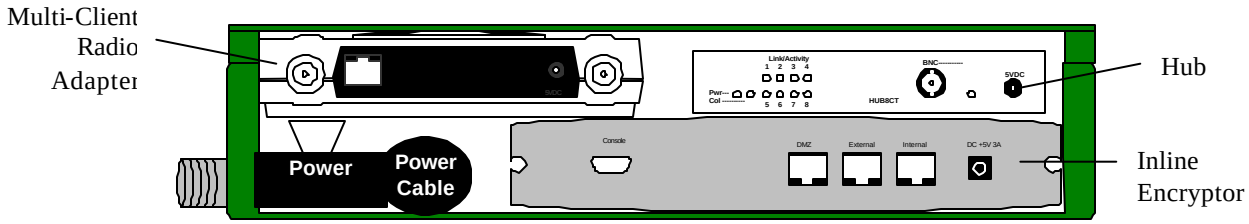


Figure 2-16 CCM Rear View

CCM rear view has already been discussed for the CBM, except for the Multi-Client Radio Adapter, Paragraph 2.9. The other components are discussed in the following Paragraphs: Paragraph 2.4 for the Inline Encryptor and Paragraph 2.6 for the Hub.

2.9 MULTI-CLIENT RADIO ADAPTER

The Multi-client Radio Adapter (WGB-342/WGB-352) have the same features. The only difference is the WGB-342 is 30mW and is white in color, whereas the WGB-352 is 100mW and gray in color.

The Multi-Client Radio Adapter overview will be discussed in 2 sections – rear and top panels.

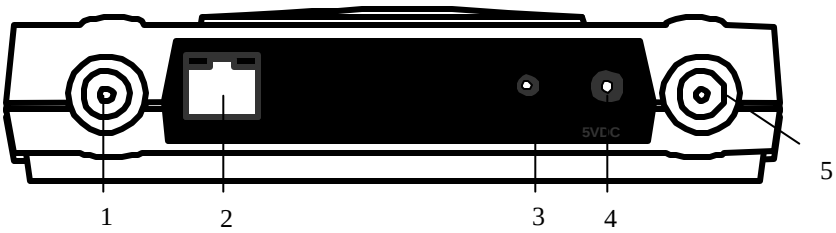


Figure 2-17 Multi-Client Radio Adapter Rear Panel

Table 2-16 Multi-Client Radio Adapter Rear Panel Controls and Indicators

KEY	CONTROL / INDICATOR	TYPE	FUNCTION
1.	LEFT		Left Antenna Connection - Not used with CAISI. Secondary antenna.
2.	ETHERNET	RJ-45 / CAT-5	10Base-T Connection - Used to connect wireless bridge to a hub or concentrator using CAT-5 cable (twisted pair).
3.	Configuration Reset Button	Small Hole	This is the reset button. Use the end of a paper clip to push this button. By pressing the reset button, the Radio Adapter configuration parameters are set back to the "factory default".

Reset Procedure -

a. With the radio powered, insert a paperclip into the tiny unlabeled hole next to the power connector (labeled "5VDC").

b. You will feel and hear a small click Press and hold the button for about ten seconds.

c. All the lights on the adapter will go out.

d. After a few seconds, the Association light (center one) will flash red, then immediately go out.

e. Continue to hold the reset button until you see the Ethernet light (the one closest to the connectors side of the radio) flicker briefly.

Table 2-16 Multi-Client Radio Adapter Rear Panel Controls and Indicators (Continued)

KEY	CONTROL / INDICATOR	TYPE	FUNCTION
4.	5VDC	Plug	Power connector for radio adapter, labeled "5VDC".
	WARNING: DO NOT use the power injector for the wireless bridge with the radio adapter. This is a 48-voltage power enhancement. The radio adapter can be damaged, if you do so.		
5.	RIGHT/PRIMARY		Primary antenna connection. In CCM – it is connected to the built-in lightning arrestor with a 12-in RF antenna cable.

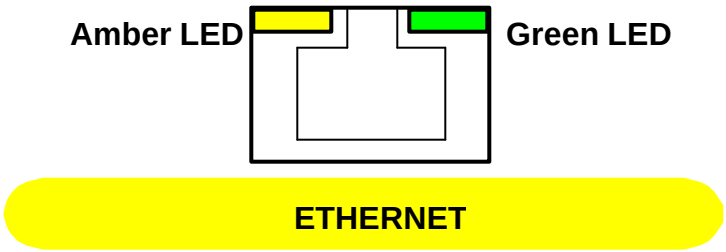


Figure 2-18 Multi-Client Radio Adapter Rear Panel LEDs

Table 2-17 Multi-Client Radio Adapter Rear Panel LEDs

KEY	CONTROL / INDICATOR	FUNCTION
1.	Amber LED	Blinks to indicate traffic
2.	Green LED	Should be solid green, to indicate the link to the encryptor.

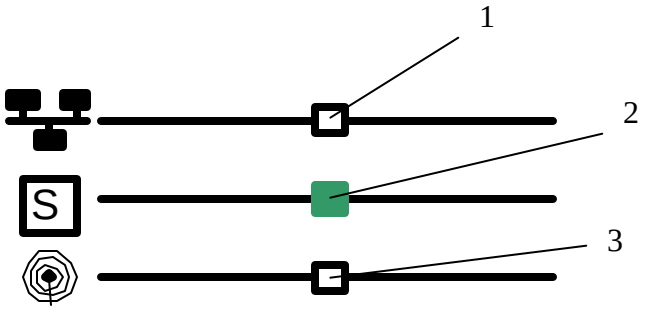


Figure 2-19 Multi-Client Radio Adapter Top Panel LEDs

The Multi-Client Radio Adapter Top Panel LEDs are the same as those for the Wireless Bridge. Refer to Table 2-4 and Table 2-5 for a detailed description of the Top Panel LEDs.

2.10 LEGACY SUPPORT ADAPTER (LSA)

Figure 2-20 LSA (MSS-100)

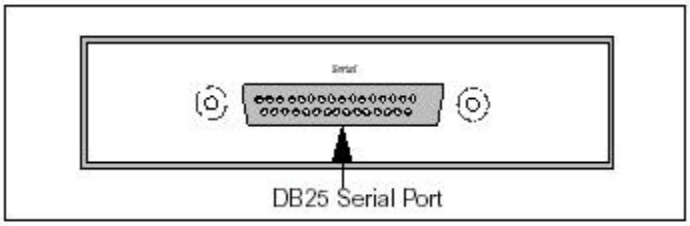


Figure 2-21 LSA (MSS-100) Front Panel

The MSS-100 has a male DB25 Serial Port connector on the front panel. Connect one end of null modem serial cable to this port and the other end to the serial port of the STAMIS computer or the SSR notebook for configuration purposes.

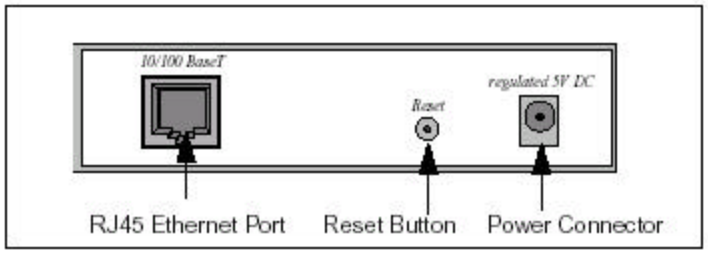


Figure 2-22 LSA (MSS-100) Rear Panel

Table 2-18 LSA (MSS-100) Controls and Indicators

KEY	CONTROL / INDICATOR	TYPE	FUNCTION
1.	10/100	RJ-45	RJ45 Ethernet Port - Connects to one of the 10Base-T ports on the CBM or the CCM using CAT-5 Ethernet cable.
2.	Reset	Small Hole	This is the reset button. Use the end of a paper clip to push this button. By pressing the reset button, the LSA will lose its configuration settings and will need to be reconfigured by the SSR. Reset procedure is explained below:
3.	5vdc	Plug	Power connector for the LSA.

Reset Procedure:

a. Removing power to the LSA.

b. Push the reset button and hold.

c. Apply power to the LSA **while still** holding in the reset button.

d. Hold this button in for 5-10 seconds until serial lights stop blinking.

All of the configuration parameters are set back to the “factory default”.

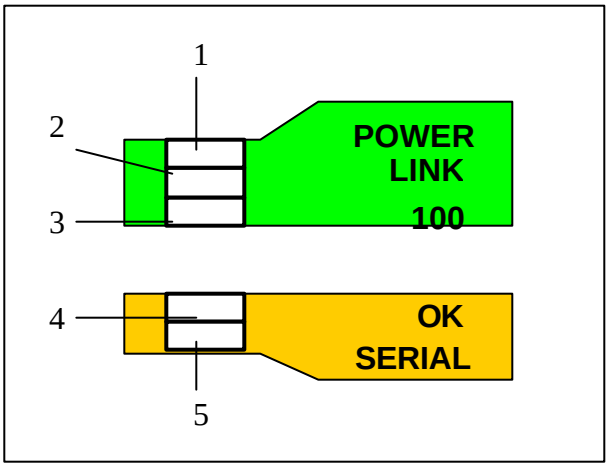


Figure 2-23 LSA LEDs

Table 2-19 LSA (MSS-100) LEDs

KEY	CONTROL / INDICATOR	COLOR	FUNCTION
1.	POWER	Green	When lit, indicates power is connected and being received.
2.	LINK	Green	When lit, indicates the CAT-5 Ethernet connector is properly linked to the hub in the CBM or CCM.
3.	100	Green	When lit, indicates the Ethernet connection is at 100MB (100Base-T). If not lit, the connection is at 10MB (10Base-T).
4.	OK	Yellow, green, red	The OK LED indicates that the device booted successfully and is operating normally (green). After booting, the OK LED will blink every two seconds.
5.	SERIAL	Yellow, green, red	When lit, indicates data is flowing through the serial connection. Blinks during the transmission. (Green normally).

NOTE: *Although a red LED during boot mode usually signals an error, red LED patterns are part of the normal operation of the MSS-100 and are not necessarily indicative of errors or dangerous operation.*

2.11 LINKSYS ROUTER

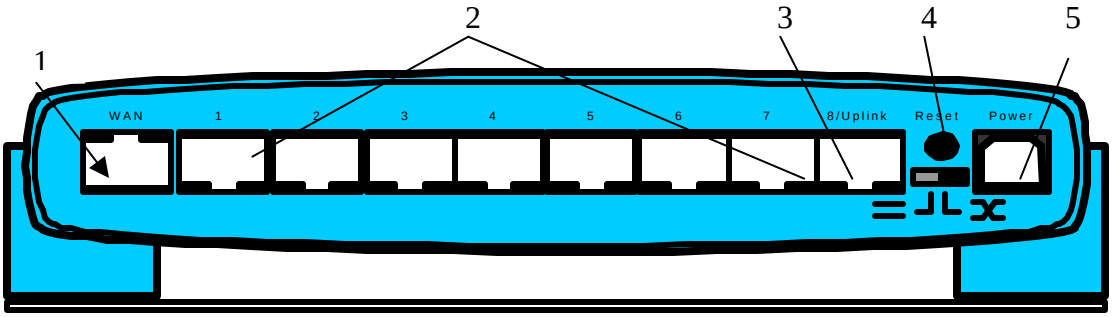


Figure 2-24 Linksys Router Rear View

Table 2-20 Linksys Router Controls and Indicators

KEY	CONTROL / INDICATOR	TYPE	FUNCTION
1.	WAN	RJ-45	The WAN (Wide Area Network) port is where you will connect your Ethernet Cable or DSL modem. **Notice** that the WAN port is upside down as compared to the LAN ports 1-7. (This is to prevent you from accidentally connecting the wrong one)
2.	Ports 1-7	RJ-45	7 ports to connect network devices to. Network devices could include STAMIS computers, CBM, CCM.
3.	8/Uplink	RJ-45	Allows you to manually select port eight as an uplink port so that you can expand your network by connecting to another switch or hub.
Version 1 router: Port 8/Uplink can be used in the straight through mode (=) or in the crossover mode (X) for an uplink to a hub or switch. A switch controls the port. Slide the switch to the left to the "=" position, if you are connecting to a computer. Slide the switch to the "X" position if you are connecting a hub, switch or another router and would otherwise need a crossover cable. Version 2 router – there is no switch, all ports are in auto-configuration mode.			
4.	Reset		Reset button is used to refresh the router's connections, potentially clearing any jammed links. By pressing the reset button, you will clear all of the router's data.

Table 2-20 Linksys Router Controls and Indicators (Continued)

	This should only be done if you are experiencing heavy router problems and have exhausted all of the other troubleshooting options.		
5.	Power	Plug	Connection of AC Power adapter for the router.

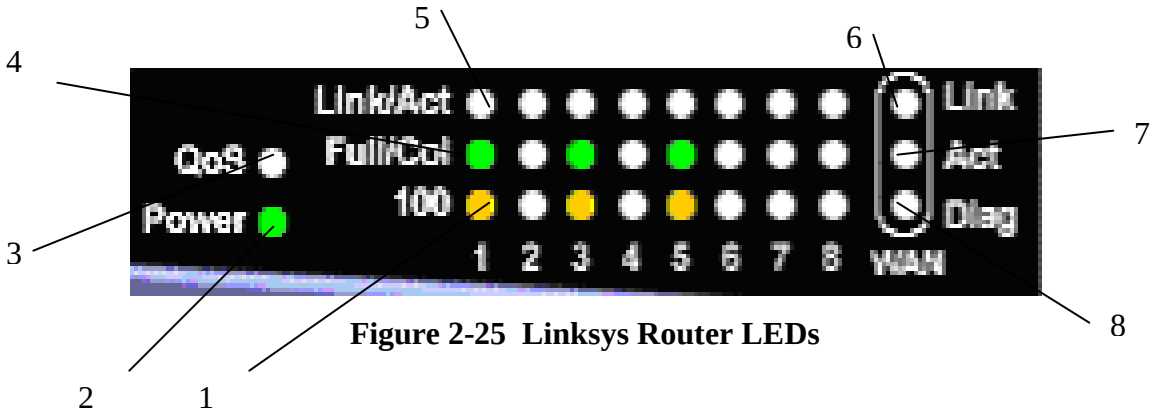


Figure 2-25 Linksys Router LEDs

Table 2-21 Linksys Router LEDs

KEY	CONTROL / INDICATOR	COLOR	FUNCTION
LAN indicators			
1.	100	Orange	When lit, indicates the Ethernet connection is at 100MB (100Base-T) on that port. If not lit, the connection is at 10MB (10Base-T).
2.	Power	Green	When lit, indicates power is connected and being received.
3.	QoS		Quality of Service is based on the idea that transmission rates, error rates and other characteristics can be measured and improved in advance. Prioritize performance by application or by specific ports. CAISI does not use this feature.
4.	Full/Col	Green	Full Duplex/Collisions.

Table 2-21 Linksys Router LEDs (Continued)

KEY	CONTROL / INDICATOR	COLOR	FUNCTION
		Serves two purposes: (1) If the LED is lit a steady green, the connection made through the corresponding port is successfully running in full duplex mode. (2) If the LED is flickering, the connection is experiencing collisions. Infrequent collisions are normal. If this LED is flickering too often, there may be a problem with your connection. Check the troubleshooting section (Paragraph 3.10) if you think there is a problem.	
5.	Link/Act	Green	Link/Activity. Serves two purposes. If the LED is lit a steady green, the Router is successfully connected to a device through the corresponding port (1 – 8). If the LED is flickering, the Router is actively sending or receiving data over that port.
WAN indicators			
6.	Link	Green	When lit, indicates a successful connection is made between the Router and your Broadband device or network.
7.	Act	Green	The Act (Activity) LED flickers when the router is sending or receiving data over the broadband port.
8.	Diag	Red	The Diag (Diagnostic) LED illuminates when the Router goes through its self-diagnosis mode during boot-up. It will turn off upon successful completion of the diagnosis. If this LED stays on for an abnormally long period of time, the device is not working properly. Try to re-flash the firmware by assigning a static IP address to the computer and then upgrade the firmware again. If that doesn't help, replace the unit. Steps for re-flash is in the troubleshooting procedures, Chapter 3.

2.12 10Base-T TRANSCEIVER

The transceiver is provided in case you need to connect a 10Base-T device to the NES. The NES connection is an Auxiliary Unit Interface (AUI) port. **Signal unit also has a 10Base-2 transceiver** to allow CAISI to connect a 10Base-2 cable.

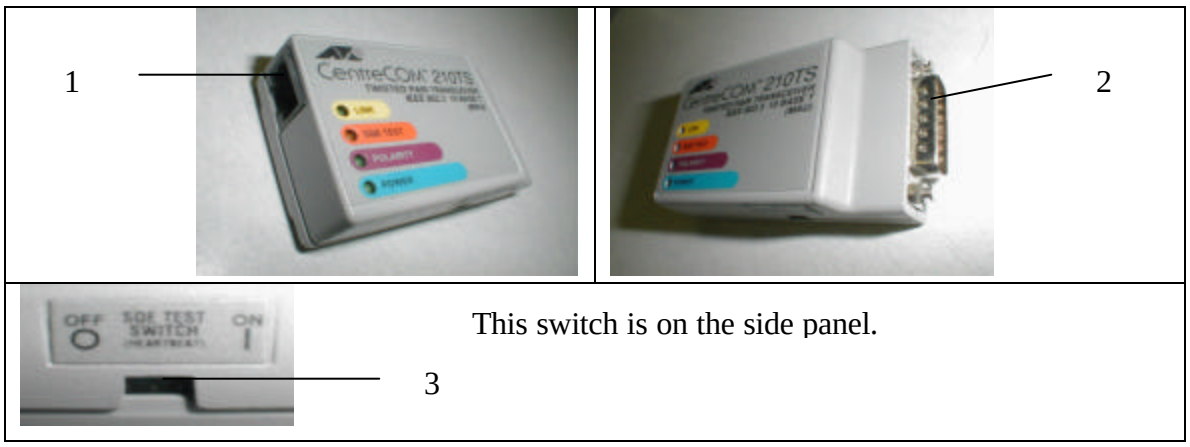
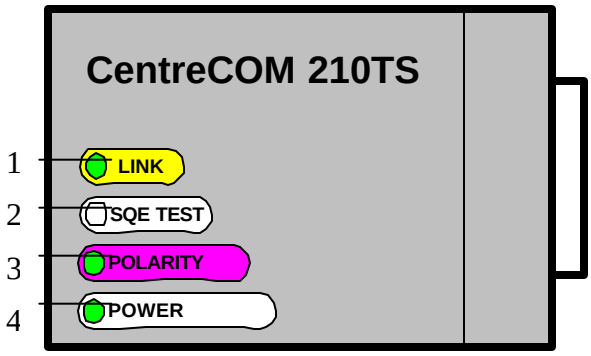


Figure 2-26 10Base-T Transceiver Controls and Indicators

Table 2-22 10Base-T Transceiver Controls and Indicators

KEY	CONTROL / INDICATOR	TYPE	FUNCTION
1.	RJ-45 Ethernet Port	RJ-45	Connects to one of the 10Base-T ports on the CBM using CAT-5 Ethernet cable. **NOTE:** *The root CBM is not the only device that can be connected to the INE. Any CBM can be used. You may often wish to connect the root CBM to the INE using the wireless bridge or DSL Bridge in the SSR Accessory Kit.* Whatever device is used, CAT-5 Ethernet cable connects to a RJ45 Ethernet port.
2.	DB15 Connection	DB15-pin Male	Connects directly to the AUI port on the INE/NES. CBM must be within 100 meters of the INE since the maximum length of a CAT-5 ethernet cable is 100 meters.
3.	SQE Test Switch	Switch	Signal Quality Error (SQE). Tests the quality of the signal. **CAISI does not use this**.
		Be sure the SQE Test Switch is set to O (off). Slide the switch to the left	



. **Figure 2-27 10Base-T Transceiver LEDs**

Table 2-23 10Base-T Transceiver LEDs

KEY	CONTROL / INDICATOR	COLOR	FUNCTION
1.	LINK	Green	When lit and flickering, indicates traffic being received and transmitted
2.	SQE TEST		Signal Quality Error (SQE). CAISI does not use this. It should be off. Set the SQE switch to “O” – (slide lever to the left).
3.	POLARITY	Green	When lit, indicates that automatic polarity reversal has not occurred.
4.	POWER	Green	When lit, indicates transceiver is receiving power (through the AUI port).

Chapter 2

Section II Preventive Maintenance Checks and Services (PMCS)

2.13 INTRODUCTION

The CAISI maintenance concept is a three level maintenance concept: **Unit/Operator**, **Direct Support** and **Depot**.

CAISI Operator level maintenance is the first and most critical level of CAISI maintenance. It is the foundation of the maintenance system and requires continuous emphasis by all commanders. The cornerstone of the operator level maintenance is the operator performing PMCS.

Preventive maintenance is the systematic care, servicing, and inspection of equipment. It can prevent the occurrence of trouble, reduce downtime, and maintain equipment in serviceable condition. To ensure the equipment is always ready for a mission, it is important to perform each scheduled PMCS procedure. The before, during, and after PMCS checks concentrate on ensuring equipment is fully mission capable (FMC).

The CAISI operator is responsible for the following:

1. Upon recognizing that the system is not functioning properly, the CAISI operator will perform PMCS.

2. Perform operator level basic troubleshooting procedures (Chapter 3, Paragraph 3.4.1). The CAISI operator will troubleshoot the Line Replacement Units (LRUs) of the CAISI before contacting the System Support Representative (SSR) or (CSS S6).

   These **LRUs** are **wireless bridge**, **multi-client radio adapter, DSL bridge, Inline Encryptor, hubs, UPS, antennas and lightning arrestors**.

3. Identify discrepancies or failures and annotate information on DA Form 2404/5988E.

4. CAISI operator will contact the SSR, CSS S6 for assistance on default items found during PMCS and in troubleshooting the network and/or communications-related failures.

5. CAISI operator will contact the Combat Service Support Automation Management Office (CSSAMO) if they isolate a fault as software related.

2.14 PMCS PROCEDURES

2.14.1 Routine Checks. Routine checks such as cleaning, dusting, washing, checking for loose and chipped paint, checking for damaged or frayed cables, storing items not in use, covering unused receptacles, checking for completeness, and checking for loose nuts, bolts, and screws are not listed as PMCS. These checks should be performed Before Operations, During Operations, After every shift, and as seen fit during normal operation for personnel and equipment safety.

Routine checks include:

1. Follow all WARNINGS, and CAUTIONS for all equipment

2. Ensure that exposed power and data cables are not burned, cut, frayed or stressed and that their plugs are securely seated in the jacks.

3. Ensure that the workspace is well ventilated. Protect equipment from overheating. Openings in the equipment must not be blocked or covered, and equipment should never be placed near a radiator or heat register.

4. Ensure that equipment is kept clean and dry. Where possible, avoid exposure to excessive dust and debris. Equipment should never be placed where it is subject to rain or being dripped upon. No food or drink should be placed where it can be spilled onto the equipment.

5. Ensure items not in use are properly stored.

6. Use a mild solution, detergent or window cleaner to clean the surface of the LSA and UPS.

   a. Do not use abrasive cleaners or solvents as they may mar the finish.

   b. Apply the mild detergent sparingly on lint free cloth, not directly to the LSA or UPS.

7. Do not use spray cleaner on the connections.

Perform the following After Operations and Weekly Checks as follows:

NOTE: *Weekly checks are the same as After Operations checks*

1. Check the equipment for completeness.

2. Wipe off the exterior surfaces with a mild detergent solution and cloth or paper towel.

NOTE: *When performing PMCS or routine checks, observe all **WARNINGS** and **CAUTIONS** listed at the beginning of this manual, at the appropriate place in all procedures, or on plates and decals attached to the equipment.*

2.14.2 Continuous Operations. If the CAISI is in continuous operations, check and service those items that can be checked and serviced without disturbing operation. Perform the complete checks and services when the CAISI is not in use.

2.14.3 Defects. Deficiencies that cannot be corrected must be reported to higher maintenance personnel. Records and reports of preventive maintenance must be made in accordance with the procedures contained in DA Pam 738-750.

2.14.4 Scheduling. PMCS must be done at the specified times, if possible, to ensure the equipment is always mission capable. If operational requirements prevent doing PMCS at the specified times, make the required checks and services at the first opportunity. During operation, PMCS must be done regularly to help identify and resolve small problems before they escalate. In addition, the specified checks and services must be performed under the following special conditions.

2.14.4.1 Before Operation. Always keep in mind the **CAUTIONS** and **WARNINGS**. Before (B) operation PMCS must be done before you operate or use the equipment for its intended purpose.

2.14.4.2 During Operation. Always keep in mind the **CAUTIONS** and **WARNINGS**. During (D) operation PMCS must be performed while you are operating or using the equipment for its intended mission, as long as the checks and services are safe for the operator to perform and do not interfere with the mission.

2.14.4.3 After Operation. After (A) operation PMCS must be performed immediately after you have operated or used the equipment. Weekly (W) PMCS checks are the same as After Operation checks.

NOTE: *There are no Monthly (M), Quarterly (Q), or Yearly (Y) PMCS checks or services required.*

2.14.5 PMCS Table. Table 2-24 contains the PMCS to be performed for the CAISI for the Operator. The CAISI equipment in Table 2-24 includes the CBM, CCM, and LSA. Table 2-24 contains the PMCS to be performed for the CAISI at the organizational level, most likely done by the SSR. The CAISI equipment in Table 2-25 includes the SSR Accessory Kit. Both tables indicate what items to check, when to check them, and how to check them. Perform the PMCS procedures thoroughly.

Warnings and Cautions. Always observe the **WARNINGS** and **CAUTIONS** appearing in your PMCS table. **WARNINGS** and **CAUTIONS** appear before applicable procedures. You must observe these **WARNINGS** and **CAUTIONS** to prevent injury to yourself and others and to prevent your equipment from being damaged.

2.14.5.1 Item No. Column. The checks and services are listed in the order that they shall be accomplished. Use this number for the TM number on DA Form 2404, Equipment Inspection and Maintenance Worksheet, to record results of checks and services.

2.14.5.2 Interval Column. The columns headed B, D, A and W contain an "•" mark in the appropriate interval column for each check and service. This indicates when to perform the PMCS procedure.

2.14.5.3 Item to Check/Service/Procedures Column. The items listed in this column indicate what part of the equipment is to be checked and how to perform the check.

WARNING

Prior to performing during-operation checks, verify **EACH** unit is grounded to prevent electrical shock.

Table 2-24 User PMCS

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES.
	B	D	A	W	M	Q	Y	
								WARNINGS • POWER DOWN AND UNPLUG CAISI COMPONENTS FROM POWER OUTLET BEFORE CLEANING. • DO NOT APPLY ANY CLEANING SOLUTION DIRECTLY ON ANY OF THE CAISI COMPONENTS • PLACE THE CLEANING SOLUTION ON A LINT FREE CLOTH AND CLEAN THE SURFACE OF THE DEVICE • DO NOT PLACE LIQUIDS ON OR NEAR CAISI COMPONENTS • NEVER SPRAY WATER OR CLEANER INTO SWITCHES, BUTTONS, DATA OR COMMUNICATIONS JACK, AIR VENTS OR OTHER OPENINGS. **NOTE:** *IF TH EQUIPMENT MUST BE KEPT IN CONTINUOUS OPERATION, CHECK AND SERVICE ONLY THOSE ITEMS THAT CAN BE CHECKED AND SERVICED WITHOUT DISTURBING OPERATION. MAKE THE COMPLETE CHECKS AND SERVICES WHEN THE EQUIPMENT CAN BE SHUT DOWN.*
	•		•					1. CHECK THE EQUIPMENT FOR COMPLETENESS 2. WIPE OFF ALL EXTERIOR SURFACES WITH A MILD DETERGENT SOLUTION AND CLOTH OR PAPER TOWEL.
								<u>VELCRO FASTENERS:</u> DO NOT DISASSEMBLE THE EQUIPMENT FOR THE EXPRESS PURPOSE OF CLEANING VELCRO FASTENERS. IF THE EQUIPMENT HAS BEEN DISASSEMBLED FOR ANY REASON, CHECK THE VELCRO AND CLEAN IT IF IS NECESSARY. USE A STIFF BRUSH TO REMOVE DIRT AND DEBRIS.
1	•		•					<u>CBM COMPONENTS: TRANSIT CASE</u> 1. CHECK THE OUTSIDE CASE FOR SIGNS OF DAMAGE – DENTS, CRACKS, PUNCTURES, AND CORROSION.
	•		•					2. CHECK PRESSURE RELEASE VALVE FOR SERVICEABILITY
	•		•					3. CLIPS ON SIDE OF CASE WORK PROPERLY.
			•					4. CHECK INTERIOR FOR SIGNS OF DAMAGE – MISSING OR DAMAGED FOAM; MISSING/DAMAGED CLIPS ON TOP COMPARTMENT

Table 2-24 User PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES.
	B	D	A	W	M	Q	Y	
2								CBM COMPONENTS: CBM CHASSIS:
	•	•						1. PERIODICALLY CHECK CABLES AND CONNECTIONS FOR TIGHTNESS, AND INSPECT FOR SIGNS OF WEAR. THIS INCLUDES BURNED, CUT OR FRAYED CABLES.
			•					2. USE A MILD SOLUTION OF DETERGENT OR WINDOW CLEANER AND A PAPER TOWEL TO CLEAN THE SURFACE.
								CAUTION: DO NOT SPRAY CLEANER INTO THE AIR VENTS.
	•		•					3. CHECK BINDING POSTS FOR SPRING-ACTION
	•		•					4. CHECK BINDING POSTS RUBBER BOOTS FOR MISSING, CRACKS OR DRY ROTTING.
	•		•					5. CHECK TO MAKE SURE TINES IN LIGHTENING ARRESTOR ARE CLOSE TOGETHER NOT SPREAD OUT. NOT WARPED.
3								CBM COMPONENTS: UNINTERRUPTIBLE POWER SUPPLY (UPS):
								CAUTIONS
								• DO NOT GET THE UPS WET.
								• DO NOT USE WITH OTHER THAN SPECIFIED COMPUTER EQUIPMENT.
								• DO NOT STORE WITH THE MASTER SWITCH ON.
								• DO NOT USE EXTERNAL SPIKE/SURGE PROTECTORS ON UPS OUTLETS.
								• DO NOT USE MORE THAN THE RATED CAPACITY.
								• DO NOT PUT ANYTHING ON TOP OF THE UPS.
								• DO NOT OPEN UPS CASE FOR ANY REASON.
								• DO NOT PLUG THE UPS LINE CORD INTO UPS OUTLETS.
								• TURN OFF THE UPS BY PRESSING THE MASTER POWER SWITCH ON THE FRONT PANEL AND UNPLUGGING IT FROM THE WALL OR GENERATOR BEFORE CLEANING. NEVER ATTEMPT TO CLEAN IN THE OUTLETS OR THE VENTS OF THE CASE.
								• USE A MILD SOLUTION OF DETERGENT OR WINDOW CLEANER AND A PAPER TOWEL TO CLEAN THE SURFACE OF THE UPS.
								ENTS, AS THEY MAY MAR THE FINISH. APPLY THE MILD CLEANING SOLUTION SPARINGLY TO THE PAPER TOWEL OR CLOTH, NOT THE UPS.
								• DO NOT SPRAY CLEANER INTO THE AIR VENTS.

Table 2-24 User PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES.
	B	D	A	W	M	Q	Y	
4								CBM COMPONENTS: 7-INCH PANEL ANTENNA
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK CONNECTIONS ON REAR FOR SIGNS OF WEAR
	•		•					3. CHECK TO MAKE SURE TINES IN ANTENNA CONNECTOR ARE CLOSE TOGETHER NOT SPREAD OUT.
	•		•					4. CHECK ANTENNA CONNECTOR FOR MOISTURE; COVER WITH TAPE OR CAP TO PREVENT MOISTURE BUILDUP WHEN NOT IN USE.
5								CBM COMPONENTS: 40-INCH BREAK-APART WHIP ANTENNA
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK PIN CONNECTIONS ON ENDS; DOES ANTENNA ASSEMBLE
	•		•					3. CHECK TO MAKE SURE TINES ARE PRESENT AND SHOULD BE CLOSE TOGETHER NOT SPREAD OUT.
	•		•					4. CHECK PLASTIC FASTENER FOR TIGHTNESS OF FIT.
6								CBM COMPONENTS: 25-FOOT RF ANTENNA CABLE
	•		•					1. CHECK FOR CRACKS, DENTS, BARE WIRE, OR ANY OTHER DAMAGE
	•		•					2. CHECK PIN CONNECTIONS ON ENDS; WHEN NOT IN USE SHOULD BE CAPPED OR COVERED WITH TAPE.
	•		•					3. CHECK TO MAKE SURE TINES ARE PRESENT AND SHOULD BE CLOSE TOGETHER NOT SPREAD OUT.
7								CBM COMPONENTS: 35-FOOT RF ANTENNA CABLE
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK PIN CONNECTIONS ON ENDS; WHEN NOT IN USE SHOULD BE CAPPED OR COVERED WITH TAPE.
	•		•					3. CHECK TO MAKE SURE TINES ARE PRESENT AND SHOULD BE CLOSE TOGETHER NOT SPREAD OUT.
8								CBM COMPONENTS: DOUBLE "N" CABLE ADAPTER (BARREL CONNECTOR)
	•		•					1. CHECK FOR CRACKS, DENTS OR OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE TINES ARE PRESENT ON BOTH ENDS AND THEY SHOULD BE CLOSE TOGETHER NOT SPREAD OUT.
9								CBM COMPONENTS: ANTENNA BRACKET FOR WHIP OR 7-INCH PANEL ANTENNA
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK FOR MISSING COMPONENTS – U-BOLTS, WING NUTS, NUTS.
10								CBM COMPONENTS: GROUNDING STRAP
	•		•					1. CHECK FOR CUTS, TEARS ON THE CABLE ITSELF
	•		•					2. CHECK METAL END TO BE SURE IT IS STRAIGHT, NOT BENT.
	•		•					3. CHECK CLAMP TO MAKE SURE IT IS OPERATIONAL
	•		•					4. CHECK GROUNDING STUD ON CBM CHASSIS FOR A WASHER AND WING NUT.

Table 2-24 User PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES.
	B	D	A	W	M	Q	Y	
11								CBM COMPONENTS: 2-PRONG (QTY 2) / 3-PRONG POWER CABLE
	•		•					1. CHECK FOR CRACKS, CUTS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE PRONGS ARE PRESENT AND ARE STRAIGHT, NOT BENT.
12								CBM COMPONENTS: ETHERNET CABLE (RED/WHITE) (QTY 1, EACH)
	•		•					1. CHECK FOR CRACKS, CUTS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND ARE NOT DAMAGED.
13								CBM COMPONENTS: 42-FOOT GUY ROPE (QTY 4)
	•		•					1. CHECK FOR CUTS, FRAYED EDGES, DRY ROT OR ANY OTHER DAMAGE.
	•		•					2. CHECK CLIPS FOR SERVICEABILITY
14								CBM COMPONENTS: REEL UNIT (RL-28) FOR GUY ROPES (FOUR GUY ROPES PER REEL UNIT) (QTY 2)
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK FOR SERVICEABILITY
15								CCM COMPONENTS: CARRYING CASE
	•		•					1. CHECK FOR RIPS, TEARS, ZIPPER WORKS OR ANY OTHER DAMAGE.
16								CCM COMPONENTS: CCM CHASSIS:
	•	•						1. PERIODICALLY CHECK CABLES AND CONNECTIONS FOR TIGHTNESS, AND INSPECT FOR SIGNS OF WEAR.
			•					2. USE A MILD SOLUTION OF DETERGENT OR WINDOW CLEANER AND A PAPER TOWEL TO CLEAN THE SURFACE. DO NOT SPRAY CLEANER INTO THE AIR VENTS.
	•		•					RESTOR ARE PED.
	•		•					4. CHECK GROUNDING STUD ON CCM CHASSIS FOR A WASHER AND WING NUT
17								CCM COMPONENTS: 24-INCH WHIP ANTENNA
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK ANTENNA CONNECTION TO MAKE SURE PIN IS PRESENT AND TINES SURROUNDING PIN ARE PRESENT AND NOT BENT.
	•		•					3. WHEN ANTENNA IS NOT IN USE, COVER ANTENNA CONNECTION WITH PLASTIC CAP OR TAPE, TO PREVENT MOISTURE OR DIRT BUILDUP.

Table 2-24 User PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES.
	B	D	A	W	M	Q	Y	
18								CCM COMPONENTS: 35-FOOT RF ANTENNA CABLE
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK CONNECTIONS ON ENDS; WHEN NOT IN USE SHOULD BE CAPPED OR COVERED WITH TAPE
	•		•					3. CHECK TO MAKE SURE TINES ARE PRESENT AND SHOULD BE CLOSE TOGETHER NOT SPREAD OUT
19								CCM COMPONENTS: ANTENNA BRACKET FOR WHIP ANTENNA
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK FOR MISSING COMPONENTS – U-BOLTS, WING NUTS, NUTS.
20								CCM COMPONENTS: GROUNDING STRAP
	•		•					1. CHECK FOR CUTS OR TEARS ON THE CABLE ITSELF
	•		•					2. CHECK METAL END TO BE SURE IT IS STRAIGHT, NOT BENT.
	•		•					3. CHECK CLAMP TO MAKE SURE IT IS OPERATIONAL
21								CCM COMPONENTS: WHITE STRAIGHT-THROUGH ETHERNET CABLE
	•		•					1. CHECK FOR CRACKS, CUTS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND ARE NOT DAMAGED.
22								CCM COMPONENTS: 2-PRONG POWER CORD
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE PRONGS ARE PRESENT AND ARE STRAIGHT, NOT BENT.
23								LEGACY SUPPORT ADAPTER COMPONENTS:
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK SERIAL CONNECTION AND RJ-45 JACK FOR DAMAGED, MISSING OR BENT PINS.
24								LEGACY SUPPORT ADAPTER COMPONENTS: 9-TO-25 PIN NULL MODEM CABLE ADAPTER
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND ARE NOT DAMAGED, PINS MISSING OR BENT.
25								LEGACY SUPPORT ADAPTER COMPONENTS: WHITE STRAIGHT-THROUGH ETHERNET CABLE
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND ARE NOT DAMAGED.

Table 2-24 User PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES.
	B	D	A	W	M	Q	Y	
26	•		•					LEGACY SUPPORT ADAPTER COMPONENTS: POWER SUPPLY 1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE 2. CHECK TO MAKE SURE PRONGS ARE PRESENT AND ARE STRAIGHT, NOT BENT.
27	•		•					LEGACY SUPPORT ADAPTER COM PONENTS: 3-PRONG POWER CORD 1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE 2. CHECK TO MAKE SURE PRONGS ARE PRESENT AND ARE STRAIGHT, NOT BENT.

Table 2-25 Organizational PMCS

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES
	B	D	A	W	M	Q	Y	
1	• • •		• • •					<u>SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: TRANSIT CASE</u> 1. CHECK THE OUTSIDE CASE FOR SIGNS OF DAMAGE 2. CHECK PRESSURE RELEASE VALVE FOR SERVICEABILITY 3. CLIPS ON SIDE OF CASE
2	• • •		• • •					<u>SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: INLINE ENCRYPTOR (QTY 2)</u> 1. CHECK FOR ANY SIGN OF DAMAGE ON THE FRONT OR REAR. 2. CHECK 10BASE-T CONNECTIONS FOR DAMAGE 3. CHECK POWER CABLE CONNECTION FOR DAMAGE.
3								<u>SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: UNINTERRUPTIBLE POWER SUPPLY (UPS):</u> **CAUTIONS** • DO NOT GET THE UPS WET. • DO NOT USE WITH OTHER THAN SPECIFIED COMPUTER EQUIPMENT. • DO NOT STORE WITH THE MASTER SWITCH ON. • DO NOT USE EXTERNAL SPIKE/SURGE PROTECTORS ON UPS OUTLETS. • DO NOT USE MORE THAN THE RATED CAPACITY. • DO NOT PUT ANYTHING ON TOP OF THE UPS. • DO NOT OPEN UPS CASE FOR ANY REASON. • DO NOT PLUG THE UPS LINE CORD INTO UPS OUTLETS .
								• TURN OFF THE UPS BY PRESSING THE MASTER POWER SWITCH ON THE FRONT PANEL AND UNPLUGGING IT FROM THE WALL OR GENERATOR BEFORE CLEANING. NEVER ATTEMPT TO CLEAN IN THE OUTLETS OR THE VENTS OF THE CASE.
								• USE A MILD SOLUTION OF DETERGENT OR WINDOW CLEANER AND A PAPER TOWEL TO CLEAN THE SURFACE OF THE UPS.
								• DO NOT USE ABRASIVE CLEANSERS OR SOLVENTS, AS THEY MAY MAR THE FINISH. APPLY THE MILD CLEANING SOLUTION SPARINGLY TO THE PAPER TOWEL OR CLOTH, NOT THE UPS.

Table 2-25 Organizational PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES
	B	D	A	W	M	Q	Y	
								• DO NOT SPRAY CLEANER INTO THE AIR VENTS.
4	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: WIRELESS BRIDGE 1. CHECK FOR ANY SIGN OF DAMAGE ON THE FRONT OR REAR.
	•		•					2. CHECK INLINE POWER ETHERNET CONNECTION FOR DAMAGE
	•		•					3. CHECK ANTENNA CONNECTION, IS THE PIN PRESENT, OR BENT.
5	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: MULTI-CLIENT RADIO ADAPTER 1. CHECK FOR ANY SIGN OF DAMAGE ON THE FRONT OR REAR.
	•		•					2. CHECK 10BASE-T AND POWER CONNECTIONS FOR DAMAGE
	•		•					3. CHECK ANTENNA CONNECTION, IS THE PIN PRESENT, OR BENT.
6	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: DSL BRIDGE 1. CHECK FOR ANY SIGN OF DAMAGE ON THE FRONT OR REAR.
	•		•					2. CHECK BINDING POSTS FOR SPRING-ACTION
	•		•					3. CHECK BINDING POSTS RUBBER BOOTS FOR MISSING, CRACKS OR DRY ROTTING.
	•		•					4. CHECK DSL/10BASE-T CONNECTIONS FOR DAMAGE
	•		•					5. CHECK RATE CONFIGURATION SWITCH (DATA SPEED) FOR DAMAGE.
7	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: INTERNAL ROUTER (Linksys) 1. CHECK FOR ANY SIGN OF DAMAGE ON THE FRONT OR REAR.
	•		•					2. CHECK 10BASE-T CONNECTIONS FOR DAMAGE
	•		•					3. CHECK POWER CABLE CONNECTION FOR DAMAGE.
8	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: HUB (QTY 2) 1. CHECK FOR ANY SIGN OF DAMAGE ON THE FRONT OR REAR.
	•		•					2. CHECK 10BASE-T CONNECTIONS FOR DAMAGE
	•		•					3. CHECK POWER CABLE CONNECTION FOR DAMAGE.
	•		•					4. CHECK BNC CONNECTOR, “T” CONNECTOR AND TERMINATOR, ARE THEY PRESENT, ARE THEY FASTENED SECURELY.

Table 2-25 Organizational PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES
	B	D	A	W	M	Q	Y	
9								SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: 10BASE-T TRANSCEIVER
	•		•					1. CHECK FOR ANY SIGN OF DAMAGE
	•		•					2. CHECK THE ON/OFF SWITCH, AND ALL PORTS.
10								SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: 40-INCH BREAK-APART WHIP ANTENNA (QTY 2)
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK CONNECTIONS ON ENDS; DOES ANTENNA ASSEMBLE
	•		•					3. CHECK TO MAKE SURE TINES ARE PRESENT AND SHOULD BE CLOSE TOGETHER NOT SPREAD OUT.
	•		•					4. CHECK PLASTIC FASTENER FOR ANY DAMAGE AND THAT IS FASTENS SECURELY.
11								SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: 4-INCH WHIP ANTENNA (QTY 2)
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK CONNECTION ON END
	•		•					3. CHECK TO MAKE SURE TINES ARE PRESENT AND SHOULD BE CLOSE TOGETHER NOT SPREAD OUT.
12								SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: LIGHTNING ARRESTOR ASSEMBLY – LIGHTNING ARRESTOR MOUNTED ON BRACKET (QTY 2)
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE PIN CONNECTORS ON BOTH ENDS ARE PRESENT AND NOT DAMAGED, NOT WARPED.
	•		•					3. CHECK TO MAKE SURE WING NUT AND WASHER IS PRESENT FOR THE GROUNDING STUD ON THE BRACKET.
13								SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: GROUNDING STRAP (QTY 2)
	•		•					1. CHECK FOR CUTS, TEARS ON THE CABLE ITSELF
	•		•					2. CHECK METAL END TO BE SURE IT IS STRAIGHT, NOT BENT.
	•		•					3. CHECK CLAMP TO MAKE SURE IT IS OPERATIONAL
14								SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS:
								12-INCH RF ADAPTER CABLE N (M) to RPTNC (M) (QTY 2)
								12-INCH RF ADAPTER CABLE N (M) to RPTNC (F) (QTY 2)
	•		•					1. CHECK FOR CUTS, TEARS ON THE CABLE ITSELF
	•		•					2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND ARE NOT DAMAGED.

Table 2-25 Organizational PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES
	B	D	A	W	M	Q	Y	
15	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: ADAPTER, RIGHT ANGLE, N (M) to N (M) (QTY 2) 1. CHECK FOR CRACKS, SCRATCHES, DENTS OR OTHER DAMAGE 2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND ARE NOT DAMAGED.
16	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: ANTENNA "DUMMY LOAD" N (M) (QTY 2) 1. CHECK FOR CRACKS, SCRATCHES, DENTS OR OTHER DAMAGE 2. CHECK TO MAKE SURE CONNECTOR ON THE END ARE PRESENT AND ARE NOT DAMAGED.
17	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: ETHERNET CABLE – WHITE/RED (QTY 4, EACH) 1. CHECK FOR CRACKS, CUTS, DENTS OR ANY OTHER DAMAGE 2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND ARE NOT DAMAGED.
18	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: ADAPTER, RJ-45 (F) to RJ-45 (F) STRAIGHT-THROUGH (QTY 3) (RJ-45 straight-through adapter) 1. CHECK FOR CRACKS, SCRATCHES, DENTS OR OTHER DAMAGE 2. CHECK TO MAKE SURE CONNECTORS ON THE ENDS ARE NOT DAMAGED.
19	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: ADAPTER, RJ-45 (F) to RJ-45 (M) CROSSOVER (QTY 3) (RJ-45 crossover adapter) 1. CHECK FOR CRACKS, SCRATCHES, DENTS OR OTHER DAMAGE 2. CHECK TO MAKE SURE CONNECTORS ON THE ENDS ARE NOT DAMAGED.
20	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: 9-PIN STRAIGHT-THROUGH SERIAL EXTENSION CABLE (M-F) (blue) 1. CHECK FOR CRACKS, CUTS, DENTS OR ANY OTHER DAMAGE 2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND NOT DAMAGED, PINS MISSING OR BENT.

Table 2-25 Organizational PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES
	B	D	A	W	M	Q	Y	
21	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: 9-PIN CROSSOVER SERIAL NULL MODEM CABLE (F-F) (beige) 1. CHECK FOR CRACKS, CUTS, DENTS OR ANY OTHER DAMAGE 2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND NOT DAMAGED, PINS MISSING OR BENT.
	•		•					
22	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: 9 TO 25-PIN NULL MODEM SERIAL ADAPTER CABLE (used with LSA) (may not have been issued) 1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE 2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND ARE NOT DAMAGED, PINS MISSING OR BENT.
	•		•					
23	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: RESET TOOL (QTY 3) 1. CHECK FOR CRACKS, CUTS, DENTS OR ANY OTHER DAMAGE 2. CHECK TO MAKE SURE POINTED END IS INTACT AND NOT DAMAGED.
	•		•					
24	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: POWER SUPPLYS POWER SUPPLY and POWER INJECTOR 48V, Wireless Bridge 5V, DSL 5V, Router 5V, 3 LEADS (QTY 2) 5V, 1 LEAD WALL STYLE (QTY 5) 1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE 2. CHECK TO MAKE SURE PRONGS ARE PRESENT AND ARE STRAIGHT, NOT BENT. *NOTE: Version 2 Router will have a 5V, 1 Lead Wall style power supply instead of a 5V power supply. 5V, 1 Lead wall style will be quantity of 6 as well as the 3-prong, 1-foot power cable.
	•		•					
25	•		•					SSR ACCESSORY KIT (SSR TRANSIT CASE) COMPONENTS: POWER CABLES 2-PRONG POWER CABLE (QTY 3) 3-PRONG POWER CABLE (QTY 2) 3-PRONG, 1-FOOT POWER CABLE (QTY 5) 1. CHECK FOR CRACKS, CUTS, DENTS OR ANY OTHER DAMAGE 2. CHECK TO MAKE SURE PRONGS ARE PRESENT AND ARE STRAIGHT, NOT BENT.
	•		•					

Table 2-25 Organizational PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES
	B	D	A	W	M	Q	Y	
26								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS: NOTEBOOK COMPUTER **CAUTION** DO NOT APPLY ANY CLEANING SOLUTION TO THE SCREEN OR KEYBOARD. DO NOT SPRAY ANY CLEANER OR WATER INTO ANY OF THE OPENINGS ON THE NOTEBOOK COMPUTER.
	•	•						1. PERIODICALLY CHECK CABLES AND CONNECTIONS FOR TIGHTNESS, AND INSPECT FOR SIGNS OF WEAR.
			•					2. USE A MILD SOLUTION OF DETERGENT OR WINDOW CLEANER AND A PAPER TOWEL TO CLEAN THE SURFACE.
					•			3. RUN SOFTWARE CHECKS USING SCANDISK AND DEFRAG.
27								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS: POWER SUPPLY AND POWER CABLE POWER SUPPLY (QTY 1) 3-PRONG POWER CABLE (QTY 1)
	•		•					1. CHECK FOR CRACKS, CUTS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE PRONGS ARE PRESENT AND ARE STRAIGHT, NOT BENT.
28								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS: "RABBIT EARS" ANTENNA
	•		•					1. CHECK ANTENNA APPENDAGES (EARS) FOR DAMAGE
	•		•					2. CHECK PC CARD CONNECTIONS ON ADAPTER CABLE
29								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS: WIRELESS NIC
	•		•					1. CHECK FOR ANY SIGN OF DAMAGE
	•		•					2. CHECK ANTENNA PORT CONNECTIONS
30								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS:
	•		•					1. CHECK FOR ANY SIGN OF DAMAGE
	•		•					2. CHECK RJ-45 PORT FOR ANY DAMAGE.
31								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS: ETHERNET CABLE – WHITE/RED (QTY 1, EACH)
	•		•					1. CHECK FOR CRACKS, CUTS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND ARE NOT DAMAGED.

Table 2-25 Organizational PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES
	B	D	A	W	M	Q	Y	
32								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS: ADAPTER, RJ-45 (F) to RJ-45 (F) STRAIGHT-THROUGH (RJ-45 straight-through adapter)
	•		•					1. CHECK FOR CRACKS, SCRATCHES, DENTS OR OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE CONNECTORS ON THE ENDS ARE NOT DAMAGED.
33								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS: ADAPTER, RJ-45 (F) to RJ-45 (M) CROSSOVER (QTY-1) (RJ-45 crossover adapter)
	•		•					1. CHECK FOR CRACKS, SCRATCHES, DENTS OR OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE CONNECTORS ON THE ENDS ARE NOT DAMAGED.
34								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS: 9-PIN STRAIGHT-THROUGH SERIAL EXTENSION CABLE (M-F) (blue)
	•		•					1. CHECK FOR CRACKS, CUTS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND NOT DAMAGED, PINS MISSING OR BENT.
35								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS: 9-PIN CROSSOVER SERIAL NULL MODEM CABLE (F-F) (beige)
	•		•					1. CHECK FOR CRACKS, CUTS, DENTS OR ANY OTHER
	•		•					2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND NOT DAMAGED, PINS MISSING OR BENT.
36								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS: ADAPTER CABLE, 12 INCH (QTY 1 EACH)
								MMCX TO N (F)
								MMCX TO RPTNC (F)
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND ARE NOT DAMAGED, PINS MISSING OR BENT.

Table 2-25 Organizational PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES
	B	D	A	W	M	Q	Y	
37								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS: ADAPTER N (M) to N (M) RIGHT ANGLE (Right angle adapter)
	•		•					1. CHECK FOR CRACKS, SCRATCHES, DENTS OR OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE CONNECTORS ON BOTH ENDS ARE PRESENT AND ARE NOT DAMAGED.
38								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS: ANTENNA "DUMMY LOAD" N (M)
	•		•					1. CHECK FOR CRACKS, SCRATCHES, DENTS OR OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE CONNECTOR ON THE END ARE PRESENT AND ARE NOT DAMAGED.
39								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS: RESET TOOL
	•		•					1. CHECK FOR CRACKS, CUTS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK TO MAKE SURE POINTED END IS INTACT AND NOT DAMAGED.
40								SSR ACCESSORY KIT (SSR NOTEBOOK CASE) COMPONENTS: BASELINE CD
	•		•					1. CHECK FOR SCRATCHES, CRACKS, OR ANY OTHER DAMAGE
41								SSR ACCESSORY KIT (SSR ANTENNA CARRYING CASE) COMPONENTS:
	•		•					1. CHECK FOR RIPS, TEARS, ZIPPER WORKS OR ANY OTHER DAMAGE.
42								SSR ACCESSORY KIT (SSR ANTENNA CARRYING CASE) COMPONENTS: 14-INCH PANEL ANTENNA (QTY 2)
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK CONNECTIONS ON REAR FOR SIGNS OF WEAR
	•		•					3. CHECK TO MAKE SURE TINES IN ANTENNA CONNECTOR ARE CLOSE TOGETHER NOT SPREAD OUT.
	•		•					4. CHECK ANTENNA CONNECTOR FOR MOISTURE; COVER WITH TAPE OR CAP TO PREVENT MOISTURE. BUILDUP

Table 2-25 Organizational PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES
	B	D	A	W	M	Q	Y	
43								SSR ACCESSORY KIT (SSR ANTENNA CARRYING CASE) COMPONENTS: 50-FOOT RF ANTENNA CABLE (QTY 4) 1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE 2. CHECK CONNECTIONS ON ENDS; WHEN NOT IN USE SHOULD BE CAPPED OR TAPED 3. CHECK TO MAKE SURE TINES ARE PRESENT AND SHOULD BE CLOSE TOGETHER NOT SPREAD OUT.
	•		•					
	•		•					
	•		•					
44								SSR ACCESSORY KIT (SSR ANTENNA CARRYING CASE) COMPONENTS: BRACKET FOR 7-INCH PANEL ANTENNA (QTY 2) BRACKET FOR 14-INCH PANEL ANTENNA (QTY 2) 1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE. 2. CHECK FOR MISSING COMPONENTS – U-BOLTS, WING NUTS, NUTS.
	•		•					
	•		•					
45								SSR ACCESSORY KIT (SSR ANTENNA CARRYING CASE) COMPONENTS: DOUBLE "N" ADAPTER (BARREL CONNECTOR) (QTY 4) 1. CHECK FOR CRACKS, SCRATCHES, DENTS OR OTHER 2. CHECK TO MAKE SURE TINES ARE PRESENT ON BOTH ENDS AND THEY SHOULD BE CLOSE TOGETHER NOT SPREAD OUT.
	•		•					
	•		•					
46								SSR ACCESSORY KIT (SSR ANTENNA CARRYING CASE) COMPONENTS: 42-FOOT GUY ROPE (RED CLIPS) (QTY 4) 1. CHECK FOR CUTS, FRAYED EDGES, DRY ROT OR ANY OTHER DAMAGE. 2. CHECK CLIPS FOR SERVICEABILITY
	•		•					
	•		•					
47								SSR ACCESSORY KIT (SSR ANTENNA CARRYING CASE) COMPONENTS: REEL UNIT (RL-28) FOR GUY ROPES (TWO GUY ROPES PER REEL UNIT) (QTY 2) 1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE 2. CHECK FOR SERVICEABILITY.
	•		•					
	•		•					

Table 2-25 Organizational PMCS (Continued)

Table 2-25 Organizational PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES
	B	D	A	W	M	Q	Y	
48								SSR ACCESSORY KIT (SSR ANTENNA CARRYING CASE) COMPONENTS: GUY STAKES (QTY 4) (Stake Assembly) 1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE 2. CHECK FOR SERVICEABILITY.
	•		•					
	•		•					
49								SSR ACCESSORY KIT (SSR ANTENNA MAST CARRYING CASE) COMPONENTS: CARRYING CASE 1. CHECK FOR RIPS, TEARS, ZIPPER WORKS OR ANY OTHER DAMAGE.
	•		•					
50								SSR ACCESSORY KIT (SSR ANTENNA MAST CARRYING CASE) COMPONENTS: UPPER MAST SECTION (QTY 5) (Mast Section Assembly (Upper)) LOWER MAST SECTION (QTY 5) (Mast Section Assembly (Lower))
	•		•					1. CHECK FOR CRACKS, DENTS, BARE METAL OR ANY OTHER DAMAGE
51								SSR ACCESSORY KIT (SSR ANTENNA MAST CARRYING CASE) COMPONENTS: UPPER MAST ADAPTER SECTION (RED RING) (Adapter Assembly (Upper)) LOWER MAST ADAPTER SECTION (BLUE RING) (Adapter Assembly (Lower)) 1. CHECK FOR CRACKS, DENTS, BARE METAL OR ANY OTHER DAMAGE
	•		•					
52								SSR ACCESSORY KIT (SSR ANTENNA MAST CARRYING CASE) COMPONENTS: 36-FOOT GUY ROPE (BLUE CLIPS) (QTY 4) 42-FOOT GUY ROPE (RED CLIPS) (QTY 4) 1. CHECK FOR CUTS, FRAYED EDGES, DRY ROT OR ANY OTHER DAMAGE. 2. CHECK CLIPS FOR SERVICEABILITY
	•		•					
	•		•					

Table 2-25 Organizational PMCS (Continued)

ITEM NO.	INTERVAL							ITEM TO BE CHECKED/SERVICED AND PROCEDURES
	B	D	A	W	M	Q	Y	
53								SSR ACCESSORY KIT (SSR ANTENNA MAST CARRYING CASE) COMPONENTS: REEL UNIT (RL-28) FOR GUY ROPES (FOUR GUY ROPES PER REEL UNIT) (QTY 4)
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK FOR SERVICEABILITY.
54								SSR ACCESSORY KIT (SSR ANTENNA MAST CARRYING CASE) COMPONENTS: GUY STAKES (QTY 4) (Stake Assembly)
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK FOR SERVICEABILITY.
55								SSR ACCESSORY KIT (SSR ANTENNA MAST CARRYING CASE) COMPONENTS:
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK FOR SERVICEABILITY.
56								SSR ACCESSORY KIT (SSR ANTENNA MAST CARRYING CASE) COMPONENTS: BASE PLATE (QTY 1) / BASE PLATE PINS (QTY 2) (Stakes)
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK FOR SERVICEABILITY.
57								SSR ACCESSORY KIT (SSR ANTENNA MAST CARRYING CASE) COMPONENTS: GUY RINGS (ONE RED, ONE BLUE)
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK FOR SERVICEABILITY.
58								SSR ACCESSORY KIT (SSR ANTENNA MAST CARRYING CASE) COMPONENTS: STRAIN RELIEF CLAMP
	•		•					1. CHECK FOR SERVICEABILITY.
59								SSR ACCESSORY KIT (SSR ANTENNA MAST CARRYING CASE) COMPONENTS: 2.5 POUND SLEDGE HAMMER
	•		•					1. CHECK FOR CRACKS, DENTS OR ANY OTHER DAMAGE
	•		•					2. CHECK FOR SERVICEABILITY.

Chapter 2

Section III Operation Under Usual Conditions

2.15 CAISI COMPONENTS SETUP FOR OPERATION

Prior to placing the CAISI components into operation in a deployed environment, it is necessary to address the configuration of the network. This section discusses some of the principles of tactical network configuration and the best solutions to be implemented using the various CAISI components. Among the issues that must be addressed prior to deployment are:

1. The number and location of the STAMIS devices requiring network connectivity. In addition, does each STAMIS support a network connection (from Network Interface Card (NIC) to a CAISI hub), or do some STAMIS require the LSAs to connect to the network? These LSAs will have to be configured and distributed prior to deployment.

2. The availability of Internet Protocol (IP) addresses and how they will be distributed.

3. The structure of the network. Connection to MSE may be made through the root CBM (recommended), through one of the other CBMs, or through the router/firewall issued with the SSR Accessory Kit.

The answer to the above questions will determine the placement of the CAISI Bridge and Client Modules in the field, and the configuration required of the STAMIS devices.

2.15.1 CAISI in the MSE Environment. The fielding of multiple bridge modules with the CAISI ensures flexibility in the application of the capabilities to best reflect the using unit's requirements. The following paragraphs describe the use of CAISI in a tactical environment, i.e., with MSE, however users may find that once comfort is achieved with the use of CAISI, there are applications for the components to be used in a garrison environment.

2.15.1.1 CAISI Root CBM. Regardless of the complexity of the fielded network, the importance of the root CBM cannot be overemphasized. One CBM must always be designated as the "root" CBM. It is not essential to do so, but an easy way to keep track of the root is by designating the CBM that makes the connection to MSE at the INE device as the root, and configure it accordingly.

Remember when configuring the network that each CCM must be able to establish radio contact with at least one CBM, and each CBM must be able to establish radio contact with at least one other CBM. The CBMs provide the "relay" function of the network, ensuring that the data continues along the network to its ultimate destination.

Figure 2-28 summarizes the various means of connectivity to the wireless CAISI:

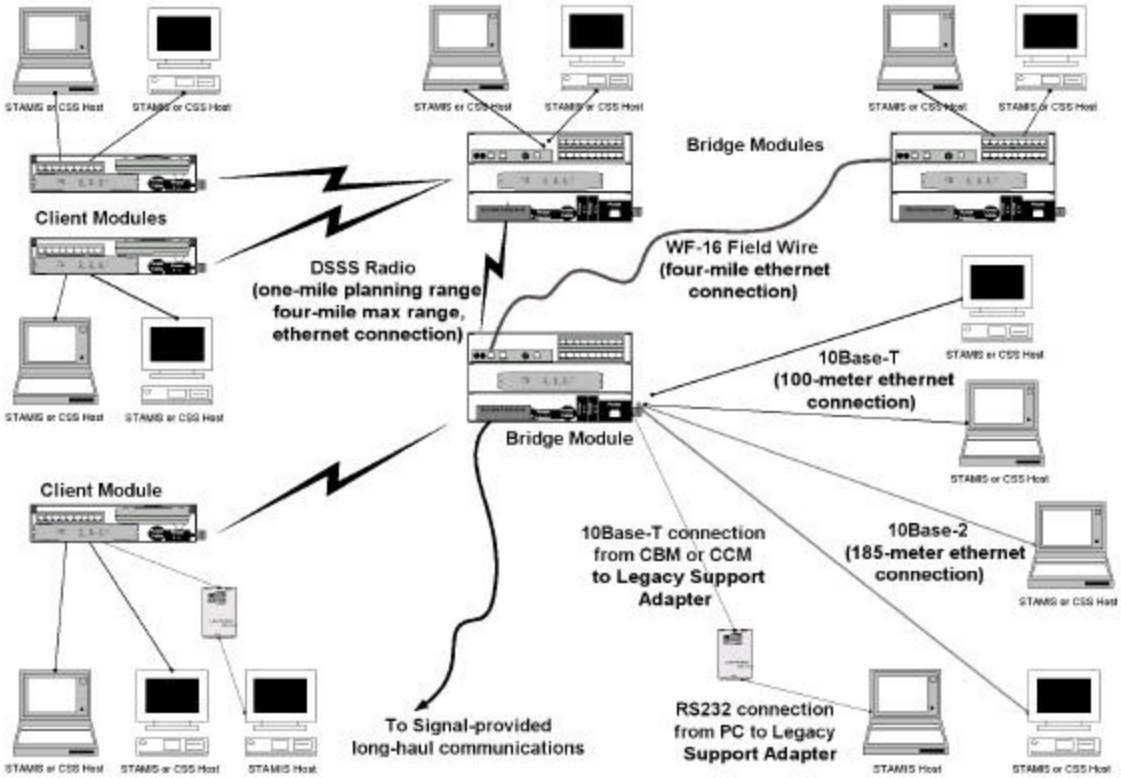


Figure 2-28 CAISI Connectivity

1. STAMIS Connections to the CCMs. Most STAMIS computers will connect to the nearest CCM, using 10BaseT, 10Base2, or the LSA. These connections will be determined based on distance, STAMIS capabilities, and local SOP.

2. CCM Connectivity to a CBM. As depicted in the top center of the above diagram, each CCM must establish connection with a CBM. It is important to note, as depicted above, more than one CCM can establish radio connectivity with the same CBM.

3. CBM Connectivity to a CBM. Each CBM must be able to establish radio contact with at least one other CBM. Each CBM will also support direct STAMIS connections. The CBMs provide the "relay" function of the network, ensuring that the data continues along the network to its ultimate destination.

4. DSL Bridge Connection. In the upper right of the above diagram, there is depicted a DSL connection to the root CBM, using WF-16 field wire. Note that it is not necessary for the DSL Bridge to connect to the root Bridge, any CBM will work.

5. Root CBM to MSE. Again, remember that the root CBM does not have to be the CBM that connects to MSE, however it is often depicted that way for the sake of simplicity.

6. STAMIS to Root CBM. The root CBM is identical to the other CBMs in that it will accept all STAMIS connections as the other CBMs. The same limitations of data cable length apply.

7. CCM to Root CBM. Multiple CCMs may also connect to the Root CBM, using the radios. The Root CBM will provide the same relay functionality through the network as the other CBMs.

2.16 CAISI PREPARATION AND INITIATION. Most CAISI components can be set up within 30 minutes. Through all preparation procedures, keep in mind the following:

CAUTIONS

- Never connect cables when the power is on.
- Never pull directly on cables.
- Always connect and disconnect using the plugs on the end of the cables.
- Provide strain relief (slack) for cables.
- Connections are polarized: Plugs are specific shapes to ensure that they are installed correctly. Always verify plugs match their connectors before installing.
- Make sure UPS power is OFF before inserting its plug into an external power source.

The next few paragraphs involve the unpack, identify, inventory, inspect and actual set up procedures for each of the CAISI components:

UNPACK THE CBM	Paragraph 2.17
UNPACK THE CCM	Paragraph 2.20
UNPACK THE LSA	Paragraph 2.22
UNPACK THE SSR ACCESSORY KIT	Paragraph 2.23
SSR Transit Case	Paragraph 2.24
SSR Notebook Case	Paragraph 2.25
SSR Antenna Carrying Case	Paragraph 2.26
SSR Antenna Mast Carrying Case	Paragraph 2.27

2.17 UNPACK THE CBM. It is essential to select a dry, protected, clean place to locate the CBM prior to unpacking. The logical place to locate the modules is in the tent or shelter that houses the STAMIS computers that will be connecting to the CAISI modules.

WARNING

The CBM transit case weighs 46 pounds – full, 15 pounds - empty. Use safe lift and carry procedures when handling the transit case. This is a **two-person** lift and carry.

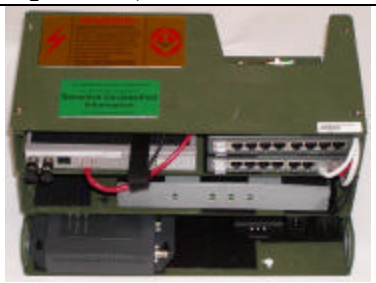
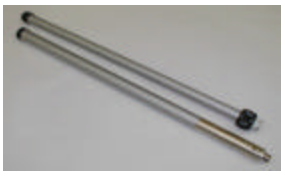
Figure 2-29 CBM Transit Case Overview

Table 2-26 CBM Transit Case - Compartments

Main Compartment	CBM Chassis is in the large cutout. It is positioned so that the lightning arrestor is pointing toward the UPS.
	The UPS is placed in the side hole in the main compartment with the power cable coiled underneath.
Top Compartment (Lid Section)	Panel antenna, whip antenna (separated into two pieces), antenna cables, grounding straps, antenna bracket, barrel connector, Ethernet cables, power supplies and power cables.

The items that you need to unpack will be dependent upon your CAISI deployment. However, you will always need to unpack the following:

Table 2-27 CBM (Minimum Unpack Components)

a. CBM chassis b. Grounding strap c. At least one RF antenna cable (25 foot or 35 foot) d. Antenna bracket e. One antenna (40-inch Whip or 7-inch panel) f. One 2-prong power cable(for the hubs and the Inline encryptor) g. One 3-prong power cable for the wireless bridge h. Uninterruptible Power Supply (UPS)		 a. CBM Chassis
 b. Grounding Strap	 c. 25 ft or 35 ft RF Antenna Cable	 d. Antenna Bracket
 e. 40-inch Whip Antenna or 7-inch Panel Antenna		 f. One 2-Prong Power Cable
 g. One 3-Prong Power Cable	 h. UPS	**NOTE:** *If you intend to use the DSL, you will need an additional 2-Prong Power Cable.*

2.17.1 Unpack the CBM Transit Case

NOTE: *If the pull-up handle on the transit case is extended (Figure 2-30), press the button that says "Push" (Button is on the middle bar) and the push the handle down. In future cases, wheel assemblies will be removed. In that case disregard this note.*

1. Place the CBM transit case on a flat surface or workbench with the front facing you. Case should be on its back.

2. Prior to unlatching, press the pressure release valve located in the front of the CBM. Should hear a hiss sound.

3 Unlatch clips and carefully open transit case lid. Be careful, it is heavy.

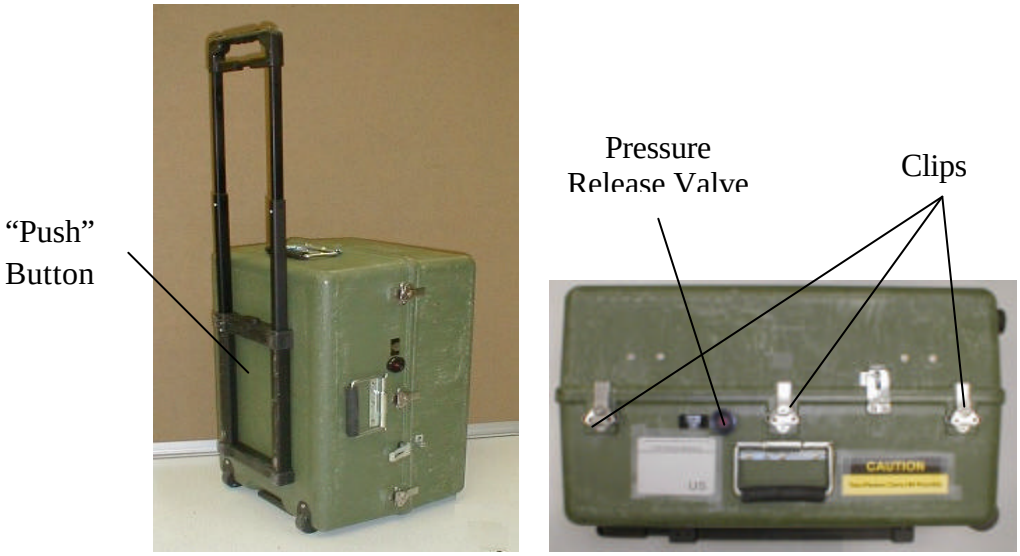
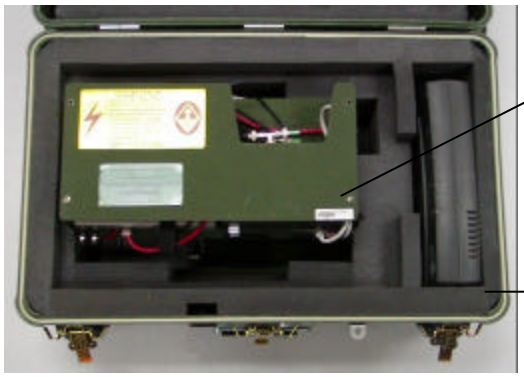


Figure 2-30 CBM Transit Case

WARNING
Keep the transit case closed and latched when not accessing equipment to minimize the probability of injury or clothing snagging on the clasp.

4. Remove the following components from transit case main compartment:



a. CBM Chassis (lightning arrestor is pointing toward UPS)

b. UPS (power cord is coiled underneath it)

Figure 2-31 CBM Transit Case – Main Compartment

5. Access components in the top compartment (lid section):

   a. Unlatch two clips on lid section.

   b. Remove the following components from the lid section.

1. 40-inch Whip Antenna or 7 in Directional Panel Antenna
2. Grounding Strap
3. Barrel Connector
4. 25 foot or 35 foot RF Antenna Cable
5. Antenna Bracket
6. Power Cables
7. Four 42-foot Guy ropes (red clips) on RL-28 reels

Figure 2-32 CBM Transit Case – Top Compartment (Lid Section)

   c. Leave anything you don't need in the lid section and re-latch it.

   d. Close transit case lid and latch clips.

2.17.2 Identify CBM Components.

NOTE: *Individual components are described in Table 2-29.*

1. The **CBM Chassis** comes in four pieces: Base section, center section, upper section and a lid.

   a. **Base section** – contains the Cisco Aironet Wireless Bridge, Lightning arrestor and the power supplies for all devices contained in the chassis (left to right - wireless bridge, DSL, hub and encyptor).

   b. **Center section** – contains the Air Fortress AF-1100 inline encryptor.

   c. **Upper section** – contains an ADC PairGain 300SBP synchronous Digital Subscriber Line (DSL) modem and two Addtron or Farallon 9-port 10Base-T hubs.

   d. **Lid** – serves as a protective cover, shielding the components of the upper section from outdoor elements.

      A cut out in the upper right section allows the user to easily view the Light Emitting Diodes (LEDs) on the back of the hubs and connect coaxial cable to 10Base2 BNC connectors.

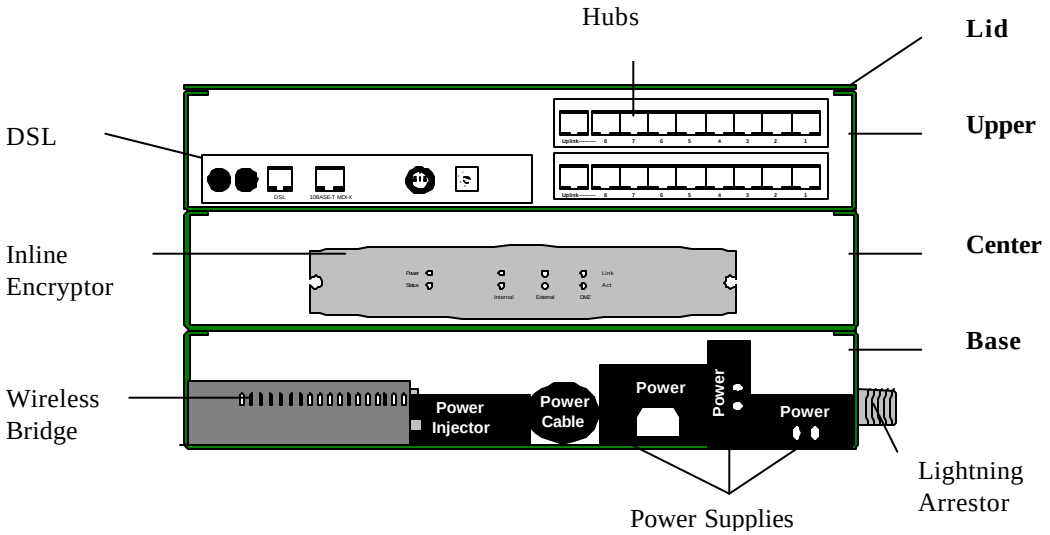


Figure 2-33 CBM Chassis Sections

Table 2-28 CBM Chassis Components

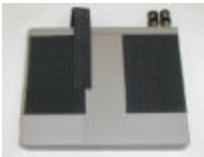
Wireless Bridge a	DSL Bridge b 	Hubs (Qty 2) c
Inline Encryptor d	Power Supply & Power Injector f or Wireless Bridge e	Power Supply for DSL Bridge f
Power Supply for Hubs & Encryptor g	Terminator & "T" Connector (2 of each) h	18-inch coaxial 10Base-2 Cable i
Lightning Arrestor j	12-inch RF Antenna Cable k	Ethernet Cables (2 Red Crossover and 2 White Straight-through) l

Table 2-29 CBM Chassis Components Description

Wireless Bridge 	a. **Wireless Bridge.** Cisco Aironet Wireless Bridge BR-352. The wireless bridge can track up to 2048 clients in the bridge table. The bridge works on U.S. channel set, at 100mW power with a 128-bit encryption. The wireless bridge serves three functions: 1. Acts as a bridge (talking to other bridges). 2. Acts as an access point (connecting clients by radio). 3. Acts as a radio relay (allowing remote bridges and radio clients to connect to the central node).
NOTE: *The wireless bridge is connected to the "external/encrypted ports of the encryptors – the untrusted ports. The data flows through the encryptor is protected, but the communications amongst the radios are not. Only the "external" radio link is encrypted, not the "internal/unencrypted" (LAN) link (connected to the hub).*	
In Figure 2-34, the illustration explains the following: (Numbers in figure correspond to the bullets.) 1. The bridge in one of the CBMs is the "root" node. It controls the network, telling the other bridges, adapters, and NICs what to do and to whom to talk. It controls frequencies, timing, routing and traffic flow. It can direct traffic in order to maximize throughput across the entire network. It also accomplishes all of the non-root tasks listed below. 2. The bridges in the non-root CBMs are simultaneously acting as bridges (talking to other bridges), relays (passing traffic from other bridges to the root node), and as access points (talking to CCMs and wireless client computers). 3. The CBMs and CCMs normally connect to the nearest bridge. They can instead connect to other bridges that are in range if directed by the user or by the root node to do so, in order to balance the traffic load. 4. The SSR Accessory Kit includes a wireless bridge that can be used as a replacement item or in stand-alone mode to connect a single computer or network device. You may find it convenient to use this wireless bridge to connect the CAISI to the Network Encryption System (NES). (Refer to Paragraph 2.34.1 for the connection procedures). In Figure 2-34, notice that an AirFortress encryptor is required between the NES and the bridge. This gives us plain test data flowing out of the AirFortress into the NES, and out of the NES into the AirFortress.	

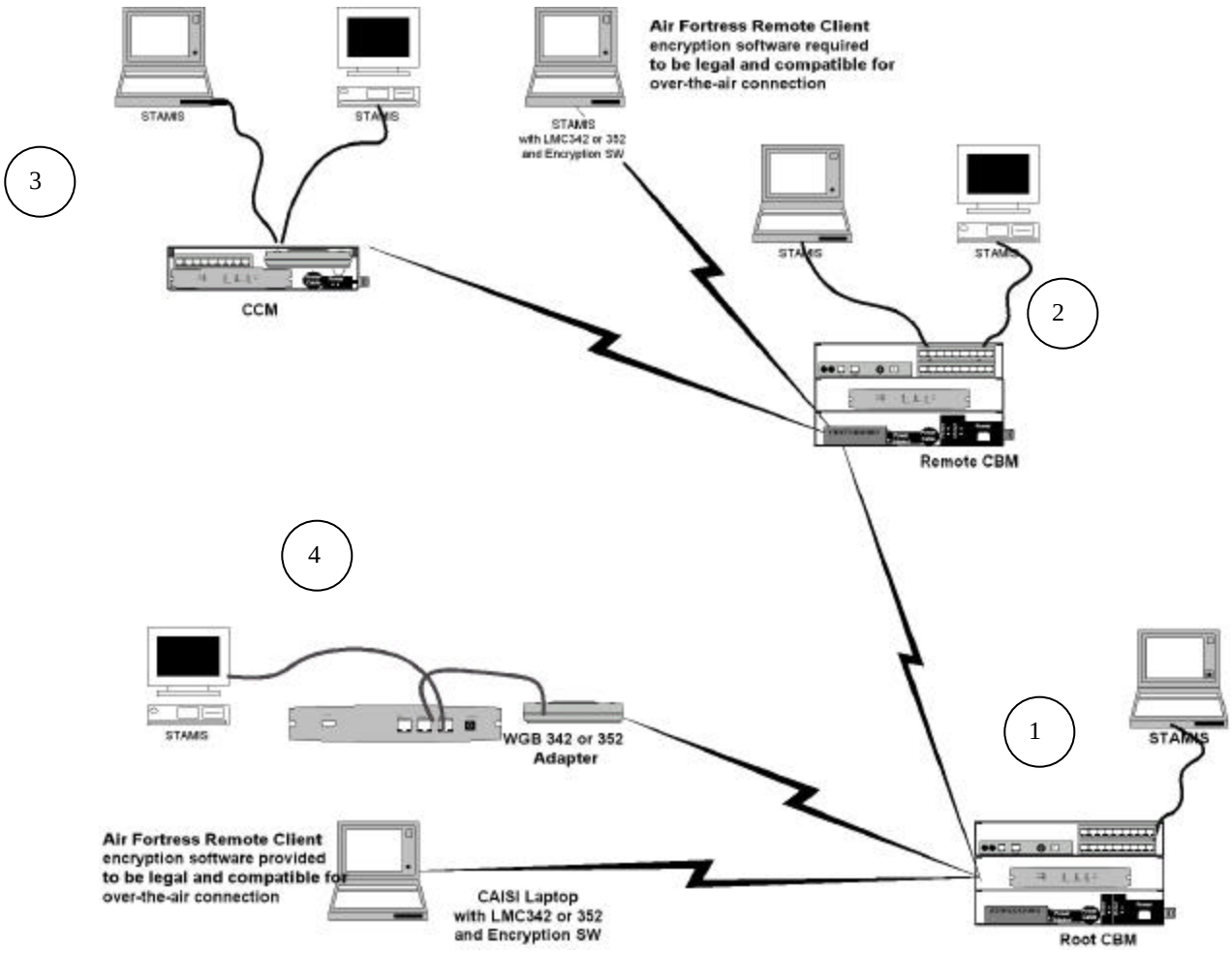


Figure 2-34 Wireless Bridge Deployment

NOTE: *The AirFortress hardware and software(SW) encryptors are shown in the diagram with each radio (the CBM and CCM, include them in the chassis).* ***The encryptors are required. You may not use the radios without them.***

Table 2-29 CBM Chassis Components Description (Continued)

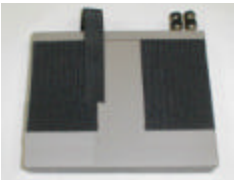
DSL Bridge 	b. **DSL Bridge.** ADC PairGain 300 SBP synchronous DSL modem. The **DSL** can be used instead of or in addition to the wireless bridge to connect to another CBM when there is no Line of Sight (LOS) or when the units must observe radio silence. It is similar to the DSL modem or cable modem that you might have at your home to connect you to the Internet. It provides a high-speed access over a single pair of WF-16 field wire. Other field wire can be used also (WD-1, WD-1a).

Table 2-29 CBM Chassis Components Description (Continued)

Basically, the DSL is a protocol converter. It takes the network traffic on its LAN port and retransmits it onto the DSL port, using a different protocol to allow it to go a long distance (up to 4 miles) over field wire. As a bridge, of course, it retransmits only those packets that it needs to. Normally network traffic can only go about a 100 meters over Category (CAT) - 5 Ethernet cable or up to 185 meters over large, heavy coaxial cable (10Base-2/RG-58). The CAISI DSL bridge can go up to four miles over field wire. And field wire is much easier to deploy, recover and repair. We would, of course, prefer not to run any field wire at all. The DSL is included in CAISI for those circumstances where you cannot use the wireless bridges, or where it is easier to use the DSL. The wireless radios use an extremely high radio frequency (and therefore create very short radio waves). These microwaves are easily absorbed by obstacles, so they need a pretty clear line-of-sight from one radio to the next. Heavy vegetation, hills and buildings all degrades the signal strength of the wireless bridge. The DSL bridges give you an alternate means of communication when dealing with Mission, Enemy, Terrain and Weather, Troops available, and Time available (METT-T) factors. In Figure 2-35, the DSL bridge in a CBM is connected to the DSL bridge in another. STAMIS or CSS network clients are connected to the hubs in the CBMs.
NOTE: *Besides the fact that you have to run wire, the DSL bridges have one other major disadvantage when compared to the wireless bridges. They are point-to-point. That is to say, each DSL bridge can be connected to only one other. To connect two points, you need a pair. To interconnect three work centers, you would need two pairs of DSL bridges. For each additional work center, you need an additional DSL* ***pair,*** *not just one more DSL. The wireless bridges, on the other hand, operate in point-to-multipoint mode. You need only one per workstation. They can talk to more than one at a time, and even relay for each other.*

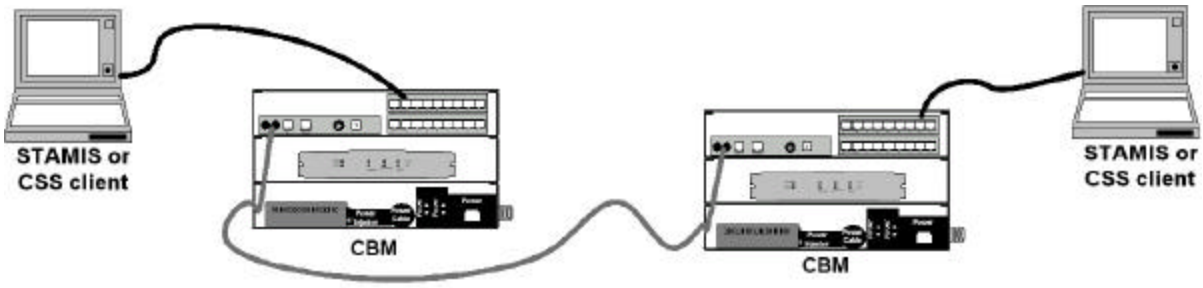


Figure 2-35 Normal DSL Bridge Deployment

NOTE: *The SSR Accessory Kit includes a DSL that can be used as a replacement item or in stand-alone mode to connect a single computer or network device. You may find it convenient to use this DSL to connect the CAISI to the Network Encryption System (NES). (Refer to Paragraph 2.34.2 for the connection procedures).*

Table 2-29 CBM Chassis Components Description (Continued)

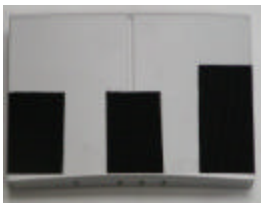
Hub (Qty 2) 	c. **Hubs.** Addtron or Farallon 9-port hub. Each hub has eight 10Base-T ports and one 10Base-2 port. The CBM contains two hubs. One 10Base-T port is used to connect to the inline encryptor (white straight-through Ethernet cable) and another is connected to the DSL Bridge (Red crossover Ethernet cable). The remaining fourteen 10Base-T ports are available to connect computers to gain network access.
Inline Encryptor 	d. **Inline Encryptor**: The Fortress Technologies AirFortress AF-1100 is a dedicated security device placed in the Ethernet link between the radio and the hubs in the CBM. CAISI is a combat service support system. As such, it handles Sensitive Unclassified Information (SUI), also referred to as Sensitive But Unclassified (SBU) data. This traffic must be protected when it traverses the wireless portion of the local network.
All traffic is encrypted prior to transmission over the wireless portion of the local network. It utilizes Triple Data Encryption Standard (3DES) encryption and is FIPS 140-1 compliant. Security protocol 802.11b. **NOTE:** *The AirFortress is not intended or certified to protect classified traffic. It is strictly for the SBU CAISI network.* The AirFortress is an inline encryptor that uses encryption and authentication techniques that are strong enough to protect this data. The AirFortress encrypts the IP packet (header and data) prior to transmission. Every other AirFortress checks the MAC address in the encrypted packet to see if it is for a computer or other network device connected to them. If not, they ignore it. If it is for a connected host, the receiving AirFortress decrypts and authenticates the packet prior to passing it on to that host. If the packet cannot be decrypted, or if it fails authentication, the AirFortress drops it. The AirFortress is a National Institute of Standards (NIST) – approved cryptographic device to protect your data. The radio has wired equivalent privacy (WEP) keys, but it is not secure enough to protect your data on its own. The encryptor is connected between the radio and the hubs. The encryptor uses an Access ID as a key. The encryptor operates at the data link layer, therefore it only works locally. The TCP/IP header is encrypted, so routers cannot route the packet.	
Remote Encryptor Software Client. The AirFortress Remote Client software works exactly like the hardware encryptor, except that it operates on the client computer. It encrypts and decrypts the network traffic as it is passes in and out of the computer. It sits between the computer and the NIC – in the same way that the AF-1100 sits between the hub and the radio. A mix of equipment is shown on Figure 2-34. Notice that the AirFortress hardware and software encryptors are shown in the diagram with each radio (the CBM and CCM include them in the chassis). **The encryptors are required. You may not use the radios without them.**	

Table 2-29 CBM Chassis Components Description (Continued)

Power Supply & Power Injector for Wireless Bridge	e. **Power Supply & Power Injector for Wireless Bridge.** Power supply and injector are permanently connected. The network connection passes through the injector and picks up a 48-volts DC to power the bridge. **CAUTION:** Do not use this injector with the multi-client radio adapter in the CCM. The radio can be damaged if you do so.
Power Supply for DSL Bridge	f. **Power Supply for DSL Bridge.** Power supply for the DSL Bridge. (The word PAIRGAIN is written on the power supply)
Power Supply for Hubs & Encryptor	g. **Power Supply for Hubs & Encryptors.** A power supply with three leads. 5V (Only power supply with three leads)
Terminator & "T" Connector (2 of each)	h. **Terminator & "T" Connector.** Terminator is a device placed on the end of the "T" connector to prevent a data signal from attempting to travel in that direction. "T" Connector is a T-shaped device with two female ends and one male BNC Connector end.
18-inch coaxial 10Base-2 Cable	i. **18-inch coaxial 10Base-2 Cable.** Coaxial cable that connects the two hubs together using the BNC ports.
Lightning Arrestor	j. **Lightning Arrestor.** The lightning arrestor protects the electrical components of the CBM from excessive voltage resulting from lightning by grounding the discharge.

Table 2-29 CBM Chassis Components Description (Continued)

12-inch RF Antenna Cable	k. **12-in RF Antenna Cable.** This antenna cable connects the wireless bridge to the lightning arrestor.
White Straight-Through Ethernet Cable (Qty 2) Red Crossover Ethernet Cable (Qty 2)	l. **White Straight-through Ethernet Cable** – used to connect network capable devices used in the network. This cable is used to connect different devices, such as computer – hub or radio – hub. **One straight-through cable connects the hub to the encryptor (internal/unencrypted port).** **The other straight-through cable connects the power injector (AP/Bridge port) to the wireless bridge (Inline Power Ethernet port).** **Red Crossover Ethernet Cable** – a network cable that crosses the transmit and receive line. It's used to connect hubs and switches together using standard Media Dependent Interface - Crossover (MDI-X) ports, which are already crossover ports. This cable is used to connect like devices, such as computer – computer or hub – hub. **One crossover cable connects the hub to the DSL Bridge** **The other crossover cable connects the encryptor (External/Encrypted port) to the power injector (network port) for the wireless bridge**.

2. Other CBM components: are explained in further detail in Table 2-30. (Stored in the top compartment or lid section of the CBM transit case)

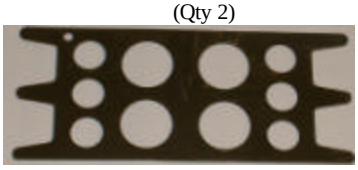
Table 2-30 CBM Components Description

Grounding Strap	a. **Grounding Strap** - serves as the path from the CBM to the earth. It is therefore, very important and must be constructed properly to ensure a good path to the ground. It is a 20-foot cable.

Table 2-30 CBM Components Description (Continued)

RF Antenna Cables 	b. **Radio Frequency (RF) Antenna Cables** – The CBM is issued with a 25 ft and 35 ft RF antenna cables. Which cable you require will be determined by the following: 1. The location of your CBM 2. Where you assemble the antenna 3. How the cable is routed from the CBM to the antenna. **NOTE:** *Use a smaller cable (length) for less decibel (dBi) loss.*
Barrel Connector 	c. **Barrel Connector** – if you cannot reach from the CBM to the antenna using either one of your RF antenna cables, you can connect the 25 ft and 35 ft cables together using the barrel connector. (Smaller the cable, the less decibel (dBi) loss).
Antenna Bracket 	d. **Antenna Bracket** – used to mount the omni-directional or the "7x7" panel antenna to a camouflage pole or mast. Consists of 2 small U-Bolts, 2 medium U-Bolts, 2 large U-Bolts, 12 wing nuts, and 12 washers.
7" Directional Panel Antenna 	e. **Directional 'Panel' Antenna (7-inch)** – METT-T (Mission, Enemy, Terrain, Troops and Time available) factors might require you to use the panel antenna. The 7- inch panel antenna is directional, concentrating most of the radio's power in one direction. This allows you to communicate over long distances or to minimize emissions in the direction of the enemy. Use of this antenna will reduce your ability to support CCMs that are not in the direct path of your radio beam.
Omni-Directional Whip Antenna 	f. **Omni-Directional "Whip" Antenna** – a 40-inch break-apart whip antenna. Unlike the "panel" antenna, the "whip" antenna is omni-directional and can pick up signals from all directions.

Table 2-30 CBM Components Description (Continued)

2-prong Power Cable (Qty 2) 	g. **Power Cables** – 2-prong (1 is used for the hubs and the encryptor and another is used with DSL bridge). 3-prong power cable is used with wireless bridge	3-prong Power Cord
UPS 	h. **Uninterruptible Power Supply (UPS)** - provides complete power protection to your entire CBM set-up. 280 VA of battery backup maintains your Internet connection, allowing you to work online through short blackouts or safely shut down during longer ones. Battery backup is 10 – 20 minutes.	
White Straight-through Ethernet Cable 	i. **White Straight-through Ethernet Cable** – used to connect network capable devices used in the network. This cable is used to connect different devices, such as computer – hub or radio – hub.	
Red Crossover Ethernet Cable 	j. **Red Crossover Ethernet Cable** – a network cable that crosses the transmit and receive line. It's used to connect hubs and switches together using standard Media Dependent Interface - Crossover (MDI-X) ports, which are already crossover ports. This cable is used to connect like devices, such as computer – computer or hub – hub.	
Guy Rope – 42ft (Red clip) (Qty 4) 	k. **Guy Rope – 42ft – red clip –** Provided to assist the operator in securing the position of the panel antenna. Four antenna guy ropes (two per RL-28 reel) are issued with each CBM transit case.	
Reel Unit for Guy Ropes (Qty 2) 	l. **Reel Unit for Guy Ropes** - two guy ropes above per reel unit. RL-28 is the nomenclature.	

NOTES:

1. Media dependent interface (MDI) is the Institute of Electrical and Electrical Engineers (IEEE) standard for the interface to unshielded twisted pair (UTP) cable.

2. For two devices to communicate, the transmitter of one device must connect to the receiver of the other device.

3. The connection is established through a crossover function, which can be a crossover cable or a port that implements the crossover function internally.

4. Ports that implement the crossover function internally are known as MDI-X ports, where X refers to the crossover function.

5. The transmitter of one device to connect to the receiver of another device, the total number of crossovers must always be an odd number.

6. A computer NIC is always MDI and hub or switch ports are usually MDI-X, thus they can be connected with a straight-through cable.

7. When connecting one hub or switch to another, you must either use a crossover cable or connect to an MDI port on one and an MDI-X port on the other.

8. Out of 8 pins in a RJ-45, only pins 1 (Transmit +), 2 (Transmit -), 3 (Receive +), 6 (Receive -) are used. Pins 4, 5, 7 and 8 are not used.

9. Crossover pin connections: pin 1 – pin 3; pin 2 – pin 6; pin 3 – pin 1; pin 6 – pin 2.

Table 2-31 Straight-Through/Crossover Cabling

Straight-through Cable			Crossover Cable		
Wire		Becomes	Wire		Becomes
1	→	1	1	→	3
2	→	2	2	→	6
3	→	3	3	→	1
6	→	6	6	→	2

NOTE: *Procedures on how to make a straight-through or crossover Ethernet cable is in Paragraph 3.12(9d).*

Figure 2-36 shows which components are MDI and MDI-X.

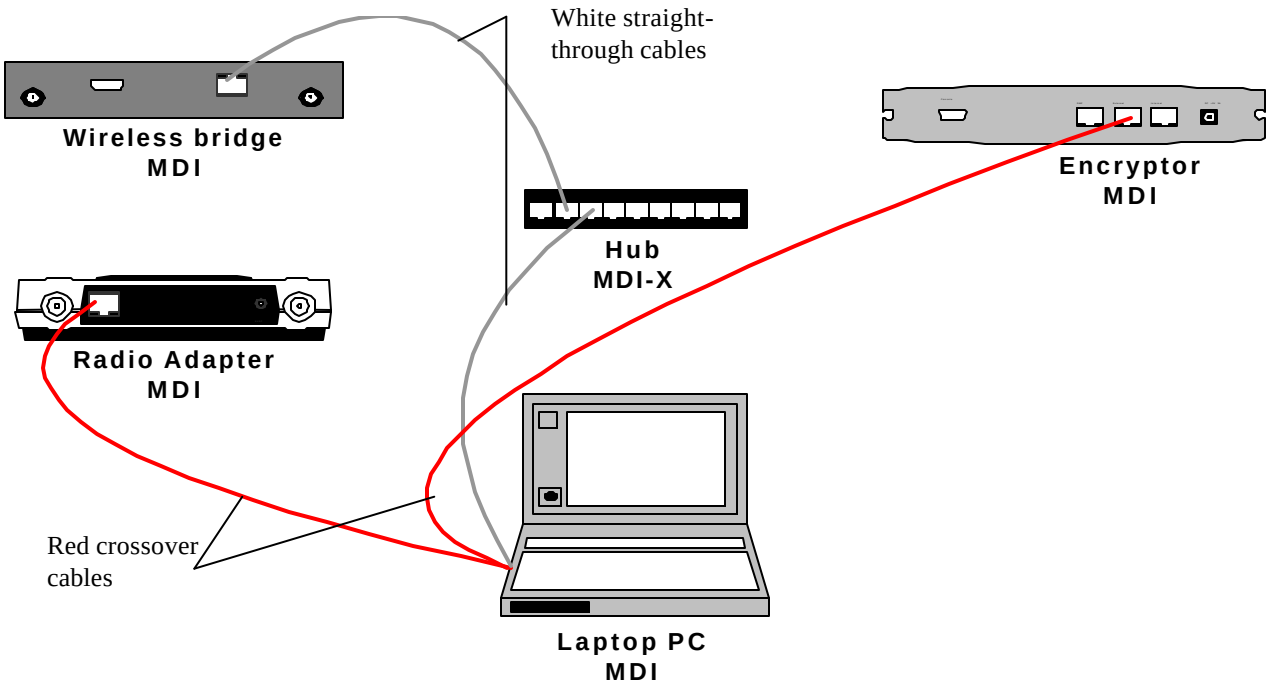


Figure 2-36 CAISI Components MDI/MDI-X

In Figure 2-36, the computer NIC, wireless bridge, multi-client radio adapter, encryptor are all MDI ports. However, the hubs have MDI-X ports.

A computer NIC is always MDI and hub or switch ports are usually MDI-X, thus they can be connected with a straight-through cable.

When connecting a MDI port to a MDI port, you must use a crossover cable. In Figure 2-36, the Laptop PC can connect to the Wireless Bridge, Radio Adapter or the Inline Encryptor with a red crossover cable.

When connecting one hub or switch to another, you must either use a crossover cable or connect to an MDI port (usually the Uplink port) on one and an MDI-X port on the other with a white straight-through cable.

2.17.3 Inventory CBM Transit Case.

1. Locate CBM Transit case inventory checklist card (shown below).

Table 2-32 CBM Inventory Checklist Card

Component	QTY	Date			
Transit Case	1				
CBM Chassis	1				
UPS	1				
7-inch Panel Antenna	1				
40-inch break-apart Whip Antenna	1				
25-foot RF Antenna Cable	1				
35-foot RF Antenna Cable	1				
Barrel Connector	1				
Antenna Bracket for Whip Antenna or 7-in Panel with U-bolts	1				
Grounding Strap	1				
3-Prong Power Cable	1				
2-Prong Power Cable	2				
White Straight-Through Cable	1				
Red Crossover Ethernet Cable	1				
Guy Ropes – 42ft (Red Clips)	4				
Reel Unit for Guy Ropes (Containing above, two guy ropes per reel unit)	2				

2. Identify each item on inventory checklist card.
3. Verify that the CBM chassis and all ancillary components are present.
4. Annotate any discrepancies or shortages on DA Form 2404 or 5988E.

2.17.4 Inspect CBM Components.

NOTE: *Refer to User PMCS Table 2-24 for specific items to look for.*

1. Inspect front and back of transit case for signs of damage.
2. Look for broken components.
3. Check for cut or frayed cables.
4. Check UPS for signs of damage.
5. Verify terminators are in good condition.

2.18 SET UP THE CBM. It is essential to select a dry, protected, clean place to locate the CBM prior to unpacking.

The logical place to locate the modules is in the tent or shelter that houses the STAMIS computers that will be connecting to the CAISI modules. Put it on a table or shelf in your tent or vehicle (not on the ground). You can use the transit case as a table if you need to.

2.18.1 Connect the Grounding Strap to the CBM. It is essential when working with antennas to properly ground the equipment. The lightning arrestor protects the electrical components of the CBM from excessive voltage resulting from lightning by grounding the discharge. The only time you do not need the grounding strap is when you don't need a lightning arrestor – when the antenna is indoors, such as when installed inside a building or the motor pool office.

Follow the procedures below to ground the CBM. For more detail on these procedures, refer to Appendix H of this manual.

Attach the grounding strap to the CBM grounding stud (on the right side of the CBM chassis, next to the lightning arrestor).

1. Loosen and remove the wing nut and washer.

2. Place the grounding strap lug on the stud, replace the washer and wing nut and then tighten the wing nut as tight as you can by hand without using tools.

NOTE: *If you've lost the washer or wing nut, get new ones from the motor pool. The bolt is a standard ¼ inch bolt with 20 threads per inch.*

3. Connect the other end of the grounding strap to a proper ground connection.

NOTE: *The grounding cable must be attached to the generator ground, vehicle ground, or a separate ground of its own. Use a complete ground rod – some come in sections. It must be at least six feet long. The ground rod must be fully sunk in permanently damp earth. In dry or rocky ground, as shown, water it once or twice a day.*

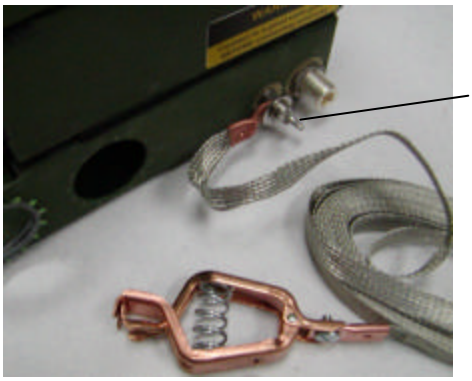


Figure 2-37 Grounding Strap Connected to CBM

Figure 2-38 Grounding Strap Connected to the Ground

2.18.2 Connect the RF Cable to the Antenna and Bracket. Keep in mind the following WARNINGS when erecting any antenna:

WARNING

- Severe injury or death can occur if this equipment, its antennas, or connected communication cables come near electrical power lines. Never erect an antenna closer than twice its height to an electrical line.
- Radios connected to pole-mounted outdoor antennas require lightning arrestors. Do not bypass the lightning arrestors or operate the equipment without a good earth ground. You can be severely injured or killed.

CAUTION

- Never operate a wireless device without an antenna. It can damage the radio.

1. Loosen and remove the two small U-bolts (labeled "strain relief") on the antenna bracket.

2. Loosen but do not remove the medium U-bolts, labeled "Whip Antenna," and the large U-bolts, labeled "Mast."

NOTE: *If you've lost any washers or wing nuts, get new ones from the motor pool. The U-bolts are standard ¼ inch bolts with 20 threads per inch.*

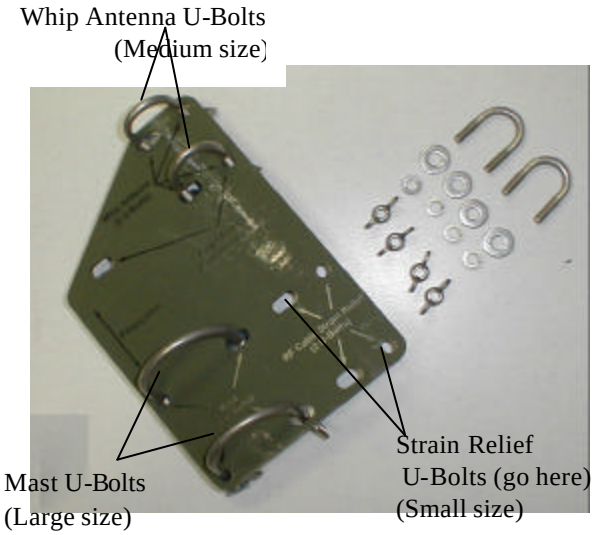


Figure 2-39 "7 in" Antenna Bracket

3. Thread the bottom of the antenna down through the "Whip Antenna" U-bolts. The connector end of the antenna goes down, toward the strain relief bolts.

   Tighten the wing nuts for the Whip Antenna U-bolts. Don't tighten all the way, so that you can rotate the antenna when you are attaching the antenna cable in the next step.

Figure 2-40 Thread Whip Antenna Through U-Bolts

Now connect the antenna cable. The antenna cable has one straight end and one right-angle end.

4. Connect the straight end to the connector on the bottom of the whip antenna. Tighten the cable as tight as you can by hand without using tools.

   (Easiest way to do this is to hold the straight end connector steady and turn the antenna to tighten the cable onto the antenna).

Figure 2-41 Connecting the Antenna to the Bracket

5. Replace the strain relief U-bolts, capturing the cable.

6. Center the connector between the whip antenna bolts and the strain relief bolts.

   There are three studs on the bottom of the connector side of the antenna. Place the first Whip Antenna U-Bolt (bottom one) slightly above these studs.

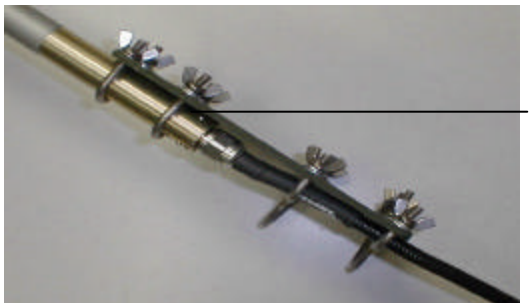


Figure 2-42 Provide Strain Relief

7. Tighten the whip antenna wing nuts as tight as you can by hand without using tools.

8. Tighten the strain relief wing nuts until they touch the cable, then one more half turn. Do **not** over-tighten these wing nuts because you can crimp the cable.

9. Connect the two sections of the whip antenna together. Insert the bottom of the top section into the top of the bottom section. By hand, screw the black plastic retaining ring on the top section down over the threads on the bottom section.

NOTE: *Make sure the two sections fit together tightly, but do not over-tighten the retaining ring. Never use a tool or lubricant on the retaining ring.*

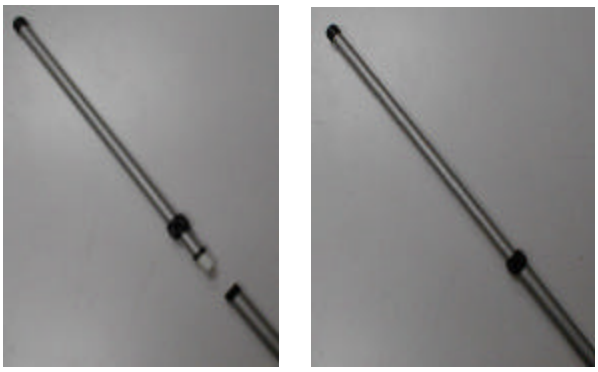


Figure 2-43 Connecting the Whip Antenna

2.18.3 Connect the Bracket to a Camouflage Pole and Erect the Antenna.

WARNING

Ensure the antenna is not erected in the vicinity of power lines or cables.

Good placement of the antenna is crucial. Ideally it should be located and secured next to the tent or shelter the hubs are located in, away from power lines, and placed clearly above any camouflage netting.

Follow the steps below to erect the Antenna:

1. Locate the camouflage pole or mast section you will be connecting to the antenna. (Camouflage pole is not included with CAISI, mast section can come from SSR Antenna Mast Carrying Case if mast is not being used and case is available).

2. Connect the camouflage pole or mast section to the bracket using the U-bolts labeled "Mast". Make sure the antenna and the mast section are lined up so that the antenna will be vertical when installed.

3. Tape the cable to the mast for additional strain relief and so that it does not blow around in the wind.

Figure 2-44 Connecting the Antenna to the Mast

CAUTION

Do not go above 19 feet with camouflage poles. If you need to go above 19 feet, you must use the AB-1244 Antenna Mast rather than a camouflage pole.

4. Position the antenna up through the camouflage net. Ensure that the entire fiberglass section (non-silver) of the antenna extends above the camouflage net.

NOTE:
The standard radar-reflective camouflage nets keep radio signals in as well as they keep radar signals out. The antenna must always protrude from the camouflage.

Figure 2-45 Good Mast Placement - Example 1

The photo to the above right shows an antenna mounted on camouflage net poles and poked through the net. No additional support for the mast was required in the short run, but since the antenna was to remain installed for more than a day, it was secured to the vehicle so that it would not pull on the net or sway in the wind.

5. The omni-directional whip antenna must be installed as near to vertical as possible, otherwise the range is significantly shortened.

Make sure the antenna protrudes above the net.

Normally you want to make sure the antenna is above the highest part of the net.

Figure 2-46 Good Mast Placement - Example 2

The radio in the van under the net in the photo to the above right was located near the edge of the Brigade Support Area (BSA) and no clients were stationed to the right side of it, so it was OK to have the antenna below the top of the net.

NOTE: *If a butterfly clamp for the camouflage net is going to be used, the mast section or camouflage pole must be high enough so that the butterfly clamp goes around the antenna. (**Only the whip antenna's can be used with the butterfly clamp**).*

2.18.4 Connect the RF Cable to the CBM Chassis.

1. Locate an appropriate opening in the vehicle, tent or shelter to run the cable through to the module.

   Do not run it through a vehicle or shelter doors, since they must be closed at night to maintain light discipline.

   The photo to the right shows two antenna cables entering a shelter through a hole in the signal entrance panel, but most vehicles do not have such a hole.

   Use your imagination to find a way in -- through holes, vents, or other openings. You need a hole one inch in diameter to get the connector through. The cable itself is only 3/8 inches in diameter.

Figure 2-47 RF Cable Entering Shelter

2. As you run the cable, loop it just before it enters the vehicle, shelter, or tent so that any rain or snow melt running down the cable will drip outside and not run all the way down the cable to the equipment.

   If you cannot put the drip loop outside, put it inside, but be sure to position it in such a way that moisture will not be able to get to the antenna connector on the CBM. If moisture gets into the connector, it can short out the antenna and limit your ability to communicate or even damage the radio.

Figure 2-48 Cable Loop inside Shelter

3. Attach the antenna cable to the wireless equipment's external antenna connector (on the right side next to the grounding strap.

   Tighten the connector as tight as you can by hand without using tools. It should not wiggle. If it does, then continue tightening it while wiggling it.

NOTE: *If the connection is not tight, your transmission and reception will suffer, and you can damage the radio.*

Figure 2-49 Antenna Cable Connection

2.18.5 Connect the Power Cables to the CBM. There are three power cords to be connected to the CBM. (These are labeled on the chassis case)

1. Attach the 3-prong power cable to the wireless bridge power supply in the front of the bottom section of the CBM. It is the leftmost of the three power supplies.

2. The DSL power supply sits in the middle and should not be connected unless the DSL is going to be used.

3. Connect the 2-prong power cord to the hub and encryptor power supply. It is the rightmost of the three power supplies.

4. Place the UPS next to the CBM chassis.

5. Plug the two or three cords into the section on the UPS labeled "Battery Backup Protected Outlets."

   Do not plug anything except the CBM into these outlets. This UPS is not big enough to power your office. If you plug your coffee pot into it, you will damage the UPS-- and possibly damage the coffee pot too.

Figure 2-50 CBM Power Connections

Figure 2-51 UPS Power Connections

2.18.6 Plug the UPS into 110VAC power.

CAUTION

Before applying power to the CBM and CCM, ensure antennas and cables are properly erected and connected. Failure to do so may cause damage to the equipment.

1. Plug the UPS into a grounded outlet and turn it on.

(The rocker switch is labeled with symbols resembling an "I" (IN) and an "O" (OUT). Power is on when the IN side of the switch is in. The green power light should come on.)

The lights on the radio, hubs, and encryptor in the CBM should also come on. Look inside the CBM for the lights.

NOTE: *(Refer to Paragraph 2.2 – 2.7 for explanation of lights (LEDs) on CBM components.)*

Figure 2-52 UPS Power Connections On/Off Switch

NOTE: *The UPS must be plugged in before it will turn on. This is a safety feature, to keep it from turning on by accident during transit. Once the UPS comes on, it operates normally. If power is lost, the UPS will stay on, running on battery power and it will beep every few seconds. .*

2.18.7 Connect Your Computers.

Now that the CBM is installed, you are ready to operate. Connect your computers.

1. Connect one end of a standard white or gray Category-5 Ethernet cable to the Legacy Support Adapter or network interface card (NIC) on your computer.

2. Connect the other end to any empty port on the hub in the CBM, except the one labeled "UpLink."

   NOTE: *Computers are always connected to the numbered ports.*

Two cables are shown in Figure 2-53: Port 1 on the top hub and Port 8 on the bottom hub. (Any port could be used).

NOTE: *The "UpLink" port is normally used to connect to another hub. It is wired differently than the numbered ports and comes with a plug in it, as shown to the right. If you use the "UpLink" port to connect another hub, move the plug from the "Uplink" port to Port 8. Port 8 and the "UpLink" port are connected together internally. You can use one or the other, but not both at the same time.*

Figure 2-53 Connect STAMIS Computers to CBM

When you connect your computer and turn it on, the link lights on your NIC and the hubs will come on. Look down through the cutout in the lid to see the link lights on the hubs inside the back of the CBM.

Figure 2-54 Hub LEDs after Connection of STAMIS

2.18.8 Connect to the INE Device. One CBM, usually the one designated as the root, will connect to the INE device located with the MSE support. This provides all users access to the TPN.

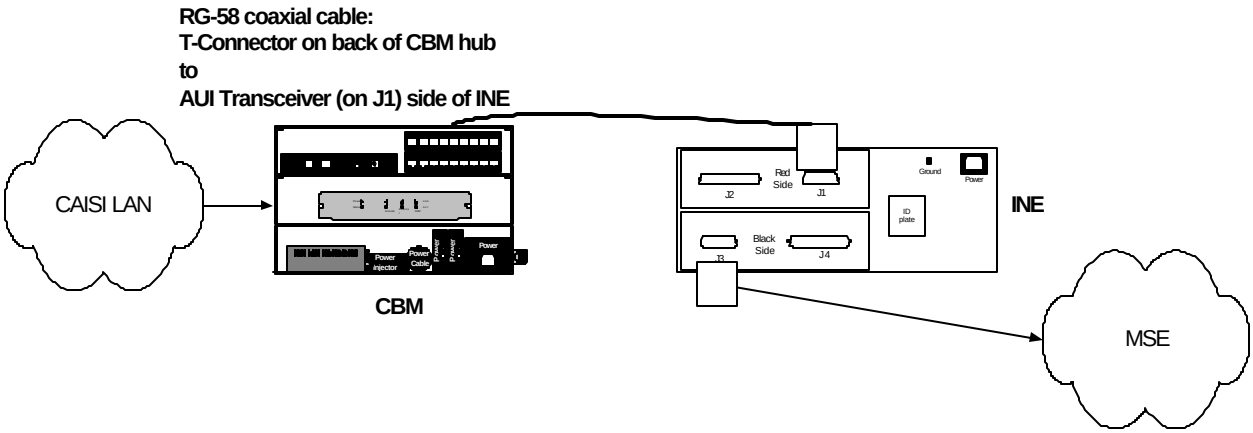


Figure 2-55 Connecting to the INE with RG-58 Cable

1. Remove the 50ohm terminator from the T-Connector on one of the CBM hubs. Place the terminator in the CBM transit case.

2. Connect one end of a RG-58 coaxial cable to the open end of the T-Connector.

   NOTE: *You can connect to the INE using any CBM; it does not have to be the root node. The 10Base-2 coaxial cable maximum length is 185 meters, so the CBM you choose must be less than 185 meters from the INE device.*

Figure 2-56 Terminator and "T" Connector

3. Remove the 50ohm terminator from the T-connector located on the 10Base-2 Auxiliary Unit Interface (AUI) transceiver located on the J-1 port (red side) of the INE device in the MSE.

4. Return the INE terminator to Signal Support.

5. Connect the other end of the RG-58 cable to the 10Base-2 AUI transceiver.

NOTE: *The Signal support will have the 10Base-2 AUI transceivers.*

Overview of INE Power LEDs:

CBM Hub - BNC light will be lit green if connected properly.
INE AUI Transceiver - Link light will be lit green.

NOTE: *Refer to Paragraph 2.34 for other ways to connect to the INE using CAISI components.*

2.19 INSTALLATION OF CBM IN SPECIAL CIRCUMSTANCES.

Occasionally you will need to install the CBM a little differently. You might need to use the DSL Bridge, use the two antenna cables together, or use the directional antenna.

2.19.1 DSL Bridge.

Use the DSL bridge in your CBM when you cannot use the radio because of Mission, Enemy, Terrain, Troops, and Time available (METT-T) factors. You might, for instance, need to communicate during times of radio listening silence or across heavy vegetation, a hill, or a city. If you are told to use the DSL, you will be connecting to the DSL in another CBM.

A single pair of field wire is required. If you have WF-16, use the green pair. Technically, it doesn't matter which pair of wires you use, the green or the brown, as long as both sides are using the same. If something happens to the green wires, a splice,

cut, you can switch over to the brown pair without running the wire again. Field wire can be used up to 4 miles.

If you have WD-1 or other single-pair wire, then just use it. Tie the wire to the handle of the CBM and then connect it to the binding posts. (Same procedures as when using WF-16).

Procedures on how to connect the DSL with WF-16 are listed below:

CAUTION

Contact with the exposed wire connected to the binding posts or direct contact with the metal portions of the binding posts can result in electrical shock. Extreme caution should be taken when handling these items and making this connection.

1. Secure a pair of field wire (WF-16) long enough to reach between the CBMs. (Any single pair wire can be used – WF-16, WD-1,WD-1a).
2. Separate the two wires of the green pair to about three inches.

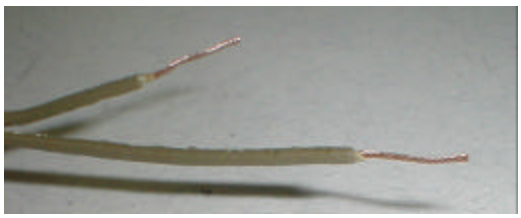


Figure 2-57 Stripped Wire

3. Cut the two green wires so that one is about one inch longer than the other.
4. Strip about 1/2 inch of insulation from the end of each of the green wires.
5. Twist the ends of each of the green wire until all the small wires within it are wound tightly so as to make one.
6. Now strip another quarter inch or so, and slide it to the end of the wire. Leave that short section of insulation on the end of each wire. This prevents "split ends." Twist the ends of wires again to tighten up the newly exposed wire.

Figure 2-58 Stripped Wire – Split Ends

7. Tie the field wire to the lifting and tie-down ring on the left front of the CBM. (This provides additional strain relief).

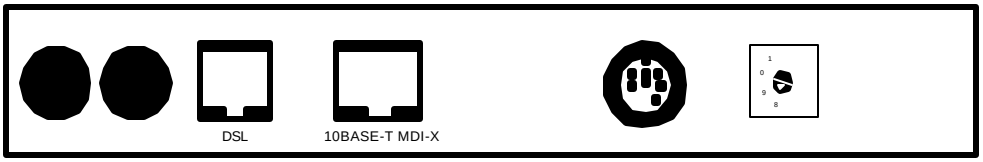
Figure 2-59 Field Wire Connected to CBM Chassis

8. Press the binding post in and insert the wire into the jaws of the binding post as it opens. Release the binding post to close the jaws and capture the wire.

NOTE: *The bare wire portion should only be as large as the jaws of the binding posts.*

Figure 2-60 Field Wire Connected to DSL

9. If required, adjust the transmission speed rate on the Rate Configuration Switch, located on the rear side of the DSL (Figure 2-61). Both ends of the connection must be on the same speed setting in order to connect and communicate. Default speed setting is 8.



1 = 128k	6 = 1536k
2 = 384k	7 = 1792k
3 = 768k	8 = 2048k
4 = 1024k	9 = reserved
5 = 1280k	0 = reserved

Default is 8.
The point end of the triangle points to the desired rate, not the screwdriver slit.

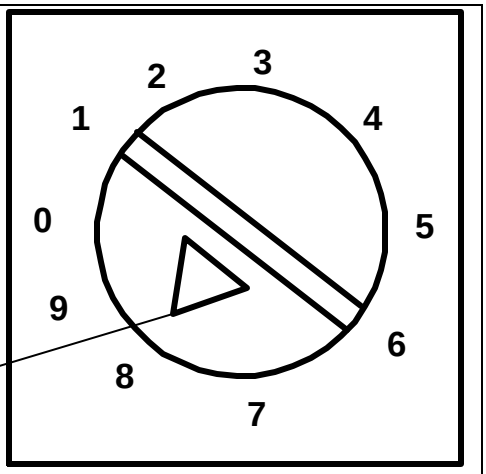


Figure 2-61 Change the Data Transmission Rate (Speed) on DSL

10. If there is a problem to get both connections in sync (synchronization), do the following:

    a. Change both ends of the connection to the slowest speed (1) to see if they can sync up. (MAR LED should stay on if they are in sync).

    b. Change both ends to the next speed (2) to see if they sync. Keep on going to faster speeds until you lose the MAR LED

    c. Once the MAR LED light goes out, go back to the previous speed where the MAR LED light was on.

    NOTE: *Both ends have to work together since the speed settings must match.*

11. Repeat the process with the other CBM.

2.19.2 Directional Panel Antenna

Again because of METT-T factors, you might be told to use your panel antenna. It is directional, concentrating most of the radio's power in one direction. This allows you to communicate over longer distances or to minimize emissions in the direction of the enemy. But it will also reduce your ability to support CCMs that are not in your radio beam. Remember, your CBM not only connects your computers to the network, it acts as an access point for the CCMs and as a relay for other CBMs. **Never use the directional antenna unless directed to do so.**

The procedures for connecting the RF cable to the directional antenna and bracket are the same as those for the whip antenna with the exception of the following:

1. Loosen and remove the two U-bolts labeled "Whip Antenna." They would be in the way of the panel. (Put the U-bolts you removed back into the transit case or tape them to the mast).

   Best way is to put the U-bolts into a ziploc bag in the transit case. Don't put them in your pocket. Whatever you do, don't lose them.

   NOTE: *Ziploc bag, tape and velcro straps are not included with CAISI.*

2. Loosen and remove the two U-bolts labeled "Strain Relief".

3. Position the panel antenna so that the antenna cable connector is at the top.

4. Remove the two wing nuts and washers from the panel antenna.

5. Thread the two mounting studs on the back of the panel antenna through the openings on the bracket labeled, "7 in. panel antenna". (The wording on the bracket will still be seen. The panel attaches to the other side of the bracket as shown in the photo to the right)

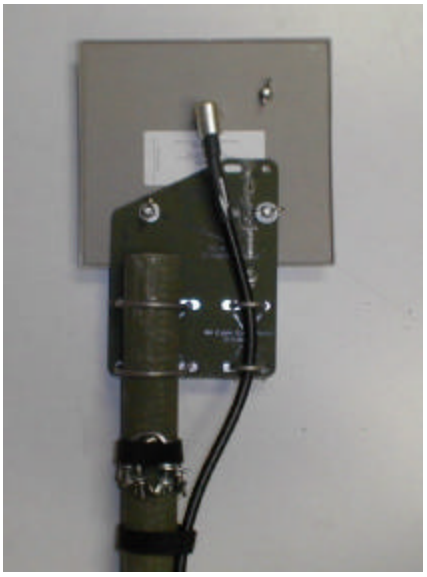


Figure 2-62 Connecting the Panel Antenna

6. Replace the wing nuts and washers on the mounting studs of the panel antenna.

7. Tighten the wing nuts as tight as you can by hand without using tools.

8. Connect the right-angle end of the antenna cable to the panel.

9. Replace the strain relief U-bolts on the bracket in order to secure the antenna cable.

10. Connect the bracket to the mast or camouflage pole and erect it. This procedure is in Paragraph 2.18.3.

11. Tape the antenna cable to the pole for additional strain relief. (Velcro straps could also be used).

12. Secure the panel antenna under **windy conditions**.

NOTE: *The following procedures to secure the position of the panel antenna need only be performed when there is wind. By securing the antenna bracket with guy ropes you will prevent the antenna from turning and will help stabilize the camouflage pole. If there is no wind you may skip this procedure and begin at number (13.*

a. The antenna bracket has a hole on each side, above the lower U-bolt holes. Connect one red guy clip into each hole.

b. Connect a second red guy clip on each side by clipping it into the first guy clip. The hole is not big enough to take two clips, so the second clip attaches to the first.

Figure 2-63 Connect Guy Ropes to Antenna Bracket

c. Erect the pole through a seam or opening in the camouflage net. The panel antenna always extends above the camouflage since it cannot go on the poles with the spreader and because it needs a clear signal path in the direction that it is aimed.

d. Aim the antenna in the general direction of the distant end (usually the root radio).

e. Fan the guys out about 45 degrees to the left and right of the direction the antenna is aimed. You may need to reach through the opening in the net and throw the guys to the edge of the net so that you can reach them from the ground at the outside of the net.

f. Using left-over camouflage net stakes, stake the guys down at or near the edge of the camouflage net.

g. Using the guys, aim the antenna and make sure you have communications.

h. Adjust the guys until they are all tight, with the antenna still aimed in the right direction.

13 Secure the panel antenna under **normal weather conditions**.

a. Position the antenna up through the camouflage net. Ensure that the entire antenna extends above the camouflage net.

b. Point the flat side of the panel toward the root CBM or the closest CBM with contact to the root. Follow these procedures:

(1) Rotate the mast until the antenna is aimed in the general direction of the root CBM or relay CBM (the smooth flat side is toward the target). You can do this visually if you can see the target, otherwise use a map and compass.

NOTE: *Contact the SSR for the use of the Link Status Meter (LSM) on the SSR notebook to be used to refine the aim of the antenna. Refer to the Software User Manual (SUM), TB 11-5895-1691-10, Paragraph 4.1.2.*

(2) Secure the mast so that it cannot rotate. Wrap rope or twine tightly around the base of the mast about eight times, tie it off, and run it to a stake or fixed object. (Rope, twine, stake or fixed object not provided with CAISI).

14 To connect the RF cable to the wireless equipment's external antenna connector, follow the procedures in Paragraph 2.18.4.

2.19.3 Long Antenna Cable using Barrel Connector.

If the antenna cable cannot reach from the CBM to the antenna using either one of your RF antenna cables, you can connect them together to make a longer one by using the barrel connector.

Screw one end of each cable onto the barrel connector.

You could also get a 50 ft RF antenna cable from the SSR Accessory Kit if you do not wish to use the barrel connector.

(Smaller the cable, the less dBi loss)

Figure 2-64 Barrel Connector

2.20 UNPACK THE CCM. It is essential to select a dry, protected, clean place to locate the CCM prior to unpacking. The logical place to locate the modules is in the tent or shelter that houses the STAMIS computers that will be connecting to the CAISI modules.

The CCM carrying case weighs 10 pounds - full, 1 pound - empty. Use safe lift and carry procedures when handling the carrying case.

Figure 2-65 CCM Carrying Case

Table 2-33 CCM Carrying Case - Compartments

Main Compartment	The 24-inch Whip antenna and antenna cable
CCM Chassis Compartment	CCM Chassis (The lightning arrestor points to the inside (the smallest compartment) not toward the outside of the case)
Bracket and Miscellaneous (Misc) Compartment	Grounding strap, Antenna Bracket with U-Bolts, Power Adapter

2.20.1 Unpack the CCM Carrying case.

1. Place the CCM carrying case on a secure table and remove its contents.

   a. CCM chassis
   b. Grounding strap
   c. 35 ft. RF antenna cable
   d. Antenna bracket
   e. 24 in. omni-directional “whip” antenna
   f. 2-prong power cable

2.20.2 Identify CCM Components

NOTE: *Individual components are described in Table 2-35.*

1. The **CCM Chassis** comes in two pieces:

   a. **Base section** - holds a workgroup bridge multi-client radio adapter, an encryptor, a nine-port hub, lightning arrestor and a single power supply:

   (One power supply is used for the multi-client radio adapter, inline encryptor and the hub)

   b. **Lid** – serves as a protective cover, shielding the components from outdoor elements. A cut out in the upper left section allows the user to easily view LEDs on the back of the hub and connect coaxial cable to 10Base2 BNC connector.

   A small cut out in the right front section allows the user to easily view the radio lights.

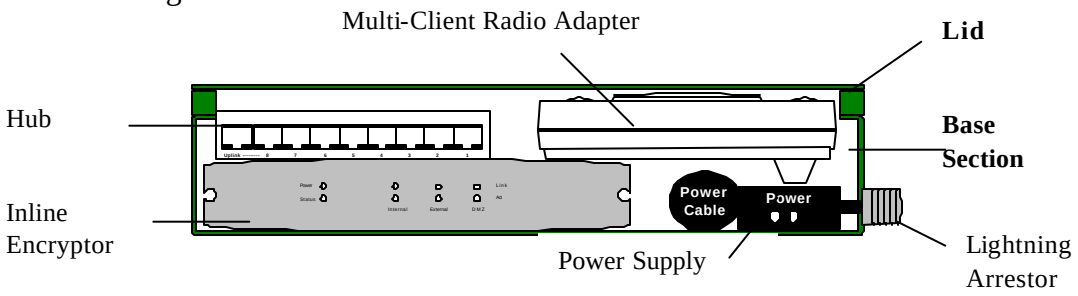


Figure 2-66 CCM Chassis Sections

Table 2-34 CCM Chassis Components

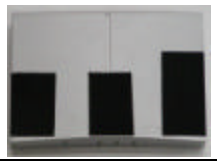
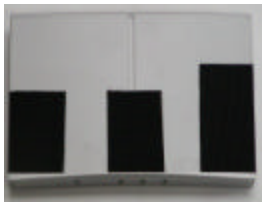
Multi-Client Radio Adapter a	Inline Encryptor b 	Hub c
Power Supply for Radio, Encryptor & Hub d	Terminators (Qty 2) & "T" connectors (Qty 1) e	Lightning arrestor f
12-inch RF antenna cable g	Ethernet Cables (1 Red Crossover and 1 White Straight-through) h	

Table 2-35 CCM Chassis Components Description

Multi-Client Radio Adapter 	a. **Multi-Client Radio Adaptor.** The multi client radio adapter (also known as a workgroup bridge) is similar to a wireless bridge, but its capabilities are much more limited. It can only serve 8 client computers at the same time, and it cannot serve as a radio relay. It also cannot serve as an access point because a client cannot see another client. WGB-342 and WGB-352 are identical except that the WGB-342 is white and has a 30mW power out, while the WGB-352 is gray and has a 100mW power out.
Inline Encryptor 	d. **Inline Encryptor**: The Fortress Technologies AirFortress AF-1100 is a dedicated security device placed in the Ethernet link between the radio and the hub in the CCM. CAISI is a combat service support system. As such, it handles Sensitive Unclassified Information (SUI), also referred to as Sensitive But Unclassified (SBU) data. This traffic must be protected when it traverses the wireless portion of the local network.

All traffic is encrypted prior to transmission over the wireless portion of the local network. It utilizes Triple Data Encryption Standard (3DES) encryption and is FIPS 140-1 compliant. Security protocol 802.11b.

NOTE: *The AirFortress is not intended or certified to protect classified traffic. It is strictly for the SBU CAISI network.*

The AirFortress is an inline encryptor that uses encryption and authentication techniques that are strong enough to protect this data. The AirFortress encrypts the IP packet (header and data) prior to transmission. Every other AirFortress checks the MAC address in the encrypted packet to see if it is for a computer or other network device connected to them. If not, they ignore it. If it is for a connected host, the receiving AirFortress decrypts and authenticates the packet prior to passing it on to that host. If the packet cannot be decrypted, or if it fails authentication, the AirFortress drops it.

The AirFortress is a National Institute of Standards (NIST) – approved cryptographic device to protect your data. The radio has wired equivalent privacy (WEP) keys, but it is not secure enough to protect your data on its own. The encryptor is connected between the radio and the hubs. The encryptor uses an Access ID as a key. The encryptor operates at the data link layer, therefore it only works locally. The TCP/IP header is encrypted, so routers cannot route the packet. (**Item also issued with CBM)**

Remote Encryptor Software Client. The AirFortress Remote Client software works exactly like the hardware encryptor, except that it operates on the client computer. It encrypts and decrypts the network traffic as it is passes in and out of the computer. It sits between the computer and the NIC – in the same way that the AF-1100 sits between the hub and the radio.

A mix of equipment is shown on Figure 2-34. Notice that the AirFortress hardware and software encryptors are shown in the diagram with each radio (the CBM and CCM include them in the chassis). **The encryptors are required. You may not use the radios without them.**

Table 2-35 CCM Chassis Components Description (Continued)

Hub 	c. **Hub.** Addtron or Farallon 9-port hub. The hub has eight 10Base-T ports and one 10Base-2 port. One 10Base-T port is used to connect to the encryptor. The remaining seven 10Base-T ports are available to connect computers to gain network access. A total of 8 computers can connect to one CCM using all ports (10Base-T and 10Base-2). **(Item also issued with CBM)**
Power Supply for Radio Adapter, Encryptor & Hub 	d. **Power Supply for Radio Adapter, Encryptor & Hub.** A power supply with three leads. 5V **NOTE:** *The radio adapters do not use the power injector. They have a 5-volt DC power input. If you connect one to a power injector that belongs to the wireless bridge, the voltage present on the Ethernet port can damage the radio.*
Terminator (Qty 2) & "T" Connector (Qty 1) 	e. **Terminator & "T" Connector.** Terminator is a device placed on the ends of the "T" connector to prevent a data signal from attempting to travel in that direction. "T" Connector is a T- shaped device with two female ends and one male BNC Connector end. **(Item also issued with CBM)**
Lightning Arrestor 	f. **Lightning Arrestor.** The lightning arrestor protects the electrical components of the CCM from excessive voltage resulting from lightning by grounding the discharge. **(Item also issued with CBM)**
12-inch RF Antenna Cable 	g. **12-in RF Antenna Cable.** This antenna cable connects the multi-client radio adapter to the lightning arrestor. **(Item also issued with CBM)**

Table 2-35 CCM Chassis Components Description (Continued)

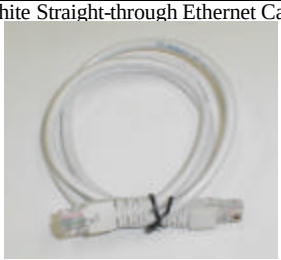
White Straight-Through Ethernet Cable	h. **White Straight-through Ethernet Cable** – used to connect network capable devices used in the network. This cable is used to connect different devices, such as computer – hub or radio – hub. **Straight-through cable connects the hub to the encryptor (internal/unencrypted port).**
Red Crossover Ethernet Cable	**Red Crossover Ethernet Cable** – a network cable that crosses the transmit and receive line. It's used to connect hubs and switches together using standard Media Dependent Interface - Crossover (MDI-X) ports, which are already crossover ports. This cable is used to connect like devices, such as computer – computer or hub – hub. **Crossover cable connects the Encryptor (External/Encrypted port) to the Ethernet port on the Radio Adapter.**

3. Other CCM components: are explained in further detail in Table 2-36. (Stored in CCM Carrying case)

Table 2-36 CCM Components Description

Grounding Strap	a. **Grounding Strap** - serves as the path from the CBM to the earth. It is therefore, very important and must be constructed properly to ensure a good path to the ground. It is a 20-foot cable. **(Item also issued with CBM)**
RF Antenna Cables	b. **Radio Frequency (RF) Antenna Cables** – The CCM is issued a 35 ft RF antenna cables. **(Item also issued with CBM)**
Antenna Bracket	c. **Antenna Bracket** – used to mount the omni-directional or the "7x7" panel antenna to a camouflage pole or mast. Consists of 2 small U-Bolts, 2 medium U-Bolts, 2 large U-Bolts, 12 wing nuts, and 12 washers. **(Item also issued with CBM)**

Table 2-36 CCM Components Description (Continued)

Omni-Directional Whip Antenna	d. **Omni-Directional "Whip" Antenna** – a 24-inch whip antenna. Unlike the "panel" antenna, the "whip" antenna is omni-directional and can pick up signals from all directions.
White Straight-through Ethernet Cable 	e. **White Straight-through Ethernet Cable** – used when configuring the multi-client radio adapter. **(Item also issued with CBM)**
2-prong Power Cord	f. **Power Cord** – 2-prong power cord, which supplies the multi-client radio adapter, hub and encryptor with power. **(Item also issued with CBM)**

2.20.3 Inventory CCM Carrying Case

1. Locate the CCM carrying case inventory checklist card

Table 2-37 CCM Inventory Checklist Card

Component	QTY	Date			
Carrying Case	1				
CCM Chassis	1				
24-inch whip antenna	1				
35-foot RF antenna cable	1				
Antenna Bracket for whip antenna with U-bolts	1				
Grounding Strap	1				
White Straight-through Ethernet Cable	1				
2-Prong Power Cord	1				

2. Identify each item on inventory checklist card

3. Verify that the CCM chassis and all ancillary components are present.

4. Annotate any discrepancies or shortages on DA Form 2404 or 5988E.

2.20.4 Inspect CCM Components.

NOTE: *Refer to User PMCS Table 2-24 to look for specific items.*

1. Inspect inside and outside of carrying case for signs of damage.

2. Look for broken components.

3. Check for cut or frayed cables.

2.21 SET UP THE CCM

2.21.1 Connect the Grounding Strap to the CCM. Same procedures as CBM in Paragraph 2.18.1.

Figure 2-67 Grounding the CCM

2.21.2 Connect the RF Cable to the Antenna and Bracket. Same procedure as CBM in Paragraph 2.18.2.

2.21.3 Connect and Erect the Omni-Directional Antenna. Same procedure as CBM in Paragraph 2.18.3.

2.21.4 Connect the RF Cable to the CCM Chassis. Same procedure as CBM in Paragraph 2.18.4.

2.21.5 CCM Power Cable Connections. There is a single power cord for the CCM.

Attach the 2-prong power cable to the power supply in the front center of the CCM. Plug it into the nearest available 110VAC to 240VAC power outlet. A surge suppressor power strip is preferred, but not required.

The lights on the radio, encryptor, and hub in the CCM should come on. Look inside the CCM for the lights.

(Refer to Paragraph 2.8 for description of lights (LEDs)).

Figure 2-68 CCM Power Cord Connection

2.21.6 Connect Your Computers to the CCM.

Now that the CCM is installed, you are ready to operate. Connect your computers. Connect one end of a standard white or gray Category-5 Ethernet cable to the Legacy Support Adapter or network interface card (NIC) on your computer. Connect the other end to any empty port on the hub in the CCM, except the one labeled "UpLink." Computers are always connected to the numbered ports. Four cables are shown in the photo below to connect four STAMIS computers.

NOTE: *The "UpLink" port is normally used to connect to another hub. It is wired differently than the numbered ports and comes with a plug in it, as shown to the right. If you use the "UpLink" port to connect another hub, move the plug from the "Uplink" port to Port 8. Port 8 and the "UpLink" port are connected together internally. You can use one or the either, but not both at the same time.*

Figure 2-69 Connect STAMIS Computers to CCM

When you connect your computer and turn it on, the link lights on your NIC and the hub will come on. Look down through the cutout in the lid to see the link lights on the hubs inside the back of the CCM.

2.22 LSA. The LSA is used to when a STAMIS device can not connect to the CBM/CCM using a standard 10Base-T or 10Base-2 connection. This may be due to limitations of hardware (no NIC), or software that is unable to support a TCP/IP connection. The LSA network-enables this type of STAMIS device. LSAs most be used in pairs in other words a LSA will only talk to another LSA.

NOTE: *Setup procedures are in Paragraph 2.35.3*

2.22.1 Unpack the LSA. It is essential to select a dry, protected, clean place to locate the LSA prior to unpacking it. The logical place to locate the LSA is next to the STAMIS computer that will be connected to it. The LSA will be stored near the CAISI system. At this time, an LSA box is not provided, just the individual components.

1. The LSA will be packed in a box for issue to the STAMIS users. The intent is for the STAMIS users to carry this item in their respective STAMIS transit case. Place the LSA transit box on a secure table and remove its contents.

   a. LSA MSS-100
   b. Null Modem Cable (9 – 25 pin)
   c. 3 ft. White Ethernet CAT-5 cable
   d. Power adapter and cable

2.22.2 Identify LSA Components

Table 2-38 LSA Components Description

LSA MSS-100 	a. **LSA MSS-100.** The CAISI LSA MSS-100 provides a virtual circuit from one host computer's serial port to another, over the 10Base-T network. The LSA makes it easy to communicate through the network for any device with a serial interface. It is connected to the STAMIS computer's serial port and then to one of the ports in the hubs on either the CBM or CCM. The MSS-100 provides a multi-protocol support over a 10/100Base-T network. It is programmed using the CAISI Virtual End to End (VEE) software.
Null Modem Cable 	b. **Null Modem Cable** – This is a 9 to 25-pin cable. The cable is used to connect non-network capable devices to the network. It is connected from the computer serial port to the serial port of the LSA. This physical connection of the serial ports simulates what would occur naturally if modems and the phone system were used for file transfer. Null modem cable is the same as a crossover cable. **NOTE:** *Null modem cables are either 18 ft or 25 ft.*

Table 2-38 LSA Components Description (Continued)

White Straight-through Ethernet Cable	c. **White Straight-Through Ethernet Cable** – connects the LSA to the nearest CBM or CCM.	
Power Adapter	Power Cord	d. **Power Adapter and Cord** – provides power to the LSA. Power cord is 3-prong.

2.22.3 Inventory the LSA.

1. Locate LSA Inventory Checklist Card. (Shown below)

Table 2-39 LSA Inventory Checklist Card

Component	QTY	Date			
Legacy Support Adapter, MSS-100	1				
9 to 25-pin Null Modem Cable Adapter	1				
White Straight-through Ethernet Cable	1				
Power Supply	1				
3-Prong Power Cord	1				

2. Identify each item on inventory checklist card

3. Verify that the LSA and all ancillary components are present.

4. Annotate any discrepancies or shortages on DA Form 2404 or 5988E.

2.22.4 Inspect LSA components.

NOTE: *Refer to User PMCS Table 2-24 for specific items to look for.*

1. Inspect inside and outside of transit box for signs of damage.

2. Look for broken components.

3. Check for cut or frayed cables.

2.23 UNPACK THE SSR ACCESSORY KIT.

The components you unpack from the SSR Accessory Kit will depend on mission requirements.

This paragraph will discuss the unpack procedures for these three components in the next 4 paragraphs:

SSR Transit Case	Paragraph 2.24
SSR Notebook Case	Paragraph 2.25
SSR Antenna Carrying Case	Paragraph 2.26
SSR Antenna Mast Carrying Case	Paragraph 2.27

NOTE: *Remember, not all of the individual components of these cases will be used. Only remove the component when it needs to be utilized.*

2.24 SSR TRANSIT CASE.

The SSR transit case is identical to the CBM transit case, with the exception that it is black instead of green and the foam interior has been modified to hold different components.

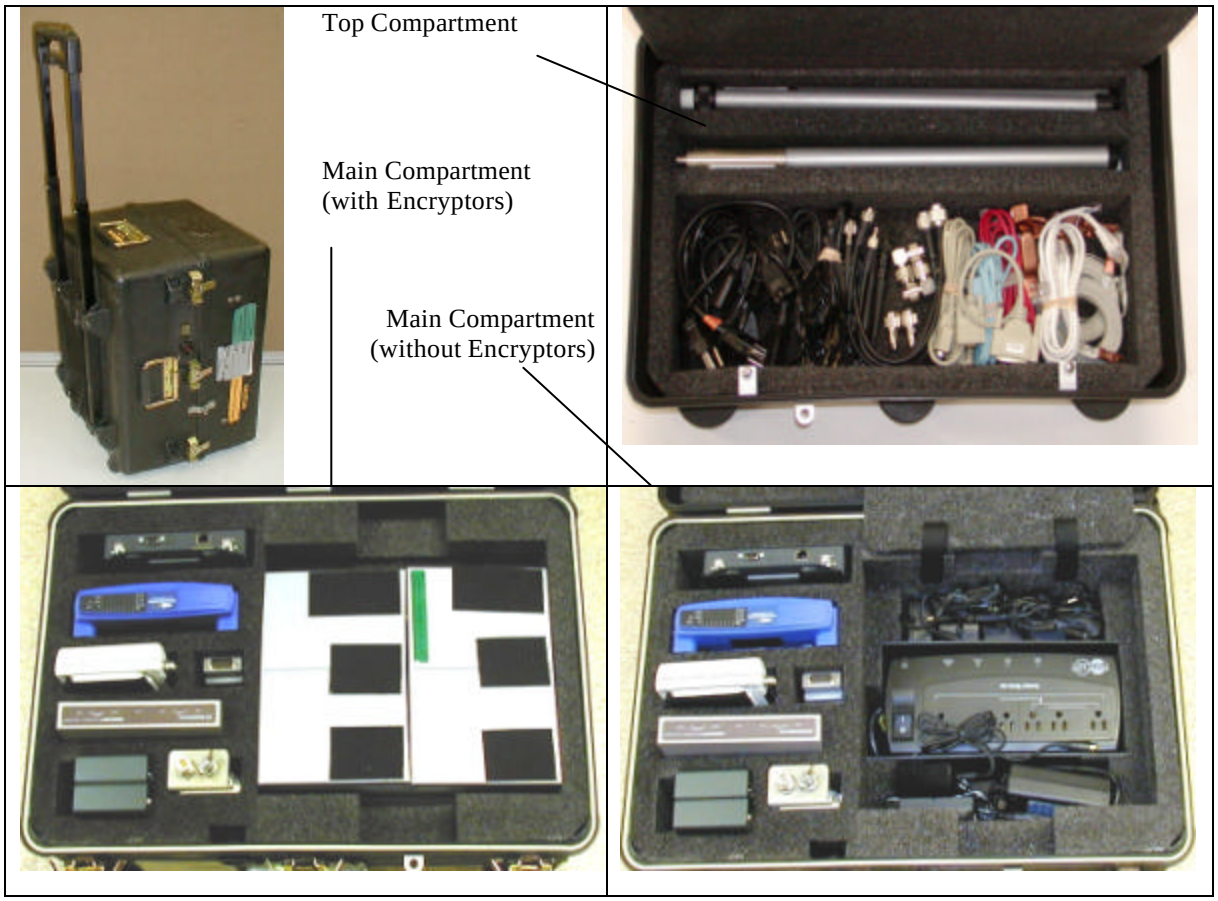


Figure 2-70 SSR Transit Case Overview

The components that you unpack from the SSR Transit case will depend on the mission requirements. Not all of the individual components of this case will be used, therefore only remove the necessary components when they need to be utilized.

NOTE: *When conducting inventory and PMCS, all items should be accounted for and inspected. Table 2-25 contains the specific items of each component to be inspected.*

Table 2-40 SSR Transit Case - Compartments

Main Compartment	Two Inline Encryptors (side by side)
	A black plastic cover folds down over the UPS.
	UPS – is stored in the center. The power cord is coiled and stored below the UPS.
	Power Supplies are on both sides of the UPS. The following power supplies are included: Power supply and injector for wireless bridge, 1 lead, 3 leads, DSL, and Router (There are 10 power supplies)
	The following components go, in order top to bottom, on the left side of the main compartment:
	Wireless Bridge
	Router(s)
	Multi-Client Radio Adapter
	DSL
	Hubs (is stored with the Hubs)
	(In slot to the right of Multi-Client Radio Adapter) 10Base-T Transceiver
	(In slot to the right of the Hubs)
	Lightning Arrestor Assembly - Lighting Arrester mounted on Grounding Plate with Grounding Stud (Qty 2) (Both are stored together, one upside down to the other).
Top Compartment	4-inch whip antenna, cables, cords and miscellaneous items. **NOTE:** *All cables should be coiled and fastened with tape or velcro straps (not provided with CAISI).*
	40-inch Whip antennas have two slots at the top. Store the antenna in two pieces.

2.24.1 Unpack the SSR Transit Case

WARNING

The SSR transit case weighs 46 pounds – full, 15 pounds - empty. Use safe lift and carry procedures when handling the transit case. This is a **two-person lift** and carry.

NOTE: *If the pull-up handle on the transit case is extended, press the button that says "Push" (Button is on the middle bar) and push the handle down. In future cases, the wheel assemblies will be removed. In this case disregard this note.*

1. Place the SSR Transit Case on a secure table, workbench or flat surface with the front facing you. To determine which side of the transit case is the front, look at serial number on the top of transit case. If you can read the serial number, you are at the front of the transit case.

2. **Prior to unlatching**, press the pressure release valve located on the front of the transit case, to release any built-up pressure within the case. Transit case will not open with pressure built-up.

3. Unlatch clips and carefully open transit case lid.

Figure 2-71 SSR Transit Case

CAUTION

Keep the transit case closed and latched when not accessing equipment to minimize the probability of injury or clothing snagging on the clasp.

4. Remove the components required for your deployment from transit case lid and main compartments.

Table 2-41 SSR Transit Case – Main Compartment

a. Inline Encryptors, AirFortress 1100 (Qty 2)	h. 10Base-T Transceiver
b. UPS	i. Lightning Arrestor Assembly – Lightning Arrestor mounted on Bracket (Qty 2)
c. Wireless Bridge, CISCO BR-352	j. Power Supply and Power Injector, 48V, Wireless Bridge
d. Multi-Client Radio Adapter (Workgroup Bridge) Cisco WGB-352	k. Power Supply, 5V, DSL
e. DSL Bridge, Pairgain 300SBP	l. Power Supply, 5V, Router
f. Internal Router, Linksys BEFSR81	m. Power Supply, 5V, 3 Leads (Qty 2)
g. Hubs, Addtron or Farallon 9-port (Qty 2)	n. Power Supply, 5V, 1 Lead, Wall-style (Qty 5)

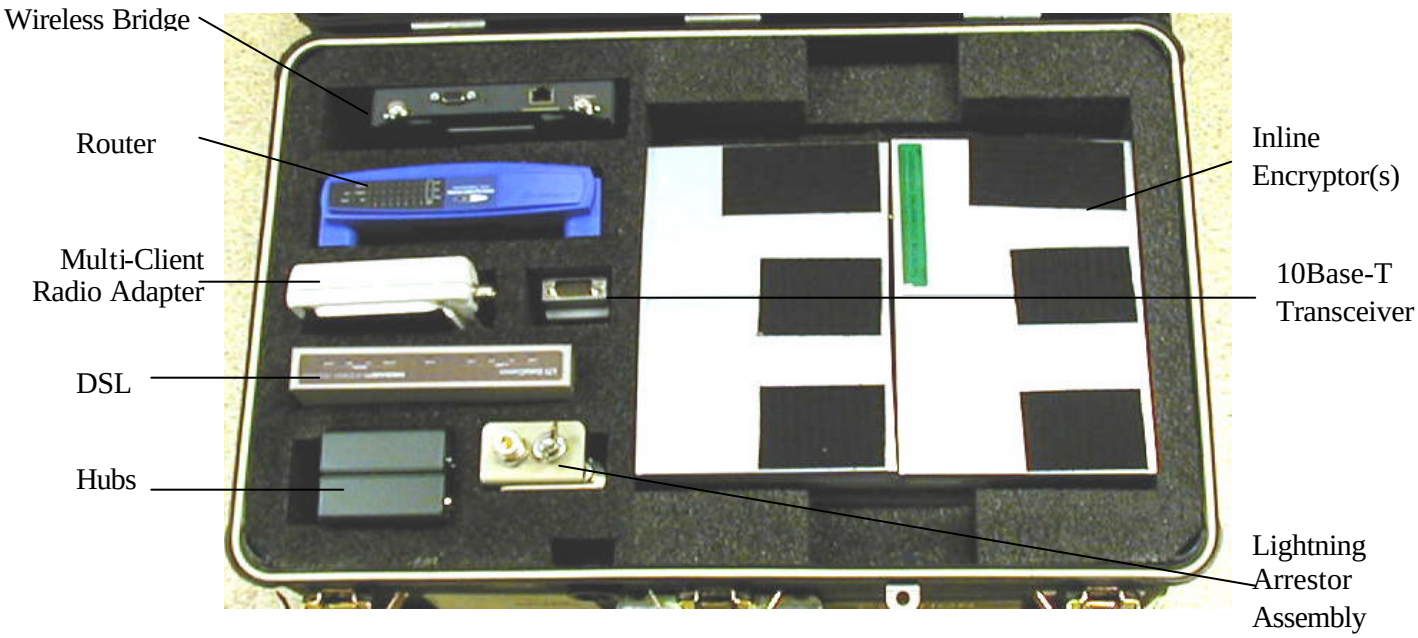


Figure 2-72 SSR Transit Case – Main Compartment (with Encryptors)

Figure 2-73 SSR Transit Case – Main Compartment (without Encryptors)

2.24.2 Identify SSR Transit Case Components.

Table 2-42 SSR Transit Case - Main Compartment Components Description

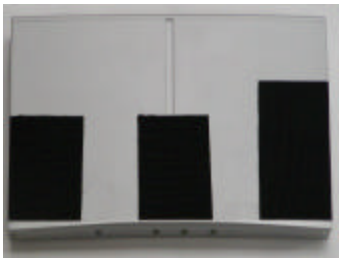
Inline Encryptor (Qty 2) 	a. **Inline Encryptor -** This is a **duplicate item** that comes with the CBM/CCM. A dedicated security device placed in the Ethernet link between the radio and the hubs in the CBM. Security protocol is 802.11b. When the wireless bridge or multi-client radio adapter is used from the SSR Accessory Kit, the inline encryptor must be used. See Paragraph 2.34.1 for connection procedures. More detailed information is in Table 2-29. (Inline Encryptor in the CBM)
UPS 	b. **Uninterruptible Power Supply (UPS) -** This is a **duplicate item** that comes with the CBM. The UPS provides complete power protection to your entire CBM set-up. 280 VA of battery backup maintains your Internet connection, allowing you to work online through short blackouts or safely shut down during longer ones. Battery backup is 10 – 20 minutes.

Table 2-42 SSR Transit Case - Main Compartment Components Description (Continued)

Wireless Bridge	c. **Wireless Bridge.** This is a **duplicate item** that comes with the CBM. The wireless bridge can track up to 2048 clients in the bridge table. The bridge works on U.S. channel set, at 100mW power with a 128-bit encryption. The wireless bridge serves three functions: Acts as a bridge (talking to other bridges), an access point (connecting clients by radio), and a radio relay (allowing remote bridges and radio clients to connect to the central node).
Connection of the wireless bridge is extremely simple, as illustrated in Figure 2-74. A straight-through Ethernet cable runs from the switch or hub and plugs into the "Internal/Unencrypted" port on the encryptor. A red crossover cable runs from the "External/Encrypted" port on the encryptor to the "Network" port on the power injector. A straight-through cable runs from the "AP/Bridge" port on the injector to the "Inline Power Ethernet" port on the back of the bridge. The console port on the bridge is not used, except during configuration.	

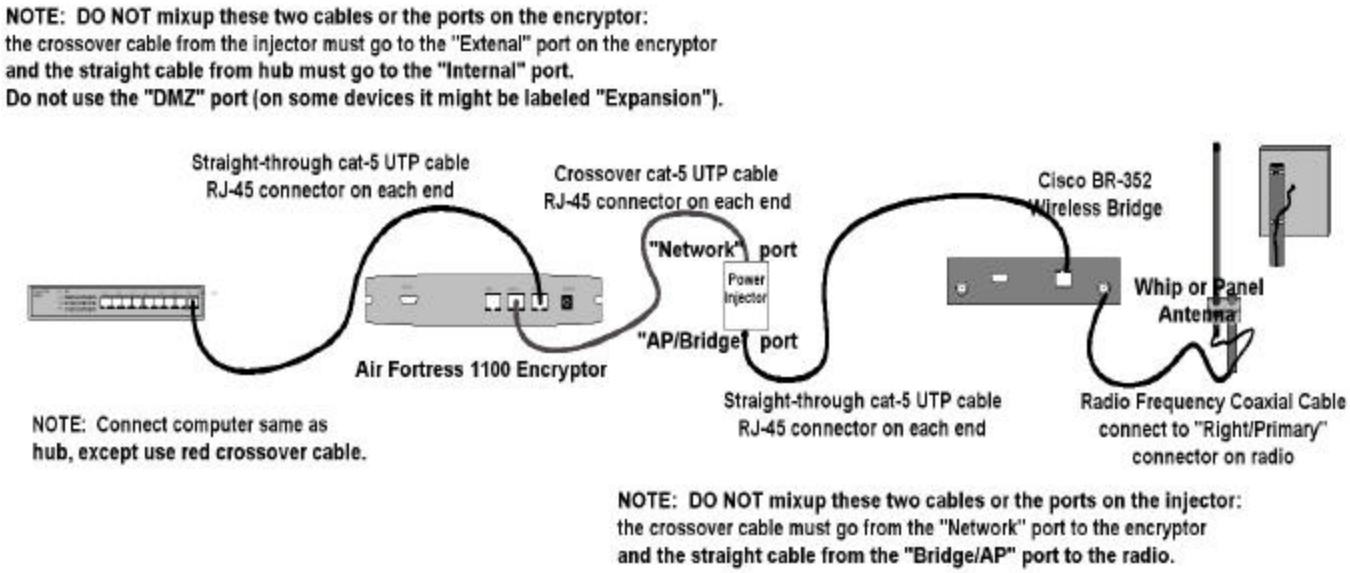
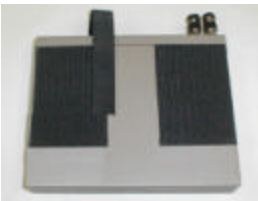


Figure 2-74 Wireless Bridge Cabling

NOTE: *The SSR wireless bridge that can be used as a replacement item or in stand-alone mode to connect a single computer or network device. You may find it convenient to use this wireless bridge to connect the CAISI to the Network Encryption System (NES). See Figure 2-76. (Refer to Paragraph 2.34.1 for the connection procedures).*

Table 2-42 SSR Transit Case - Main Compartment Components Description (Continued)

Multi-Client Radio Adapter	d. **Multi-Client Radio Adaptor.** This is a **duplicate item** that comes with the CCM. The multi client radio adapter (also known as a workgroup bridge) is similar to a wireless bridge, but its capabilities are much more limited. It can only serve 8 client computers at the same time, and it cannot serve as a radio relay. It also cannot serve as an access point because a client cannot see another client. (CCM can not see another CCM) WGB-342 and WGB-352 are identical except that the WGB-342 is white and has a 30mW power out, while the WGB-352 is gray and has a 100mW power out.
DSL Bridge 	e. **DSL Bridge.** This is a **duplicate item** that comes with the CBM. The DSL can be used instead of or in addition to the wireless bridge to connect to another CBM when there is no Line of Sight (LOS) or when units must observe radio silence. It provides high-speed access over a single pair of WF-16 field wire. Other field wire can be used also (WD-1, WD-1a).

The DSL can be connected to a hub or switch or it can be connected directly to a STAMIS or CSS client computer, as shown in below.

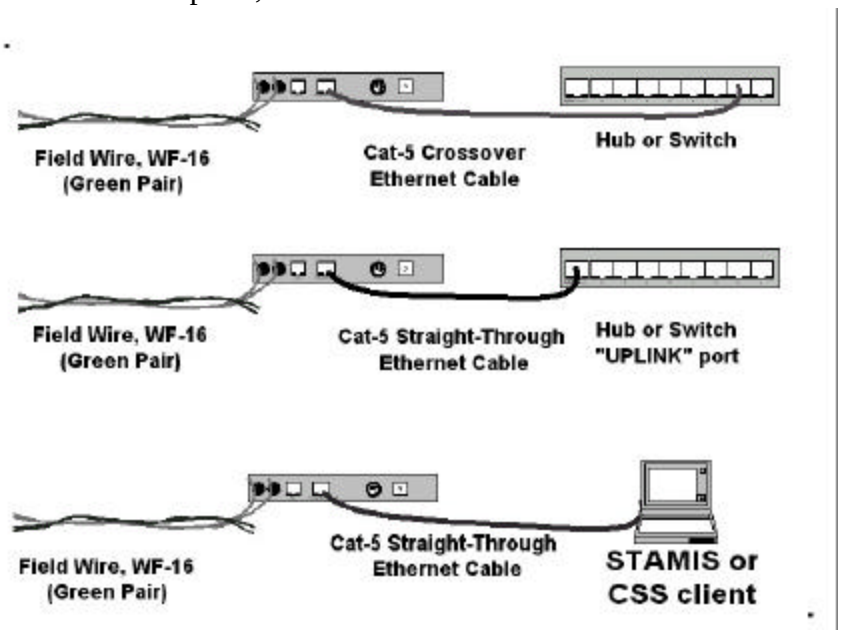


Figure 2-75 DSL Cabling

NOTE: *The SSR Accessory Kit includes a DSL that can be used as a replacement item or in stand-alone mode to connect a single computer or network device. You may find it convenient to use this DSL to connect the CAISI to the Network Encryption System (NES). (Refer to Paragraph 2.34.2 for the connection procedures). See Figure 2-76.*

Table 2-42 SSR Transit Case - Main Compartment Components Description (Continued)

Router 	f. **Router. (SSR Accessory Kit unique item).** (In future versions, the Netscreen NS-5xp will replace the Linksys BEFSR81). Functionality will not change. The Ethernet Cable/DSL Router segments the network to provide firewall security to STAMIS and CSS clients connected behind the firewall. If you choose to use it, it splits the network into two segments – one "public" and one "private."
 Netscreen NS-5xp Router	**Public segment**: 1. The router effectively limits the number of hosts that need to appear on the Public segment to a relatively small number of servers that require connection from clients at other sites or that require Domain Name Server (DNS) entries for their clients to find them. 2. The public segment has IP addresses controlled by Signal or by the Director of Information Management (DOIM) in garrison - usually the CSS S6 or network operations center (NOC). Each host requires an assigned static or dynamic IP registered with the DNS.

Private segment:

1. It serves as a network address translator (NAT) server. This allows non-routable IPs to gain access to Real IPs. The router allows 253 non-routable (private) IPs for one routable (public) IP address. This also allows units to quickly operate in the field with the IPs they use in garrison.
2. It serves as a firewall, Dynamic Host Configuration Protocol (DHCP) server, and gateway for the private segment.
3. It also acts as a traditional router for outbound traffic from the private segment.

NOTE: *Refer to Paragraph I.3.9 for more information on when and how to use the router*

Table 2-42 SSR Transit Case - Main Compartment Components Description (Continued)

Hubs (Qty 2) 	g. **Hubs.** This is a **duplicate item** that comes with the CBM/CCM. 9-port hub. Each hub has eight 10Base-T ports and one 10Base-2 port. The CBM contains two hubs. One 10Base-T port is used to connect to the inline encryptor and another is connected to the DSL Bridge. The remaining fourteen 10Base-T ports are available to connect computers to gain network access. The CCM contains one hub. One 10Base-T port is used to connect the hub to the inline encryptor. The remaining seven 10Base-T ports are available to connect computers to gain network access.
10Base-T Transceiver 	h. **10Base-T Transceiver. (SSR Accessory Kit unique item).** The 10Base-T transceiver is a CentreCOM 210TS. The transceiver is provided in case you need to connect a 10Base-T device to the NES. The NES connection is an Auxiliary Unit Interface (AUI) port. The Signal unit has a 10Base-2 transceiver to allow CAISI to connect using a 10Base-2 cable.
NOTE: *Be sure the Signal Quality Error (SQE) Test Switch (heartbeat) on the side of the transceiver is set to O (off). Slide the switch to the left. Also make sure that both ends of the 10Base-2 connection are terminated.* 	
The 10Base-2 Transceiver has to be removed in order for the 10Base-T transceiver to connect. 10Base-2 connections are available in the CBM, however you may wish to connect the root CBM to the NES with the Wireless bridge or DSL bridge in the SSR Accessory Kit, instead of with a long coax cable or separate remote CBM. The transceiver is shown using the SSR wireless bridge and SSR DSL used as in Figure 2-76.	

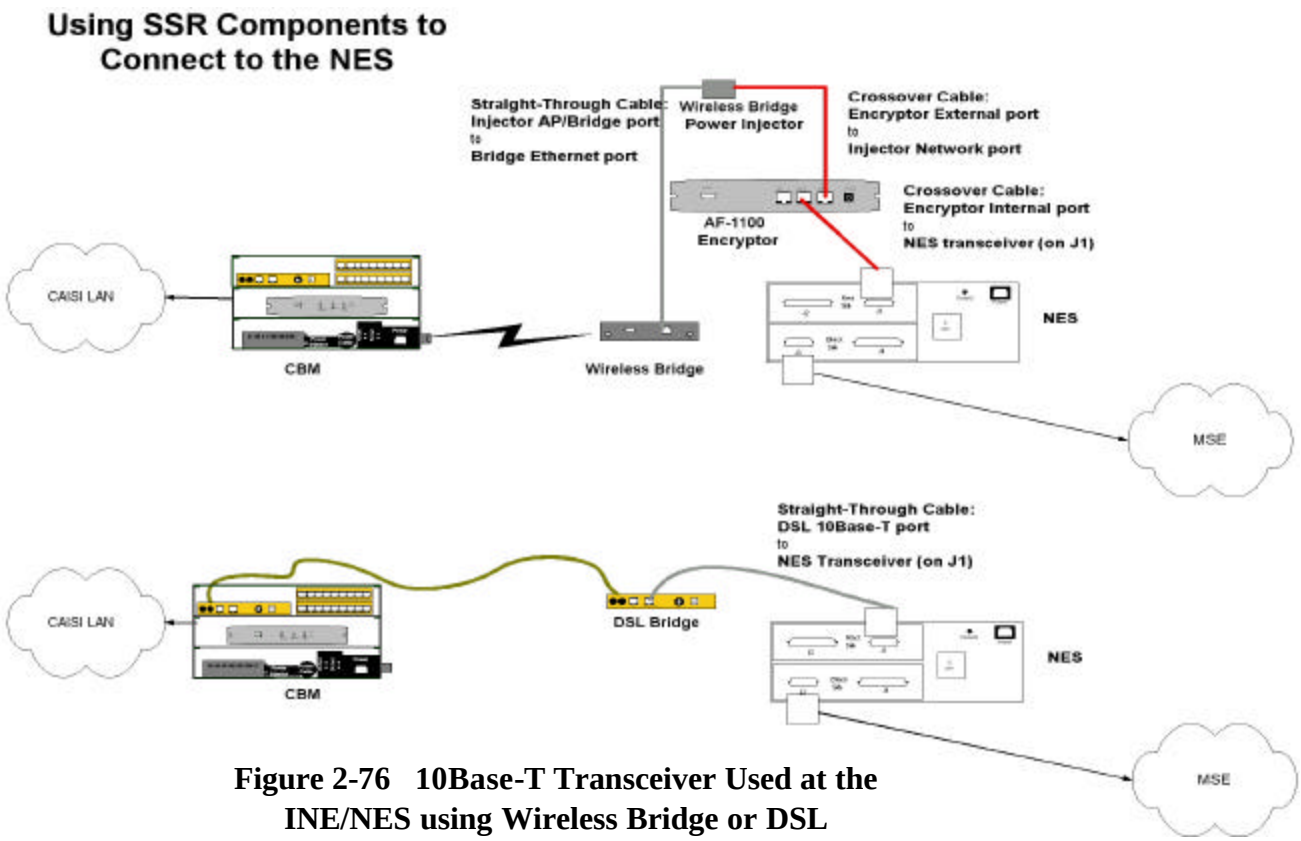


Figure 2-76 10Base-T Transceiver Used at the INE/NES using Wireless Bridge or DSL

Table 2-42 SSR Transit Case - Main Compartment Components Description (Continued)

Lightning Arrestor Assembly (Qty 2) 	i. **Two Lightning Arrestor Assembly – Lightning Arrestor mounted on bracket.** This is a **duplicate item** that comes with the CBM/CCM although this is mounted on a small bracket. The lightning arrestor protects the electrical components of the CBM/CCM from excessive voltage resulting from lightning by grounding the discharge.

Table 2-42 SSR Transit Case - Main Compartment Components Description (Continued)

Power Cords. Some of these cords are **duplicate items** found with CBM/CCM modules: (j, k and m)

j. Power Supply and Power Injector, 48V, for Wireless Bridge (duplicate)

k. Power Supply, 5V, DSL (duplicate)

l. Power Supply for Linksys Router (Will be replaced with two Netscreen routers).

m. Power Supply, 5V, 3 leads (Qty 2) –used for encryptor, (can simultaneously power a hub and radio or two hubs (duplicate)

n. Power Supply, 5V, 1 leads (Qty 5) - Wall style – for each router, each hub and radio adapter.

Power Supply & Power Injector for Wireless Bridge j	Power Supply for DSL Bridge k	Power Supply for Router l
Power Supply, 5V, 3 Leads (Qty 2) m	Power Supply, 5V, 1 lead (Qty 5) n	

NOTE: *There are a total of 10 powered items in the SSR Accessory Kit. Basically, that means there are 10 power supplies. Power cords are in top compartment and will be described in Table 2-44.*

The wireless bridge, DSL and encryptor (3-lead) power supplies each require a 2-prong power cord.

The 5V, 1-lead power supply for the router requires a 3-prong power cord.

The 5V, 1-Lead power supplies are wall style and do not require a power cord, but they take more than one position on a power strip (not provided with CAISI).

The 1-foot power cords are provided so that the user can connect each of these power supplies to a single plug on a power strip.

Table 2-43 SSR Transit Case – Top Compartment

a. 40-inch break-apart Whip Antenna (Qty 2)	j. RJ-45 Straight-through Adapter, RJ-45 (F) to RJ-45 (F) (Qty 3)
b. 4-inch Whip Antenna (Qty 2)	k. RJ-45 Crossover Adapter, RJ-45 (F) to RJ-45 (F) (Qty 3)
c. Grounding Strap (Qty 2)	l. 9-Pin Straight-Through Serial Extension Cable (M-F) (Blue)
d. 12-inch RF Adapter Cable N (M) to RPTNC (M) (Qty 2)	m. 9-Pin Crossover Serial Null Modem Cable (F – F) (Beige)
e. 12-inch RF Adapter Cable N (M) to RPTNC (F) (Qty 2)	n. 9 to 25-Pin Null-Modem Serial Adapter Cable
f. Adapter, N (M) to N (M) Right Angle (Qty 2)	o. Reset Tool (Qty 3)
g. Antenna "Dummy Load" N (M) (Qty 2)	p. Power Cable, 2-Prong (Qty 3)
h. White Straight-through Ethernet Cable (Qty 4)	q. Power Cable, 3-Prong (Qty 2)
i. Red Crossover Ethernet Cable (Qty 4)	r. 3-Prong, 1-foot Power Cable (Qty 5) for use with Power Supply, 5V, 1 lead

Figure 2-77 SSR Transit Case – Top Compartment

Table 2-44 SSR Transit Case – Top Compartment Components Description

40-inch break-apart Whip Antenna (Qty 2) 	a. **Omni-Directional "Whip" Antenna**. This is a **duplicate item that comes with the CBM.** Two 40-inch break-apart whip antenna. Unlike the "panel" antenna, the "whip" antenna is omni-directional and can pick up signals from all directions.
4-inch whip antenna (Qty 2) 	b. **4-inch "Whip" Antenna. (SSR Accessory Unique item)** An alternative to the larger whip antennas, the SSR may connect this 2.2 dBi antenna to the wireless bridge or multi-client radio adapter to perform configuration and troubleshooting of components. This antenna is recommended for use in an **indoor**, testing or garrison environment. May be connected directly to the SSR wireless bridge and radio adapter or connected via adapter cable to a CBM or CCM. Distance is 50 feet.
Grounding Strap (Qty 2) 	c. **Grounding Strap.** This is a **duplicate item** that comes with the CBM/CCM. The grounding strap serves as the path from the CBM to the earth. It is therefore, very important and must be constructed properly to ensure a good path to the ground. It is a 20-foot cable.
12-inch RF Antenna Cable N (M) to RPTNC (M) (Qty 2) 	d. **12-in RF Antenna Cable N (M) to RPTNC (M).** This is a **duplicate item** that comes with the CBM/CCM. This antenna cable can be used with the notebook, wireless NIC and an external antenna – whip or panel. (In the CBM/CCM, this 12-in RF antenna cable is already connected in the chassis from the wireless bridge/multi-client radio adapter to the lightning arrestor.) This cable is required to connect a stand-alone wireless bridge or multi-client radio adapter to the lightning arrestor and bracket. May be used to troubleshoot radios, lightning arrestors, RF cables and antennas.

Table 2-44 SSR Transit Case – Top Compartment Components Description (Continued)

12-inch RF Antenna Cable N (M) to RPTNC (F) (Qty 2) 	e. **12-in RF Antenna Cable N (M) to RPTNC (F) (SSR Accessory Unique item)**. Same functionality as the cable in (d) above expect different end. May be used to connect the lightning arrestor on a CBM/CCM to the 4-inch whip antenna for use in testing or for use in an indoor environment. May be used to troubleshoot radios, lightning arrestors, RF cables and antennas.
Adapter, Right Angle (N-M to N-M) (Qty 2) 	f. **Adapter, Right Angle (N-M to N-M). (SSR Accessory Unique item)** The Right Angle adapter may be used to connect a large omni-directional whip antenna directly to a CBM/CCM lightning arrestor without the RF antenna cable. Provides a practical alternative for testing and garrison environments in which there is not sufficient room to use the RF cables.
50 Ohm, Antenna "Dummy Load" (N-M) (Qty 2) 	g. **Antenna "Dummy Load" (N-M), 50 Ohm (SSR Accessory Unique item)** This resistor can be substituted for an antenna for test purposes. The dummy load permits transmitter testing without radiating a signal more than a very short distance (about 25 feet). Remember that you should never operate a radio without an antenna – the dummy load serves as an antenna and prevents damage to the radio.

Table 2-44 SSR Transit Case – Top Compartment Components Description (Continued)

White Straight-through Ethernet Cable (Qty- 4) 	h. **Four White or Gray Straight-through Ethernet Cables.** This is a **duplicate item** that comes with the CBM/CCM. The White Straight-through Ethernet cable is used to connect network capable devices used in the network. This cable is used to connect different devices, such as computer – hub or radio – hub. Commonly referred to as Category-5 (Cat-5) cable.
Red Crossover Ethernet Cable (Qty- 4) 	i. **Four Red or Orange Crossover Ethernet Cables.** This is a **duplicate item** that comes with the CBM/CCM. These are network cables that crosses transmit and receive lines. It is used to connect two hubs together using standard MDI-X ports, which are already crossover ports. This cable is used to connect like devices, such as computer – computer or hub – hub.
RJ-45 Straight-Through Adapter (Qty 3) 	j. **RJ-45 Straight-Through Adapter (Qty-3). (SSR Accessory Kit Unique item)** Extends the length of two CAT-5 Ethernet cables by allowing you to connect the two together to make a longer one. Two cables of lengths 25 and 15 ft, can becomes 40 ft by using this connector. (Is useful when a larger cable is not available). All eight lines are wired straight-through. **NOTE**: *Writing on this adapter may not be present*.
RJ-45 Crossover Adapter (Qty 3) 	k. **RJ-45 Crossover Adapter (SSR Accessory Kit Unique item)** Allows the SSR to turn a white straight-through Ethernet cable into a red crossover cable and turn a red crossover Ethernet cable into a white straight-through cable. Can be used if you need more red or white cables than you have. Also can be used in troubleshooting cables and connections. It is a convenience when configuring or troubleshooting – a single white cable can be used, with or without the adapter as required, without changing cables.

Table 2-44 SSR Transit Case – Top Compartment Components Description (Continued)

9-pin Straight-through Serial Extension Cable, (M-F) (blue) 	l. **9-Pin Straight-Through Serial Extension Cable (M-F) (Male – Female end) (Blue) (SSR Accessory Kit Unique item)** Used to connect the SSR notebook to the Wireless Bridge so configuration can be performed
9-pin Crossover Serial Null Modem Cable (F-F) (beige) 	m. **9-Pin Crossover Serial Null Modem Cable (F – F) (Female – Female) (Beige) (SSR Accessory Kit Unique item)** Used to connect the SSR notebook to the inline encryptor so configuration can be performed.
9-to-25 null modem cable 	n. **9 to 25-Pin Null-Modem Serial Adapter Cable** (used with LSA)
Reset Tool (Qty 3) 	o. **Reset Tool (SSR Accessory Kit Unique item).** A pin punch that can be used to reset the router, multi-client radio adapter and LSA back to factory default settings. (A paper clip will work also, if one is available). If lost, can be replaced by a 1/16-inch pin punch
2-prong power cord (Qty 3) 	p. **2-Prong Power Cord.** This is a **duplicate item** that comes with the CBM. 2-prong power cords are required for the DSL.

Table 2-44 SSR Transit Case – Top Compartment Components Description (Continued)

3-prong power cord (Qty 2)	q. **3-Prong Power Cord.** This is a **duplicate item** that comes with the CBM. 3-prong power cords are required for the wireless bridge and the router(s).
3-prong, 1-foot Power Cable (Qty 5) for use with Power Supply, 5V, 1 lead	r. **3-Prong, 1-foot Power Cable (SSR Accessory Kit unique item). U**sed to connect each of the power supplies to a single plug on a power strip. (used for troubleshooting)

2.24.3 Inventory SSR Transit Case.

1. Locate the SSR Transit Case inventory checklist card.
2. Identify each item on inventory checklist card.
3. Verify that all of the SSR Transit Case Components are present.
4. Annotate any discrepancies or shortages on DA Form 2407 or 5504.

Table 2-45 SSR Transit Case Inventory Checklist Card

Component	QTY	Date			
Transit Case	1				
Inline Encryptor, Air Fortress 1100	2				
UPS	1				
Wireless Bridge, Cisco BR-352	1				
Multi-Client Radio Adapter (Workgroup Bridge) Cisco WGB-342 or WGB-352	1				
DSL Bridge, Pairgain 300SBP	1				
Router, Netscreen 5xp or Router, Linksys BEFSR81	2				
	1				
Hubs, Addtron or Farallon 9-port	2				
10Base-T Transceiver	1				
40-inch break-apart whip antenna	2				
4-inch whip antenna	2				

Table 2-45 SSR Transit Case Inventory Checklist Card (Continued)

Component	QTY	Date			
Lightning Arrestor Assembly – Lightning Arrestor mounted on bracket	2				
Grounding Strap	2				
12-inch RF adapter cable N (M) to RPTNC (M)	2				
12-inch RF adapter cable N (M) to RPTNC (F)	2				
Right Angle Adapter, N (M) to N (M)	2				
Antenna “Dummy Load” N (M)	2				
White Straight-Through Ethernet Cable	4				
Red Crossover Ethernet Cable	4				
RJ-45 Straight-through Adapter, RJ-45 (F) to RJ-45 (F)	3				
RJ-45 Crossover Adapter, RJ-45 (F) to RJ-45 (F)	3				
9-pin Straight-Through Serial Extension Cable (M – F) (blue)	1				
9-pin Crossover Serial Null Modem Cable (F – F) (beige)	1				
9 to 25-Pin Null Modem Serial Adapter Cable	1				
Reset Tool	3				
Power Supply and Power Injector, 48V, Wireless Bridge	1				
Power Supply, 5V, DSL	1				
Power Supply for Linksys Router	1				
Power Supply, 5V, 3 Leads (for each encryptor) (Can simultaneously power a hub and radio or for two hubs	2				
Power Supply, 5V, 1 Lead, Wall Style (for each router, each hub and the radio adapter)	5				
Power Cable, 2-Prong	3				
Power Cable, 3-Prong	2				
3-prong, 1-foot Power Cable for use with Power supply, 5V, 1 lead	5				

2.24.4 Inspect SSR Transit Case Components.

NOTE: *Refer to User PMCS Table 2-25 for specific items to look for*

1. Inspect front and back of transit case for signs of damage.
2. Look for broken components.
3. Check for cut or frayed cables.
4. Check UPS for signs of damage.

2.25 SSR NOTEBOOK CASE

The SSR Notebook is packed in a briefcase-style carrying case, along with an assortment of NICs, adapters and cables. The components that you unpack from the SSR Notebook Case will depend on the mission requirements. Not all of the individual components of this case will be used, therefore only remove the necessary components when they need to be utilized.

NOTE: *When conducting inventory and PMCS, all items should be accounted for and inspected. Table 2-25 contains the specific items of each component to be inspected.*

Figure 2-78 SSR Notebook Case

All of the components except the notebook, power supply and power cord are in the bottom left of the case (under the notebook). The notebook is strapped into the large slot above the other components. The power supply and cord are in the slot to the right of the notebook. Coil the cords with velcro or rubber bands (not provided with CAISI).

2.25.1 Unpack the SSR Notebook Case.

The SSR Notebook Case weighs 20 pounds – full, 2 pounds - empty. Use safe lift and carry procedures when handling the transit case.

1. Place the SSR Notebook Case on a secure table, workbench or flat surface with the front facing you. To determine which side of the carrying case is the top, look at Identification tag.

2. Press the center buttons and clasp the bottom edge of the latch and carefully lift the notebook case lid.

Figure 2-79 SSR Notebook Case Latch

Table 2-46 SSR Notebook Case – Main Compartment

a. SSR Notebook, MITAC 7020/7251 with Baseline Software installation CD	i. RJ-45 Crossover Adapter, RJ-45 (M) to RJ-45 (F)
b. Power Supply and Cord for Notebook Computer	j. 9-Pin Straight-Through Serial Extension Cable (M-F) (Blue)
c. Wireless NIC, Cisco LMC-342 or 352	k. 9-Pin Crossover Serial Null Modem Cable (F-F) (Beige)
d. “Rabbit Ears” Antenna	l. Adapter Cable, 12 inch, MMCX to N (F)
e. Wired NIC	m. Adapter Cable, 12 inch, MMCX to RPTNC (F)
f. White Straight-through Ethernet Cable	n. Right Angle Adapter, N (M) to N (M)
g. Red Crossover Ethernet Cable	o. Antenna “Dummy Load” N (M)
h. RJ-45 Straight-through Adapter RJ-45 (F) to RJ-45 (F)	p. Reset Tool

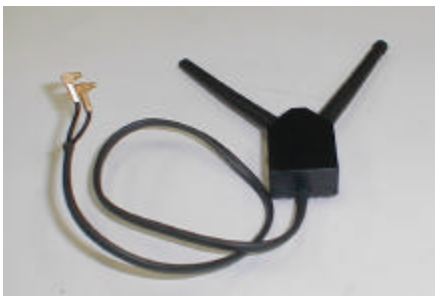
2.25.2 Identify SSR Notebook Case Components.

Table 2-47 SSR Notebook Case Components Description

SSR Notebook 	a. **SSR Notebook with baseline CD and software. (SSR Accessory Kit unique item).** The notebook will contain the following: 1. A current version of Microsoft Windows 2000 will be loaded on the notebook because of security concerns and the need for a FTP server to support some SSR administration functions. 2. Commercial off the Shelf (COTS) software that includes utilities and drivers for the various CAISI components. 3. A Government-developed systems administration application to assist the SSR in configuring the various CAISI components and perform monitoring as required by regulations and local policies. 4. AirFortress Encryptor Remote Client Software – operates on the SSR notebook. It encrypts and decrypts the network traffic as it passes in and out of the computer. It sits between the computer and the NIC – in the same way that the hardware inline encryptor sits between the hub and the radio.	
Power Supply for Notebook 	Power Cord (2-prong) 	b. **Power supply and cord for Notebook**
Wireless NIC 	c. **Wireless NIC. (SSR Accessory Kit unique item).** The wireless NIC is a Cisco Aironet LMC340 series PCMCIA radio card. This particular model is the LMC-342. Like the bridges, it operates on the U.S. channel set, with 128-bit encryption, but only has 30mW (milli-watt) power out and a 11.0 Mbps (milli-bits per second) connection. It comes with a removable “rabbit ears” antenna. The wireless card may be used for configuration changes during operations, for monitoring, and for routine operations from the immediate vicinity of a CBM. This model will be upgrade to the LMC-352 which is similar but has 100mW power out.	

Table 2-47 SSR Notebook Case Components Description (Continued)

Rabbit Ears Antenna	d. **Rabbit Ears Antennas. (SSR Accessory Kit unique item).** The removable "rabbit ears" antenna is used with the wireless NIC (LMC-342). The antenna connectors are rather delicate and should be handled carefully when connecting or disconnecting them. The rabbit ears antenna and the wireless card (LMC-342) are shown in Figure 2-80. The rabbit ears antenna can be used to monitor the trusted side of the network. Distance is 50 feet.



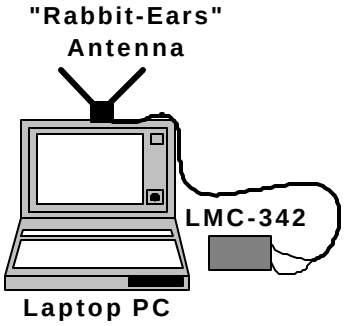


Figure 2-80 Rabbit Ears Antenna

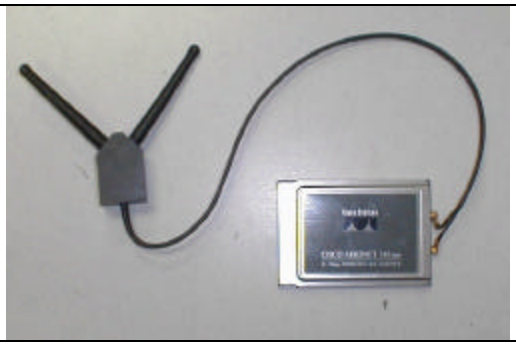


Figure 2-81 Rabbit Ears Antenna and Wireless NIC

Connection Procedures of the PCMCIA card is the following: (Figure 2-80 and Figure 2-81)

1. Insert the card into the PCMCIA slot on the notebook.
2. Insert the connectors on the rabbit-ears antenna cable into the two holes on the end of the card. (Be extremely careful when connecting and disconnecting the connectors, because they are very delicate).

NOTE: *If you need to use your notebook with a large external antenna such as the whips (40-inch or 24-inch) or panels (7-inch) issued with the CBM or CCM, you will need adapter cables (Figure 2-82).*

The SSR Accessory Kit also includes two 40-inch Whip antennas and a 14-inch Panel antenna. This is only for a limited time so that you can check the network configurations. (MMCX – multimedia communication exchange)

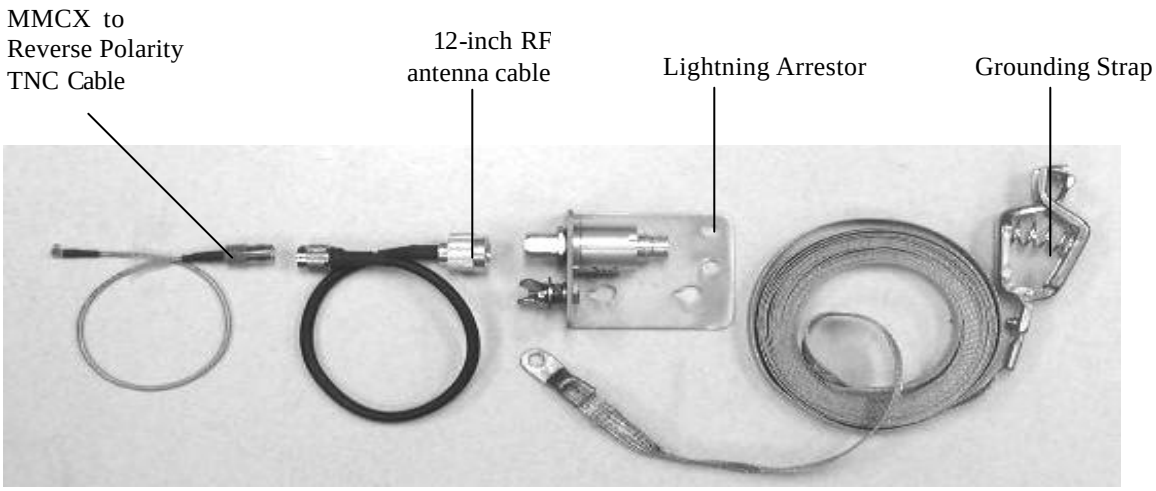


Figure 2-82 Wireless NIC Antenna Adapter Cables

NOTE: *More detail will be covered in Paragraph 2.30.6 but the actual connections on how these work is the following:*

Permanent use: Notebook will stay in place for a long period of time.

1. Connect the end of the MMCX to RPTNC Cable to the small end of the 12-inch RF antenna cable.

2. Connect the large end of the 12-inch RF antenna cable to the small end of the lightning arrestor.

3. Connect a (25, 35 or 50 ft) RF antenna cable (not shown) to the large end of the lightning arrestor (outside edge of bracket).

4. Connect the terminal lug of the grounding strap to grounding stud (next to lightning arrestor, remove wing nut and washer, then attach terminal lug, then refasten washer and wing nut).

5. Connect the end of the RF antenna cable to the antenna used.

Temporary use: If you are only going to check a configuration, make a quick change to the configuration, aim an antenna or monitor the network for a short period of time, (less than 6 hours), you will only need to do the following: **(Indoor use only)**

1. Connect the end of the MMCX to RPTNC Cable to the small end of the 12-inch RF antenna cable.

2. Connect the large end of the 12-inch RF antenna cable to the antenna.

Table 2-47 SSR Notebook Case Components Description (Continued)

Wired NIC 	e. **Wired NIC**. **(SSR Accessory Kit unique item).** The wired NIC is a Xircom RealPort 10/100 PC-Bus card. This NIC allows you to physically connect to the network for **the initial configuration of the SSR notebook**. It is also used for troubleshooting the CAISI components as well as any network problems that may occur. You may also use the wired NIC anytime that radio operations are limited for any reason. The CAISI notebook may be carried anywhere it is required.
Connection Procedure for the Wired NIC: 1. It has a port into which you insert the CAT-5 network cable RJ-45 connector. There is no dongle to get lost or broken. 2. Insert the other end of the cable into any appropriate hub, switch, or bridge on the network.	
White Straight-through Ethernet Cable 	f. **White Straight-through Ethernet Cable.** This is a **duplicate item** that comes with the CBM/CCM/SSR Transit Case. The White Straight-through Ethernet cable is used to connect network capable devices used in the network. This cable is used to connect different devices, such as computer – hub or radio – hub. Commonly referred to as Category-5 (Cat-5) cable.
Red Crossover Ethernet Cable 	g. **Red Crossover Ethernet Cable.** This is a **duplicate item** that comes with the CBM/CCM/SSR Transit Case. These are network cables that crosses transmit and receive lines. It is used to connect two hubs together using standard MDI-X ports, which are already crossover ports. This cable is used to connect like devices, such as computer – computer or hub – hub.

Table 2-47 SSR Notebook Case Components Description (Continued)

RJ-45 Straight-Through Adapter 	h. **RJ-45 Straight-Through Adapter.** This is a **duplicate item** that comes in the SSR Transit Case. Extends the length of two CAT-5 Ethernet cables by allowing you to connect two cables together to make a longer one. Two cables of lengths 25 and 15 ft, can becomes 40 ft by using this connector. (Is useful when a larger cable is not available). All eight lines are wired straight-through. **NOTE**: *Wording on this adapter may be missing*.
RJ-45 Crossover Adapter 	i. **RJ-45 Crossover Adapter.** This is a **duplicate item** that comes in the SSR Transit Case. Allows the SSR to turn a white straight-through Ethernet cable into a red crossover cable and turn a red crossover Ethernet cable into a white straight-through cable. Can be used if you need more red or white cables than you have. Also can be used in troubleshooting cables and connections. It is a convenience when configuring or troubleshooting – a single white cable can be used, with or without the adapter as required, without changing cables.
9-pin Straight-through Serial Extension Cable, (M-F) (Blue) 	j. **9-Pin Straight-Through Serial Extension Cable (M-F) (Blue).** This is a **duplicate item** that comes in the SSR Transit Case. Used to connect the SSR notebook to the Wireless Bridge so configuration can be performed
9-pin Crossover Serial Null Modem Cable (F-F) (Beige) 	k. **9-Pin Crossover Serial Null Modem Cable (F – F) (Beige).** This is a **duplicate item** that comes in the SSR Transit Case. Used to connect the SSR notebook to the inline encryptor so configuration can be performed.

Table 2-47 SSR Notebook Case Components Description (Continued)

Adapter Cables MMCX to N 	l. **Adapter Cable, 12 inch, MMCX to N (F) (SSR Accessory Kit unique item).** If you need to use your laptop with a large external antenna, such as the whips or panels issued with the CBM or CCM, you need adapter cables. Connects the SSR notebook to a lightning arrestor from the SSR kit or when troubleshooting, to the lightning arrestor in a CBM/CCM. (Refer to Wireless NIC card previously discussed for connection procedures).
Adapter Cables MMCX to RPTNC 	m. **Adapter Cable, 12-inch, MMCX to RPTNC (Reverse Polarity TNC) (F) (SSR Accessory Kit unique item).** If you need to use your laptop with a large external antenna, such as the whips or panels issued with the CBM or CCM, you need adapter cables. RPTNC is the threaded version of BNC. (Female with a male pin adapter cable). Connects the SSR notebook to a 4-inch whip antenna or to the 12” adapter cable -- to test the cables in the SSR Accessory Kit or inside CBM/CCM. (Refer to Wireless NIC card previously discussed for connection procedures).
Adapter, Right Angle (N-M to N-M) 	n. **Adapter, Right Angle (N-M to N-M)** This is a **duplicate** item that comes in the SSR Transit Case. The Right Angle adapter may be used to connect a large omni-directional whip antenna directly to a CBM/CCM lightning arrestor without the RF antenna cable. Provides a practical alternative for testing and garrison environments in which there is not sufficient room to use the RF cables.

Table 2-47 SSR Notebook Case Components Description (Continued)

50 Ohm, Antenna "Dummy Load" (N-M) 	o. **Antenna "Dummy Load" (N-M), 50 Ohm** This is a **duplicate** item that comes in the SSR Transit Case. This resistor can be substituted for an antenna for test purposes. The dummy load permits transmitter testing without radiating a signal more than a very short distance (about 25 feet). Remember, that you should never operate a radio without an antenna – the dummy load serves as an antenna and prevents damage to the radio. **NOTE:** *The dummy load must have the same resistance as the antenna it replaces*.
Reset Tool 	p. **Reset Tool.** This is a **duplicate** item that comes in the SSR Transit Case. A pin punch that can be used to reset the router, multi-client radio adapter and LSA back to factor default settings. (A paper clip will work also, if one is available). If lost, can be replaced by a 1/16-inch pin punch.

2.25.3 Inventory SSR Notebook Case.

1. Locate the SSR Notebook Case inventory checklist card (Table 2-48).

2. Identify each item on inventory checklist card.

3. Verify that all of the SSR Notebook Case Components are present.

4. Annotate any discrepancies or shortages on DA Form 2407 or 5504.

Table 2-48 SSR Notebook Case Inventory Checklist Card

Component	QTY	Date			
Carrying Case	1				
SSR Notebook Computer	1				
Baseline Software Installation CD	1				
Power Supply for Notebook Computer	1				
Power Cord for Notebook Computer	1				
"Rabbit Ears" Antenna	1				
Wireless NIC, Cisco LMC-342 or LMC-352	1				
Wired NIC	1				
White Straight-Through Ethernet Cable	4				
Red Crossover Ethernet Cable	4				
RJ-45 Straight-through Adapter, RJ-45 (F) to RJ-45 (F)	1				
RJ-45 Crossover Adapter, RJ-45 (F) to RJ-45 (M)	1				
9-pin Straight-Through Serial Extension Cable (M – F) (Blue)	1				
9-pin Crossover Serial Null Modem Cable (F – F) (Beige)	1				
Adapter Cable, 12-inch, MMCX to N (F)	1				
Adapter Cable, 12-inch, MMCX to RPTNC (F)	1				
Right Angle Adapter, N-M to N-M					
Antenna "Dummy Load" N (M)	1				
Reset Tool	1				

2.25.4 Inspect SSR Notebook Case Components.

NOTE: *Refer to User PMCS Table 2-25 for specific items to look for.*

1. Inspect front and back of case for signs of damage.
2. Look for broken components.
3. Check for cut or frayed cables.

2.26 SSR ANTENNA CARRYING CASE

The SSR Antenna Carrying Case contains additional antennas and ancillary components, including two large panel antennas. These antennas are used when a stronger point-to-point link is required. For example, use the panel antenna over difficult terrain where the whip antennas do not work as well. Line of sight is poor.

Figure 2-83 SSR Antenna Carrying Case

2.26.1 Unpack the SSR Antenna Carrying Case.

The SSR Antenna Carrying Case has carrying handles and backpack straps. This case weighs 25 lbs. Unpack only those items that are needed.

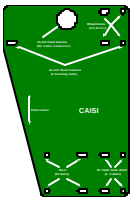
Antenna Carrying Case

a. Two 14-inch Directional Panel Antennas

b. Four 50 ft RF Antenna Cables

c. Two 7-inch Antenna Bracket

d. Two 14-inch Antenna Brackets



e. Four Barrel Connectors

f. Antenna guy rope on reel (42-ft) (red) (Qty 8) (two per reel)

g. Reel Unit for Guy Ropes (Qty 4)

h. Antenna guy stake (Qty 8)

Figure 2-84 SSR Antenna Carrying Case and Components

Table 2-49 SSR Antenna Carrying Case Contents Layout

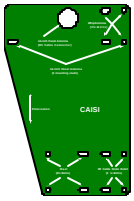
	Component	Qty	Location in case
a.	"14x14" flat Directional Panel Antennas	2	Store in center section
b.	50 ft RF Antenna Cables	4	Store in the two outer sections
c.	"7" antenna brackets	2	Store in one outer section with cables
d.	"14" antenna brackets	2	Store in other outer section with cables
e.	Antenna Barrel connectors	4	Store in outer pocket
f.	42-foot Guy Rope (Red Clip)	8	Store in outer section with cables
g.	Reel Unit for Guy Ropes (two guy ropes per reel)	4	Store in outer section with cables
h.	Guy Stakes	8	Store in outer section with cables

2.26.2 Identify SSR Antenna Carrying Case Components

Table 2-50 SSR Antenna Carrying Case Components Description

14" Directional Panel (Qty 2)	a. **Two "14 x 14" Directional Panel Antennas. (SSR Accessory Kit unique item).** These directional panel antennas are for use with the CBM/CCM in special circumstances. (Four of the 7-inch panels will make one 14-inch panel)
50 ft. RF Antenna Cable (Qty 4)	b. **Four 50 ft RF Antenna Cables. (SSR Accessory Kit unique item).** May be loaned to CBM or CCM operators for use with their equipment. Also can be used in conjunction with the AB-1244B antenna mast – Paragraph 2.27.
7 " Antenna Bracket (Qty 2)	c. **Two "7 in" Antenna Brackets.** This is a **duplicate item** of the bracket provided with the CBM/CCM. A single bracket is used to mount either an omni-directional or the "7x7" directional panel antenna to a camouflage pole or mast

Table 2-50 SSR Antenna Carrying Case Components Description (Continued)

14” Antenna Bracket (Qty 2) 	d. **Two “14 in” Antenna Brackets**. **(SSR Accessory Kit unique item).** A single bracket is used to mount the “14 x 14” panel antenna to a camouflage pole or mast.
Four Barrel Connectors (Qty 4) 	e. **Four Antenna Barrel Connector**. Allows you to extend the length of the RF cable by connecting two or more cables. (Smaller the cable, the less dBi loss)
Guy Rope – 42ft (Red clip) (Qty 8) 	f. **Guy Rope – 42ft – red clip –** used to stabilize the antenna bracket when mounted using the guy stakes below.
Reel Unit for Guy Ropes (Qty 4) 	g. **Reel Unit for Guy Ropes (RL-28)** - two guy ropes above per reel unit.
Guy Stakes Assembly (Qty 8) 	h. **Guy Stakes Assembly** – used to stabilize the antenna with guy ropes

2.26.3 Inventory SSR Antenna Carrying Case.

1. Locate SSR Antenna Carrying Case Inventory Checklist Card.

Table 2-51 SSR Antenna Carrying Case Inventory Checklist Card

Component	QTY	Date			
Carrying Case	1				
14-inch Panel Antenna (store in center section)	2				
50-foot RF Antenna Cable (store in the two outer sections)	2				
Bracket for 7-inch Panel or Whip Antenna (with U-bolts, washers and wing nuts) (store in one of the outer section with cables)	2				
Bracket for 14-inch Panel (with U-bolts, washers and wing nuts) (store in other outer section with cables)	2				
Barrel Connector (Double-N Adapter) (store in outer pocket)	4				
Guy Ropes – 42ft (Red Clips) (store in outer section with cables)	8				
Reel Unit for Guy Ropes (Containing above, two guy ropes per reel unit) (Store in outer section with cables)	4				
Guy Stakes Assembly (Store in outer section with cables)	8				

2. Identify each item on inventory checklist card.

3. Verify all SSR Antenna Carrying Case Components are present.

4. Annotate any discrepancies or shortages on DA Form 2407 or 5504.

2.26.4 Inspect the SSR Antenna Carrying Case Components.

NOTE: *Refer to the Organizational PMCS Table 2-25 for specific items to look for.*

1. Inspect exterior and interior of carrying case for signs of damage.

2. Check components for signs of damage.

3. Ensure RF cable ends are not loose.

2.27 SSR ANTENNA MAST CARRYING CASE. The Mast Assembly, AB-1244B is used to elevate the omni-directional and directional antennas above ground and is held by eight guy ropes. It is designed for hand or vehicular transportation. It consists of a Mast section and an Antenna Mast Kit.

Figure 2-85 SSR Antenna Mast Carrying Case

The mast consists of five lower and five upper mast sections, a lower adapter assembly, an upper adapter assembly, and a mast and base assembly. Each tubular mast section has a male and female end, which permits the sections to be fitted together. The lower adapter assembly mates the lower and upper mast sections into a single unit. The upper adapter assembly is the interface between the mast and the antenna.

NOTE: *The overall height of the mast assembly will vary based on the type of antenna used. The mast assembly is approximately 30 ft, and can reach 33 ft, 4 in. depending on the CAISI antenna used. Specific information on the heights for each antenna is in Figure 1-12 and Table 1-3.*

The Mast and Base Assembly consists of a base plate, a fabricated metal plate used to distribute the load of the mast and base assembly. The plate is fixed to the ground by the use of two driven stakes which secure the plate from movement. Guy assemblies, guy plates, guy snubbers, and guy stakes hold the mast assembly in the vertical position.

Another guy plate (blue) is slid onto the male end of the lower adapter assembly, before it is assembled to the upper mast sections. A second guy plate (red) is slid onto the male end of the upper adapter assembly before being mated with the antenna. The upper and lower guy ropes attach to these plates.

2.27.1 Unpack the SSR Antenna Mast Carrying Case. The SSR Antenna Mast Carrying Case is a nylon fabric roll case with pockets and straps to hold the antenna components for transportation in the field. An adjustable shoulder strap is provided for easy carrying. Due to its size and weight (35 lbs), it is easier to carry it over one shoulder.

2.27.2 Identify SSR Antenna Mast Carrying Case Components.

NOTE: *Words in parenthesis are the component nomenclature that is in the Technical Manual 11-5895-357-13, Operator's Organizational Direct Support Maintenance Manual for Antenna Group OE-254/GRC.*

a. **Mast Sections:**

1. Five upper mast sections. (mast section assembly (upper))

2. Five lower mast sections. (mast section assembly (lower))

3. Upper mast adapter section (red-ring). (adapter assembly (upper))

4. Lower mast adapter section (blue-ring). (adapter assembly (lower))

Figure 2-86 Antenna Mast Sections

b. **Antenna Mast Kit:**

1. Four (36) ft. guy ropes (blue clips).

2. Four (42) ft. guy ropes (red clips).

3. Four reel units (RL-28) for guy ropes, two guy ropes per reel unit.

4. Four guy stakes. (stake assembly)

5. Mast Base Assembly

6. Base plate.

7. Two base plate pins. (stakes)

8. Two guy rings (one red, one blue). (If the colors wear off, the blue ring has a larger hole in the center than the red ring)

9. 2.5 lb sledgehammer.

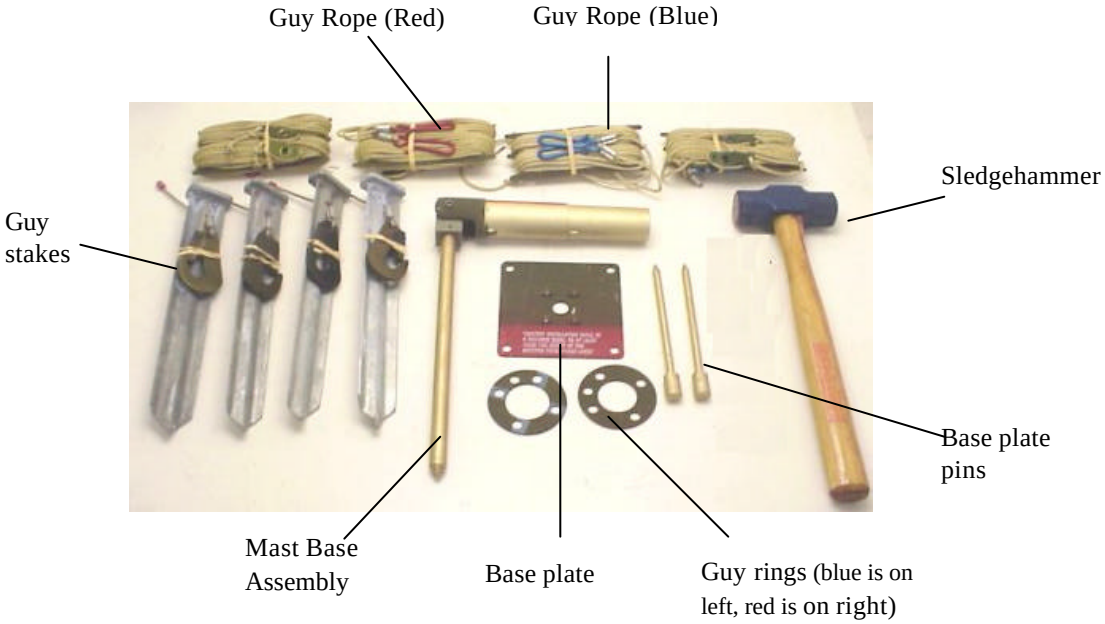


Figure 2-87 Antenna Mast Kit

2.27.3 Inventory SSR Antenna Mast Carrying Case.

1. Locate SSR Antenna Mast Carrying case inventory checklist card (Table 2-52).

2. Identify each item on inventory checklist card.

3. Verify all SSR Antenna Mast Carrying Case Components are present.

4. Annotate any discrepancies or shortages on DA Form 2407 or 5504.

Table 2-52 SSR Antenna Mast Carrying Case Inventory Checklist Card

Component	QTY	Date			
Carrying Case	1				
Upper Mast Section	5				
Lower Mast Section	5				
Upper Mast Section (Red Ring)	1				
Lower Mast Section (Blue Ring)	1				
36-foot Guy Rope (Blue Clips)	4				
42-foot Guy Rope (Red Clips)	4				
Reel Unit for Guy Ropes (RL-28) – (containing above two ropes; two Guy Ropes Per Reel Unit)	4				
Guy Stakes	4				
Mast Base Assembly	1				
Base Plate	1				
Base Plate Pins	2				
Guy Rings (One Red, One Blue)	2				
2.5 Pound SledgeHammer	1				

2.27.4 Inspect the SSR Antenna Mast Carrying Case Components.

NOTE: *Refer to the Organizational PMCS Table 2-25 for specific items to look for.*

1. Inspect interior/exterior of Antenna Mast Carrying Case for signs of damage.

2. Look for broken or damaged components.

3. Check for cut or frayed ropes.

2.28 SET UP THE ANTENNA MAST EQUIPMENT.

WARNING

Never erect the antenna where power lines could possibly sag or break or come in contact with the antenna or transmission line.

1. Select a site free and clear of all obstructions within a 25-foot radius (7.62 meters). Initial assembly of the antenna system will require an assembly area approximately 8 feet wide and 42 feet long.

2. Unpack the components and place them on a clean, dry surface. Inspect all components for damage and signs of wear. Do not erect the mast assembly and CAISI antenna if any components are missing or damaged.

3. Do as much of the assembly work as possible on the ground.

4. When erecting the mast assembly and CAISI antenna, allow only personnel required to erect the antenna in the erection area.

5. Ensure the area for the anchor is firm. If the ground is marshy or sandy, get specific instructions on how to reinforce the anchors from your supervisors.

6. Stay away from high traffic areas, high voltage wire or any overhead obstructions.

7. Never erect your mast assembly and CAISI antenna closer than two times it's height from overhead wires or lines.

8. Ensure your site is clear of high trees, buildings, and is accessible if maintenance personnel are needed at the field site.

9. Find a place free of obstruction so you will have a good LOS.

10. When erecting the antenna mast under camouflage net, make sure the antenna is extended outside the net otherwise the radio signal will be reflected back into the net.

2.28.1 Connect the RF Cable to the Omni-Directional Antenna and Bracket. Same procedure as in Paragraph 2.18.2.

2.28.2 Connect the RF Cable to the Directional Panel Antenna and Bracket. Same procedure as in Paragraph 2.19.2.

There are different size brackets used with the directional antennas.

1. A large “14” to accommodate the “14x14” panel antenna

2. A small “7” to accommodate both the omni-directional and the “7x7” panel antennas. (Four of the “7x7” panel antennas put together in a square will make one “14x14” panel).

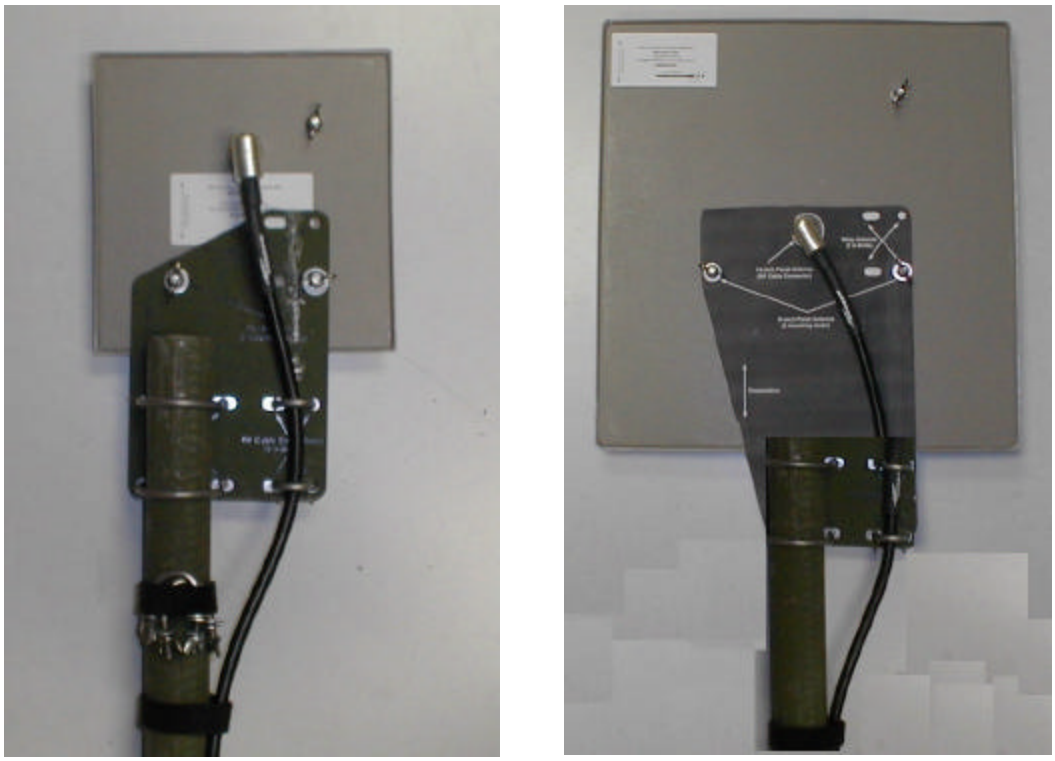


Figure 2-88 Connecting the Panel Antenna – “7x7” antenna on left, “14x14” antenna on the right

NOTE: *The only difference between the “7x7” panel and the “14x14” is the size and in the connection point on the bracket. When connecting the bracket to the “14x14” panel antenna, the antenna connector will protrude through the large round hole.*

2.28.3 Connect Bracket to the Mast Section or Camouflage Pole. Same procedure 2.18.3 for the Whip antenna or Panel Antenna.

CAUTION

- Do not attempt to go above 19 feet with the camouflage poles.
- Do not mount the 14-inch panel on camouflage poles – its too heavy, must be used with the antenna mast.

2.29 SET UP FOR ANTENNA MAST PROCEDURES

2.29.1 Positioning the Base Plate and Guy Stakes. Perform the following steps to position the base plate for the antenna:

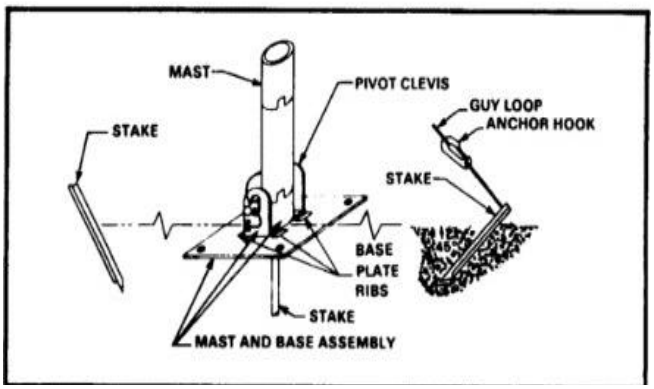


Figure 2-89 Ground Anchor/Pivot Clevis Attachment

1. Place the base plate, with the ribs up, where the antenna is to be erected.

2. Drive the stake of the mast and base assembly through the center hole of the base plate with the hammer. (Figure 2-89).

WARNING

Use extreme care in driving the stake with the hammer. The space between the ears of the stake is barely enough to clear the hammer. Hitting one of the ears with the hammer will break it.

3. Drive the two pin stakes through the opposite corner holes of the base plate.

2.29.2 Assembling the Antenna Mast. Perform the following steps to assemble the antenna mast:

1. Assemble the five lower mast sections by inserting the male ends into the female ends. Place the bottom section of the assembly over the movable portion of the mast and base assembly.

2. Slide the lower guy plate, (color-coded blue or the larger center hole), onto the male end of the lower adapter assembly and join it to the mast.

3. Assemble three upper mast sections on the lower adapter assembly.

4. To approximate the guy stake positioning radius, walk the assembled mast around the mast and base assembly. Locate the position of the four guy stakes at a maximum radius of 25 ft (7.62 meters) from the center of the base plate and a 90-degree angle between stakes. (Figure 2-90).

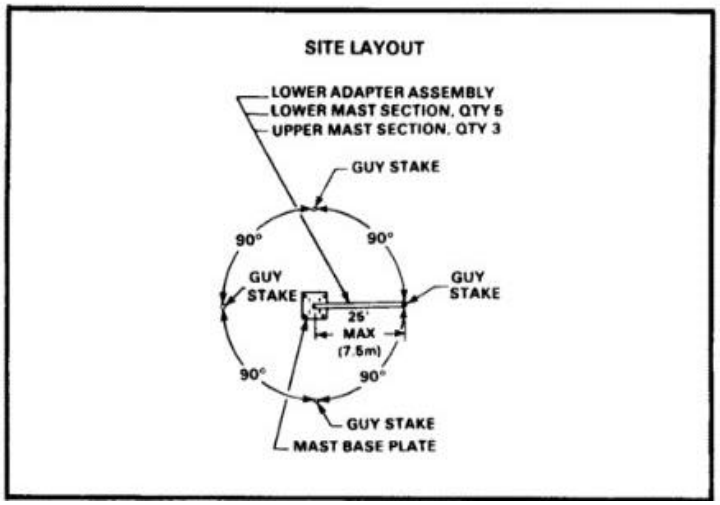


Figure 2-90 Positioning the Guy Stakes

5. Drive the four guy stakes at a 45-degree angle into the earth facing away from the mast. (Figure 2-89) (The angle will depend on the terrain). Ensure the hooks of the guy stakes are facing the base plate.

   NOTE: *Make sure the area for the anchors is firm. If the ground is marshy or sandy, get specific instructions from your supervisor on how to reinforce the anchors.*

6. Return the mast and base assembly to the alignment shown in Figure 2-90.

7. Assemble the two remaining upper mast sections on the nine previously assembled.

   NOTE: *If the antenna is not to be raised to its full height, reduce the number of mast sections. Eliminate the upper mast sections first. The lower and upper adapter assemblies and the insulating extension must be used.*

8. Slide the upper guy plate, (color-coded red or smaller center hole), onto the male end of the upper adapter assembly and join it to the mast.

9. Turn the guy plates so that one hole of each is uppermost.

10. Attach the guy hooks of the lower guy ropes, (color coded blue), to the holes of the lower guy plate. See Figure 2-91.

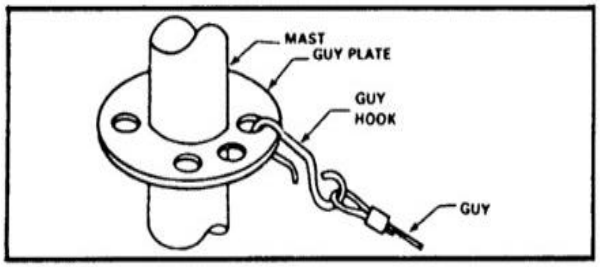


Figure 2-91 Attaching Guy Hooks to Guy Plate

11. Extend the guy assemblies to the side and back anchor hooks and attach the guy loops. See Figures 2-92 and 2-93.

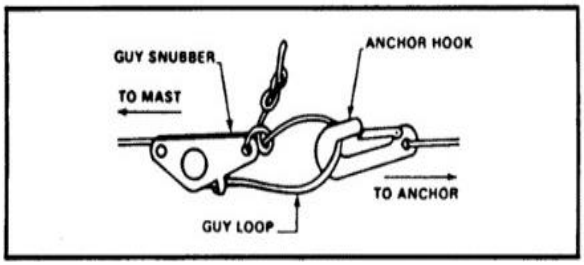


Figure 2-92 Attaching Guy Loops to Ground Anchor

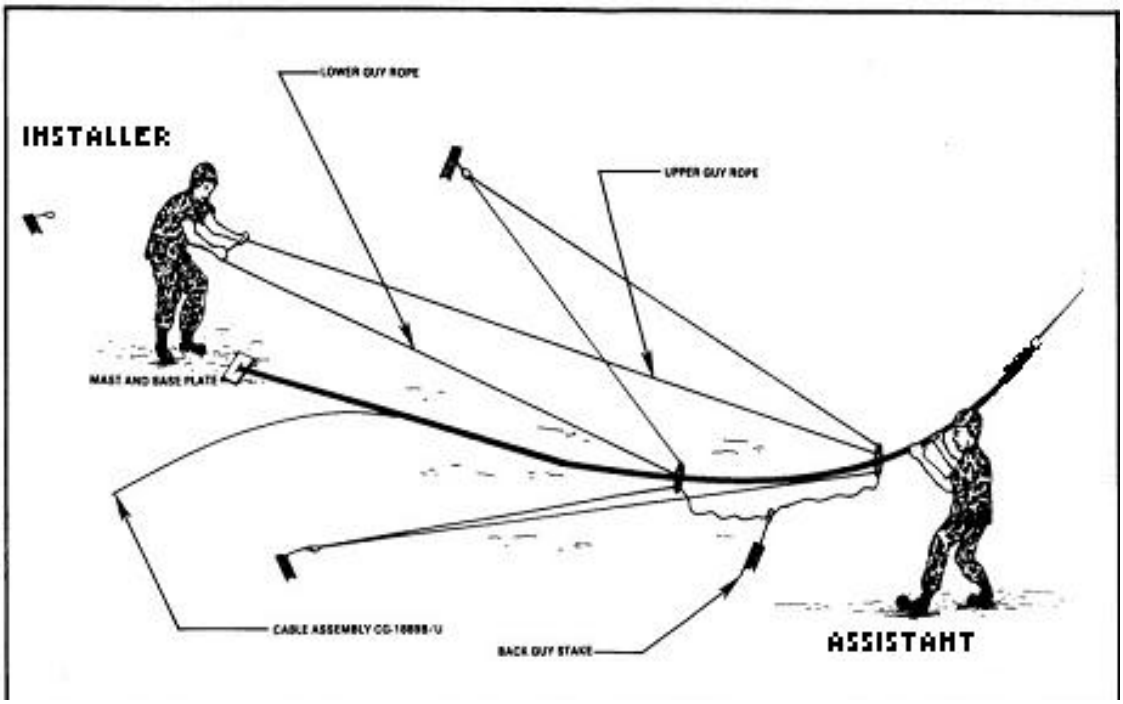


Figure 2-93 Attaching Guy Loops to Side and Back Guy Stakes

12. Attach the hooks of the upper guy assemblies (color coded red) to the upper guy plate. See Figure 2-92.

13. Extend the guy assemblies to the side and back anchor hooks and attach the guy loops. See Figure 2-92 and 2-93.

    NOTE: *Make sure the mast assembly is laid out straight and crosses behind one guy stake (the back guy stake, Figure 2-93).*

14. Pull the four side guy ropes, two upper and two lower, tight and secure them. Figure 2-94 and 2-95. Make sure the mast assembly is not pulled out of line.

The method for pulling guy lines taut is as follows:

a. Remove the guy from the snubber lock.

b. Pull the snubber along the guy in the direction towards the mast.

c. Secure the guy by looping the guy under the snubber.

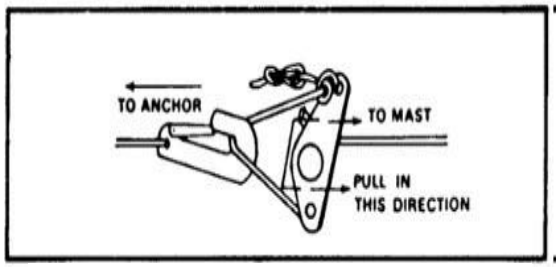


Figure 2-94 Pulling Guy Rope Tight

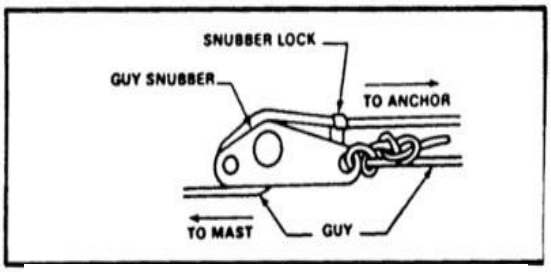


Figure 2-95 Securing Guy with Snubber Lock

15. Lay the two bottom (upper and lower) guy ropes along one of the tightened side guy ropes and adjust them to the same length. Attach the bottom guy ropes to the back guy stake. (Figure 2-93)

16. Attach the antenna and antenna cable to the antenna bracket using procedures detailed in Paragraph 2.18.3 of this manual.

17. Connect the antenna bracket to the top of the mast (Paragraph 2.18.4).

18. If using the panel antenna and the weather is windy, you need to secure it. Follow the procedures in Paragraph 2.19.2 (step 11). If not windy, skip this procedure.

19. Provide strain relief by attaching the strain relief clamp through the fifth hole of the upper guy plate and attaching it to the RF cable.

    Leave a loop in the cable to prevent strain. Tape the cable to the mast, using electrical tape, or velcro straps to provide additional strain relief.

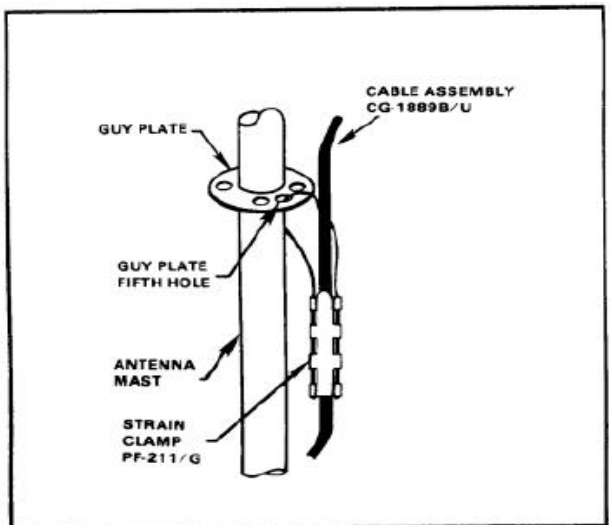


Figure 2-96 Strain Clamp Closed

2.29.3 Erecting the Mast and Antenna. Perform the following steps to erect the mast and antenna. This is a **two-person operation** – installer and assistant. Additional uniform requirements include goggles, helmet and gloves.

WARNING

WATCH OUT FOR ANY POWERLINES. Observe the warnings elsewhere in this manual.

When erecting the antenna, allow only team personnel in the erecting area.

Clearly mark all guys with warning flags or signs (supplied by your unit). In an emergency, use strips of white cloth as warning streamers.

1. **Preparation.**

   a. Installer – stands near the baseplate assembly in line with the far guy stake holding the free guys. (Figure 2-97)

   b. Assistant – stands at the top holding the antenna at shoulder length.

   NOTE: *If available, raise the masthead off the ground up to four feet by using a gin pole, box, or concrete block.*

2. **Raising.**

   a. Installer – bow the top end by pulling the guys tight and walk backward pulling the mast slowly and firmly erect.

   b. Assistant – walk toward the base pushing the mast upward.

3. **Adjusting.**

   a. Connect the free guy ropes to the remaining guy stake assembly (Figure 2-93) and tighten the guys (Figure 2-95).

   b. Adjust all the guy ropes evenly. Check for vertical positioning by comparing the mast with a building, pole, or other vertical object.

   NOTE: *Leave a slight slack in each guy rope to allow for expansion and contraction of the mast and guy ropes. Check the tension in the morning and during the day. Experience with temperature conditions in the area will determine how tight the guy ropes should be.*

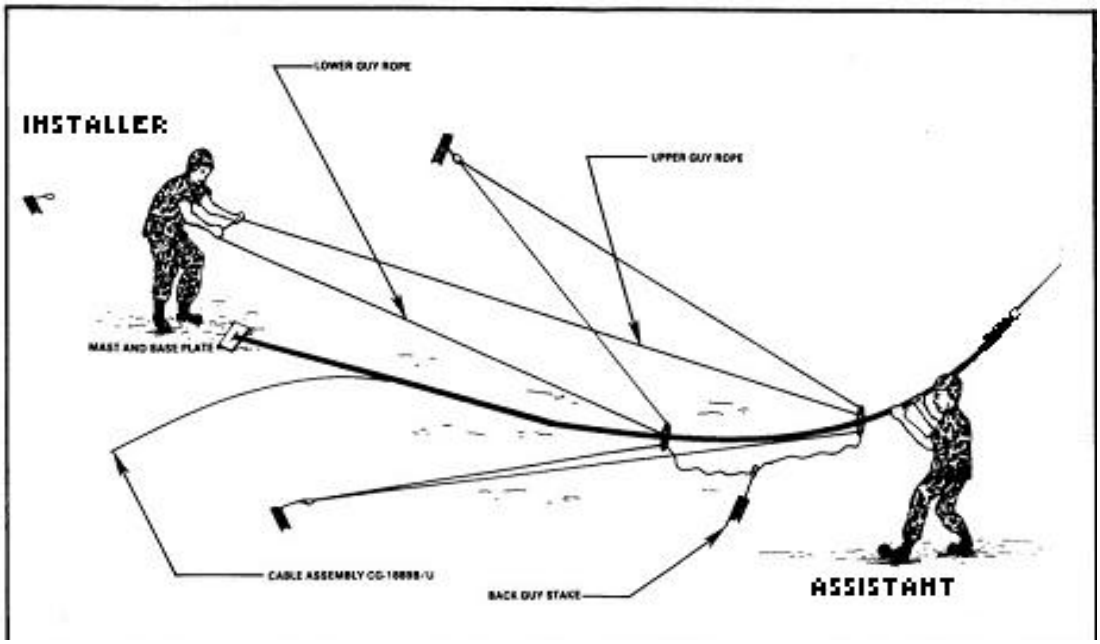


Figure 2-97 Erecting the Antenna Mast

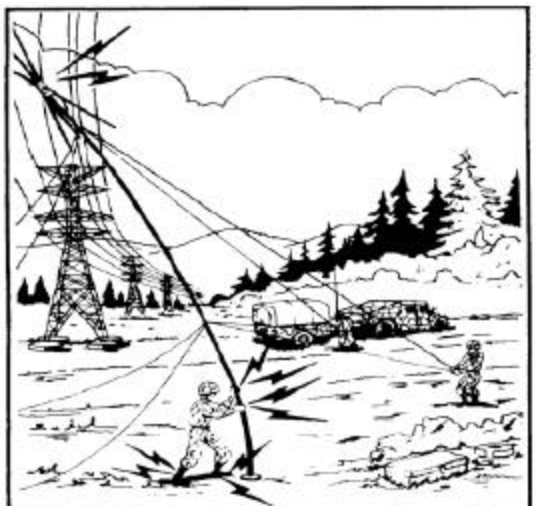


Figure 2-98 Antenna Site With Inadequate Distance Between Power Lines and Antenna Mast

WARNING

If the weather in your area can cause ice to form on the antenna and guys, add extra guys to support the system. Rope off the area and post it with warning signs, such as beware of falling ice. Keep a sharp eye on the anchors and guys. Check them **daily** and immediately before and after bad weather.

2.29.4 Connect the RF Cable to the CBM/CCM Chassis. Same procedure as in Paragraph 2.18.4.

2.30 OPERATING PROCEDURES

2.30.1 CAISI Components Requiring Configuration

The following CAISI components require configuration: (Some of these components are in the CBM, CCM, SSR Transit Case and SSR Notebook Case). Regardless where the component is located, they require the same configuration. Those components specifically in the CBM/CCM are CBM – Wireless Bridge and Inline Encryptor; CCM – Multi-Client Radio Adapter and Inline Encryptor.

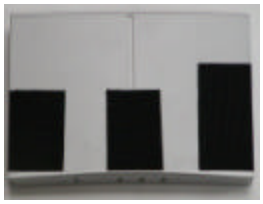
 1. Notebook Computer (SSR Notebook Case)	 2. Wired NIC (SSR Notebook Case)	 3. Wireless NIC (SSR Notebook Case)
 4. Linksys Router (SSR Transit Case) or Netscreen Router (SSR Transit Case)		 5. Wireless Bridge (CBM/SSR Transit Case)
 6. Inline Encryptor (CBM/CCM/SSR Transit Case)	 7. Multi-Client Radio Adapter (CCM/SSR Transit Case)	

Figure 2-99 CAISI Components Requiring Configuration

2.30.2 SSR Notebook Setup and Configuration. The SSR Notebook is used for configuring and monitoring the CAISI components – CBM, CCM, SSR Accessory Kit components. The next few paragraphs will deal with the physical setup of individual components. The actual software configuration is covered in the TB 11-5895-1691-10 using manual or automated configuration.

Table 2-53 CAISI Components Requiring Configuration

#	Component	TM – Physical	TB - Software Manual / Automated
1.	Notebook Computer	Paragraph 2.30.3 - 2.30.7	Paragraph 2.3 – 2.6
2.	Wired NIC	Paragraph 2.30.4	Paragraph 2.7
3.	Wireless NIC Card (public side) With Rabbit Ears Antenna With Large External Antenna	Paragraph 2.30.5 - 2.30.7	Paragraph 2.8
4.	Router	Paragraph 2.31	Paragraph 2.10 / 3.5.1
	CBM	Paragraph 2.32	
5.	Wireless Bridge	Paragraph 2.32.1	Paragraph 2.11.1 / 3.5.2
6.	Inline Encryptor	Paragraph 2.32.2	Paragraph 2.11.6
7.	DSL (Physical connection)	Paragraph 2.32.3 / 2.19.1	N/A
	CCM	Paragraph 2.33	
8.	Multi-client Radio Adapter	Paragraph 2.33.1	Paragraph 2.12.1 / 3.5.3
9.	Inline Encryptor	Paragraph 2.33.2	Paragraph 2.11.6
10.	10Base-T Transceiver (Physical connection only)	Paragraph 2.34	N/A
11.	LSA	Paragraph 2.35.3 – 2.35.4	Paragraph 2.13

Each of the radios, router and encryptors has its own unique way of configuration and firmware update.

1. The wireless bridges are configured from the console or via web pages. You must initially configure them from the console to assign an IP address before you can connect to them over the network.

2. The client radio adapters are configured via web pages only. They do not have console ports.

3. The hardware encryptors are configured from the console port or via secure web pages (https). You must initially configure them from the console to assign an IP address before you can connect to them over the network.

4. The notebook NICs and the encryptor software clients are both configured from utilities installed on the PC.

5. The router does not have a "console" port for configuration. It can only be configured over the network. Neither does it have a telnet server. You can only connect through a web browser.

2.30.2.1 Security Considerations for the CBM

The radios and encryptors contain encryption keys that must be protected along with the rest of the configuration.

SECURITY CONSIDERATIONS

- There is no reset button or "zeroize" switch to reset or remove the configuration, encryption key, or passwords. The wireless bridges and encryptors retain their settings until reset by software.
- Even when you reset a bridge, the radio card inside it retains the encryption key. The only way to remove it is to replace it with another. Set it to all zeros or to the default training key.
- Only the radio link is encrypted, not the LAN link (connected to the hubs). The encryptor sits between the hubs and the radio. Likewise, the DSL links are not encrypted, because they are a part of the protected distribution system (PDS).

The wireless bridges are connected to the "external" ports of the encryptors – the untrusted ports. The data that flows through the encryptor is protected, but communications amongst the radios are not.

SECURITY CONSIDERATIONS

- The radios are in the unprotected zone and you cannot communicate with them from the protected zone.
- In order to configure a radio, you should connect to the console port. Once you are confident in the operation of the radio, you may disable remote access to avoid vulnerabilities associated with the unprotected wireless LAN.

The encryptors are only as secure as the keys used to control the encryption. The AirFortress "Access ID" serves as the preshared encryption key.

SECURITY CONSIDERATIONS

- You must periodically change the encryptor Access IDs.

The DSL bridge has a manual speed switch. You should normally leave it set to "8" for all distances up to four miles. You may have to set it to a slower speed if you go beyond four miles, if your wire is full of splices, or if your wire has some poor splices.

SECURITY CONSIDERATIONS

- The two DSLs must have matching speeds. If the speeds do not match, the DSLs will not synchronize.
- Your field wire line should be included in your PDS. The DSL link is not encrypted.

The hubs have no hardware or software configuration settings. They do, however, have what appears to be an "extra" port. The "Uplink" port is actually connected internally to port number 8. You can use one or the other, but not both.

SECURITY CONSIDERATIONS

- Your network cables from your computers or LSA to the hubs in the CBM should be included in your PDS. They are not encrypted – only the radio links are encrypted.

2.30.2.2 Security Considerations for the CCM:

The multi-client radio adapter has an external reset button. (Refer to Paragraph 2.33.1 for instructions on how to reset the radio adapter).

SECURITY CONSIDERATIONS

- The reset button on the multi-client radio adapter will reset or remove the configuration and passwords, but will not "zeroize" the WEP key.
- If the configuration is reset, the radio will be useless until the SSR reconfigures it. The STAMIS or CSS user has neither the instructions nor the configuration information needed to reconfigure it.

Security for the CCM is the same as that for the CBM, except that the CCM has no DSL bridge.

2.30.3 Using the SSR Notebook. The SSR notebook is a MITAC 7020/7251. This model can change without notice. The notebooks could, theoretically, also require firmware loads, but as of this writing, there is neither a firmware load required nor are there procedures identified. Procedures for upgrading firmware will be developed and promulgated along with required firmware if the need arises.

The notebooks' system setup will depend on the brand and model of the computer used. Some notebooks will have a built-in network interface card (NIC). In these cases, the wired NIC will not be issued.

These notebooks are loaded with the software baseline and are configured when issued by Tobyhanna Army Depot. The using unit need only configure it to their unit.

The software baseline includes the operating system (Windows 2000), utilities and drivers, and application software. A copy of the software baseline is provided on the CD in the SSR Accessory Kit, in case it needs to be reloaded.

NOTE: *Refer to the configuration for the notebook in the TB 11-5895-1691-10, Paragraph 2.3 – 2.8.*

Two network interface cards are provided with the notebook.

1. The **wired NIC** or **built-in NIC** allows you to physically connect to the network for initial configuration and for troubleshooting network problems. You may also use the wired NIC anytime that radio operations are limited for any reason.

2. The **wireless NIC** allows you to connect to the wireless portion of the network. You can easily switch back and forth between the Public and Private segments of the network, or even switch to other networks entirely.

Wired NIC

Wireless NIC

Figure 2-100 Wired NIC and Wireless NIC

The wired NIC is a RealPort 10/100 PC-Bus card. It has a port into which you insert the network cable RJ-45 connector. There is no dongle to get lost or broken. Insert the other end of the cable into any appropriate hub, switch, or bridge on the network. The SSR notebook may be carried anywhere it is required. The SSR notebook will normally be somewhere in a logistics support area. It will normally plug into the nearest remote, but may operate wirelessly.

The wireless NIC is a Cisco Aironet 342 or 352 card. The procedures and utilities for the two cards are identical.

Two major points on when to use the wireless NIC:

1. The wireless NIC may not be used to pass traffic without the remote client encryption software active on the notebook.

2. The wireless NIC should not be used for over-the-air configuration of the CAISI wireless bridges or multi-client radio adapters. It can be used for troubleshooting and aiming the antennas, but you should avoid logging into the radios over the air, since an intruder who has a sniffer and has broken the WEP key could subsequently spoof your address and userid.

   The AirFortress inline encryptor has a management pass-through capability to allow you to view and configure the radios from the trusted side of the network without having to do so over the air. This is the preferred method of operation.

Since there are two types of NIC and they can be connected to either the Public or Private segment of the network, there are four possibilities for connection of the CAISI notebook.

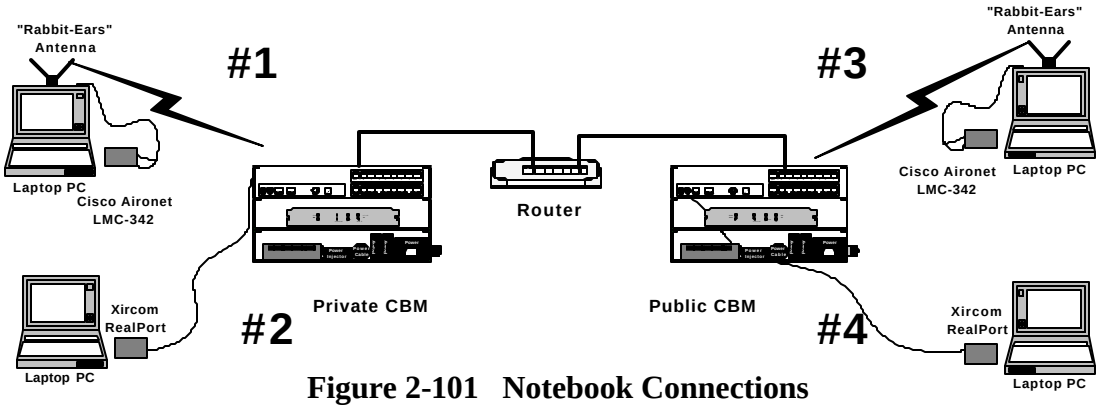


Figure 2-101 Notebook Connections

The notebooks in Configuration #1 and Configuration #3 (using Wireless NICs) include Air Fortress remote encryptor client software. The remote client must be in secure mode when the notebook is passing traffic. If the notebook is used for troubleshooting, such as aiming antennas, it may be in non-secure mode. But you may never pass traffic over the air in non-secure mode. It not only is prohibited, it would just not work, because the encryptors in the CBMs would discard the packets when they were found to be incoming but not properly encrypted.

The notebooks in Configuration #2 and Configuration #4 (using Wired NICs) must have their remote encryptor client software in non-secure mode, because they are coming in to the plain-text side of the encryptors in the CBMs.

Explanation of Figure 2-101: (Numbers in figure correspond to bullets below.)

1. The default configuration for normal operations is Configuration Number 1: the notebook is connected wirelessly to the Private network segment. This allows you to connect from the notebook to any host connected to either the Private or Public network. You can also switch quickly and easily to the Public network if required. The default IP address for the notebook is 192.168.1.2. The default IP address for the wireless bridge through which you are connected is 192.168.1.3

2. Configuration Number 2 is used for initial configuration of the router if the Private wireless bridge is not yet configured. A gray or white straight-through CAT-5 Ethernet cable runs from the Wired NIC to any available port on the Private segment. The default IP address for the notebook is 192.168.1.2, the same as in Configuration Number 1. The default IP address for the router (Private side) is 192.168.1.1

3. Configuration Number 3 and Configuration Number 4 are for use when configuring Public Legacy Support Adapters. Your notebook must be connected to the Public segment to load new firmware, software, or configuration files into Public LSA devices.

2.30.4 Using the SSR Notebook with the Wired NIC. The wired NIC or built-in NIC allows you to physically connect to the network for initial configuration and for troubleshooting network problems within CAISI. You may also use the wired NIC anytime that radio operations are limited for any reason. The CAISI notebook may be carried anywhere it is required.

Connection Procedure:

1. Insert the card into the PCMCIA slot on the notebook.

2. It has a port into which you insert the CAT-5 network cable RJ-45 connector.

Figure 2-102 Wired NIC

3. Insert the other end of the cable into any appropriate device (hub, router or bridge) on the network that you wish to connect to.

In order to use the wired NIC, you must configure TCP/IP. (The drivers for the wired NIC should already be loaded from Tobyhanna). (You do not need to have the Cat-5 network cable attached when you are configuring the card).

NOTE: *The remaining configuration steps are in the TB 11-5895-1691-10, Paragraph 2.7.*

2.30.5 Using the SSR Notebook with the Wireless NIC and Rabbit Ears Antenna.
The Wireless NIC may be used for configuration changes during operations, for monitoring, and for routine operations from the immediate vicinity of a CBM.

The wireless NIC allows you to connect to the wireless portion off the network. You can easily switch back and forth between the Public and Private segments of the network or even switch to other networks entirely.

SSR Notebook

Wireless NIC

Rabbit Ears Antenna

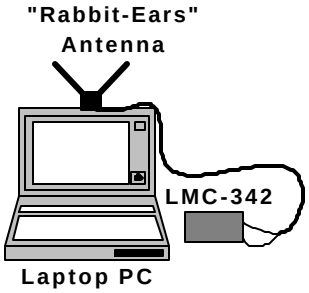


Figure 2-103 SSR Notebook with Wireless NIC and Rabbit Ears Antenna

Connection Procedures of the PCMCIA card is the following: (Figure 2-104)

1. Insert the connectors on the rabbit-ears antenna cable into the two holes on the end of the card. (Be extremely careful when connecting and disconnecting the connectors, they are very delicate).

Figure 2-104 Rabbit Ears Antenna and Wireless NIC

2. Insert the card into the PCMCIA slot on the notebook.

3. Place the rabbit-ears antenna on the velcro patch on the back of the notebook screen.

In order to use the wireless NIC, you must configure TCP/IP, load the wireless NIC drivers, the wireless NIC utilities and the remote encryptor client software.

NOTE: *The notebook should come from Tobyhanna with the drivers for the wireless NIC, the wireless NIC utilities, and the remote encryptor client software already loaded. Without the remote encryptor client software, you cannot communicate, because the radios have remote access disabled and the encryptors are protecting the rest of the network.*

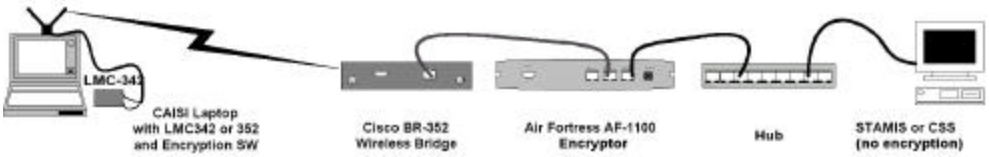


Figure 2-105 Wireless Client Encryption

NOTE: *The remaining configuration steps are in the TB 11-5895-1691-10, Paragraph 2.8.*

2.30.6 Using the SSR Notebook with the Wireless NIC and Large Antennas. If you need to use your notebook with a large external antenna such as the whips (40-inch or 24-inch) or panels (7-inch) issued with the CBM or CCM, you will need adapter cables.

The antenna adapter cables in Figure 2-106 can be used with the SSR Notebook in order to configure or troubleshoot components.

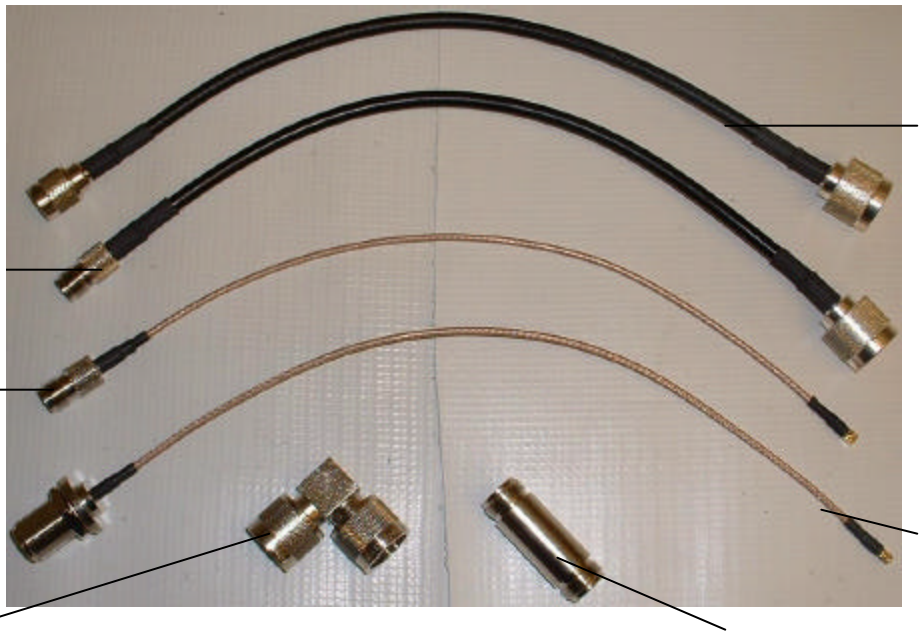
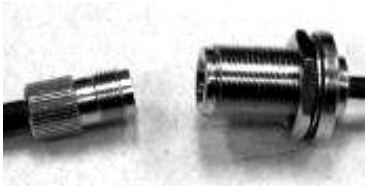


Figure 2-106 Antenna Adapter Cables, Right Angle Adapter and Barrel Connector

NOTE: *There are two nearly identical cables in the SSR kit. One goes from an MMCX connector (the tiny connector that goes to the PCMCIA card) to an RPTNC (the same connector as that on the bridge and radio adapter). The other goes from an MMCX to a female N (the same connector as that on the back of the panel antennas. The RPTNC is smaller than the N connector*



RPTNC **N**

Figure 2-107 RPTNC and N Connector

MMCX is a very small snap-in antenna connector that looks like a miniature version of the push-on type cable television connectors. TNC is a threaded version of the BNC (British Naval Connector) commonly found on network coaxial cables.

Which cable you use depends on what you are doing.

1. Use the cables listed above if you are installing a large antenna outdoors.

2. Use some or all of them to troubleshoot the radio, cables, and lightning arrestor inside a CBM or CCM.

3. Use the MMCX to N (F) adapter to connect directly to the antenna cable for troubleshooting or aiming the antenna.

The SSR Accessory Kit also includes two 40-inch Whip antennas and a 14-inch Panel antenna. These antennas can be set up on a temporary or permanent use.

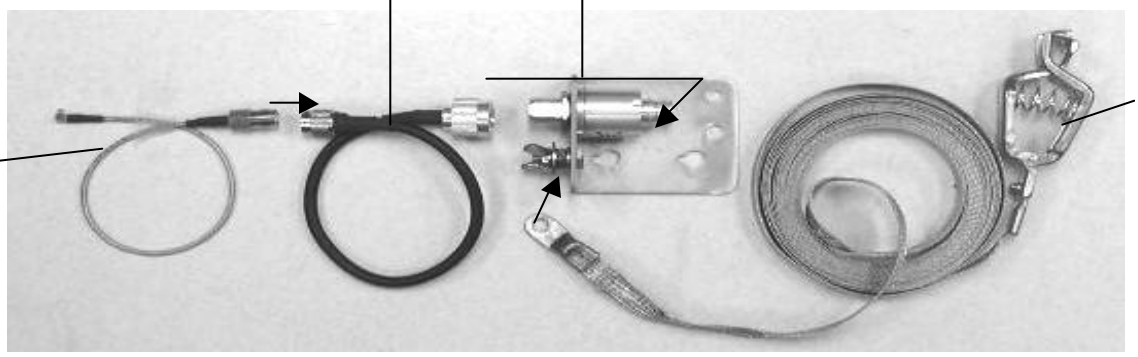


Figure 2-108 Wireless NIC Antenna Adapters

The four items you need are shown on Figure 2-108 and listed below. (Arrows show how they connect). They are included in your SSR Transit Case for use in troubleshooting, as spares, or with the wireless bridge or radio adapter.

1. An MMCX to reverse-polarity TNC (RPTNC) adapter cable (this RPTNC is female with a male pin).
2. A 12-in RF Antenna N (M) to RPTNC (male with female pin) adapter cable.
3. A lightning arrestor assembly (lightning arrestor mounted in the bracket).
4. A grounding strap.

Permanent use: Notebook will stay in place for a long period of time.

1. Connect terminal lug of grounding strap to the ground stud, and then connect the other end (clamp) to a grounding rod.
2. Connect the end of the MMCX to RPTNC Cable to the small end of the 12-inch RF antenna cable.
3. Connect the large end of the 12-inch RF antenna cable to the small end of the lightning arrestor.
4. Connect a RF antenna cable (25, 35, or 50 ft) (not shown) to the large end of the lightning arrestor.
5. Connect the end of the RF antenna cable to the antenna used. Steps are shown in Paragraph 2.18.3.
6. Insert wireless NIC into notebook.
7. Connect the small end of the MMCX to RPTNC Cable to the right connector on the Wireless NIC card.

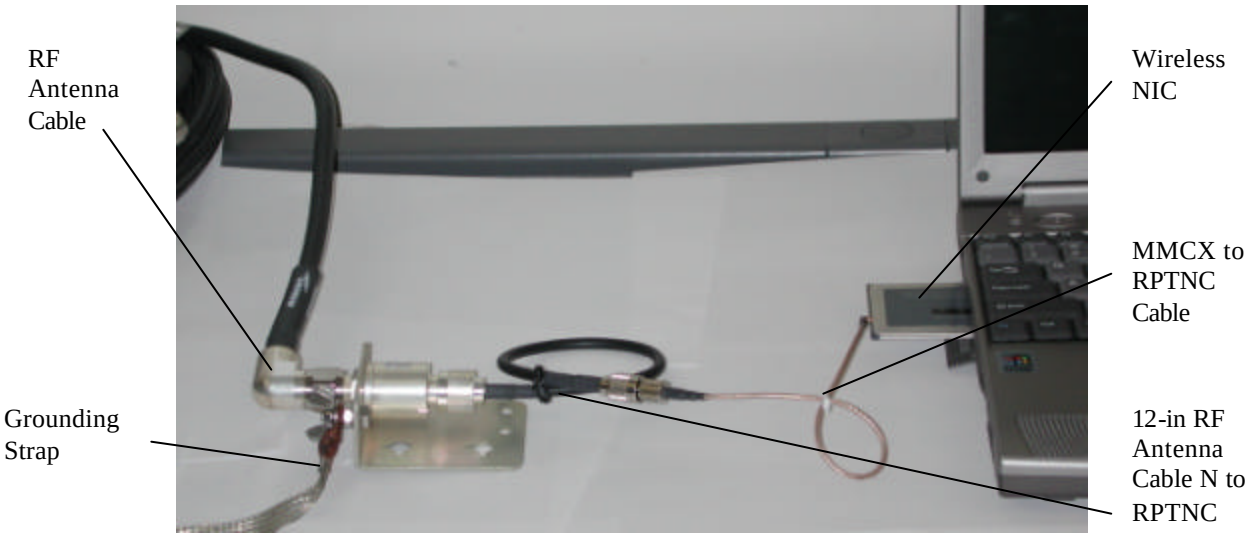


Figure 2-109 Permanent Connection of Large Antenna to SSR Notebook

Temporary use: If you are only going to check a configuration, make a quick change to the configuration, aim an antenna or monitor the network for a short period of time, (less than 6 hours), you will only need to do the following:

1. Connect the small end of the MMCX to RPTNC cable to the right connector on the Wireless NIC card.

2. Connect the end of the MMCX to RPTNC Cable to the small end of the 12-inch RF antenna cable.

3. Connect the right angle adapter to the 24-inch or 40-inch Whip antenna. Panel antenna will not need this adapter. (The 4-inch Whip antenna can also be used here. The right angle adapter would not be needed).

4. Connect the large end of the 12-inch RF antenna cable to the right angle adapter, panel antenna or the 4-inch Whip antenna, if used.

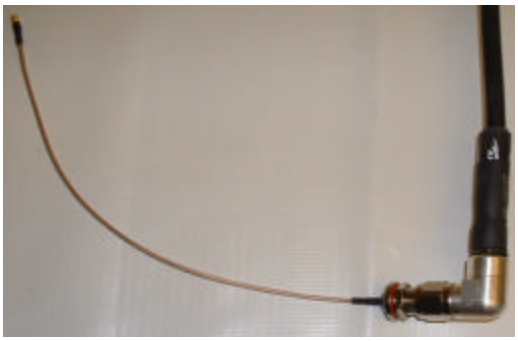


Figure 2-110 Temporary Connection of Large Antenna to SSR Notebook

NOTE: *The remaining configuration steps for the wireless NIC are in the TB 11-5895-1691-10, Paragraph 2.8.*

2.31 CONFIGURE THE ROUTER.

The Router segments the network to provide firewall security to STAMIS and CSS clients connected behind the firewall. If you choose to use it, it splits the network into two segments – one "public" and one "private." For more information on when to utilize a Router, refer to Paragraph I.3.9.

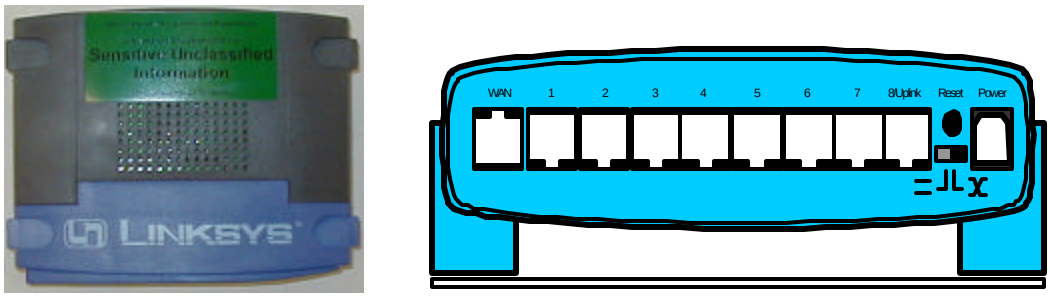


Figure 2-111 Router Configuration Ports

The router does not have a "console" port for configuration. It can only be configured over the network. Neither does it have a telnet server or a ssh (secure shell) server. You can only connect through a non-secure web browser (http, not https).

1. Due to this limitation, you should disconnect the router from the network to configure it. This will prevent anyone from monitoring the network and picking up your configuration password.

2. If you do not know the IP address or password, you can still configure the router. To reset the router to factory defaults, insert the reset tool or a paper clip in the reset button hole and hold it for 10 seconds. During this process, the "Diag" light is lit, the "Link" light is lit and then both lights will go off indicating the router is reset. (Both lights are located on the right front panel of the router).

There are eight LAN port connections on the back of the router. Port number eight is labeled "8/Uplink" and can be used in either straight-through mode or in crossover mode for an uplink to a hub or switch.

a. A switch controls the port. Slide the switch to the left to the "=" position if you are connecting a computer. Slide the switch right to the "X" position if you are connecting a hub and would otherwise need a crossover cable.

Connection of the router:

1. Remove the router, power adapter, 3-prong power cord and a white straight-through Ethernet cable from the SSR Transit Case.

2. Connect the power adapter to the port labeled "Power" on the back of the router.

3. Connect the female end of the 3-prong power cord to the power adapter. Plug the male end of the 3-prong power cord into an external power source.

   NOTE: *If the router is receiving power, the "Power" LED on the front of the router will be lit green.*

4. Insert the wired NIC into the SSR notebook.

5. Connect one end of a white straight-through Ethernet cable to the Wired NIC on your SSR Notebook and the other end into an available port on the router (ports 1-7).

   NOTE: *Or you can use a red crossover cable connected to port 8 with the uplink switch set to crossover mode (set the "=/X" switch set to "X").*

   NOTE: *Do not connect to the WAN port. The WAN port is upside down relative to the LAN ports. This is intentional to help keep you from accidentally connecting to the wrong*

6. Apply power to the SSR Notebook.

NOTE: *The remaining configuration steps are in the TB 11-5895-1691-10, Paragraph 2.10 (manual) / 3.5.1 (CAISI Admin).*

2.32 CONFIGURE THE CBM.

The CBM includes three components that require configuration before it can be put into operation. They are the wireless bridge, inline encryptor and the DSL. (DSL is a physical connection not software configuration. DSL will only be connected when it is actually being used).

2.32.1 Using the SSR Notebook to Configure the Wireless Bridge.

The wireless bridges are included in the CBM. This particular model included in the CAISI is a BR352. As noted, a spare is also included in the SSR Accessory Kit as a maintenance spare or use as a stand-alone in exceptional circumstances.

Procedures to configure are the same for the Wireless Bridge in the CBM as it is for the Wireless Bridge in the SSR Accessory Kit.

Bridges are configured from the console or via web pages. You must **initially configure them from the console to assign an IP address before you can connect with a web browser over the network.**

At a minimum, you need to change the SSID, WEP key, and passwords; and, when you are done, you need to disable remote access to the bridges. Additionally you need to set one of the CBM bridges in each CAISI to root bridge mode.

The BR-352 does not have a reset button like the Multi-Client Radio Adapter (WGB-352). If you receive a new bridge from the factory, or if you have to **reset** your bridge because of lost passwords or for any other reason, you need to configure it from scratch – it will not be at Tobyhanna preset configurations.

The SSR notebook must have the current set of drivers, firmware images, and program files. It must be assigned a static TCP/IP address of 192.168.1.2. It must have its Wired NIC installed if this is the initial configuration.

Physical Connections:

1. Connect CBM power cables.

    a. Remove the CBM Chassis, UPS, a 3-prong and a 2-prong power cord from the CBM transit case.

    b. Attach the 3-prong power cable to the wireless bridge power supply; which is the leftmost power supply located in the base section of the CBM chassis.

    c. Connect the 2-prong power cord to the hub and encryptor power supply; which is the rightmost power supply on the chassis base section.

    d. Place the UPS next to CBM chassis.

    e. Plug the wireless bridge, hub and encryptor power cords into the section on the UPS labeled "Battery Backup Protected Outlets."

    f. Plug the UPS into a grounded outlet. **DO NOT APPLY POWER AT THIS TIME.**

2. Connect an antenna and grounding strap to CBM. There are several antennas you can use when configuring the wireless bridge.

    a. Connecting the grounding strap is in Paragraph 2.18.1.

    b. Procedures for using the 40-inch Whip is in Paragraphs 2.18.2 – 2.18.4. Procedures for the 7-inch Panel antenna is in Paragraph 2.19.2.

    c. Use of the 4-inch whip in the SSR Transit (**Indoor use only**)

        (1) Remove the 4-inch whip, N to RPTNC (F) RF adapter cable from the SSR Transit case.

        (2) Connect the large end of the RF Adapter cable to the lightning arrestor on the CBM.

(3) Connect the small end of the RF Adapter cable to the antenna connection on the 4-inch whip. (Use a Velcro strap or wire tie to hold the antenna upright against the CBM chassis).

Figure 2-112 Connect 4-inch Whip Antenna to CBM

d. Use of the right-angle adapter and 40-inch whip antenna.

(1) Remove a right-angle adapter from the SSR Transit Case or the SSR Notebook Case. You may get the 40-inch whip out of the CBM transit case or the SSR Transit Case.

(2) Connect the right-angle adapter to the lighting arrestor on the CBM.

(3) Connect the 40-inch whip antenna to the other end of the right-angle adapter

Figure 2-113 Connect Right-Angle Adapter and 40-inch Antenna to CBM

3. Connect CBM wireless bridge to notebook Wired NIC.

a. Disconnect the red crossover cable from the port labeled “External” or “encrypted” on the back of the Inline encryptor.

b. Remove the RJ-45 straight-through adapter and a straight-through cable from your SSR Notebook case.

c. Connect the free end of the red crossover cable to the RJ-45 straight through adapter.

d. Plug one end of the straight-through cable into the RJ-45 straight-through adapter and the other end of the cable into the Wired NIC.

e. You are now connected from your Wired NIC to the “Network” port on the power injector.

f. Connect the blue straight-through nine-pin serial cable (M-F) from the SSR notebook to the console port on the bridge.

Figure 2-114 Wireless Bridge Serial Connection

NOTE: *The remaining configuration steps are in the TB 11-5895-1691-10, Paragraph 2.11.1 (manual) / Paragraph 3.5.2 (CAISI Admin).*

2.32.1.1 Physical Connection of SSR Wireless Bridge for Configuration. If the wireless bridge is not in a CBM**,** be aware that you must connect to the "Network" port of the power injector. If you connect to the "AP/Bridge" port, you can damage your Wired NIC. If you bypass the injector and connect directly into the bridge "Ethernet" port, the bridge will not work because it will not be getting power.

First, you must attach an antenna to the wireless bridge before adding power.

1. Remove the wireless bridge, power supply and injector, 3-prong power cord, lightning arrestor assembly, 12-inch RF (N) to RPTNC (M) adapter cable, red Ethernet crossover cable and a white straight-through Ethernet cable.

2. Connect terminal lug of grounding strap to the ground stud of the lightning arrestor assembly, and then connect the other end (clamp) to a grounding rod.

3. Connect small end of the 12-inch RF antenna cable to the "Right/Primary" antenna connector on the rear of the wireless bridge.

Figure 2-115 Connect Antenna to SSR Wireless Bridge

4. Connect the large end of the 12-inch RF antenna cable to the small end of the lightning arrestor.

5. Connect a RF antenna cable (25, 35, or 50 ft) (not shown) to the large end of the lightning arrestor.

6. Connect the end of the RF antenna cable to the antenna used. Steps are shown in Paragraph 2.18.3.

Second, connect the SSR Notebook to the SSR Wireless Bridge.

1. Connect a red Ethernet crossover cable from the notebook network port to the bridge power injector network port.

2. Connect a white straight through Ethernet cable from the "AP/Bridge" port on the power injector to the "Inline Power Ethernet" port on the bridge.

NOTE: *The remaining configuration steps are in the TB 11-5895-1691-10, Paragraph 2.11.1 (manual) / Paragraph 3.5.2 (CAISI Admin).*

Figure 2-116 SSR Wireless Bridge, Power Supply and Power Injector

2.32.1.2 Physical Connections of SSR Wireless Bridge for Operation.

NOTE: *The SSR Wireless Bridge must be used with the SSR Inline Encryptor when in operation. The connections are the same as those that are in the CBM chassis. Refer to Paragraph 1.19.1 for the CBM Architecture. The use of a SSR hub is optional but it will allow more computers to connect to the SSR wireless bridge at its location. The steps for connecting the wireless bridge to the inline encryptor are below:*

The SSR Wireless Bridge and Inline Encryptor must be configured before operation. Procedures are in Paragraph 2.32.1.1

First, you must attach an antenna to the wireless bridge before adding power.

1. Remove the wireless bridge, power supply and injector, 3-prong power cord, Inline encryptor, 3-lead power supply, 2-prong power cord, one hub (optional), UPS (optional), lightning arrestor assembly, 12-inch RF (N) to RPTNC (M) adapter cable, one of the antennas: 4-inch whip, 40-inch whip, 7-inch panel, or 14-inch panel), grounding strap, RF antenna cable (25, 35 or 50ft), red crossover Ethernet cable and two white straight-through Ethernet cables.

2. Connect terminal lug of grounding strap to the ground stud of the lightning arrestor assembly, and then connect the other end (clamp) to a grounding rod.

3. Connect small end of the 12-inch RF antenna cable to the "Right/Primary" antenna connector on the rear of the wireless bridge.

4. Connect the large end of the 12-inch RF antenna cable to the small end of the lightning arrestor.

5. Connect a RF antenna cable (25, 35, or 50 ft) (not shown) to the large end of the lightning arrestor.

6. Connect the end of the RF antenna cable to the antenna used. Steps are shown in Paragraph 2.18.3.

Second, the cable connections for SSR Wireless Bridge, Inline Encryptor and Hub.

1. A red crossover Ethernet cable runs from the "External/Encrypted" port of the inline encryptor to the "Network" port on the power injector of the wireless bridge.

2. A white straight-through Ethernet cable runs from the "AP/Bridge" port on the power injector to the "Inline Power Ethernet" port on the back of the bridge.

3. (If you want to add an SSR hub): A white straight-through Ethernet cable runs from a 10Base-T port of a hub to the "Internal/Unencrypted" port on the inline encryptor.

4. Connect the 3-prong power cord to the wireless bridge power supply. Connect the leads of the 3-lead power supply to the inline encryptor and hub. Then connect the 2-prong power cord to the 3-lead power supply.

5. Connect all of the power cords to an UPS.

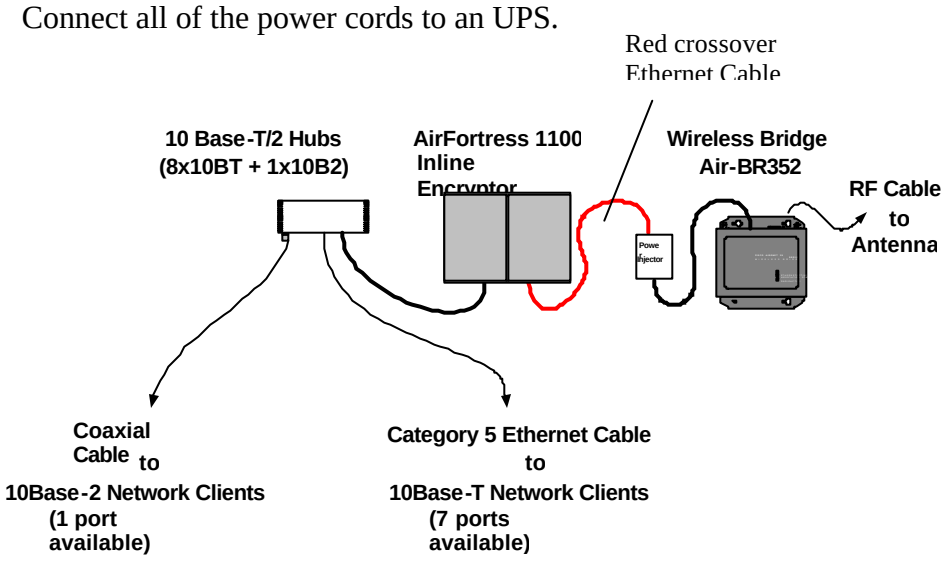


Figure 2-117 SSR Wireless Bridge and Inline Encryptor Connections

2.32.2 Configuring the Inline Encryptor.

The encryptor has been discussed along with the radios, and its connection was even bundled into the radio connection instructions. But configuration is another matter. The encryptors are configured separately from the radios. Changes to one have no effect on the other.

The inline encryptors you receive from Tobyhanna Army Depot will be preset to the CAISI standard configuration. This includes the encryptors in the SSR Accessory Kit as well as the encryptors installed in the CBMs/CCMs.

At a minimum, the SSR needs to change the Access ID and passwords. The encryptors can be configured over the console port or via secure web pages (https).

The SSR notebook must have the current set of drivers, firmware images, and program files. It must be assigned a static TCP/IP address of 192.168.1.2. It must have its Wired NIC installed.

1. Ensure the encryptor is receiving power. Refer to physical connection procedures in Paragraph 2.32.1.

2. Connect your notebook to the serial port of the encryptor with the beige nine-pin (F – F) null model (crossover) serial cable from the SSR Transit Case.

3. Insert Wired NIC into SSR Notebook. Connect the wired NIC to the hub in the CBM/CCM with a white straight-through Ethernet cable.

4. Ensure the Notebook is receiving power.

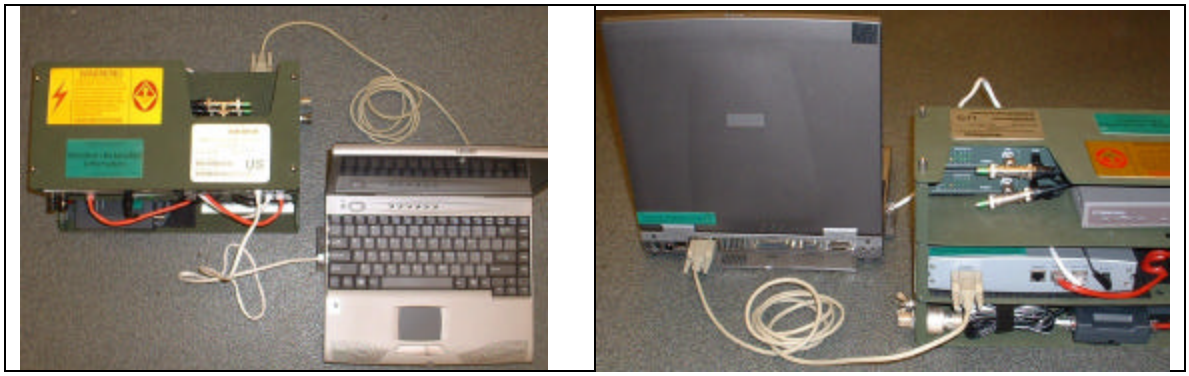


Figure 2-118 Inline Encryptor Console Configuration

NOTE: *The remaining configuration steps are in the TB 11-5895-1691-10, Paragraph 2.11.6 (manual).*

2.32.3 Configuring the DSL in the CBM. There is no software configuration for the DSL only the physical connection. The procedures for the physical connection of the DSL are in Paragraph 2.19.1.

2.33 CONFIGURE THE CCM.

The CCM includes two components that require configuration before it can be put into operation. They are the multi-client radio adapter and the inline encryptor.

2.33.1 Using the SSR Notebook to Configure the Multi-Client Radio Adapter.

The multi-client radio adapter does not have a console port. You can only configure it over the network. If you are changing parameters on an operational adapter, you can only configure over the wired portion of the network.

At a minimum, you need to change the SSID, WEP key, and passwords; and, when you are done, you need to disable remote access.

The SSR notebook must have the current set of drivers, firmware images, and program files. It must be assigned a static TCP/IP address of 192.168.1.2. It must have its Wired NIC installed.

Physical Connections:

1. Connect CCM power cables.

   a. Remove the CCM Chassis, and a 3-prong cord from the CCM carrying case.

   b. Attach the 3-prong power cable to the multi-client radio adapter, hub and encryptor power supply located in the base section of the CCM chassis.

   c. **DO NOT APPLY POWER AT THIS TIME.**

2. Connect an antenna and grounding strap to CCM. There are several antennas you can use when configuring the multi-client radio adapter – 4-inch whip, 24-inch whip.

   a. Connecting the grounding strap is in Paragraph 2.18.1.

   b. Procedures for using the 24-inch Whip are the same as the 40-inch Whip in Paragraphs 2.18.2 – 2.18.4.

   c. Use of the 4-inch whip in the SSR Transit Case (**Indoor use only**)

      (1) Remove the 4-inch whip, N to RPTNC (F) RF adapter cable from the SSR Transit case.

      (2) Connect the large end of the RF Adapter cable to the lightning arrestor on the CCM.

      (3) Connect the small end of the RF Adapter cable to the antenna connection on the 4-inch whip. (Use a Velcro strap or wire tie to hold the antenna upright against the CCM chassis).

Figure 2-119 Connect 4-inch Whip Antenna to CCM

d. Use of the right-angle adapter and 24-inch whip antenna.

(1) Remove a right-angle adapter from the SSR Transit Case or the SSR Notebook Case. Remove the 24-inch whip from the CCM carrying case.

(2) Connect the right-angle adapter to the lighting arrestor on the CCM.

(3) Connect the 24-inch whip antenna to the other end of the right-angle adapter.

Figure 2-120 Connect Right-Angle Adapter and 24-inch Antenna to CCM

3. Connect CCM Multi-Client Radio Adapter to notebook Wired NIC.

a. Disconnect the red crossover cable from the port labeled “External” or “encrypted” on the back of the AF-1100 encryptor.

b. Remove the RJ-45 straight-through adapter and a straight-through cable from your SSR Notebook case.

c. Connect the free end of the red crossover cable to the RJ-45 straight through adapter.

d. Plug one end of the straight-through cable into the RJ-45 straight-through adapter and the other end of the cable into the Wired NIC.

e. You are now connected from your Wired NIC to the Ethernet port on the multi-client radio adapter.

NOTE: *The remaining configuration steps are in the TB 11-5895-1691-10, Paragraph 2.12.1 (manual) / Paragraph 3.5.3 (CAISI Admin).*

2.33.1.1 Reset Multi-Client Radio Adapter. Unlike the wireless bridges, the radio adapters ***do*** have a ***physical reset*** button. Use it as follows to reset the radio back to factory default.

1. With the radio powered, insert the reset tool, a paperclip, awl, or similar tool into the tiny unlabeled hole next to the power connector (labeled "5VDC).

2. You will feel and hear a small click. Press and hold the button for about ten seconds.

3. All the lights on the adapter will go out.

4. After a few seconds, the Association light (the center one) will flash red, then immediately go out.

5. Continue to hold the reset button until you see the Ethernet light (the one closest to the connector's side of the radio) flicker briefly.

If the radio is fresh from Tobyhanna, the CAISI preset address (Tobyhanna default) is "192.168.1.5" for all radio adapters. The Cisco factory default address is "192.168.200.1".

2.33.1.2 Physical Connection of SSR Multi-Client Radio Adaptor for Configuration.

First, you must attach an antenna to the multi-client radio adapter before adding power.

1. Remove the radio adapter, 3-prong power cord, lightning arrestor assembly, 12-inch RF N to RPTNC (M) cable, and a red Ethernet crossover cable.

2. Connect terminal lug of grounding strap to the ground stud of the lightning arrestor assembly, and then connect the other end (clamp) to a grounding rod.

3. Connect small end of the 12-inch RF antenna cable to the "Right/Primary" antenna connector on the rear of the wireless bridge.

Figure 2-121 Connect Antenna to SSR Multi-Client Radio Adapter

4. Connect the large end of the 12-inch RF antenna cable to the small end of the lightning arrestor.

5. Connect a RF antenna cable (25, 35, or 50 ft) (not shown) to the large end of the lightning arrestor.

6. Connect the end of the RF antenna cable to the antenna used. Steps are shown in Paragraph 2.18.3.

Second, connect the SSR Notebook to the Multi-Client Radio Adapter.

1. Connect a red Ethernet crossover cable from the wired NIC in the SSR Notebook to the Ethernet port on the multi-client radio adapter.

NOTE: *The remaining configuration steps are in the TB 11-5895-1691-10, Paragraph 2.12.1 (manual) / Paragraph 3.5.3 (CAISI Admin).*

2.33.1.3 Physical Connections of SSR Multi-Client Radio Adapter for Operation.

NOTE: *The SSR Multi-client radio adapter must be used with the SSR Inline Encryptor when in operation. The connections are the same as those that are in the CCM chassis. Refer to Paragraph 1.19.2 for the CCM Architecture. The use of a SSR hub is optional but it will allow more computers to connect to the SSR multi-client radio adapter at its location. The steps to for connecting the multi-client radio adapter and inline encryptor are below:*

SSR Multi-Client Radio Adapter and Inline Encryptor must be configured before use. Refer to Paragraph 2.32.2 and Paragraph 2.33.1.

First, you must attach an antenna to the multi-client radio adapter before adding power.

1. Remove the radio adapter, 3-prong power cord, Inline encryptor, 3-lead power supply, 2-prong power cord, one hub (optional), lightning arrestor assembly, 12-inch RF N to RPTNC (M) cable, one of the antennas – 4-inch whip, 24-inch whip, grounding strap, RF antenna cable (35 or 50 ft), a red Ethernet crossover cable and a white straight-through Ethernet cable.

2. Connect terminal lug of grounding strap to the ground stud of the lightning arrestor assembly, and then connect the other end (clamp) to a grounding rod.

3. Connect small end of the 12-inch RF antenna cable to the “Right/Primary” antenna connector on the rear of the multi-client radio adapter.

4. Connect the large end of the 12-inch RF antenna cable to the small end of the lightning arrestor.

5. Connect a RF antenna cable (25, 35, or 50 ft) (not shown) to the large end of the lightning arrestor.

6. Connect the end of the RF antenna cable to the antenna used. Steps are shown in Paragraph 2.18.3.

Second, the cable connections for SSR Multi-client Radio Adapter, Inline Encryptor and Hub.

1. A white straight-through Ethernet cable runs from any port on the hub to the “Internal/Unencrypted” port on the inline encryptor.

2. A red crossover Ethernet cable runs from the “External/Encrypted” port of the inline encryptor to Ethernet port on the Multi-Client Radio Adapter.

3. Connect the leads of the 3-lead power supply to the radio adapter, inline encryptor and hub. Then connect the 2-prong power cord to the 3-lead power supply. Connect power cord to power source.

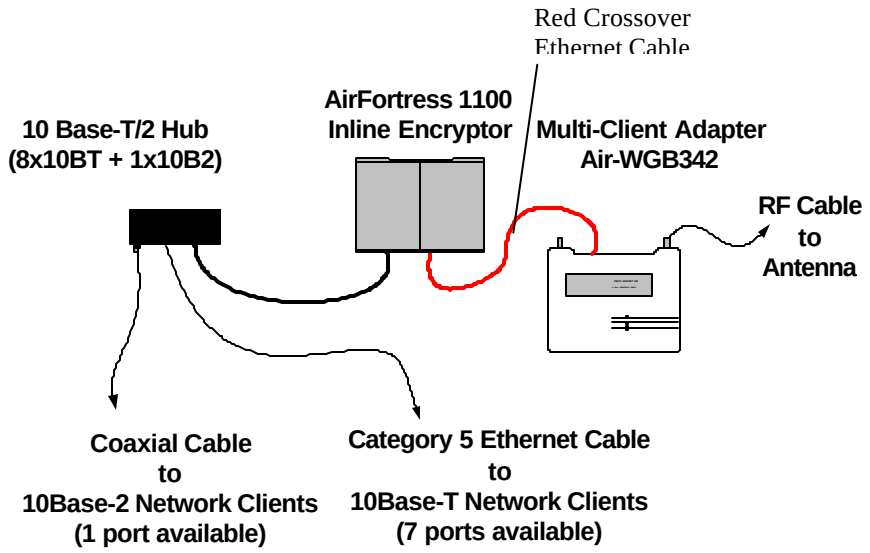


Figure 2-122 SSR Multi-Client Radio Adapter and Inline Encryptor Connections

2.33.2 Configure the Inline Encryptor. Configuration of the inline encryptor was already discussed with the CBM in Paragraph 2.32.2. It is the same procedure.

2.34 10Base-T TRANSCEIVER CONNECTION. Transceivers allow you to connect media other than an Auxiliary Unit Interface (AUI) cable to an AUI port on a computer or network device. The SSR Accessory Kit includes a 10BaseT transceiver. The current model is CentreCOM 210TS.

The transceiver is provided in case you need to connect a 10Base-T device to the NES. The NES connection is an Auxiliary Unit Interface (AUI) port. The Signal unit has a 10Base-2 transceiver to allow CAISI to connect a 10Base-2 cable (RG-58), but does not have a 10Base-T transceiver.

Figure 2-123 10Base-T Transceiver

NOTE: *Be sure the Signal Quality Error (SQE) Test Switch (heartbeat) on the side of the transceiver is set to O (off). Slide the switch to the left.*

Connection procedures for the 10Base-T Transceiver are:

1. Remove the 10Base-2 transceiver at the INE/NES that is attached to the AUI port, the J (1) port (red side). (Signal personnel will probably do this).

2. Connect the 15-pin connector of the 10Base-T transceiver to the AUI port, the J(1) port (red side).

3. Connect a CAT-5 Ethernet cable to the RJ-45 port on the transceiver.

4. Connect other end of the CAT-5 Ethernet cable to one of the 10Base-T ports on the CBM. (Remember, maximum length of CAT-5 ethernet cable is 100 meters).

There are **four ways** that CAISI can connect to the INE/NES.

1. CBM to INE using RG-58 cable (discussed in Paragraph 2.18.8)

2. CBM to INE using 10Base-T Transceiver (discussed above)

3. SSR Wireless Bridge to INE using 10Base-T Transceiver

4. SSR DSL Bridge to INE using 10Base-T Transceiver.

Instead of using the root CBM or remote CBM to connect to the NES, the SSR Wireless Bridge or DSL bridge can be used. The transceiver is used as shown in Figure 2-124.

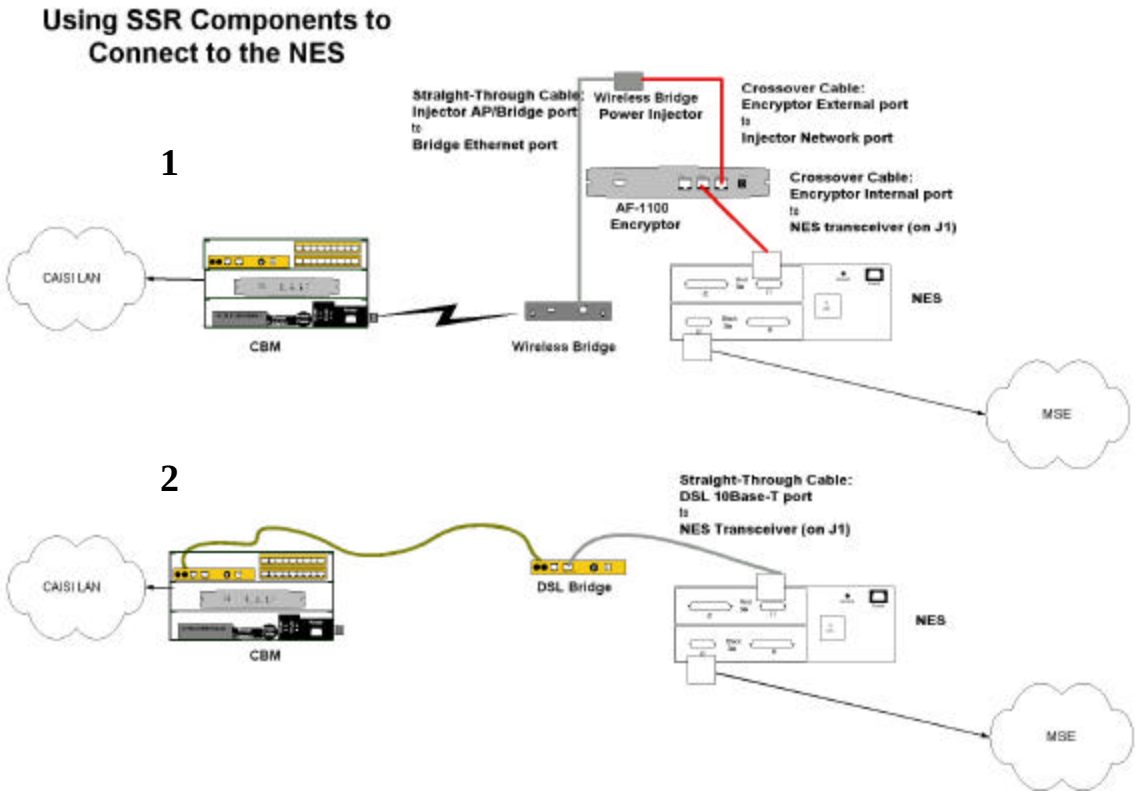


Figure 2-124 10Base-T Transceiver Used at the NES

NOTE: *The transceiver does not require configuration.*

The radios in the two networks depicted in Figure 2-124 (Number 1) are all encrypted, although at different levels:

1. MSE has type-1 cryptographic devices in the radio vans operating at the SECRET level. Command and control voice and data traffic is protected from interception and intrusion. The NES is required in addition to the cryptographics in the radio vans, to keep the SBU traffic separate from the SECRET traffic. It protects the SECRET network from CAISI users, in the same way that the cryptographics in the vans protect the over-the-air network from outsiders. It also, of course, protects the CAISI network from SECRET users.

2. The CAISI radios are secured by the built-in WEP, however WEP is not sufficient to protect SBU traffic. So the CAISI network has the AirFortress in addition to WEP. WEP protects the radios themselves from casual interception and manipulation. The AirFortress encryptors protect the traffic.

2.34.1 Connect SSR Wireless Bridge to the INE/NES. This procedure is illustrated as number 1 in Figure 2-124 and explained further in Table 2-54.

1. You will need the SSR Wireless Bridge, Power & Injector for wireless bridge, inline encryptor, a white 10BaseT straight through cable, two red crossover Ethernet cables, lightning arrestor assembly, and the SSR 10Base-T Transceiver, power supply for inline encryptor, 2-prong power cord. (Figure 2-125)

NOTE: *You cannot substitute the SSR Multi-Client Radio Adapter for this connection. It must be the Wireless Bridge.*

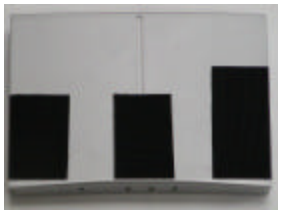
Wireless Bridge	Power Supply & Power Injector for Wireless Bridge	 Inline Encryptor
White 10Base-T Straight-Through Ethernet Cable	Red Crossover Ethernet Cable (Qty 2)	10Base-T Transceiver
Lightning Arrestor Assembly	40-inch Whip Antenna	Power Supply, 5V, 3 Leads (will only use 1 of the leads for the inline encryptor)
2-prong power cord	Hub (Optional)	The hub is an optional component that can be used so that other users can connect to the SSR Wireless Bridge where it is set up. The hub will use one of the leads from the above power supply.

Figure 2-125 Connect to INE Using SSR Wireless Bridge Components

2. The Root CBM will connect wirelessly to the SSR Wireless Bridge.

3. Be sure the Signal Quality Error (SQE) Test Switch (heartbeat) is set to O (off) (Slide the switch to the left).

4. Connect one end of a white straight-through CAT-5 Ethernet cable from the "Ethernet" port on the wireless bridge to the "AP/Bridge" port on the power injector.

CAUTION

The power injector has two ports: one labeled "Network" and one labeled "AP/Bridge." Be careful not to connect network components to the "AP/Bridge" port. The voltage present on that port can damage equipment other than the bridges.

5. Connect one end of a red crossover CAT-5 Ethernet cable from the "Network" port on the power injector to the "External/Encrypted" data port on the encryptor.

6. Use a red crossover cat-5 Ethernet cable to go from the "Internal/Unencrypted" data port on the encryptor to the 10Base-T port on the transceiver.

7. Disconnect the Signal 10Base2 transceiver from the AUI port (J1) on the NES. (Signal unit will do this).

8. Connect the transceiver to the "Red" ("Plain Text") AUI port (J1) on the NES. (Same place where you took the 10Base2 transceiver from). ***Never connect to the "Black" ("Cypher Text") port.***

NOTE: *If TACLANE is used instead of NES, no transceiver is required.*

Although the TACLANE has AUI ports, it also has RJ-45 Ethernet ports, so The10Base-T Transceiver is not needed.

Connect to the "Plain Text (PT)" RJ-45 port, near the top in the center section section of the back of the TACLANE.

Never connect to the "CYPHER TEXT (CT)" port.

CAUTION

The back of the TACLANE also has connectors that look like 10Base-2 connectors, but are not. If you use these connectors, you can damage the TACLANE or your CAISI equipment.

Never connect anything to a TACLANE except a cat-5 cable to the plain text RJ-45 port or a transceiver to the plain text AUI port

9. Connect grounding strap and erect the antenna for the wireless bridge in accordance with procedures in Paragraph 2.32.1.1.

10. Connect power cords.

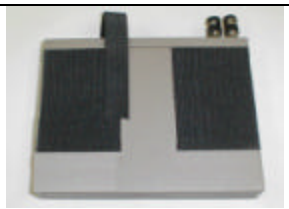
Table 2-54 Cable Connections for SSR Wireless Bridge to the INE

Type of Cable	**Wireless Bridge**	Power Injector	Encryptor	10Base-T Transceiver
Straight-through	Inline Power Ethernet Port	AP/Bridge Port		
Cross-over		Network Port	External/Encrypted Port	
Cross-over			Internal / Unencrypted Port	Ethernet Port of transceiver attached to J1 of NES

2.34.2 Connect SSR DSL Bridge to the INE/NES. This procedure is illustrated as number 2 in Figure 2-124 and explained further in Table 2-55).

This is a good connection to make when for reason of terrain or vegetation, you cannot reach the INE device through radio shots. The DSL bridge is to be used when using the wireless bridge is impractical or impossible.

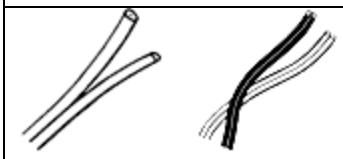
1. You will need the SSR DSL Bridge, DSL power supply, 2-prong power cord, a white (straight through) 10BaseT cable, the SSR 10Base-T Transceiver, and WF-16 field wire. (WD-1 or WD-1A can be used also). (Figure 2-126)



DSL Bridge

White 10Base-T Straight-Through Cable

10Base-T Transceiver



WD-1 or WF-16
WD-1A

DSL Power Supply

2-Prong Power Cord

Figure 2-126 Connect to INE Using DSL Components

NOTE: *No encryptor is needed with the DSL bridge. The plain-text output of the NES or TACLANE is connected through the DSL bridges and field wire to the hub in the CBM. It is encrypted by the encryptor in the CBM before being transmitted over the radio in the CBM.*

2. Connect the two DSLs using WF-16 field wire. (Procedure is in Paragraph 2.19.1)

3. Connect one end of a straight-through 10Base-T cable from the 10BaseT port on the SSR DSL Bridge to the 10Base-T port on the transceiver.

4. Be sure the Signal Quality Error (SQE) Test Switch (heartbeat) is set to O (off) (Slide the switch to the left).

5. Disconnect the Signal 10Base2 transceiver from the AUI port (J1) on the NES. (Signal unit will do this).

6. Connect the transceiver to the "Red" ("Plain Text") AUI port (J1) on the NES. (Same place where you took the 10Base2 transceiver from). ***Never connect to the "Black" ("Cypher Text") port.***

7. Connect power supply and power cord to the DSL. Connect power cord to external power source.

NOTE: *Remember, both DSLs must have the same transmission speed rate. Default is 8.*

Table 2-55 Cable Connections for SSR DSL Bridge to the INE

Type of Cable	**DSL**	Power Injector	Encryptor	10Base-T Transceiver
WF-16	DSL in CBM to SSR DSL			
Straight-through	10Base-T port			Ethernet Port of transceiver attached to J1 of NES

2.35 STAMIS CONNECTIVITY TO CAISI. Once the CAISI components are unpacked, antennas are erected, components are powered on, and connectivity to the network is established, the CAISI is ready for STAMIS devices to connect and transmit data over the network. The method employed by the STAMIS to connect will be determined by hardware and software capabilities and limitations, and distance from the nearest CBM or CCM. This Paragraph discusses the various methods of connectivity, advantages and disadvantages, and the steps required to accomplish each method of connectivity.

CAISI supports two classes of users: Network Capable systems and Non-Network Capable systems:

1. **Network Capable systems**. (Figure 2-127)

   a. Systems that are inherently Network capable and implement TCP/IP and FTP.

   b. Network capable users may access CAISI through 802.3 coaxial LAN Cable (RG-58) or category 5 unshielded twisted pair (UTP).

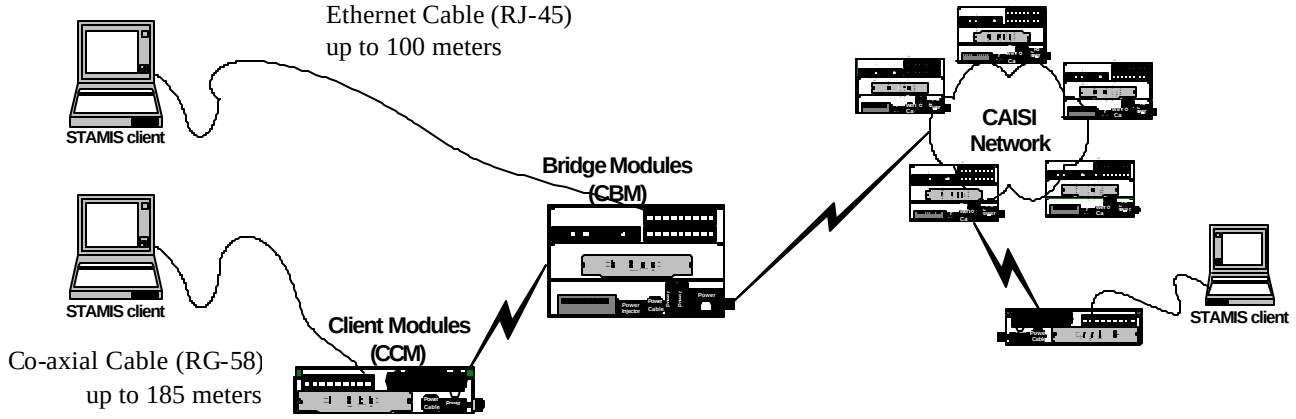


Figure 2-127 Connect Network Capable STAMIS to CAISI

2. **Non-Network capable systems**. (Figure 2-128)

   a. Non-network capable systems interface only through serial connections. These systems will need a device called LSA to assist them in sending serial over network.

   b. Legacy Systems that communicate only through RS-232 serial ports are using the Blocked Asynchronous Transport (BLAST) protocol.

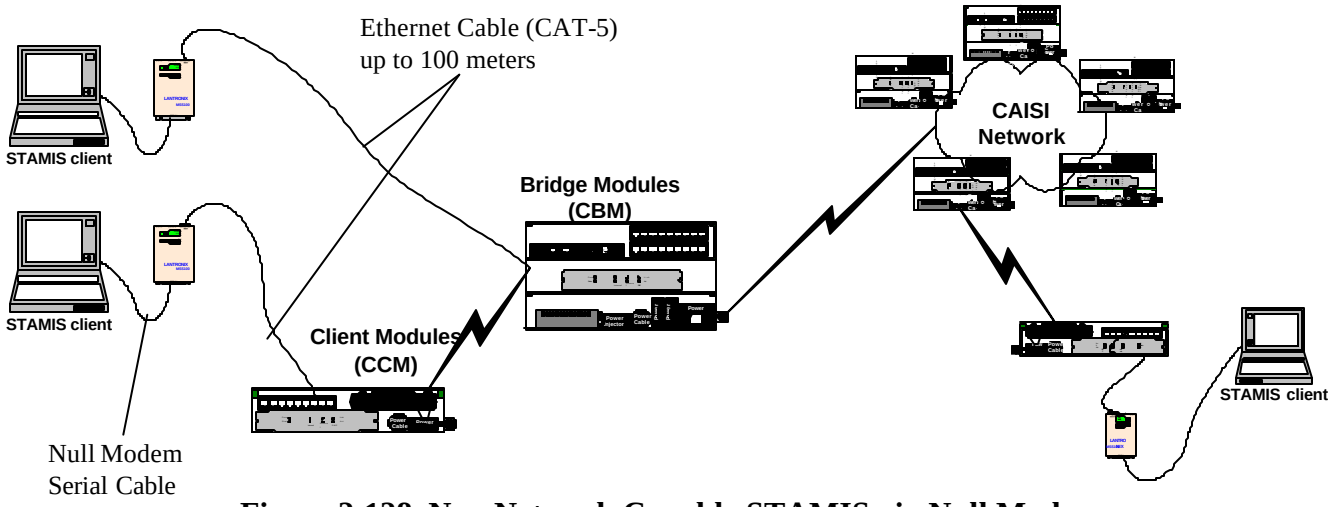


Figure 2-128 Non-Network Capable STAMIS via Null Modem

CAISI connects STAMIS users to the local area network; it connects to the network by wireless radios. A CBM or CCM will reside in your vehicle or tent and you will connect your STAMIS to it.

CBM/CCM have the following connections as discussed in previous Paragraphs:

1. 10 Base-2/RG-58 or 10Base-T/RJ-45 connections are used for Network Capable hosts.

2. The CBM has two coaxial (10Base-2/RG-58) and fourteen Cat-5 (10Base-T/RJ-45) connections for connecting to the network.

3. The CCM has one coaxial (10Base-2/RG-58) and seven Cat-5 (10Base-T/RJ-45) connections for connecting to the network.

2.35.1 Connecting to CAISI Using 10Base-2. There are legacy STAMIS devices that use a 10Base-2 (RG-58) cable to connect to the network. Each hub has one 10Base-2 port for these connections, so there are two available with each CBM, one available with each CCM. Here are some specifications when using 10Base-2/RG-58:

1. Coaxial connections can have a 10Base-2/RG-58 segment connected to a maximum length of 185 meters.

2. Each segment must be at least .5 meters in length.

3. Up to 15 clients can connect to each 10Base-2 BNC port.

4. Ensure STAMIS Network Interface Cards (NICs) are configured.

5. STAMIS devices may need terminating.

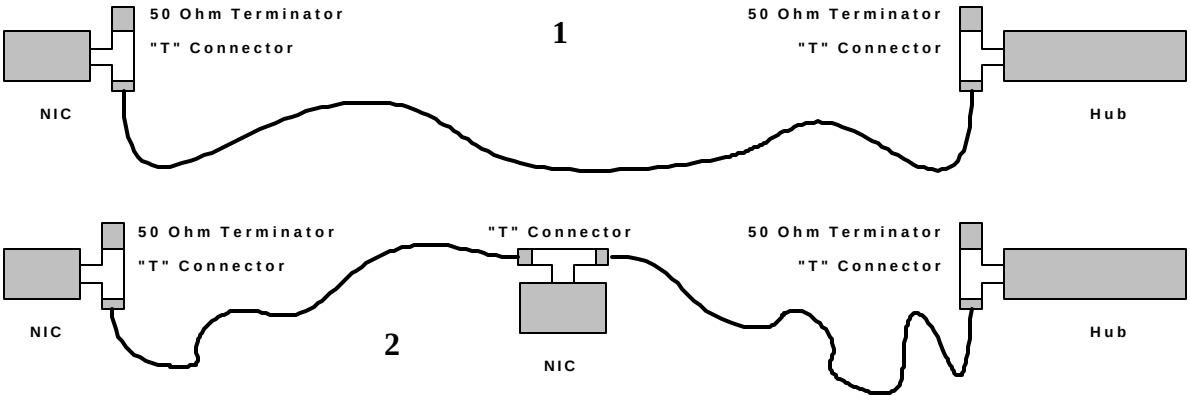


Figure 2-129 RG-58 Cable Connection with Terminator

In Figure 2-129, diagram 1 is connecting just one STAMIS device to the hub in the CBM/CCM using one RG-58 cable. Diagram 2, on the other hand, has two STAMIS devices connecting to the hub in the CBM/CCM using two RG-58 cables.

Connection Procedures using 10Base-2 are: (Diagram 1 in Figure 2-129)
(One STAMIS computer connected to the hub in the CBM/CCM)

Locate the nearest CBM or CCM that is connected to the network and is operational.

Secure an adequate length of 10Base-2 coaxial cable, not to exceed 185 meters, two T-connectors, and two 50-ohm terminators. (not supplied with CAISI).

Do not remove the T-connectors and terminators from the CBM/CCM. Contact your CSSAMO for T-connectors and terminators.

1. Connect a 50-ohm terminator and T-connector to one end of an RG-58 coaxial cable.

2. Connect the end of the RG-58 cable to the STAMIS Network Interface Card (NIC).

3. Remove terminator from either hub of your CBM/CCM.

4. Connect the other end of the RG-58 cable to the T-Connector on the hub from which you removed the terminator.

5. Place the terminator in CBM transit case or CCM carrying case for safekeeping.

Diagram 2 in Figure 2-129 connections are similar to the above except there will be an additional RG-58 cable.

2.35.2 Connecting to CAISI Using 10Base-T. Network capable STAMIS will connect from their NIC to the nearest CBM or CCM.

1. Some specifications when using 10Base-T devices.

   a. For two devices to communicate, the transmitter of one device must connect to the receiver of the other device.

   b. The connection is achieved through a crossover function, which can be a crossover cable or a port that implements the crossover function internally.

   c. Ports that implement the crossover function internally are known as MDI-X ports, where X refers to the crossover function.

   d. For the transmitter of one device to connect to the receiver of another device, the total number of crossovers must always be an odd number.

   e. A computer NIC is always MDI and hub or switch ports are usually MDI-X, thus they can be connected with a straight-through cable.

   f . When connecting one hub or switch to another, you must either use a crossover cable or connect to an MDI port on one and an MDI-X port on the other.

2. Some specifications when using 10Base-T cable:

   a. Each of the available RJ-45 connections can have a 10Base-T/RJ-45 segment connected to a maximum length of 100 meters.

   b. Each segment must be at least .5 meters in length.

   c. Ensure STAMIS NICs are configured.

Connection Procedures using 10Base-T:

Locate the nearest CBM or CCM that is connected to the network and is operational.

1. Secure a segment of 10BaseT (RJ-45) cable not to exceed 100 meters in length.

2. Connect one end of the cable to the connector on your NIC on the back of the STAMIS. Connect the other end to one of the open 10Base-T ports on the hubs contained in the CBM or CCM.

NOTE: *If you have more than 14 10Base-T clients to connect to a CBM, you can add a hub of your own. Use either a coaxial cable with "T" connectors and terminators or use a crossover cable. Use one or the other but not both.*

Connecting an additional hub can be done in several different ways. These connections are shown in Figure 2-130. (Numbers in the figure correspond to those items below). Remember that you can use either the "uplink" port or port 8 on the CBM/CCM hub, but not both at the same time.

1. Use a white straight-through cable from one of the CBM MDI "uplink" ports to a normal MDI-X port on your hub.

2. Use a red cat-5 crossover cable from any MDI-X port to any MDI-X port.

3. Use a coaxial cable with a "T" connector and terminator to the BNC port on your hub if it has one.

NOTE: *You can connect a hub of your own to a CCM as well, but remember that you can have only eight clients connected to a CCM. However, if you have several computers in each of two tents close together, you can put the CCM in one tent and your own hub in the other, interconnecting them as shown.*

Make sure that the Ethernet or coaxial cable is run so that it will be protected from foot and vehicle traffic and will not create a safety hazard, especially in the dark

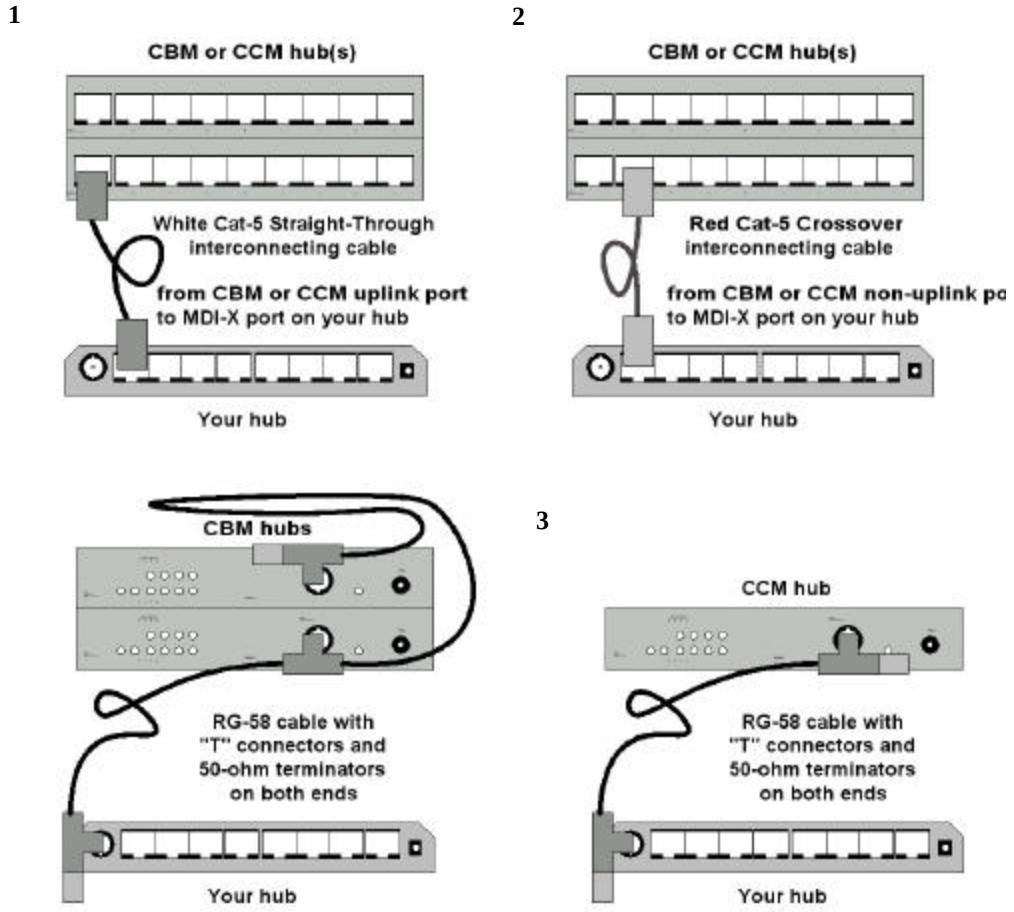


Figure 2-130 Connecting an Additional Hub

2.35.3 Connecting to CAISI Using the LSA. Many STAMIS devices are not capable of connecting to a CAISI hub using a standard 10Base-T or 10Base-2 network connection. This may be due to limitations of hardware (no NIC), or software that is unable to support a TCP/IP connection. These users currently use the CAISI Virtual End-to-End (VEE) software to establish network connectivity and communication. In the new CAISI environment, this functionality is provided by the Legacy Support Adapters (LSAs) fielded with the CAISI.

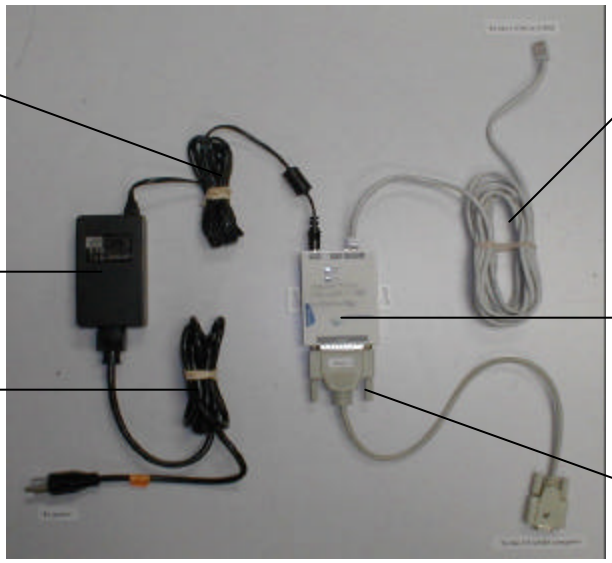


Figure 2-131 LSA Components

1. You will need a configured LSA, a null modem cable (no longer than 25 feet), and a Cat-5 Ethernet Cable (up to 100 meters long).

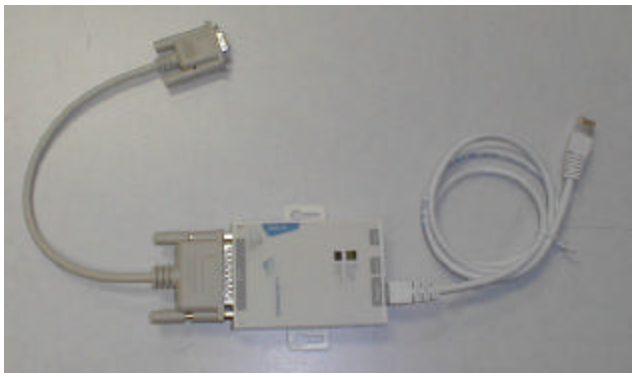


Figure 2-132 LSA with Null Modem and Cat-5 Cable

2. Connect one end of the null modem cable to the serial port of a STAMIS computer. Connect the other end to the LSA in the port labeled “Serial”.

3. Connect one end of a standard Cat-5 Ethernet cable from the network port on the LSA labeled “10/100”. Connect the other end to one of the 10Base-T ports of the hub in the CBM or CCM.

4. Connect power supply to the LSA (labeled 5vdc) and plug the AC power cord for the LSA into an external power source (power strip).

5. Apply power to external power source.

CAUTION

Do Not Press the Reset Button. There is a small hole located between the power and network connectors on one end of the LSA. This is the reset button. If you press the reset button, the LSA will lose its configuration settings and will need to be reconfigured by the SSR. Until it is reconfigured, it will be entirely useless to you.

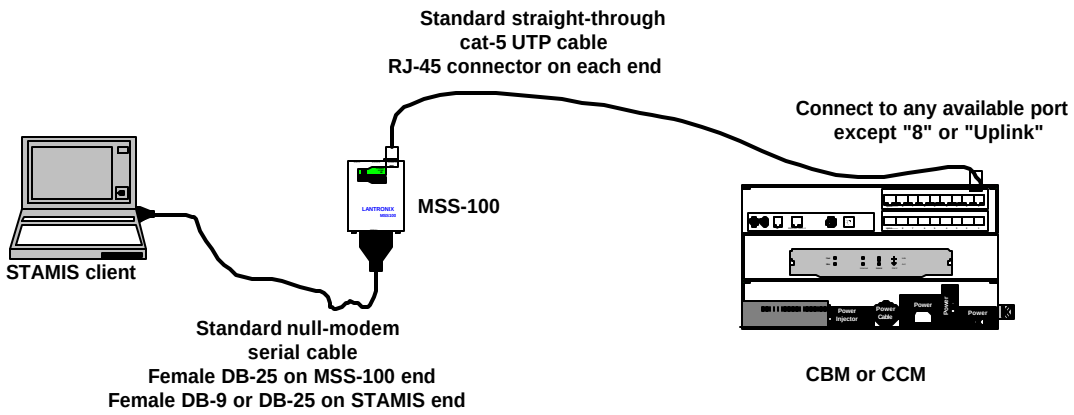


Figure 2-133 CAISI LSA Connection with Null Modem Cable

In order to communicate with the LSA, there must be two LSAs. The STAMIS client has the client LSA who connects to the STAMIS server via a Server LSA.

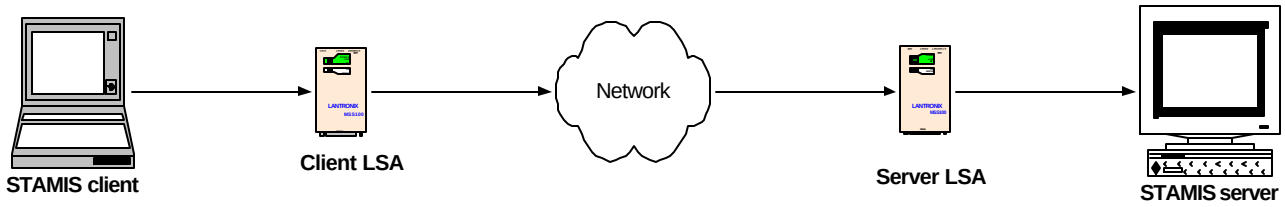


Figure 2-134 LSA SchematicView

2.35.4 LSA Configuration. The SSR notebook can be connected directly to the LSA (Figure 2-135) or can be connected to the LSA via a hub (same connection as in Paragraph 2.35.3 with the additional step of connecting the SSR notebook to the hub of the CBM/CCM that the LSA is connected to with a CAT-5 straight-through ethernet cable).

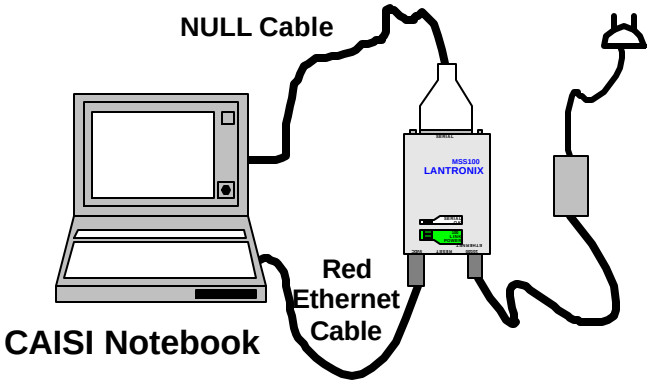


Figure 2-135 CAISI Notebook Direct Configuration of LSA

Connect the SSR notebook to the LSA as follows:

1. Connect a DB9 (female) to DB25 (female) pin null modem serial cable from the notebook serial port to the “serial” port of the LSA

2. Connect the Cat-5 Crossover ethernet cable from the Wired NIC in the notebook to the 10/100 network port on the LSA

3. Apply power.

The procedure to restore factory default parameters: (**Reset the LSA**)

1. Complete initial connections.

2. Remove power to the LSA.

3. Push the reset button (use pointed end of a paper clip) and **keep the button pressed in**.

4. Apply power to LSA **while also holding in the reset button**.

5. Hold it until the serial lights stop blinking (about 5-10 seconds).

6. All configuration parameters are set back to factory defaults.

NOTE: *The remaining configuration steps are in the TB 11-5895-1691-10, Paragraph 2.13 (manual).*

2.35.5 Monitoring Procedures. CAISI is designed to operate with minimal user input or monitoring during normal operations. However, some user monitoring is useful to ensure optimal operation and to identify and correct minor problems before they develop into a more serious problem. The following monitoring procedures should be practiced during normal operation:

1. Periodically inspect all CAISI cable connections for tightness and inspect for signs of damage or wear.

2. Periodically inspect the LEDs on the CAISI components during normal operation. Consult Chapter 2, Paragraph 1 for a description of the types and functions of the LEDs of the CAISI components.

2.36 CAISI EQUIPMENT TEARDOWN.

2.36.1 CBM Cable Disconnection Procedures. The procedures for disconnecting and packing the CBM and CCM are similar enough to be addressed together. The exception is the CBM connected to the INE device. This device will have the extra cable to collect and terminators to replace at each end of the connection. Follow the steps below:

NOTE: *Each of these steps is explained in more detail with pictures in the next few Paragraphs.*

1. Turn off the UPS.

2. Disconnect the power cables from the UPS and the chassis. Coil them and set them aside.

3. Disconnect the grounding cable from the ground. At the chassis end, be sure to replace the washer and wing nut.

4. Disconnect the RF cable from the chassis. Do not use tools to loosen it, as you may damage the connector.

5. Teardown and disassemble the antenna, bracket, and cable. Secure the U-bolts to the bracket, and coil and secure the cable with the Velcro strap provided.

6. Disconnect the grounding strap from the CBM/CCM chassis.

7. Disconnect the wire from DSL binding posts – push in on binding post to remove wire. Untie wire from chassis. (If the DSL was used)

8. Inventory and inspect all items, using the inventory lists provided with the transit or carrying cases.

2.36.2 Disconnect CBM Root Node from the INE. (Figure 2-136)

1. Disconnect RG-58 coaxial cable from T-Connector located on the J-1 port (Red-Side) of the INE device (AUI 10Base-2 port).

2. Obtain terminator from Signal Support and return to T-Connector on the J-1 port.

3. Disconnect other end of RG-58 coaxial cable from T-Connector on CBM root node hub.

4. Remove terminator from transit case and put it back on CBM hub T-Connector.

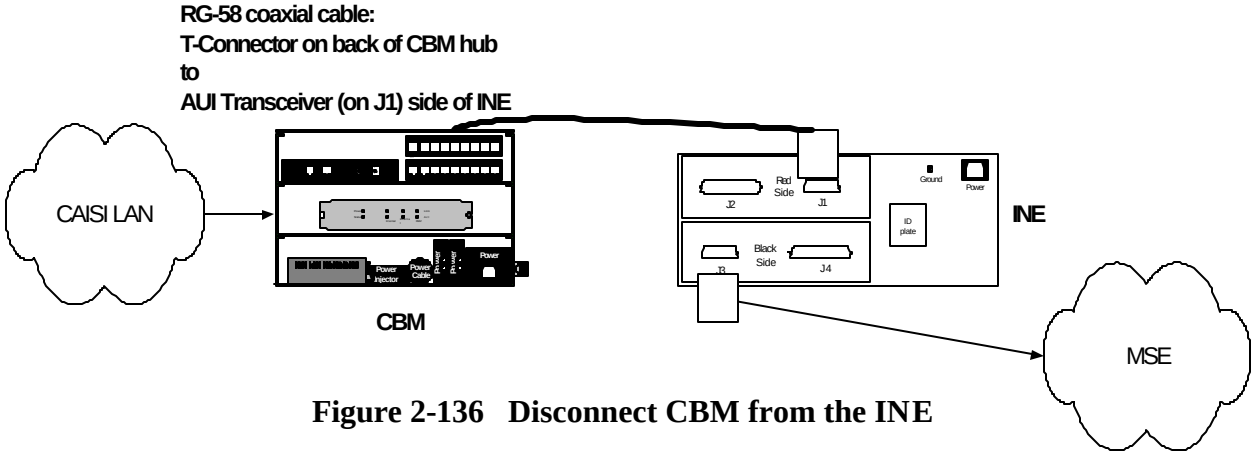


Figure 2-136 Disconnect CBM from the INE

2.36.3 Disconnect STAMIS Users from the CBM.

1. **Disconnect Network Capable STAMIS from the CBM.**

   a. 10Base-2/RG-58 disconnection procedures:

      (1) Disconnect RG-58 cable from the hub T-Connector.

      (2) Locate terminator in CBM transit case and attach it to the hub T- Connector.

      (3) Disconnect other end of RG-58 cable from the STAMIS Network Interface Card (NIC).

      (4) Remove the 50-ohm terminator and “T” connector from the end of the RG-58 cable and put them in CBM transit case.

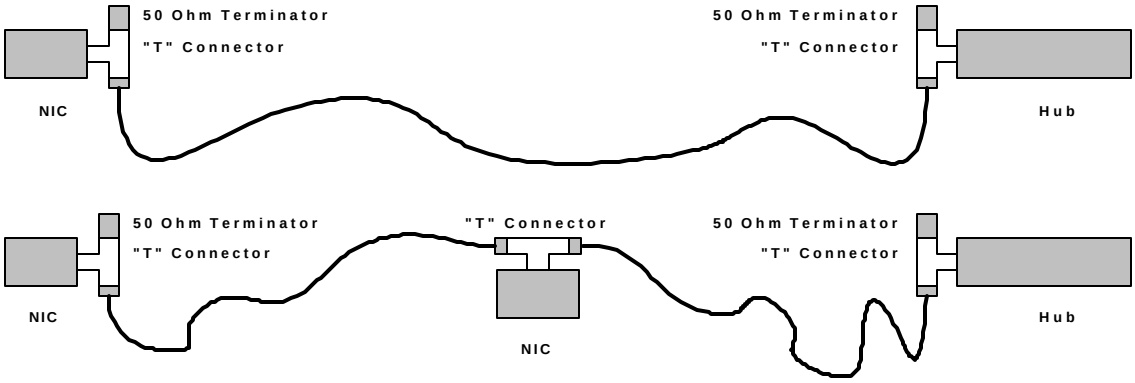


Figure 2-137 Disconnect RG-58 and T-Connectors

b. 10Base-T/RJ-45 disconnection procedures:

(1) Disconnect RJ-45 cable from CBM hub port.

(2) Disconnect the other end of RJ-45 cable from the STAMIS NIC.

2. **Disconnect Non-Network Capable STAMIS from the CBM.**

a. LSA cable disconnection procedures: (Null Modem (RS-232))

(1) Disconnect power supply from LSA and unplug AC power cord from LSA and external power source.

(2) Disconnect null modem cable from the STAMIS device's serial port.

(3) Disconnect other end of null modem cable from the LSA serial port.

(4) Disconnect 10Base-T/RJ-45 Ethernet cable from the LSA.

(5) Disconnect other end of 10Base-T/RJ-45 Ethernet cable from the 10Base-T port on either CBM hub.

Figure 2-138 Disconnect LSA Cables

2.36.4 Disconnect CBM Connections.

2.36.4.1 Disconnect UPS.

1. Turn off the UPS. Press the rocker switch so that the "O" (OFF) symbol is depressed. The green power light should be off.

2. Unplug the UPS power cord from its external power source.

Figure 2-139 Turn off UPS/Disconnect CBM Power Cables

2.36.4.2 Disconnect CBM Power Cables.

1. Unplug the wireless bridge and hub power cords from the UPS "Battery Backup Protected Outlets." (Figure 2-139)

2. Disconnect DSL (center) from its power supply, **if the DSL was used.**

3. Disconnect the 2-prong power cable from the hub and inline encryptor power supply on the far right.

4. Disconnect the 3-prong power cable from the wireless bridge power supply. (far left).

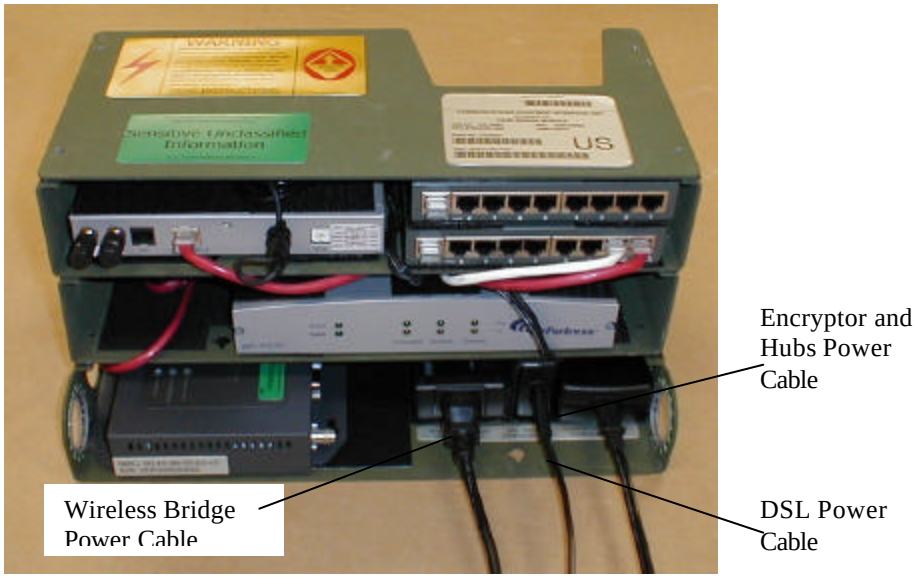


Figure 2-140 Disconnect CBM Power Cables from CBM Chassis

2.36.4.3 Disconnect RF Cable from CBM Chassis.

1. Locate the wireless equipment's external antenna connector (on the right side of the CBM chassis next to the grounding strap).

2. Using your hand, loosen the RF cable from the connector by turning it to the left.

   If it is too tight, try wiggling it as you turn. If you still cannot loosen it try using an adjustable wrench. **Do not use slip-joint pliers, you could damage the connector.**

3. Remove the antenna cable from the wireless equipment's external antenna connector.

4. Pull the loose end of the RF cable through the opening in the vehicle, shelter or tent.

Figure 2-141 Disconnect RF Cable from CBM Chassis

2.36.4.4 Teardown CBM Wireless RF Antenna.

1. Disconnect CBM Omni-directional "whip" antenna procedures:

   a. Pull the antenna through the camouflage net.

   b. Remove the tape from the camouflage pole to free the RF cable.

   c. Disconnect the bracket from the camouflage pole or mast section by loosening the U-bolts labeled "Mast."

   d. Tighten all wing nuts on the bracket to prevent losing them.

Figure 2-142 Disconnect RF Antenna from Bracket

2.36.4.5 Disconnect RF Cable from the Antenna and Bracket.

CBM Omni-directional “whip” antenna procedures:

1. Unscrew, by hand, the black plastic retaining ring on the top section of the antenna from bottom section.

2. Disconnect the two sections of the whip antenna by removing the bottom Paragraph from the top section.

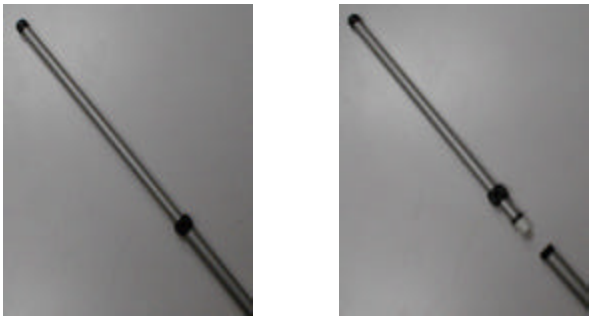


Figure 2-143 Disconnect Whip Antenna

3. Remove the strain relief wing nuts until they no longer touch the cable.

4. Loosen the whip antenna wing nuts by hand without using tools, but do not remove the larger U-bolts, labeled “Whip Antenna”.

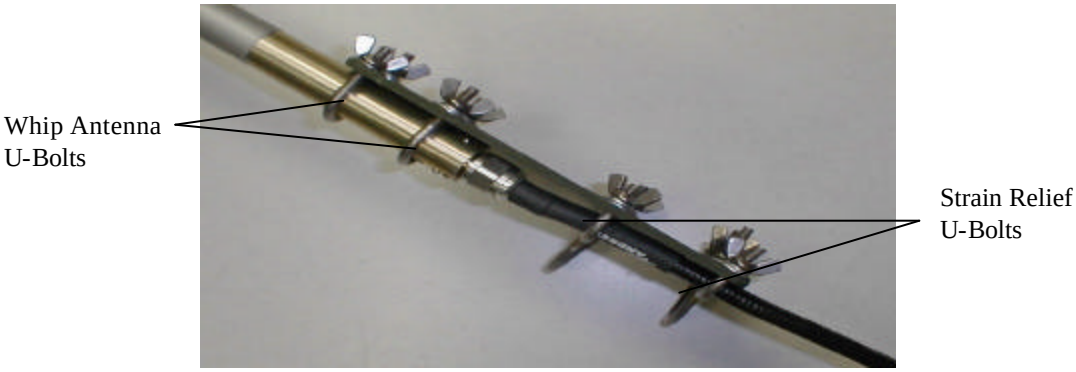


Figure 2-144 Disassemble Whip Antenna from Bracket

5. Disconnect the straight end of the antenna cable from the connector on the bottom of the whip antenna.

6. Remove the bottom of the antenna up through the “Whip Antenna” U-bolts.

7. Replace and secure all U-bolts and wing nuts on the bracket.

2.36.4.6 Disconnect CBM from Ground.

Figure 2-145 Disconnect Grounding Strap from CBM and the Ground

1. Disconnect grounding strap from the ground. (If the grounding rod is not a permanent fixture, remove it also).

2. Disconnect the grounding strap from the CBM grounding stud (on the right side of CBM chassis, next to the lightning arrestor).

   a. Loosen and remove the wing nut and washer by hand without using tools.

   b. Remove the grounding strap lug from the grounding stud.

   c. Replace the washer and wing nut.

2.36.4.7 Disconnect DSL or Directional Panel Antenna.

1. Disconnect DSL Bridge.

   a. Press the binding post in and remove the wire from the jaws of the binding post as it opens.

   b. Untie the wire from the handle of the CBM.

NOTE: *Needs to be done on both ends*

   c. Recover field wire.

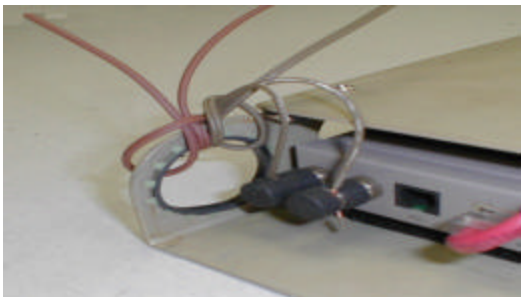


Figure 2-146 Disconnect DSL Bridge

2. 7-inch Directional 'Panel' Antenna Teardown procedures:

   a. To disconnect the RF cable from the wireless equipment's external antenna connector, follow the procedures listed above for the whip antenna.

Figure 2-147 Teardown Directional 'Panel' Antenna

Normal Weather Condition procedures:

(1) Pull antenna through the camouflage net.

(2) Remove the tape from the antenna cable and mast.

(3) Disconnect the bracket from the mast or camouflage pole by loosening the U-bolts labeled "Mast".

(4) Disconnect the right-angle end of the antenna cable from the panel.

(5) Remove the antenna wing nuts by hand without using tools.

(6) Remove the panel antenna from the bracket.

(7) Replace the two U-bolts labeled "Whip Antenna" (these were not used since the panel had to be in one of the holes, they should be in the CBM transit case) and secure them with the wing nuts.

Windy Weather Condition Procedures

(1) Loosen the guy ropes.

(2) Remove the camouflage net stakes from the ground

(3) Pull the camouflage pole and through the opening in the camouflage net.

(4) Remove the tape from the antenna cable and pole.

(5) Disconnect the second red guy clip on each side of the bracket by removing it from the first guy clip.

(6) Disconnect the remaining red guy clips from the holes in the bracket.

Figure 2-148 Remove Guy Ropes from Directional Panel Antenna

(7) Disconnect the bracket from the camouflage pole or mast section by loosening the U-bolts labeled “Mast.”

(8) Disconnect the right-angle end of the antenna cable from the panel.

(9) Remove the antenna wing nuts by hand without using tools.

(10) Remove the panel antenna from the bracket.

(11) Replace the two U-bolts labeled “Whip Antenna” and secure them with wing nuts.

2.37 CBM PACKUP PROCEDURES.

2.37.1 Inventory CBM and ancillary components.

1. Locate the CBM transit case inventory checklist card. See Table 2-32, p. 2-67 or in Appendix J.

2. Identify each item on inventory checklist card.

3. Verify that the CBM chassis and all ancillary components are present.

4. Annotate any discrepancies or shortages on DA Form 2404 or 5988E.

2.37.2 Packup CBM Transit Case

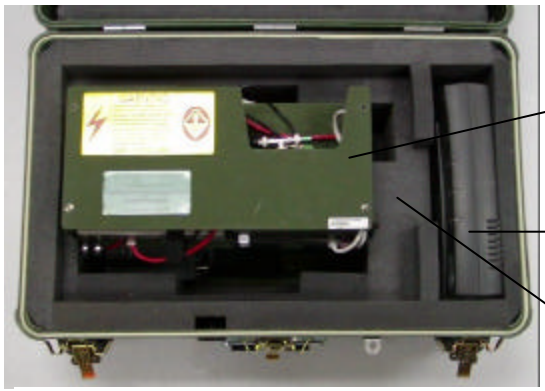
Follow the steps below to pack the CBM and ancillary components:

Figure 2-149 CBM Transit Case

CAUTION

The CBM transit case weighs 46 pounds – full, 15 pounds - empty. Use safe lift and carry procedures when handling the transit case. This is a two-person lift and carry.

1. Place CBM transit case on a flat surface or workbench with front facing you.
2. Lay case on its back.
3. Prior to unlatching, press pressure release valve located in front of the CBM (should hear a hiss if pressure has built up).
4. Unlatch latches and carefully open transit case lid.
5. Pack the following components in the main compartment of the transit case:



a. CBM Chassis (lightning arrestor is pointing toward UPS)

b. UPS (power cord is coiled underneath it)

c. Barrel connector (a slit in foam to the right of the CBM chassis) not shown.

Figure 2-150 CBM Transit Case – Main Compartment

6. Pack the following components in the transit case top compartment (lid section)

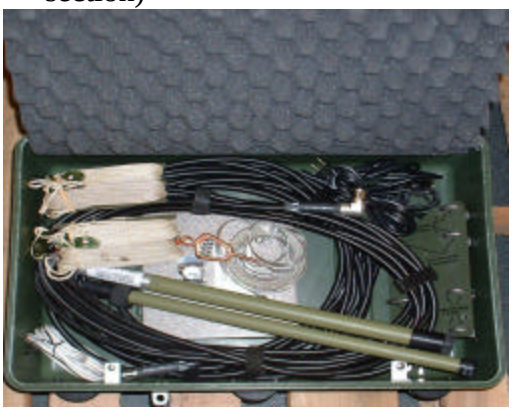


Figure 2-151 CBM Transit Case – Top Compartment (Lid Section)

a. 40-inch Whip Antenna or 7 in Directional Panel Antenna

(Store the 40-inch whip in two pieces)

b. Grounding Strap

c. 25 foot or 35 foot Antenna Cable

d. Antenna Bracket

e. Power Cables

f. 42-foot Guy Ropes on RL-28

NOTE: *Coil the RF cables and all power cables and secure them with wire ties, tape or velcro before storing them in the transit case.*

7. Close transit case lid and re-latch clips.
8. Close transit case and latch clips.

2.38 CCM DISCONNECTION PROCEDURES. The procedures for the CCM are similar to those for the CBM. In this case where procedures are the same, the text will refer you to that paragraph.

2.38.1 Disconnect STAMIS Users from the CCM. Same procedure as CBM in Paragraph 2.36.3

2.38.2 Disconnect CCM Connections.

2.38.2.1 Disconnect CCM power cables.

Figure 2-152 Disconnect CCM Power Cables

1. Unplug CCM power cable from power outlet.
2. Disconnect the 2-prong power cable from the power supply in the bottom right of the CCM.

2.38.2.2 Disconnect RF Cable from CCM Chassis. Same procedure as the CBM in Paragraph 2.36.4.3.

2.38.2.3 Teardown CCM Wireless Radio Frequency (RF) Antenna. Same procedures as the CBM in Paragraph 2.36.4.4 except that this is the 24-inch whip antenna which is only one piece.

2.38.2.4 Disconnect RF cable from Antenna and Bracket. Same procedure as the CBM in Paragraph 2.36.4.5.

2.38.2.5 Disconnect CCM from Ground. Same procedure as the CBM in Paragraph 2.36.4.6.

2.39 CCM Packup Procedures. The CCM and its ancillary components are packed in a carrying case.

2.39.1 Inventory CCM Carrying Case.

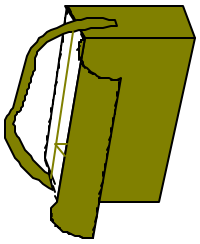
1. Locate the CCM Carrying Case Inventory Checklist Card.
   See Table 2-37, p. 2-88 or in Appendix J.

2. Identify each item on inventory checklist card.

3. Verify that the CCM chassis and all ancillary components are present.

4. Annotate any discrepancies or shortages on DA Form 2404 or 5988E.

2.39.2 Packup CCM Carrying Case



Main (Cable and Antenna) Compartment	
Bracket and Misc Compartment	CCM Chassis Compartment

Figure 2-153 CCM Carrying Case

The CCM carrying case weighs 10 pounds – full, 1 pound - empty. Use safe lift and carry procedures when handling the carrying case.

1. Place the CCM carrying case on a clean, dry secure table.

2. Place the CCM Chassis in its designated compartment. Place it so that the **antenna connector points to the inside** (towards the Bracket and Miscellaneous (Misc) compartment not towards the outside of the case.

3. Place the following components in the main compartment.

   a. 24-inch Whip antenna.
   b. 35-foot RF antenna cable.
   c. Grounding strap
   d. Power Cables

NOTE: *Coil all cables (Power and RF antenna) and secure them with wire ties, tape or velcro before storing them in the carrying case.*

4. Place the antenna bracket and left over equipment in the miscellaneous (misc) compartment.

5. Zip up the CCM Carrying case and store.

2.40 LSA DISCONNECTION PROCEDURES.

2.40.1 Disconnect STAMIS Users from the LSA. Same procedures as CBM for Non-Network Capable STAMIS in Paragraph 2.36.3.

2.40.2 Disconnect LSA Connections.

1. Unplug the LSA power cable from the power outlet and disconnect the power adapter from the LSA power input.

2. Disconnect the Cat-5 cable from the RJ-45 connector on the LSA and the other end that connected to the 10Base-T port on the CBM or CCM.

3. Disconnect the null modem cable from the LSA serial connection.

Figure 2-154 Disconnect LSA Connections

2.41 LSA PACKUP PROCEDURES

2.41.1 Inventory LSA and Ancillary Components.

1. Locate the LSA inventory checklist card. See Table 2-39, p. 2-92 or in Appendix J.

2. Identify each item on inventory checklist card.

3. Verify that the LSA and all ancillary components are present.

4. Annotate any discrepancies or shortages on DA Form 2404 or 5988E.

2.41.2 Packup LSA

1. Pack the LSA in its transit box along with the following components:

   a. LSA MSS-100
   b. Null modem cable
   c. White Straight-through Ethernet cable.
   d. Power adapter and cable.

NOTE: *At this time, a transit box has not been selected. Store the LSA and its components in with your STAMIS system case.*

2.42 SSR ACCESSORY KIT PACKUP PROCEDURES. The SSR Accessory Kit consists of the transit case, the notebook carrying case, the Antenna Carrying Case and the Antenna Mast Carrying Case. The packup procedures for these three components are in the following paragraphs.

SSR Transit Case	Paragraph 2.43
SSR Notebook Carrying Case	Paragraph 2.44
SSR Antenna Carrying Case	Paragraph 2.45
SSR Antenna Mast Carrying Case	Paragraph 2.46

2.42.1 Tear down AB-1244B Antenna Mast. Follow the procedures to tear down the AB-1244B Antenna Mast: (**Two person task** – Assistant and Installer)

WARNINGS

- If there are power lines nearby lower the antenna in the direction opposite the power lines.
- Clear the area of personnel, equipment and vehicles before starting to lower the antenna.

CAUTION

Allow only a slight bow in the mast during the lowering operation

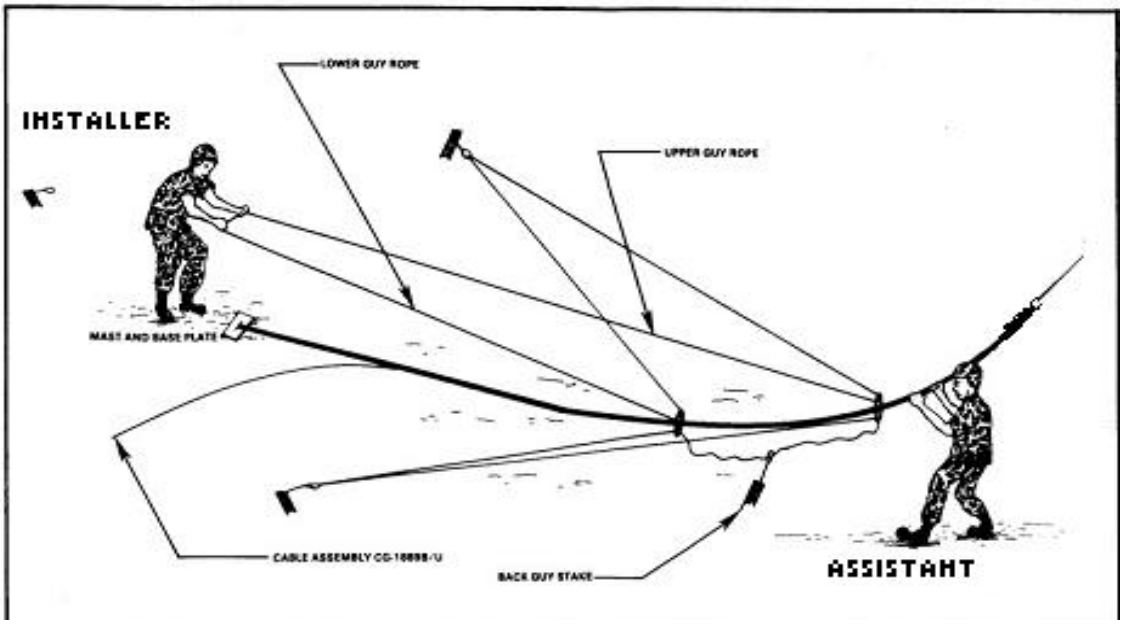


Figure 2-155 Tearing Down the Antenna Mast

1. Ensure CBM/CCM is powered down.

2. Disconnect RF cable from the CBM/CCM chassis. This procedure is covered in Paragraph 2.36.4.3.

Tear down Antenna Mast Procedures:

1. **Preparation.**

   a. Assistant: Holds the antenna mast section

   b. Installer: Loosens upper and lower guy ropes. Unhook upper and lower guy ropes from **one** of the stakes.

CAUTION

Leave the other ropes on the remaining 3 stakes hooked.

2. **Lowering.**

   a. Assistant: While holding the antenna mast section overhead, walk away from its base toward the top of the mast.

   b. Installer: Grasp upper and lower guy ropes in hand. Walk towards the base of the antenna mast section and slowly lower the antenna mast to the ground.

2.42.2 Disassemble the Whip Antenna and Bracket. This procedure is covered in Paragraph 2.36.4.5 for the 40-inch break-away whip antenna.

2.42.3 Disassemble the Directional "Panel" Antenna. This procedure is covered in Paragraph 2.36.4.7 for the 7-inch panel antenna. The 14-inch panel procedures are the same.

2.42.4 Disassemble the Antenna Mast Section.

NOTE: *When disconnecting guy ropes from the stake assembly, do not release all of the slack of the rope. Just release enough to remove it from the stake assembly. The reason for this, is so the next time the antenna is raised, the ropes will be at the correct length.*

1. Disconnect red guy ropes from the red guy plate on the upper mast assembly.

2. Disconnect red guy ropes from stake assembly.

3. Disassemble upper mast section.

4. Disconnect blue guy ropes from blue guy plate on lower mast assembly.

5. Disconnect blue guy ropes from stake assembly.

6. Disassemble lower mast section.
7. Secure your four red upper guy ropes around a RL-28.
8. Secure your four blue lower guy ropes around a RL-28.
9. Pull the mast base assembly out of the ground.
10. Remove the two guy stakes from the base plate.
11. Remove the four stakes from the ground.

2.43 PACKUP SSR TRANSIT CASE PROCEDURES.

2.43.1 Inventory SSR Transit Case.

1. Locate the SSR Transit Case inventory checklist card. See Table 2-45, p. 2-109 or in Appendix J.
2. Identify each item on inventory checklist card.
3. Verify that all of the SSR Transit Case Components are present.
4. Annotate any discrepancies or shortages on DA Form 2407 or 5504.

   NOTE: *DA Form 2407 is an organizational form not a unit/operator form like DA Form 2404.*

2.43.2 Packup SSR Transit Case.

CAUTION

The SSR Transit case weighs 46 pounds – full, 15 pounds - empty. Use safe lift and carry procedures when handling the transit case. This is a two-person lift and carry.

1. Place the SSR Transit case on a secure table, workbench or flat surface with the front facing you. To determine which side of the transit case is the front, look at the serial number on the top of transit transit case. If you can read the serial number, you are at the front of the transit case.
2. Prior to unlatching, press pressure release valve located on the front of the transit case.

Figure 2-156 SSR Transit Case

3. Unlatch clips and **carefully** open the transit case lid.

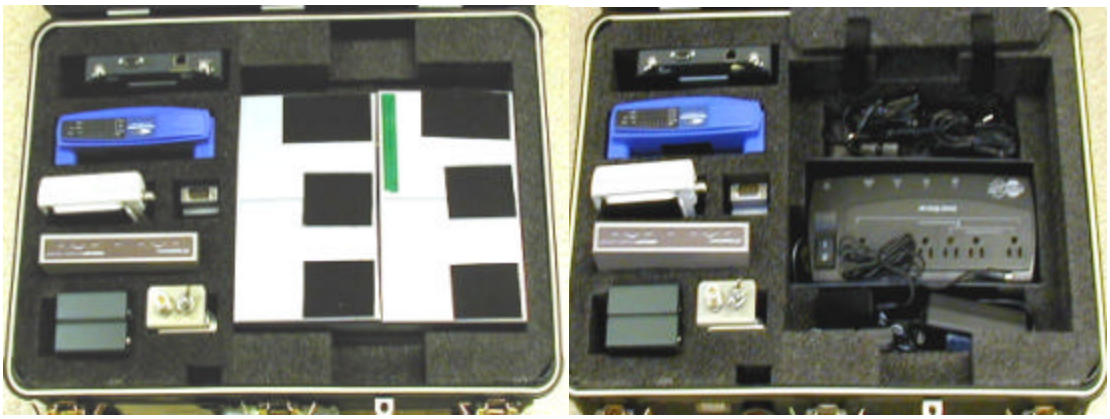


Figure 2-157 SSR Transit Case – Main Compartment

4. Pack the following in the Main Compartment of the SSR Transit Case. Starting on the left side from top (closest to the hinge) to the bottom:

   a. Wireless Bridge

   b. Router (Future cases will have 2 Netscreen routers instead of 1 Linksys Router)

   c. Multi-Client Radio Adapter

   d. 10Base-T Transceiver place the 10Base-T Transceiver (to the right of radio adapter)

   e. DSL Bridge

   f. Hubs (point BNC connector toward the inside)

   g. Lightning Arrestor Assembly place the Lighting arrestor assemblies (Qty 2) position one of them upside down (to the right of hubs)

   h. UPS goes in the open cutout on the right side of the transit case. Coil the power cord underneath it.

   i. Power supplies are placed around the UPS. Coil all of the power supplies with wire ties, tape or velcro.

   j. Fold down the plastic cover or foam over the UPS and power supplies.

   k. Two inline encryptors, side by side, on top of UPS compartment.

Figure 2-158 SSR Transit Case – Top Compartment (Lid Section)

5. In the top compartment of the transit case, place the following:

   a. Two 40-inch whip antennas go in the foam cutouts at the top.

   b. Place the remaining power cords, cables and miscellaneous items in the large foam cutout. These include the following:

      (1) 4-inch Whip antenna (Qty 2)
      (2) Grounding Strap (Qty 2)
      (3) 12-inch RF adapter cable N to RPTNC(M) (Qty 2)
      (4) 12-inch RF adapter cable N to RPTNC(F) (Qty 2)
      (5) Right Angle Adapter N to N (Qty 2)
      (6) Antenna Dummy Load (Qty 2)
      (7) White Straight-Through Ethernet cables. (Qty 4)
      (8) Red Crossover Ethernet cables. (Qty 4)
      (9) RJ-45 Straight-through Adapter (Qty 3)
      (10) RJ-45 Crossover Adapter (Qty 3)
      (11) 9-pin straight-through serial extension cable (blue) (Qty 1)
      (12) 9-pin crossover serial adapter cable (beige) (Qty 1)
      (13) 9 to 25-pin Null Modem cable (if issued)
      (14) Reset Tool (Qty 3)
      (15) Power cords. (2-prong (Qty 3), 3-prong (Qty 2))
      (16) 3-prong, 1-foot Power cable, 5V (Qty 6)

NOTE: *Coil all cables (Power, RF antenna and ancillary) and secure them with wire ties, tape or velcro before storing them in the SSR transit case.*

2.44 PACKUP SSR NOTEBOOK CASE PROCEDURES.

2.44.1 Inventory SSR Notebook Case.

1. Locate the SSR Notebook Case inventory checklist card. See Table 2-48, p. 2-120 or in Appendix J.
2. Identify each item on inventory checklist card.
3. Verify that all of the SSR Notebook Case Components are present.
4. Annotate any discrepancies or shortages on DA Form 2407 or 5504.

2.44.2 Packup SSR Notebook Case.

The SSR Notebook Case weighs 20 pounds – full, 2 pounds - empty. Use safe lift and carry procedures when handling the transit case.

1. Place the SSR Notebook Case on a secure table, workbench or flat surface with the front facing you. To determine which side of the carrying case is the top, look at Identification tag.
2. Unlatch clips and **carefully** open the transit case lid.

Figure 2-159 SSR Notebook Case

3. Press the center buttons and clasp the bottom edge of the latch and carefully lift the SSR notebook case.

Figure 2-160 Unlatch SSR Notebook Case

Figure 2-161 SSR Notebook Case – Main Compartment

4. Pack the following components underneath the notebook (picture on right):

   a. Wireless NIC
   b. "Rabbit Ears" Antenna
   c. Wired NIC (if issued)
   d. White Straight-Through Ethernet Cable
   e. Red Crossover Ethernet Cable
   f. RJ-45 Crossover Adapter
   g. RJ-45 Straight-through Adapter
   h. 9-Pin Straight-through Serial Extension Cable (Blue)
   i. 9-Pin Crossover Serial Null Modem Cable (Beige)
   j. 12-inch Adapter Cable, MMCX to N
   k. 12-inch Adapter Cable, MMCX to RPTNC
   l. Right Angle Adapter
   m. Antenna "Dummy Load"
   n. Reset Tool

NOTE: *Coil all cables and secure them with wire ties, tape, velcro before storing them in the notebook case.*

5. Place the notebook in the large area above the components in step 3. Use the permanent fixed velcro straps to secure the notebook (as shown in the picture on the left in Figure 2-161).

6. Put the power supply and cord in the opening to the right of the notebook.

7. Place the Baseline CD in the Lid pocket. (The technical manual and technical bulletin could also be placed here.)

8. Close the case.

2.45 PACKUP SSR ANTENNA CARRYING CASE PROCEDURES.

Figure 2-162 SSR Antenna Carrying Case

2.45.1 Disassemble Omni-Directional and Directional Panel Antennas.

1. Disassemble 40-inch Whip Antenna (Omni-Directional). Same procedure as Paragraph 2.36.4.5.

2. Disassemble 7-inch/14-inch Directional Panel Antenna. Same procedure as Paragraph 2.36.4.7. (The 14-inch Directional panel antenna procedures are the same as the 7-inch).

2.45.2 Inventory SSR Antenna Carrying Case Components.

1. Locate the SSR Antenna Carrying Case inventory checklist card. See Table 2-51, p. 2-124.

2. Identify all CAISI antenna items on inventory checklist card.

3. Verify that the SSR Antenna Case components are present.

4. Annotate any discrepancies or shortages on DA Form 2407 or 5504.

2.45.3 Packup SSR Antenna Carrying Case.

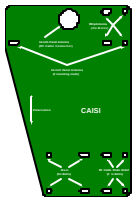
Antenna Carrying Case

a. Two 14-inch Directional Panel Antennas

b. Four 50 ft cables

c. Two 7-inch Antenna Bracket

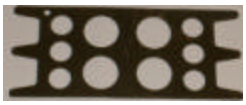
d. Two 14-inch Antenna Brackets



e. Four Barrel Connectors

f. Antenna guy ropes on reel (42-ft) (red) (Qty 4) (two per reel)

g. Reel Unit for Guy Ropes (Qty 2)



h. Antenna guy stake (Qty 4)

Figure 2-163 SSR Antenna Carrying Case and Components

Table 2-56 SSR Antenna Carrying Case Contents

	Component	Qty	Location in case
a.	“14x14” flat Directional Panel Antennas	2	Store in center section
b.	50 ft RF cables	4	Store in the two outer sections
c.	“7” antenna brackets	2	Store in one outer section with cables
d.	“14” antenna brackets	2	Store in other outer section with cables
e.	Antenna Barrel connectors	4	Store in outer pocket
f.	42-foot Guy Rope (Red Clip)	4	Store in outer section with cables
g.	Reel Unit for Guy Ropes (two guy ropes per reel)	2	Store in outer section with cables
h.	Guy Stakes	4	Store in outer section with cables

NOTE: *Coil all 50 ft RF cables secure them with wire ties before storing them in the carrying case.*

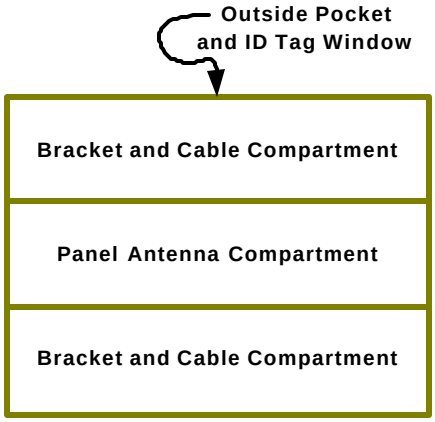


Figure 2-164 Schematic Layout of SSR Antenna Carrying Case

2.46 PACKUP SSR ANTENNA MAST CARRYING CASE PROCEDURES.

Figure 2-165 SSR Antenna Mast Carrying Case and Components

2.46.1 Teardown AB-1244 Antenna Mast. Procedure is in Paragraph 2.42.1.

2.46.2 Inventory SSR Antenna Mast Carrying Case Components.

1. Locate the SSR Antenna Mast Carrying case inventory checklist card. See Table 2-52, p. 2-128 or in Appendix J.

2. Identify each item on inventory checklist card

3. Verify that all of the SSR Antenna Mast Carrying Case Components are present.

4. Annotate any discrepancies or shortages on DA Form 2407 or 5504.

2.46.3 Packup SSR Antenna Mast Carrying Case

1. Gather all equipment and secure in your antenna mast carrying case for movement/storage.

2. 30” Antenna Mast comprised of:

   a. Five upper mast sections. (mast section assembly (upper))
   b. Five lower mast sections. (mast section assembly (lower))
   c. Upper mast adapter section (red-ring). (adapter assembly (upper))
   d. Lower mast adapter section (blue-ring). (adapter assembly (lower))

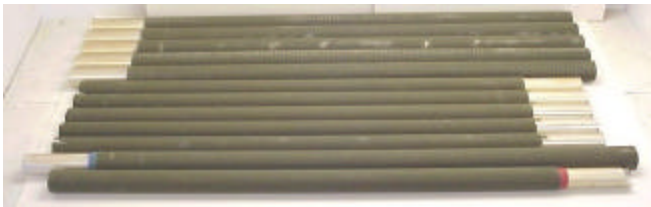


Figure 2-166 Mast Sections

3. Antenna Mast Kit consists of:

   a. Four (36) ft. guy ropes (blue clips).
   b. Four (42) ft. guy ropes (red clips).
   c. Four reel units (RL-28) for guy ropes, two guy ropes per reel unit.
   d. Four guy stakes. (stake assembly)
   e. Mast base assembly.
   f. Base plate.
   g. Two base plate pins (stakes).
   h. Two guy rings/plates (one red, one blue)
   i. 2.5lb sledgehammer

Figure 2-167 Antenna Mast Kit

4. Pack the CAISI antenna (omni-directional or panel), RF antenna cables and antenna brackets in their appropriate transit case/carrying case. Table 2-57 is a summary of where all the antenna and ancillary components are located.

Table 2-57 Location of Antenna and Antenna Ancillary Components

Location	Antenna/Ancillary Component
CBM	40-inch Whip break-away antenna (omni-directional)
	7-inch Directional Panel antenna
	7-inch Antenna bracket
	25-ft RF antenna cable
	35-ft RF antenna cable
CCM	24-inch Whip antenna
	7-inch Antenna bracket
	35-ft RF antenna cable
SSR Transit Case	40-inch Whip break-away antenna (omni-directional) (Qty 2)
	4-inch Whip antenna (Qty 2)
	"Dummy Load" antenna (Qty 2)
SSR Notebook Case	"Rabbit Ears" antenna
	"Dummy Load" antenna
SSR Antenna Carrying Case	14-inch Directional Panel antenna (Qty 2)
	7-inch Antenna bracket (Qty 2)
	14-inch Antenna bracket (Qty 2)
	50-ft RF antenna cable (Qty 4)

Chapter 2

Section IV Operation Under Unusual Conditions

2.47 INTRODUCTION

The CAISI components (CBM/CCM) have been placed in ruggedized cases to allow operation in a variety of field conditions. However, the actual components of the CBM/CCM (hubs, radios, DSL modems) are COTS equipment and have not been ruggedized. The following precautions should be observed to ensure the safety of operators and maintainers, and the operational readiness of the equipment in unusual or more extreme conditions.

2.47.1 Operation Under Extreme Heat or Desert Conditions.

In hot, dry climates, the equipment, connectors, and receptacles are subject to damage from windblown sand and dust. Do not leave equipment covers open or any cable connectors and receptacles uncovered. Position the equipment to minimize the exposure to wind blown particles.

2.47.2 Operation Under Extreme Cold or Artic Conditions.

Extreme cold conditions will cause cables to become hard, brittle, and difficult to handle. Before unrolling cables, if possible, allow them to warm up until they are more pliable. When handling and connecting cables, avoid kinks and unnecessary cable loops or damage to the cable may result. Make sure all connections are free of frost, ice, and snow. Never drag a cable connector on the ground or place an uncovered or open cable connector in the snow.

2.47.3 Operation Under High Humidity or Tropical Conditions.

Moist climates typically cause condensation to form on the equipment, which becomes a fertile environment for the growth of a variety of fungi. Make frequent PMCS inspections to detect corrosion before it damages equipment or the connectors. Use a dry, lint-free cloth to wipe moisture and fungi off the equipment. Also, make sure all electrical equipment and cables are kept off the ground and out of any puddles of water, which would cause injury to personnel and damage to the equipment

Chapter 3

OPERATOR MAINTENANCE INSTRUCTIONS

Section I Lubrication Instructions

3.1 LUBRICATION

The CAISI suite of equipment does not require lubrication.

Section II Troubleshooting Procedures

3.2 OPERATOR TROUBLESHOOTING

Operator Troubleshooting, in the event of a malfunction, mainly consists of ensuring that all CAISI components and cables are properly connected, and a power source is correctly applied. The operator will then attempt to operate the CAISI component a second time. If the malfunction persists the operator will follow the procedures detailed in this section for obtaining maintenance for the failed component.

3.3 DIAGNOSTIC FEATURES SUMMARY

3.3.1 Diagnostic LEDs. Most CAISI components have LEDs that provide information concerning the status of CAISI operations and alert the user to potential problems. Chapter 2, Section 1 of this manual describes the LEDs of the various components and their meaning, and are summarized below.

NOTE: *When evaluating the LED status during CAISI diagnosis, any red LED is usually indicative of a problem.*

3.3.2 Audible Alarms. The UPS contains an audible alarm that alerts the user when a problem arises with the operation of the UPS. A warning is sounded whenever the power supply is interrupted and the UPS switches to battery power, or when the UPS battery is low or in need of replacement.

3.4 DIAGNOSTIC PROCEDURES. Short of catastrophic failure, a problem with CAISI will usually manifest itself as a data transmission problem. However, it is possible that the problem may also be caused by the STAMIS hardware or software or a problem with the network. When a data transmission problem occurs, it must be determined if the problem is CAISI, STAMIS, MSE, INE, or DNS related.

CAISI is made up of Line Replaceable Units (LRU). Basically, this means that a unit that is not working properly can be replaced.

CAISI LRUs are: Wireless Bridge, Multi-Client Radio Adapter, DSL Bridge, Inline Encryptors, Hubs, Power Supplies, Lightning Arrestors, Router, Notebook Computer, UPS, Antennas and antenna cables.

Below are the basic user level troubleshooting procedures for the CAISI components.

3.4.1 Troubleshooting Procedures. The unit level personnel using the CAISI may perform only limited troubleshooting on the CAISI components. Paragraph 3.13 contains troubleshooting flowcharts that should assist the user in isolating and diagnosing a problem with the CAISI. However, performing software diagnostics is primarily the responsibility of the SSR personnel, who should be contacted when a problem arises. These personnel, as well as the software help desk may, during telephonic consultation, "talk" the user through some diagnostic procedures in an attempt to diagnose the problem.

The Customer Assistance Office (CAO) phone numbers, fax numbers and E-Mail address are:

Comm 804-734-1051
DSN: 687-1051
Fax Comm: 804-734-2947
Fax DSN: 687-2947
Email: cao@lee-dns2.army.mil

These procedures are detailed in the following paragraphs. Users experiencing a problem with the CAISI components should never hesitate to contact the system support representative or their designated next higher level of support.

NOTE: *PMCS should be done **before** troubleshooting.*

Performing authorized troubleshooting involves a three-step process:

1. **Identify** the problem. The user must first identify that a problem exists and the nature of the problem prior to taking steps to correct the problem. **This is the hardest part – being able to clearly define and communicate what problem has occurred.** Most problems with the CAISI will initially appear as a data transmission problem by a STAMIS user(s) connected to a CAISI bridge.

2. **Isolate** the problem. Once a problem has been identified, the user should attempt to isolate the exact component that is causing the problem. This process includes eliminating potential causes of the problem through the steps described below, with the end result being identification of the root cause of the problem.

3. **Correct** the problem. Once the root cause of the problem is identified, Corrective action may be taken. Corrective actions performed by the user could be one of the following: fixing, reattaching, reseating, or replacing the malfunctioning components or evacuating the component for service at a higher-level of maintenance

Keep the following items in mind while troubleshooting:

1. Review actions to be taken to ensure they adhere to standard operating procedures.

2. Always document and take notes. Taking notes will help in troubleshooting the problem while in contact with CAISI help desk consultant.

3. If the problem needs to be elevated to a higher-level of support, this will make communicating the entire problem easier.

4. If troubleshooting does not resolve the issue, prepare DA Form 2404/5988E and contact the next higher-level of support.

Potential problem areas that can be addressed through unit level troubleshooting relating directly to the bridge modules include **Installation**, **Connections** and **Network** problems. Each of these problem areas are discussed below:

1. **Installation:** CAISI is not set up in acceptable operating conditions. Some identifying problems are failing test conditions, LEDs not lit, and error lights on.

2. **Connections:** CAISI is set up correctly, but a problem has occurred either immediately after setup or during normal operation. Usually has to do with connections, ports, and cables.

3. **Network problems:** All CAISI modules appear to be operating normally, but the users can not connect to other STAMIS computers. Problems external to the CAISI components that could affect data transmissions include problems with MSE, to include the INE device, the DNS, and the STAMIS computers connected to the CAISI hubs.

3.4.2 Individual Component Troubleshooting. The next few paragraphs will cover the troubleshooting of the individual components.

It is important to understand how the components in the CBM/CCM work together in order to troubleshoot when the system is not working properly. For this reason, we will troubleshoot the CBM/CCM as a whole. The individual components of each module will be discussed under the appropriate module.

Table 3-1 CAISI Troubleshooting

Network Connections	Paragraph 3.5
SSR Notebook	Paragraph 3.6
CBM	Paragraph 3.7
General Troubleshooting	Paragraph 3.7.1
Hubs	Paragraph 3.7.2
Inline Encryptor and Wireless Bridge	Paragraph 3.7.3
Antenna System	Paragraph 3.7.4
DSL Bridge	Paragraph 3.7.5
UPS	Paragraph 3.7.6
CCM	Paragraph 3.8
General Troubleshooting	Paragraph 3.8.1
Hub	Paragraph 3.8.2
Inline Encryptor and Multi-Client Radio Adapter	Paragraph 3.8.3
Antenna System	Paragraph 3.8.4
LSA	Paragraph 3.9
Router	Paragraph 3.10
10BaseT Transceiver	Paragraph 3.11
AB1244-B Antenna Mast	Paragraph 3.12
Troubleshooting Flowcharts	Paragraph 3.13

3.5 TROUBLESHOOTING THE NETWORK. See Appendix B to Field Manual 24-7, Tactical Local Area Network (LAN) Management for network troubleshooting procedures.

Problem: STAMIS users cannot communicate through the CBM, CCM or LSA.

1. Most users can communicate through CAISI but, if at least one cannot:

   a. Ensure STAMIS communications module is properly configured.

   b. Verify connections from STAMIS users to the CAISI Modules. Make sure all cables and wires are firmly connected and none appear to be loose to the touch or gentle tugging.

   c. Inspect cables and wires for damage.

   d. Verify that the connection does not exceed its maximum length.

   e. Verify that the user has correctly registered with CAISI (Each STAMIS may have a different registration procedure). You may need to contact a higher level of STAMIS support.

2. If the problem still occurs, contact a higher-level of maintenance.

Specific troubleshooting actions are included in the preceding paragraphs for the various CAISI components. Here are some general things to try, in the order that they most frequently fix the problem.

1. **Check your lights.** Frequently, communications are down because the equipment is not receiving power and you don't know it.

2. **Check to see if the computer next to you has communications**. If not, then check your CBM or CCM. It may be down.

   a. To verify a CBM is receiving power, verify the following:

      (1) Ensure the power cords for the individual components are plugged into their corresponding power adapters and that the other ends of the power cords are seated firmly in the outlets on the UPS.

      (2) Ensure the UPS is plugged into an operational external power source and the "**I**" (ON) side of the UPS rocker switch is pressed in.

   b. To verify the CCM is receiving power, ensure the power cord is seated firmly in the power adapter and the external power source.

   c. If none of the computers connected to the CBM/CCM can communicate, then the problem lies in the CBM/CCM. Refer to Paragraph 3.7 for CBM troubleshooting procedures and Paragraph 3.8 for the CCM.

   d. If others can communicate, but one cannot, then the problem probably lies in the computer or connecting cables. Refer to Step 5 below.

3. **Check the network to be sure it's up.** Often another user within the CAISI LAN has accidentally cut power to their module or tripped over an antenna cable and the network is down.

   a. Look at the radio lights in the CBM/CCM to see if it is associated. If the center light is solid green or blinking about 7/8s on and 1/8 off, the network is up – at least to the next closest CBM.

4. **Reboot or Cycle Power.** It's amazing how often this fixes mystery problems. This is true for network components like the wireless bridges as well as for computers.

   a. Reboot the CBM/CCM.

      (1) To reboot a CBM, remove power from the UPS by pressing the "**O**" (OFF) side of the UPS rocker switch in. Wait 10 seconds, and then turn the UPS back on by pressing the "**I**" (ON) side of the UPS rocker switch in. Watch the lights.

      (2) To reboot a CCM, unplug either end of the power cord, wait 10 seconds, then plug it back in. Watch the lights.

   b. Reboot the computer(s) connected to the CBM/CCM.

      (1) Click the "Start" button on the desktop menu toolbar. Select the "Shut Down" option and press the "OK" button.

      (2) Alternatively, perform a hard reboot of the computer.

         (a) Press the power button on the compute monitor and then press the power button on the Central Processing Unit (CPU).

   NOTE: *When rebooting the computer, do not interrupt the disk defragmentation or virus scan. Not only are these essential utilities to the health of the computer, there are often actions, such as loading the network card drivers, that come after them and would be inadvertently cancelled. If you don't load the drivers, the computer cannot communicate.*

5. **Check Your Cables** If you have intermittent problems (sometimes it works and sometimes it doesn't) – cables are often the problem. Cables frequently work even when loose. They look OK, but aren't plugged in tightly. This may be because they were not originally plugged in properly, or they may have been vibrated loose or pulled loose when someone tripped on them. .

NOTE: *When you check the cables,* ***look*** *and* ***feel*** *the cable for possible problems.*

a. **Antenna Cables.**

(1) Wiggle the antenna cable while hand-tightening the connector. Do not use a wrench to tighten them.

(2) Loosen and retighten the connector. Sometimes the connectors are cross-threaded. If the connector only turns once or twice, it is not properly connected. They should turn between six and ten times as you tighten them.

b. **10Base-T Ethernet Cables.**

(1) Check the Ethernet cables to make sure that they are lock into the ports. Spread the little locking tab if necessary. You should hear and feel it snap into place when you insert it into the port.

(2) If the locking tab is missing or loose, replace the cable or the RJ-45 connector.

c. **10Base-2 Coax Cables.**

(1) Ensure that the connector is locked. When you turn it to the right, the bumps on the hub or transceiver connector should seat into the indentions on the ends of the slots on the cable connector.

d. **Power Cables.**

(1) Make sure that power cables are firmly seated. They do not have locks, but are held in by friction. Push it all the way in and wiggle the cable gently to make sure that it stays.

Antenna Cables | 10Base-T Ethernet Cables | 10Base-2 Coaxial Cables | Power Cables

Figure 3-1 Troubleshoot Antenna, Ethernet, Coaxial and Power Cables

6. **Check your antenna and cable connectors.** Ensure that all antenna cables and connectors are tight, dry and not cross-threaded.

   There are three problems that sometimes occur with the antenna connectors.

   a. Water can get in the connectors and short out the signal. If this happens, just dry them out and use tape to keep it from happening again.

   b. Sometimes the tines that surround the pin sometimes get spread out.

      (1) The "female" connector consists of four tines that form a cup or tube into which the pin on the "male" connector is seated when the two are joined. Normally the tines are close enough together that they are touching. If they are spread out so that they no longer resemble a tube, you need to gently squeeze then back together.

      (2) Insert the CAISI reset tool into the center of the connector, and then squeeze the tines with a pair of needle-nose pliers. The reset tool keeps you from flattening the connector or closing it up so much that the male connector will not fit.

   c. Occasionally the connector will break internally, so that it is no longer connected to the cable. If the connector pulls off the end of the cable or rotates freely on the end of the cable, the cable needs to be replaced. This is usually the result of having used a wrench to tighten the cable onto the radio or antenna.

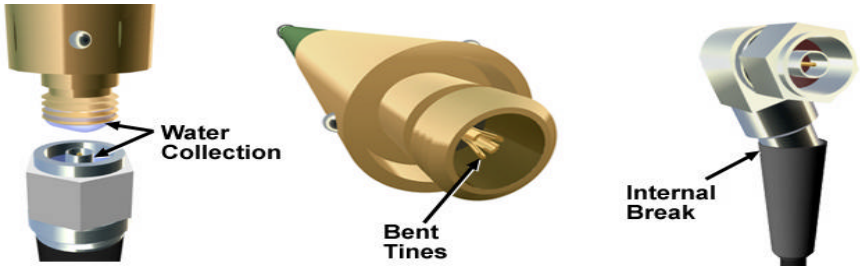


Figure 3-2 Troubleshoot Antenna & Cable Connectors

7. **Check your antenna orientation.**

a. **Omni directional whip antennas -**

(1) Ensure that it is erected as vertical as possible. This is extremely important for good bandwidth and radio communications, especially for shots over a half-mile.

(2) This antenna is designed to provide a 360 degree radiation pattern. It is used when coverage in all directions from the antenna is required.

(3) The radio signal around the antenna resembles a flattened or squashed donut.

Figure 3-3 Omni-Directional Whip Antenna Gain

(4) If the antenna is tilted, the donut is tilted and may be transmitting over the top of the other radio. (Figure 3-4 (left figure))

(5) If there is a significant difference in elevation between two radio sites, then you might need to deliberately tilt the antenna. Or use a panel antenna. (Figure 3-4 (right figure))

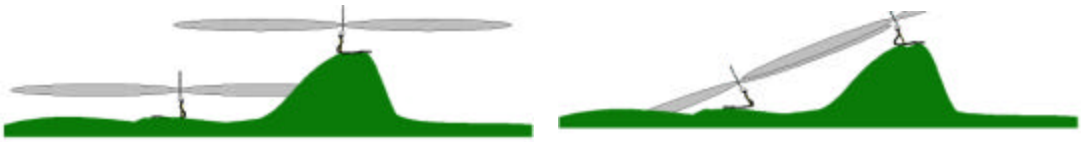


Figure 3-4 Omni-Directional Whip Elevation Difference

NOTE: *If there is a lot of humidity in the air, this will effect the radio transmissions. Water will slow the radio transmissions down. A good comparison for this is how you move through water, when you are out of the water, you can run, but when you are in the water, your movement is slower. The same is true for radio waves.*

b. **Directional (panel) antenna.** These antennas are point to point. When connecting two points or modules together, the distance, obstructions and antenna locations must be considered.

(1) Ensure panel antennas are used in situations in which clear line of sight (LOS) can be maintained or when very long distances exist between modules.

(2) Ensure antennas are installed as high as possible and above obstructions such as trees.

(3) Ensure antennas are aligned so that their main radiated power is directed at each other.

Figure 3-5 Directional Panel Gain

(4) To **verify directional antenna alignment/orientation** perform the following procedures:

(a) Connect a 25', 35' or 50' RF cable to the directional antenna and erect it. (Paragraphs 2.18.1, 2.18.2, 2.18.4, 2.19.2)

(b) Connect the MMCX to N (F) adapter cable (in SSR Notebook case) to the right antenna connection port on the wireless NIC. (You may have to remove the rabbit ears connectors from the wireless NIC).

(c) Connect the other end of the MMCX to N adapter cable to the RF antenna cable. Insert the wireless NIC into your notebook.

(d) Use the Link Status Meter (LSM) to check signal quality. Refer to the TB 11-5895-1691-10, Paragraph 4.1 (item 7b).

Figure 3-6 Wireless NIC and MMCX to N (F) Adapter Cable

NOTE: *The panel antennas concentrate all the radio output power in a "beam" – in one direction. The bigger the panel, the tighter the beam, and the more gain. Again, the more gain, the greater the range. However, there is a trade-off. As the gain goes up, aiming the beam becomes more difficult.*

Elevation differences are less of a factor than with the whip antenna, but you must aim the flat side of the panel antenna toward the distant end. The larger panel has a tighter beam and extends farther from the antenna. Use a map to determine the direction and compass to aim the antenna if you cannot see to the distant end or very accurately estimate its direction. Refer to Paragraph I.5.2 for a discussion on the range of radios with the different antennas.

8. **Check your radio speed**. On shots that are difficult because of distance or obstacles, you may find that your transmission speed is erratic, or you may even not be able to associate with the distant CBM.

   Try reducing the "Allowed bit rates in megabits/second" on the configuration "Radio" menu in the CCM or remote CBM from "**1_11**" to "**1_2**," or even "**1**." Refer to the TB 11-5895-1691-10, Paragraph 4.1 (item 8).

   Although the maximum speed is reduced, this will sometime improve total throughput because the radios are much more reliable at slower data rates when the signal is poor.

9. **Check you CBM root radio "Bridge Spacing".** If you have any long shots, the spacing must reflect the length (in kilometers) of your longest shot. This setting affects timeouts and can even keep you from associating if it is too short. The setting on your root radio controls the entire network. Refer to the TB 11-5895-1691-10, Paragraph 4.1 (item 9).

10. **Check Your Configuration.** Configuration parameters often seem to mysteriously change themselves. Well, not really, but it seems like it sometimes.

    a. Verify your parameters are set to their original values. Sometimes parameters were changed during some earlier troubleshooting session or the user changed them during experimentation. Make sure they are back to their original values. If necessary, follow the configuration procedures in the preceding appendices to reset them to their defaults. Then adjust them as necessary for the current deployment.

    b. Verify that parameters that were supposed to be changed to support deployment were changed.

    c. Finally, check to make sure that you, or someone, didn't "fat-finger" something. A typographical error in the SSID or WEP key, for instance, will cause a great deal of problems. **Refer to the TB 11-5895-1691-10, Paragraph 4.1 (item 10) for specific guidelines.**

11. **Check the following Network Operation Rules.** One thing you really have to watch out for is that users tend to add equipment to the network that you don't know about. This should not normally be a problem, unless they fail to follow the rules.

Here are a couple of rules that are most often violated and cause problems:

a. **The Eight-Client Rule**. You can connect no more than eight network devices to a CCM. This includes not only computers, but also any device with a MAC address.

Symptoms: Some of the clients cannot communicate, while the others can.

(1) The inline encryptor counts as one of the 8 clients. It communicates with other inline encryptors whenever it needs to negotiate keys. Once it has a key, it sends all traffic with the computers' MAC addresses. But keys must be negotiated every time there is a new computer-to computer pairing. And keys need to be renegotiated periodically as well.

(2) If a STAMIS computer has both their network card and a LSA connected, that's two clients.

(3) If the user adds a "smart hub" or "smart switch", that's another client.

(4) If the user adds a dumb hub with three of four clients behind it, that's three or four more clients.

b. **The Hundred-Meter Rule**. The twisted pair cables on the LAN can be no longer than 100 meters.

Symptoms: The computer on the too-long cable may have no or slow communications. The rest of the network will also see excessive collisions, causing outages or slow communications.

(1) This does not mean that every computer has to be within 100 meters of every other, but they must be within 100 meters of the hub.

(2) If you connect two cables together to make a long one, the total cannot be over 100 meters.

(3) When you cascade hubs, you are not creating separate collision domains, but you are extending the total length of the cable. If you need to go over 100 meters, use a hub instead of a butt connector (line coupler) to join the cables.

c. **The 5-4-3 Rule**. The collision domain cannot contain more than five segments joined by four hubs with a maximum of three mixing segments with users. User segments include your connection, the gateway connection and the connections in the CBMs where the twisted pair hubs are joined by coaxial cable. (Figure 3-7)

Symptoms: The network will see excessive collisions, outages, or slow communications.

(1) Ensure there are no more than two additional hub connected to any CBM or CCM.

(2) Remove all power from the unit. Unplug power cables and disconnect them from the unit. Then reconnect it. (Recycle power).

In the path between User A and User E

- Segments 1,4, and 5 have users.
- Segments 2 and 3 do not.
- Users B, C, and D do not count, except that every pairing (User "X" to User "Y") must conform to the rule.

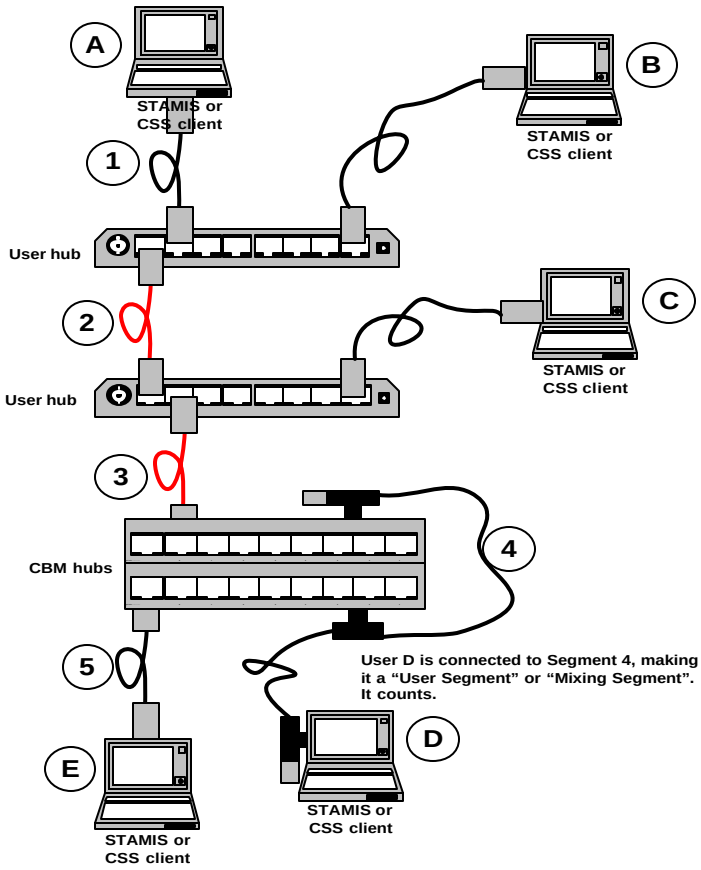


Figure 3-7 5-4-3 Rule

The Ethernet protocol requires that a signal sent out over the LAN reach every part of the network within a specified length of time. The 5-4-3 rule ensures this. Each repeater that a signal goes through adds a small amount of time to the process, so the rule is designed to minimize transmission times of the signals.

d. **The Twisted Pair Rule**. Twisted pairs must be cabled correctly. The transmit pair must be twisted, and the receive pair must be twisted – separately. Pins 1, 2, 3, and 6 are used in Ethernet connectors. But within the cable, wires 1 and 2, 3 and 4, 5 and 6, and 7 and 8 are twisted in pairs.

Commercial cables (Cat-5) are acceptable, but users often make their own cables and fail to use the correct pairs.

Symptoms: The computer or devices on or behind the bad cable may have no, slow or intermittent communications – even though the link lights on both ends will light.

(1) Inside a Cat-5 cable are 8 thin, color-coded wires that run from one end of the cable to the other. All 8 wires are used

(2) In a straight-through cable, wires 1, 2, 3, and 6 at one end of the cable are also wires 1, 2, 3 and 6 at the other end.

(3) In a crossover cable, the order of the wires change from one end to the other: wire 1 becomes 3 and wire 2 becomes 6.

Table 3-2 Straight-Through/Crossover Cabling

Straight-through cable			Crossover cable		
Wire	Becomes		Wire	Becomes	
1	→	1	1	→	3
2	→	2	2	→	6
3	→	3	3	→	1
6	→	6	6	→	2

(4) Most cables use the Electronics Industries Alliance (EIA) / Telecommuncations Industry Association (TIA) 568B standard on both ends for straight cable but you can use the EIA/TIA 568A as well. If you mix the standards you get a properly configured crossover cable.

(5) To determine which wire is number 1, hold the cable so that the end of the plastic RJ-45 tip (the part that goes into the wall jack first) is facing away from you. Face the clip so that the copper side faces up (the springy clip will now be parallel to the floor). When looking down on the copper side, wire 1 will be on the far left.

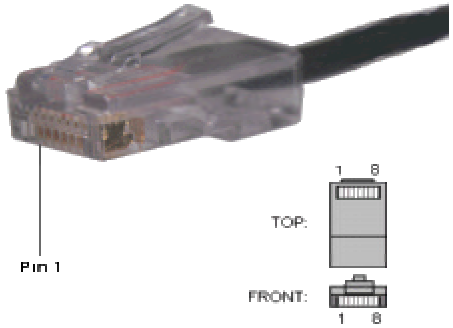


Figure 3-8 RJ-45 Connector

Table 3-3 Pinout for 10Base-T/100Base-T Ethernet Connections

Pin #	Ethernet 10BASE-T 100BASE-TX	EIA/TIA 568A	EIA/TIA 568B
1	Transmit +	White with green stripe	White with orange stripe
2	Transmit -	Green with white stripe or solid green	Orange with white stripe or solid orange
3	Receive +	White with orange strip	White with green stripe
4	N/A	Blue with white stripe or solid blue	Blue with white stripe or solid blue
5	N/A	White with blue stripe	White with blue stripe
6	Receive -	Orange with white stripe or solid orange	Green with white stripe or solid green
7	N/A	White with brown strip or solid brown	White with brown strip or solid brown
8	N/A	Brown with white stripe or solid brown	Brown with white stripe or solid brown

The only real difference between 568A and 568B is that the White/Orange-Orange/White and White/Green-Green/White pairs are swapped.

A good Cat-5 termination provides a proper wire crimp, a wire insulation strain relief crimp and a cable strain relief crimp.

Also important is not unwinding the wires more than necessary; maintaining the twists as far as possible. Do not however, let this stop you from inserting the wires as far as possible.

(6) Procedures on how to make a good straight and crossover cable.

(a) Strip the cable's jacket back one full inch.

(b) Untwist the wires back to within 1/8" of the jacket.

(c) Arrange the wires in the order in which you want to crimp them, (ie. 568B, or 568A, etc).

For standard straight-through cables, wires 1 and 2 (orange-white and orange) must be connected to pins 1 and 2. Wires 3 and 6 (green-white and green) must be connected to pins 3 and 6.

For crossover cables one end is the same as a straight-through cable, but the other end is different. Wires 1 and 2 (orange-white and orange) must be connected to pins 3 and 6. Wires 3 and 4 (green-white and green) must be connected to pins 1 and 2.

(d) Grasp the wires firmly, between your thumb and forefinger, flatten them, and even wiggle them a bit, to take out the curliness, (concentrate your efforts on the bottom 1/2") the wires must lay flat and together, aligned as close as possible.

(e) While holding the wires firmly, cut off the wires 1/2" from the cables jacket utilizing some sharp wire strippers or even high quality scissors. (Avoid using wire cutters that flatten the ends of the wires insulating material, this makes stuffing the wires very difficult).

(f) Stuff the wires into the connector, making sure the wires stay lined up.

(g) The wires should reach the end of the tube they are in, if possible, or at least past the farthest point of that "little Gold Plated thingy" above it, which will terminate it.

(h) The jacket should go even with the end of the first indent, if possible, it's a strain relief for the cable. Insert it into the crimping tool, and Crimp it!

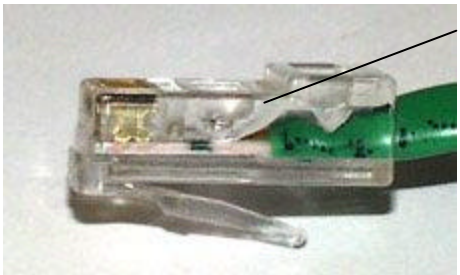


Figure 3-9 Crimp Strain Relief

(i) All of this is very dependent on the tools you are using, the connectors you are using, and the cable you are using.

In Figure 3-10, the color layouts are abbreviated. The first color listed in the color pair is the dominant color of the wire. In other words, WHT/ORG is a white wire with orange stripes.

Color abbreviations used are:

WHT – White	ORG – Orange	BLU - Blue
GRN - Green	BRN - Brown	

How to wire a CAT5 (EIA 568-B*) Cable.

connector #1	connector #2
1 WHT/ORG	1 WHT/ORG
2 ORG/WHT	2 ORG/WHT
3 WHT/GRN	3 WHT/GRN
4 BLU/WHT	4 BLU/WHT
5 WHT/BLU	5 WHT/BLU
6 GRN/WHT	6 GRN/WHT
7 WHT/BRN	7 WHT/BRN
8 BRN/WHT	8 BRN/WHT

How to wire a CAT5 (EIA 568-A*) Cable.

connector #1	connector #2
1 WHT/GRN	1 WHT/GRN
2 GRN/WHT	2 GRN/WHT
3 WHT/ORG	3 WHT/ORG
4 BLU/WHT	4 BLU/WHT
5 WHT/BLU	5 WHT/BLU
6 ORG/WHT	6 ORG/WHT
7 WHT/BRN	7 WHT/BRN
8 BRN/WHT	8 BRN/WHT

Figure 3-10 Straight-through (EIA 568-B/568-A) Cabling

How to wire a "Crossover" Cable (EIA 568-B)

Connector # 1	Connector # 2
1. WHT/ORG	1. **WHT/GRN (normally 3)**
2. ORG/WHT	2. **GRN/WHT (normally 6)**
3. WHT/GRN	3. **WHT/ORG (normally 1)**
4. BLU/WHT	4. WHT/BLU
5. WHT/BLU	5. BLU/WHT
6. GRN/WHT	6. **ORG/WHT (normally 2)**
7. WHT/BRN	7. BRN/WHT
8. BRN/WHT	8. WHT/BRN

Figure 3-11 Crossover (EIA 568-B) Cabling

e. **The Uplink-Is-Not-An-Extra-Port Rule**. Many devices, such as the hubs in the CCMs and CBMs have an uplink port that is shared with one of the normal ports. You can use one or the other but not both

Symptoms: One or both of the two connected devices will have no communications or will have slow communications.

(1) The hubs in the CCMs and CCMs have an uplink port shared with port 8. Port 8 is for connecting a computer or other "terminal" device. The uplink port is for connecting to a normal port on another hub or switch.

(2) Many other devices have similar arrangements. The "normal" ports have a built-in crossover and may be labeled "MDI-X." The "uplink" port is not crossed over and is labeled "MDI", "Uplink", or "WAN".

f. **The You-are-Not-Allowed-to-Pirate-IP-Addresses Rule**. Many times users connect computers to the network without approval to do so. Often they use a friend's computer to determine the network address range and ping the network with a series of address until they find one that doesn't answer. They then configure their own machine to use the "free" address.

Symptoms: The STAMIS device will have no commo (communication). And often won't know it. The users will keep trying to communicate, but assume the server is busy. And they have no tools to find out any different.

(1) Just because an IP address is not in use at the moment, doesn't mean that it's free. This is especially true of the STAMIS computers using ftp under DOS. Their computers only answer a ping when they are in an active session.

If you have a DOS-based ULLS machine that cannot connect over the network, it is entirely possible that one of your compatriots is pirating the address. Use the SSR notebook to ping the ULLS' assigned address while the ULLS box is not in ftp mode. If you get an answer, someone is using the address. Track down the individual and address them in accordance with unit SOP.

(2) DHCP may be available. If you are using the optional router, DHCP is available for the private segment and should be used for everything except STAMIS computers that require static addresses. Signal may be providing DHCP on the public segment. If so, it should be used for everything except STAMIS computers that require static addresses.

3.6 TROUBLESHOOTING THE SSR NOTEBOOK. All of the procedures below will be discussed in full detail in the CAISI Technical Bulletin 11-5895-1691-10. The specific paragraphs will be stated next to each procedure.

1. **If the notebook fails to boot**, you made need to do one of the following: (Try these procedures in this order)

   a. Check and adjust the Complementary Metal Oxide SemiConductor (CMOS) settings:

      Set all the Basic Input/Output System (BIOS) settings back to their original values, as listed in the "Notebook System Setup (BIOS Settings)" Paragraph 2.3 of the CAISI TB 11-5895-1691-10, Software User's Manual.

   b. Reload the hard disk image:

      If you can not boot from the hard disk, reload the CAISI Z13-4B-xx baseline from the CD, as instructed in the "Notebook Software Load" Paragraph 2.4 of the CAISI TB 11-5895-691-10, Software User's Manual. (Replace the xx's with the baseline that you are using).

      Any accounts you have created will be lost and will have to be rebuilt.

      If the baseline will not load, you have a hardware problem.

   c. Replace the hardware components:

      Send the notebook to the Forward Repair Activity (FRA) for replacement of components or the notebook itself.

      NOTE: *FRAs are listed in Table 3-15, p. 3-74.*

2. **If the notebook boots properly, but you can not log on because you forgot the password:**

   Get the password envelope from the security officer. If the password envelope is not available or was never turned in, you will have to reload the software using the CD provided. This will reset the notebook to its default settings, including the password.

3. **If the software locks up so that you cannot enter any commands on the notebook computer, try pressing the Escape (ESC) key.**

   a. If that doesn't work, use the Task Manager to check for any tasks not responding, and end them through the Task Manager.

   b. If the Task Manager won't come up, or there are no tasks listed as not responding, remove any CD or floppy disks and perform a soft reboot by pressing Ctrl-Alt-Del.

c. If the notebook will not soft boot, turn it off, by holding the OFF button for up to 10 seconds, wait a few seconds and then turn it back on.

4. **If any of the CAISI Toolbox utilities do not appear to working properly, verify that you have the current CAISI baseline loaded.**

a. The baseline identification is shown on the wallpaper screen under the DOD warning banner.

b. More specific information on version and date can be found in the C:\version.txt file.

c. There may be upgrades that need to be loaded. If the baseline is not current, load the current baseline.

NOTE: *If all else fails, contact the Customer Assistance Office (CAO) at Ft. Lee, VA, DSN 687-1051 or 804-734-1051. Indicate that you need assistance with CAISI baseline Z13-4B-xx (replace x's with the baseline you are using).*

5. **If you are logged on but cannot connect from the wired NIC,** try the following:

Problems with the wired NIC are usually because of a bad cable, speed synchronization problems, network configuration problems, or having the encryption client turned on. (TB 11-5895-1691-10, Paragraph 4.2.1.3)

a. Check your cables.

b. Check for lights on the NIC to indicate it is receiving power. Check the lights on the hub that you are connected to. If possible, replace the cable or try a different port. Check your lights again.

c. Check your TCP/IP settings. See TB 11-5895-1691-10, Paragraph 2.7.

d. Make sure you have an IP.

e. Reboot the notebook. (Make sure you stop the NIC card, first). If that fails, reboot the devices to which you are connected to.

First, you must stop the NIC card. Double-click the card icon in the lower right hand corner of the notebook screen. The "Local Area Connections Properties" menu will appear. Select the card you want to stop by clicking the mouse on it, then press the stop button.

f. Remove the wired NIC and try the wireless one. If that one is OK, replace the wired NIC.

g. If all the above fails, reload the software from the CD, the drivers may be corrupted.

6. **If you are logged on OK but cannot connect to the network with your wireless NIC**, try the following: TB 11-5895-1691-10, Paragraph 4.2.1.4.

Problems with a wireless NIC are usually because of antenna problems, wireless configuration problems, network configuration problems, or remote encryption client configuration problems.

a. Ensure the Wireless NIC is properly installed in the notebook.

(1) Check to see if the radio card is installed in the PCMCIA slot. Push it in. If it wasn't fully in, you will hear a chirp from the notebook.

(2) Verify the rabbit ears antenna cable connectors are seated firmly into the holes on the end of the card.

(3) Ensure the rabbit ears antenna has been attached to the back of the notebook screen with Velcro and that the antenna extends above the top of the screen.

Figure 3-12 Wireless NIC, Rabbit-Ears Antenna and SSR Notebook

b. Ensure you are operating in secure mode if you are communicating on the trusted side of the network or to other STAMIS computers.

c. If you are troubleshooting the wireless radios you want to be in non-secure mode. Refer to the TB 11-5895-1691-10, Paragraph 2.9.

d. Check the Wired Equivalent Privacy (WEP) key and the Service Set Identification (SSID) using the CISCO Aironet Utilities. Refer to the TB 11-5895-1691-10, Paragraph 2.8.

e. Check your TCP/IP settings and make sure you have an IP. (Right-click on "My Network Places" Icon on desktop. Select "Properties".)

f. Check for lights on the Wireless NIC. If no lights, reseat the wireless NIC. (See steps above to stop the NIC card, 5e).

g. Check your antenna and antenna connection.

h. Make sure you are in radio range to a CBM. (Refer to Paragraph 3.5(6))

i. Check that the bridge to which you are trying to connect is up, and that is a root bridge or is associated with a root bridge. Verify your parameters on the root CBM or the bridge that you are connected to.

j. Reboot the notebook. (Make sure you stop the NIC card, first). If that fails, reboot the devices to which you are connected to.

k. Remove the wireless NIC and try the wired one. If that one is OK, replace the wireless NIC.

l. If all the above fails, reload the software from the CD, the drivers may be corrupted.

Table 3-4 Notebook Computer Troubleshooting Procedures

PROBLEM	POSSIBLE CAUSES	RECOMMENDED ACTION
Notebook computer does not power on.	Power Adapter not connected. Power source not functioning. Battery dead.	Verify connections. Verify power source. Contact support personnel. (SSR)
Computer has problem running on AC adapter.	AC adapter incorrectly connected. UPS not providing power.	Check AC adapter connections. Check UPS connections and functions.
LCD Screen is blank.	Computer is in Sleep or Suspend mode. Lid has been closed.	Place in Full On mode. Normal. Screen returns after lid is opened.
Failure during boot process	Powering off without performing graceful shutdown has corrupted software.	Contact support personnel. (SSR). See step 1 above in 3.5
Computer locks up.	Software Problem.	Contact support personnel. (SSR). Refer to TB 11-5895-1681-10.
Screen images are not clear.	Contrast and clarity out of adjustment.	Adjust.

3.7 TROUBLESHOOTING THE CBM. The CBM includes a wireless bridge, an encryptor, a DSL bridge, two hubs, two antennas (although you only use one at a time), an UPS, and the cables to connect them all together.

This paragraph contains some additional information to help you with the "**Isolate**" troubleshooting step, determining where the fault actually lies, for those times that the general procedure and rules fail to resolve the problem.

The CBM should be treated as a system. Each of the components inside the CBM chassis can affect your ability to communicate. If you have an idea where the problem lies, go directly to that troubleshooting procedure. Otherwise, work through them all until your problem is solved.

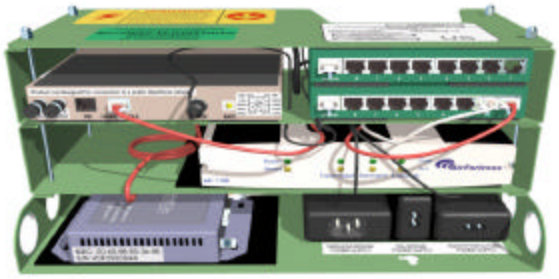


Figure 3-13 Troubleshoot the CBM

3.7.1 CBM General Troubleshooting Procedures.

1. Checked your cables IAW procedures outlined in Paragraph 3.5, or TB 11-5895-1691-10, Paragraph 4.1.

2. Cycled power (turned the UPS, and therefore the CBM, off for about ten seconds, then turned it back on). When the CBM is first powered on the lights should conform to the following:

   a. **Wireless Bridge**

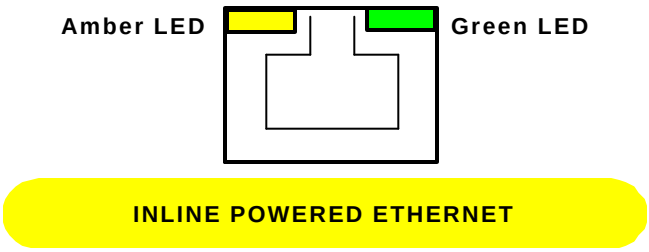


Figure 3-14 Wireless Bridge Rear Panel

(1) There are two LEDs built in to the top of the Ethernet port (Figure 3-13).

(a) The right LED should be solid green, to indicate the link to the encryptor.

(b) The left LED will flash amber (yellow) to indicate traffic.

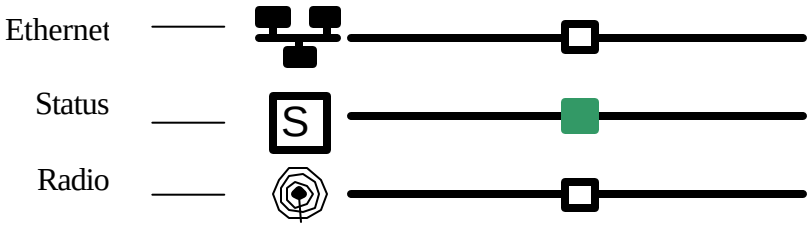


Figure 3-15 Wireless Bridge Top Panel

(2) There are also three LEDs on the top of the bridge. (Figure 3-15)

They first come on with one amber, one green, and one red. Then they all turn amber for a few seconds and all go out for about 10 seconds. Then they come on all solid red, then off, then all solid green, off, then all solid green again, then off, then the center light solid green, then all off, then the center light will blink green,

(3) Once the bridge is finished booting (The whole process takes about three and a half minutes), the lights on the top of the wireless bridge should conform to the following:

(a) Center LED "**Association status**".

- If it is steady green, this indicates that it is associated to the root CBM and there are clients present.
- If it blinks 50% on and 50% off, it is not connected to the CBM root node and there are no clients connected.
- If it blinks 7/8 of a second on and 1/8 of a second off, it means it is connected to the root CBM but there are no CCMs connected to the bridge.

(b) The top LED "**Ethernet traffic**" represents data flowing on the Ethernet side of the bridge which connects to the inline encryptor. If there are no other bridges on the network, the center light will blink steadily, and the Ethernet light will flicker occasionally.

(c). The bottom LED "**Radio traffic**" should flicker to indicate that data is being passed through radio waves.

b. **Encryptor**. When the encryptor is first powered on the lights should conform to the following:

(1) The "**Power**" light will come on steady and the "**Status**" light will begin a blink immediately. Within about 2 seconds, the top "**Encrypted**" and "**Unencrypted**" Link lights will come on steady green. After about 30 seconds, the status light will go to steady green.

(2) The bottom "**Encrypted**" and "**Unencrypted**" Activity lights will flicker amber to indicate passing traffic.

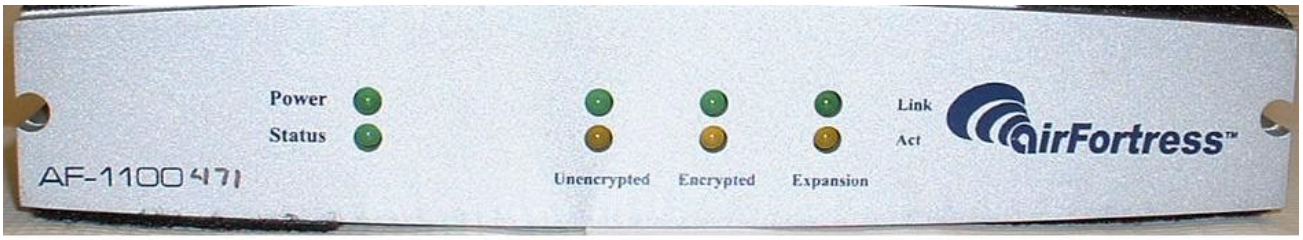


Figure 3-16 Inline Encryptor LEDs

c. **DSL Bridge**. When the DSL Bridge is first powered on the lights should conform to the following:

(1) The "**POWER**" light comes on and the "**SYNC**" light blinks twice.

(2) If field wire is connected and there is a DSL bridge connected at the distant end, the "**SYNC**" light blinks several times when you first connect the field wire. As soon as the bridges on each end synchronize, the "**SYNC**" light comes on steady.

(3) Usually the "**MAR**" light comes on at the same time, to indicate that the modems have a strong enough signal to provide a margin for error for reliable operations over time.

(4) If the "**SYNC**" light comes on steady but "**MAR**" light does not come on, contact the operator at the distant end and adjust the speed until it does come on.

Figure 3-17 DSL Bridge LEDs

NOTE: ***Both ends must make matching speed adjustments. If the two DSL bridge speeds do not match, they won't sync you will not be able to communicate.***

c. **Hubs**. When the hubs are first powered on, every light on the hub comes on for about 2 seconds. Then they all go out except the power light and any port lights with a computer or network device actively communicating. Figure 3-16.

(1) Port lights flicker to indicate outgoing traffic.

3.7.2 Troubleshooting the CBM Hubs. Start with the hubs. With the lights on the back, inside the CBM, hub problems are not always obvious. Lean over and look through the cutout on the top of the CBM. The hub lights are just to the right of the "T" connectors. (If you look in from the back, they are on the left).

During normal operations the CAISI hub LEDs should be as follows:

Figure 3-18 Hub LEDs

Table 3-5 CBM Hub LEDs Description

LED	INDICATOR
PWR	Should remain lit when the hub is receiving power.
Link/Activity 1	Should remain lit when the hub is operational.
BNC	Normally off, it will blink when passing data, indicating the connection between the hubs is good.
"1" LED (bottom hub)	Indicates when lit the link from the hub to the bridge is good.
"2" LED (bottom hub)	Indicates when lit the link from the hub to the DSL is good. (DSL must be in operation)
"2"-"6" LEDs	When lit, indicates the connection from the connected computer (on that port) and the hub is good. These LEDs will blink to indicate traffic on the LAN (Ethernet) connection.
COL	Blinks to indicate data collisions. This is normal.

Troubleshooting techniques for the hub:

1. **If the hub has no lights**, check the power cord connection to the power adapter – the rightmost power supply in the front of the CBM.

   a. If the encryptor also has no power, this power supply is the problem, since the hubs and encryptor share the same power supply.

   b. If the encryptor has power but one or both hubs don't, make sure that the power leads in the back of the hubs are seated properly. They sometimes vibrate loose.

2. The **Link/Activity** LEDs (Normal operations)

   a. Port number "1" light should be lit (green) on the bottom hub. This corresponds to the white straight through Ethernet cable coming from the encryptor.

   b. Port number "2" light may also be lit. This corresponds to the red crossover cable coming from the DSL Bridge. If the DSL Bridge is not on, the light will not be lit.

   c. There should also be lights on every port that has a connected computer or network device that is active. If the computer is off, the light will be off.

   NOTE: *If the computer is a DOS-based STAMIS host, like ULLS, the light will be off except when the STAMIS application is attempting to communicate.*

3. The **Link/Activity** lights flicker to indicate that there is activity – traffic is passing. Not every light flickers, only those that originate traffic.

   a. If your computer connected to port 3 and is communicating with a distant host, ports 3 and 1 will both flicker – 3 because of the local computer, and 1 because of the distant computer answering through the radio and encryptor.

   b. If you don't see the answering flicker, check the encryptor and radio.

4. The "**BNC**" LED on each hub is normally off. It blinks when passing traffic, thus indicating that the link between the hubs is good. The BNC LEDs unlike the Link/Activity LEDs show received traffic, not originated traffic.

   a. If your computer is connected to the bottom hub and is communicating through the radio and encryptor, also connected to the bottom hub, then only the top hub BNC light blinks.

   b. If your computer is connected to the top hub, communicating via the bottom one, then they both blink. (The bottom shows your traffic and the top shows the reply.)

5. **If you can communicate while plugged into the bottom hub, but not while connected to the top hub**, perform the following:

   a. Check that the "T" connectors, coaxial cable, and terminators are seated properly.

   b. If that does not work, replace the terminators, one at a time until you can communicate. Sometimes the resistors in the terminators break down.

   c. If that doesn't work, replace the cable.

   d. If that doesn't work, remove the terminators, cable, and "T" connectors entirely. Remove the red crossover cable from the CBM transit case and

connect port "#" of the bottom hub to port "1" of the top hub. That's what it is for – to interconnect the hubs in case of problem or if you have lots of clients connected through the BNC connectors.

6. **If the LEDs are all normal and users still cannot pass data, do the following:**

   a. Check the internal cables and connections inside the bridge.

   b. Cycle the power – turn it off for ten seconds then turn it back on to reset the hub and its connections. Pull the power cord from the brick.

7. **If the LEDs are all normal, but a connected computer doesn't get a link light or cannot communicate:**

   a. Check the Ethernet cable from the computer to the hub. Replace it if necessary.

   b. Cycle the power – turn it off for ten seconds then turn it back on to reset the hub and its connections. Pull the power cord from the brick.

8. **If, after all of the above procedures, you still have a problem, try replacing one or both hubs**. If the hubs check out, and you have local communications but no communications with distant hosts, go on to the encryptor and wireless bridge. Or to the DSL bridge if you are using it instead of the wireless bridge.

3.7.3 Troubleshooting CBM Encryptor and Wireless Bridge.

The Air Fortress encryptor and the Cisco wireless bridge should always be checked together, since they work together, and a problem with one often looks like a problem with the other.

1. During normal operations the lights on the front of the encryptor, should be as follows: Figure 3-16

   a. The "**Power**" and "**Status**" lights both should be solid green.

   b. The top "**Unencrypted**" and "**Encrypted**" lights should also be solid green, to indicate that the ports are linked.

   c. The bottom "**Unencrypted**" and "**Encrypted**" lights should be out when there is no traffic and flickering amber when there is traffic.

   d. Neither "**Expansion**" light should be lit since that port is not used.

2. During normal operations, the wireless bridge lights should be as follows:

   a. Turn the CBM chassis around or lean over the back of the CBM and look at the light on the top of the power injector. It should be solid green to indicate that the power supply is plugged in and working.

   b. There are two LEDs built in to the top of the Ethernet port on the radio. Figure 3-14.

      (1) Look in from the front or back of the CBM. The lights are on the top of the port on the radio where the white Ethernet cable is connected.

         (a) The right (rearmost) light should be solid green, to indicate the link to the encryptor.

         (b) The left (frontmost) one will flash to indicate traffic.

   c. There are also three lights on the top of the bridge. They are visible just under the front of the second section of the CBM chassis. Figure 3-15.

      (1) The center light (**Association Status**) indicates that the bridge is associated with at least one other radio.

         (a) If it is steady green, this indicates that it is associated to the root CBM and there are clients present.

         (b) If it blinks 50% on and 50% off, it is not connected to the CBM root node and there are no clients connected.

         (c) If it blinks 7/8 of a second on and 1/8 of a second off, it means it is connected to the root CBM but there are no CCMs connected to the bridge.

      (2) The top (right) light (**Ethernet Activity**) and bottom (left) light (**Radio Activity**) should flicker to indicate that data is being passed.

Troubleshooting procedures:

1. **If you are not associated and you know the network is up**, either you do not have the right WEP key, SSID, or your radio is not reaching the next bridge

   a. Refer to CAISI TB 11-5895-1691-10, Paragraph 4.3.3.

2. **If you still are not associated, check the antenna system** IAW procedures outlined in Paragraph 3.7.4.

3. **If you are associated and indications are normal**, connect your SSR notebook wired NIC to the hub in the CBM and attempt to pass traffic to a distant host that you know is up. Watch the lights. **Verify that you are associated.**

   a. On the hub, the port light for the port that you are connected to should flicker, to indicate that traffic is originating at the hub port.

   b. On the encryptor, the "**Encrypted**" activity light should flicker, in time with the light on the hub, to indicate that there is outbound traffic and that it has been encrypted.

   c. On the wireless bridge,

      (1) The amber activity light on the Ethernet port should flicker in time with the light on the encryptor.

      (2) The "**Ethernet Activity**" and "**Radio Activity**" lights should both flicker to indicate that traffic has been received on the Ethernet port and transmitted on the radio port.

   d. If you are receiving a response on the encryptor, the "**Unencrypted**" light will flicker to indicate that traffic has been received and unencrypted. The two activity lights on the encryptor will blink in time with the two activity lights on the bridge. On the hub, the port light will also blink on the port to which the encryptor is connected (normally port "1" on the bottom hub.

   e. **If you are not receiving a response**, try communicating with a different distant host. The gateway (usually the NES or a CAISI router) is a good candidate.

   f. **If you can communicate with some hosts and not others**, either parts of the network are down or your encryptor is not synchronizing with one or more other encryptors. Cycle power on the encryptor to clear the MAC tables.

   g. **If you cannot communicate with any distant host**, the problem might be in your encryptor or the radio. First cycle power on the encryptor and, if that doesn't fix it, cycle power on the radio.

h. **Verify you have the correct SSID and WEP key for the network**.

(1) Refer to CAISI TB 11-5895-1691-10, Paragraph 4.3.3. (Also in Paragraph 2.8).

i. **If you cannot communicate through the wireless NIC and this CBM is not the root**, make it the root and try again.

(1) Refer to CAISI TB 11-5895-1691-10, Paragraph 4.3.3.

j. If you cannot communicate through the wireless NIC, leave the ping running while you perform the following:

(1) Refer to CAISI TB 11-5895-1691-10, Paragraph 4.3.3.

k. **If you still cannot communicate**, perform a complete reset and reconfiguration on both the wireless bridge and encryptor IAW procedures outlined in TB 11-5895-1691-10, Paragraph 2.11 or 3.6 for the wireless bridge configuration utilizing CAISI Admin.

3.7.4 Troubleshooting CBM Antenna System

CBM communications are dependent upon the antenna system. It must not be defective, must be properly installed, and must be high enough and properly oriented.

If the wireless bridge is not associated (has a blinking status light), check the root node. It might not yet be up, or it might be temporarily down due to an extended power outage or other circumstance.

If the root bridge is up but you are not associated, or if any other troubleshooting indicates that you should check the antenna system, proceed as follows.

1. **Check the antenna installation.**

   a. Verify the entire fiberglass portion (painted OD green) of the omni-directional antenna is outside the camouflage net.

Figure 3-19 Troubleshooting Omni-Directional Antenna

   b. Verify the antenna is clean and free of damage (breaks, cracks, bullet holes).

   c. Verify the antenna is erected as vertical as possible and it is positioned away from metallic objects.

   d. Verify the antenna is erected as high as it should be for the length of the shot.

   e. If it is a panel antenna, verify it is pointed in the right direction (toward the target wireless bridge).

   f. If a panel antenna is mounted to a fixed object or field expedient mast without the use of the CAISI antenna bracket, check the polarity. The antenna must be vertically polarized.

      (1) The antenna should have a label on the back showing the polarization. The arrow must be pointing up and down, not side-to-side.

      (2) If the label is missing, you can go by the mounting bolts. The three mounting bolts on the back must be positioned relative to the RF cable connector as follows.

         (a) One to the right above it.

         (b) One to the right below it.

         (c) One to the left below it.

Figure 3-20 Troubleshooting Directional Antenna

2. **Check the antenna cable connections**.

   a. Verify they are tight and not cross-threaded. All antenna connections require numerous turns to tighten. If a connector only turns once or twice, it is probably cross-threaded and it will only work intermittently or for very short ranges.

   b. Verify cable connectors are clean and dry.

3. **Test the CBM antenna**.

PROCEDURAL NOTE: In order to perform the following procedures affectively, you must have an additional root radio with the same WEP and SSID. It is best if you separate the two radios and lower their power to a setting where the signal strength and quality are below average. If you don't do this, at close range, and high power, it is very difficult to know if you have a bad antenna.

When testing the suspected antenna compare its results with the known good antenna. **Before disconnecting the suspected antenna from the CBM/CCM chassis, ensure power to the radio is turned off**.

MMCX to N (F)
Adapter Cable

Right Angle
(Double N) adapter

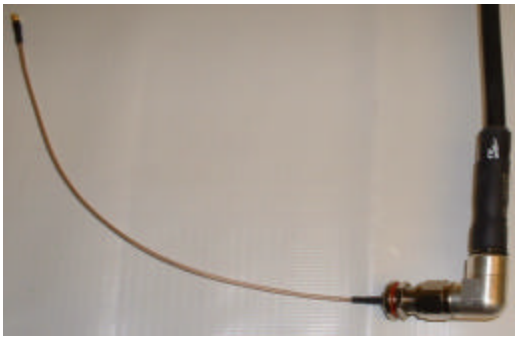


Figure 3-21 Testing 4", 24" or 40" Whip Antenna

   a. Connect the MMCX to N (F) adapter cable from the right port on the wireless NIC in the notebook to one side of the right angle (Double N) adapter.

   b. Connect the other end of the right angle adapter to the antenna, with the antenna oriented vertically.

   c. Use the Link Status Meter (LSM) to compare and check the signal quality. Refer to the TB 11-5895-1691-10, Paragraph 4.3.4.

When finished, disconnect the MMCX cable from the wireless NIC, right angle adapter and the antenna being tested. Reconnect the antenna to the chassis and apply power to the radio.

4. **Test Antenna Cable.**

PROCEDURAL NOTE: In order to perform the following procedures affectively, you must follow the procedural guidelines noted above for testing the CBM antenna as well as those that follow. When comparing cables, make sure you use the same length of cable. If you use different lengths when comparing, the longer cable will have greater signal losses and therefore will have a lower signal strength and quality.

When testing the suspected cable, compare its results with the known good cable. **Before disconnecting the suspected antenna from the CBM/CCM chassis, ensure power to the radio is turned off**.

a. Disconnect the RF antenna cable from the outside of the CBM lightning arrestor.

b. Connect the MMCX to N (F) to the N (Male) antenna cable connector you just disconnected from the lightning arrestor. (Or to the cable you wish to test).

c. Connect the other end of the MMCX cable to the right port of the wireless NIC installed in your SSR notebook.

d. Use the LSM to compare and check the signal quality IAW procedures outlined in the TB 11-5895-1691-10, Paragraph 4.3.1.2.

When finished, disconnect the MMCX cable from the wireless NIC and the N (Male) antenna cable. Reconnect all components and cables.

5. **Troubleshoot the CBM Lightning Arrestor**.

a. Disconnect the small RF cable inside the CBM (connected to the wireless bridge) from the inside of the lightning arrestor.

b. Connect the right angle (Double N) adapter to the lightning arrestor.

c. Connect the MMCX to N cable to the right angle adapter.

d. Connect the other end of your MMCX cable to the right port of the wireless NIC installed in the SSR notebook.

e. Use the LSM to check signal quality IAW procedures outline in the TB 11-5895-1691-10, Paragraph 4.3.1.2.

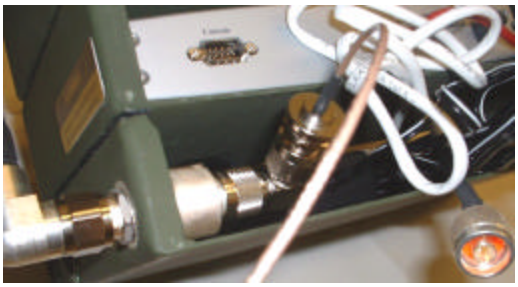


Figure 3-22 Troubleshoot Lightning Arrestor in CBM

When finished, disconnect the MMCX cable from the wireless NIC, right angle adapter and the lightning arrestor. Reconnect all cables.

6. **Troubleshoot the CBM Internal 12" RF cable.**

a. Disconnect the small RF cable inside the CBM from the radio.

NOTE: *If necessary remove the wireless bridge power injector and the white straight through cable connected to the wireless bridge Ethernet port so you can access the 12" cable.*

b. Connect the MMCX to RPTNC adapter cable from the right port on the notebook wireless NIC to the free end of the 12" cable inside the module.

Figure 3-23 MMCX to RPTNC and 12-inch RF Antenna Cable

c. Use the LSM to check signal quality IAW procedures outline in the TB 11-5895-1691-10, Paragraph 4.3.1.2.

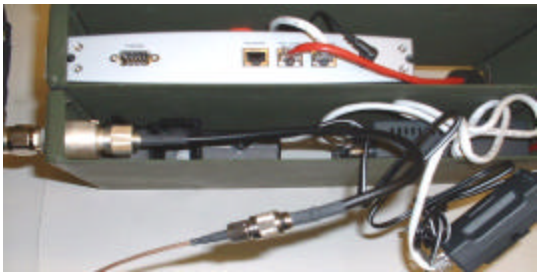


Figure 3-24 Troubleshoot 12" RF Antenna Cable in CBM

When finished, disconnect the MMCX cable from the wireless NIC, and the 12-inch RF cable. Reconnect all cables.

3.7.5 Troubleshooting the DSL Bridge. During normal operations, the “LINK”, “PWR”, “SYNC”, and “MAR” LEDs should be lit green. The others should flicker. A summary of what each one means is below:

Figure 3-25 DSL Bridge Front View

Table 3-6 DSL Bridge LEDs Description

LED	INDICATOR
LINK	When lit, indicates the Link from the Bridge to the Hub is good.
PWR	When lit, indicates the Bridge is receiving power.
SYNC	When lit, indicates the Bridges on each end are synchronized.
MAR	When lit, indicates the two Bridges have a strong enough signal to provide a margin of error for reliable data transmission.
LAN TX and RX	Flickers occasionally to indicate traffic on the network.
COL	Flickers occasionally to indicate data collisions on the network. This is normal

1. The center LED, “PWR”, indicates that the bridge is getting power. If the bridge has no lights, check the power cables to the power brick and from the power brick to the bridge.

2. The leftmost LED “LINK” indicates that the Link from the bridge to the hub is good.

3. The LAN TX and RX light blink to indicate traffic on the LAN (Ethernet) connection.

4. The COL light may also blink occasionally to indicate collisions on the network. This is normal.

5. The SYNC light blinks several times when you first connect the field wire.

   a. As soon as the bridges on each end synchronize, the SYNC light comes on steady.

   b. Usually the MAR light comes on at the same time, to indicate that the modems have a strong enough signal to provide a margin for error for reliable operations over time.

c. If the SYNC light comes on steady, but MAR light does not come on, it is likely the DSL bridges are operating at different speeds. Verify with the destination bridge, the correct speed setting and adjust the speed at each end, if necessary, until the MAR led is lit.

NOTE: *Both ends must make matching speed adjustments. If the two DSL bridge speeds do not match, you will not be able to communicate.*
Default speed is 8.

Other troubleshooting techniques for DSL bridges include:

1. **If you connect the wire and do not get a SYNC light, then the distant end is not yet connected, or there is a problem with the field wire.**

   a. Contact the distant end to be sure that the wire is connected.

   b. Make sure that both ends have the same speed setting. The speed should normally be set to "8".

Figure 3-26 DSL Bridge Speed Setting

   c. **Procedure to change the speed setting is the following:**

      (1) Change both ends of the connection to the slowest speed (1) to see if they can sync up. (MAR LED should stay on if they are in sync).

      (2) Change both ends to the next speed (2) to see if they sync up. Keep on going to faster speeds until you lose the MAR LED.

      (3) Once the MAR LED light goes out, go back to the previous speed where the MAR LED light was on.

   d. Check for a good metal-to-metal connection at each end. The bare wire ends of the wire must be firmly clamped in the jaws of the binding posts.

   e. If you are using WF-16 field wire, check that both ends are connected to the **same color** pair of the WF-16.

   f. If you are using WF-16 field wire, check that all splices are to matching color pairs – green must splice to green and brown must splice to brown.

   g. Check the field wire for shorts, breaks or bad splices. Usually you can detect problems by visual inspection but you may have to do a physical inspection.

h. Check the field wire for wet splices. If water gets into a splice, it can create a short between the two wires of the pair. A splice should never lie on the ground or be at the bottom of a loop. Either can cause water to get into the splice.

3.7.6 Troubleshooting the UPS.

To perform a self-test on the UPS, press and hold the On/Off Test button until the On-Line LED flashes. This takes about four seconds. During the self-test, the UPS briefly operates the loads on-battery (the On-Battery LED comes on). If the UPS passes the self-test, it returns to on-line operations. The On-Battery LED goes off and the On-Line LED displays a steady green indication. If the UPS fails the self-test, it immediately returns to on-line operation and lights the Replace Battery LED. The loads are not affected. At the earliest possible opportunity, recharge the battery overnight and perform the self-test again.

Typical battery backup time is 10 - 20 minutes. Battery recharge rate (up to 90% charge) is 4 – 6 hours.

> **NOTE**: *The UPS must be plugged in and getting good power before it will turn on. This is a safety measure, to keep it from turning on by accident during transit*. ***Make sure the UPS is in the "OFF" position before storing, otherwise it will beep and deplete its battery charge.***

During normal operations, the UPS LEDs should be as follows: "**PWR ON/OFF**" should be lit to indicate the UPS is receiving power. During power outages, the "**Using Battery**" LED will be lit to indicate that you are on battery power. If the other LED lights are lit, you have a problem.

Below are common UPS problems and possible solutions:

Table 3-7 Common UPS Problems

PROBLEM	POSSIBLE CAUSES	RECOMMENDED ACTION
All indicator lights are OFF.	UPS is not plugged into a live AC outlet.	Plug the UPS into a live AC outlet. If power is not present, make sure that your building's circuit breaker has not been accidentally turned OFF.
	Very low or no utility voltage.	Check the AC power supply to the UPS by connecting another electrical device to the power source.
Circuit breaker button pops up	The Surge Protected Outlets are overloaded	Unplug at least one piece of equipment from any Surge Protected Outlet. Press the circuit breaker button back into place.

Table 3-7 Common UPS Problems (Continued)

PROBLEM	POSSIBLE CAUSES	RECOMMENDED ACTION
UPS does not provide expected run time	Battery is not charged enough or has been depleted by frequent power outages	After saving files and switching off your computer, turn the UPS OFF and charge the battery for 4 – 6 hours. Switching OFF the UPS will prevent the battery from unnecessary draining.
UPS beeps occasionally.	Normal UPS operation.	None.
"Check Battery" LED lights	Internal battery has failed or will soon fail.	Notify maintenance. Replacement batteries are available from any vendor.
"UPS Overload" LED lights, and is accompanied by a constant audible alarm. Run time is diminished	The Battery Backup Protected/Surge Protected Outlets are overloaded.	Unplug at least one piece of equipment from the Battery Backup Protected/Surge Protected Outlets.
	NOTE: *You should have nothing except your CBM plugged into these outlets. The other outlets may be used for your computer, but not your printer, coffee pot or any other high current draw device.* If this light comes on and stays one when you have only the CBM plugged in, notify maintenance. The internal circuits are failing.	
"Building Wiring Fault" LED lights	Some sort of wiring problem with the outlet that it is plugged into.	Usually it is a ungrounded outlet that causes this light to come on. Find another grounded outlet and notify maintenance of the faulty outlet.
Clicking noise	This is normal.	The clicking sound comes from relays opening and closing inside the UPS to adjust varying voltage.
	NOTE: *If you are connected to generator power, check the generator, its voltage is drifting. If you cannot correct the problem, report it to organizational maintenance.*	
All indicators are illuminated and the UPS emits a constant tone.	Internal UPS fault.	Do not attempt to use the UPS. Turn the UPS off and have it serviced immediately.

3.8 TROUBLESHOOTING THE CCM.

The CCM includes a radio adapter, an encryptor, a hub, an antenna, and the cables to connect them all together. Troubleshooting the CCM is very much like troubleshooting the CBM, but is easier because there are fewer components.

The procedures and rules in the preceding Paragraph 3.1 will resolve most problems with the CCM.

This paragraph contains some additional information to help you with the "Isolate" troubleshooting step, determining where the fault actually lies, for those times that the general procedure and rules fail to resolve the problem.

The CCM should be treated as a system. Each of the components inside the CCM chassis can affect your ability to communicate. If you have an idea where the problem lies, go directly to that troubleshooting procedure. Otherwise, work through them all until your problem is solved.

Figure 3-27 Troubleshoot the CCM

The CCM has a limitation on the number of users that can connect through it at one time. You can connect only eight users and one of those is the Air Fortress encryptor. If there are more that seven users physically connected, the multi-client radio adapter will honor the first requests to communicate and ignore additional requests. When one of the connected users quits communicating, the radio will automatically drop it from the list and accept communications from other clients. This process does not happen immediately it takes a couple of minutes. If there are too many clients and you need to speed up the process, cycle power on the radio. That will immediately flush the MAC table.

3.8.1 CCM General Troubleshooting Procedures

1. Checked your cables IAW procedures outlined in Paragraph 3.5 or in the TB 11-5895-1691-10, Paragraph 4.1.

2. Cycled power (removed the power cord from the power adapter, **waited about ten seconds**, then plugged it back in).

3. When the radio adapter is first powered on, the lights should conform to the following:

a. Multi-client radio adapter.

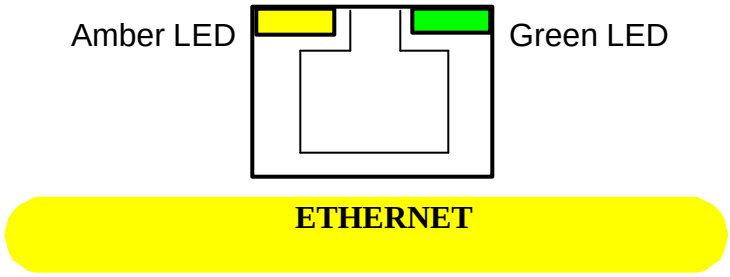


Figure 3-28 Multi-Client Radio Adapter Rear Panel

There are two LEDs built into the top of the Ethernet port:

1. The right LED should be solid green, to indicate the link to the encryptor.

2. The left LED will flash amber (yellow) to indicate traffic.

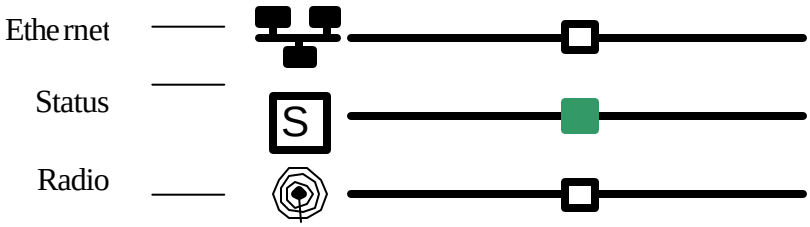


Figure 3-29 Multi-Client Radio Adapter Top Panel

There are also three LEDs on the top of the Multi-Client Radio Adapter (These are same as those on the wireless bridge).

1. They will be momentarily solid green, then flicker. They then go off and back on and even blink amber and red occasionally during the boot up process. Then they go out and the center one blinks frantically green for a while. Then they all go out and come back on steady green for a few seconds.

2. Once the radio adapter is finished booting (The whole process takes about a 20 seconds), the lights on top of the multi-client radio adapter should conform to the following:

   - The center "**Status**" LED should be steady.
   - The top, "**Ethernet**" and bottom "**Radio**" LEDs will blink when there is traffic.
   - If there are no wireless bridges (CBMs) with which to associate, all three LEDS will be off.

b. **Encryptor.**

(1) When the encryptor is first powered on, the lights should conform to the following:

(a) The "**Power**" light will come on steady and the "**Status**" light will begin a fast green blink immediately. Within about 2 seconds, the top "**Encrypted**" and "**Unencrypted**" Link lights will come on steady green. After about 30 seconds, the status light will go to steady green.

(b) The bottom "**Encrypted**" and "**Unencrypted**" Activity lights will flicker amber to indicate passing traffic.

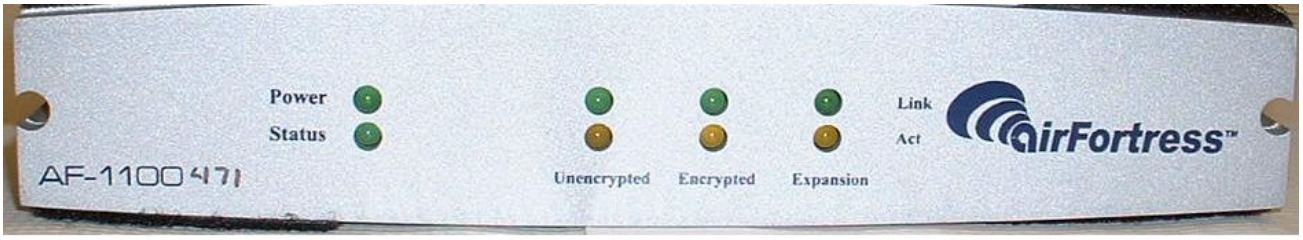


Figure 3-30 Inline Encryptor LEDs

c. **Hub.**

(1) When the hub first powers on, every light on the hub comes on for about 2 seconds. Then they all go out except the power light and any port lights with a computer or network device actively communicating.

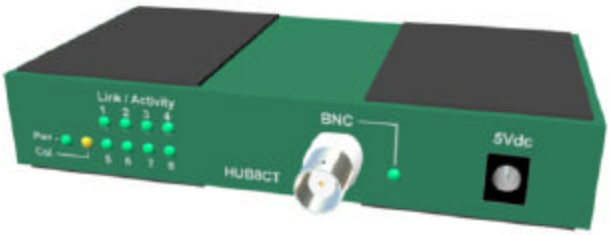


Figure 3-31 Hub LEDs

(2) Port lights flicker to indicate outgoing traffic.

3.8.2 Troubleshooting the CCM Hub. Start with the hub. With the lights on the back, inside the CCM, hub problems are not always obvious. Lean over and look through the cutout on the top of the CBM. The hub lights are just to the right of the "T" connectors. (If you look in from the back, they are on the left).

During normal operations the CAISI hub LEDs should be as follows

Table 3-8 CCM Hub LEDs Description

LED	INDICATOR
PWR	Should remain lit when the hub is receiving power.
Link/Activity 1	Should remain lit when the hub is operational.
BNC	Normally off, it will blink when passing data, indicating the connection between the hubs is good.
"1" LED	Indicates when lit the link from the hub to the encryptor is good.
"2"-"6" LEDs	When lit, indicates the connection from the connected computer (on that port) and the hub is good. These LEDs will blink to indicate traffic on the LAN (Ethernet) connection.
COL	Blinks to indicate data collisions. This is normal.

Troubleshooting techniques for the hub:

1. **If the hub has no lights**, check the power cord connection to the power adapter – the rightmost power supply in the front of the CBM.

   a. If the encryptor also has no power, this power supply is the problem, since the hubs and encryptor share the same power supply.

   b. If the encryptor has power but one or both hubs don't, make sure that the power leads in the back of the hubs are seated properly. They sometimes vibrate loose.

2. The **Link/Activity** LEDs (Normal operations)

   a. Port number "1" light should be lit (green) on the bottom hub. This corresponds to the white straight through Ethernet cable coming from the encryptor.

   b. Port number "2" light may also be lit. This corresponds to the red crossover cable coming from the DSL Bridge. If the DSL Bridge is not on, the light will not be lit.

   c. There should also be lights on every port that has a connected computer or network device that is active. If the computer is off, the light will be off.

NOTE: *If the computer is a DOS-based STAMIS host, like ULLS, the light will be off except when the STAMIS application is attempting to communicate.*

3. The **Link/Activity** lights flicker to indicate that there is activity – traffic is passing. Not every light flickers, only those that originate traffic.

   a. If your computer connected to port 3 and is communicating with a distant host, ports 3 and 1 will both flicker – 3 because of the local computer, and 1 because of the distant computer answering through the radio and encryptor.

   b. If you don't see the answering flicker, check the encryptor and radio.

4. The "**BNC**" LED on each hub is normally off. It blinks when passing traffic, thus indicating that the link between the hubs is good. The BNC LEDs unlike the Link/Activity LEDs show received traffic, not originated traffic.

   a. If your computer is connected to the bottom hub and is communicating through the radio and encryptor, also connected to the bottom hub, then only the top hub BNC light blinks.

   b. If your computer is connected to the top hub, communicating via the bottom one, then they both blink. (The bottom shows your traffic and the top shows the reply.)

5. **If the LEDs are all normal and users still cannot pass data, do the following:**

   a. Check the internal cables and connections inside the bridge.

   b. Cycle the power – turn it off for ten seconds then turn it back on to reset the hub and its connections. Pull the power cord from the brick.

6. **If the LEDs are all normal, but a connected computer doesn't get a link light or cannot communicate:**

   a. Check the Ethernet cable from the computer to the hub. Replace it if necessary.

   b. Cycle the power – turn it off for ten seconds then turn it back on to reset the hub and its connections. Pull the power cord from the brick.

7. **If, after all of the above procedures, you still have a problem, try replacing the hub**. If the hub checks out, and you have local communications but no communications with distant hosts, go on to the encryptor and radio adapter.

3.8.3 Troubleshooting CCM Encryptor and Multi-Client Radio Adapter.

The encryptor and the multi-client radio adapter should always be checked together, since they work together, and a problem with one often looks like a problem with the other.

1. During normal operations the lights on the front of the **encryptor**, should be as follows: Figure 3-30
   a. The "**Power**" and "**Status**" lights both should be solid green.
   b. The top "**Unencrypted**" and "**Encrypted**" lights should also be solid green, to indicate that the ports are linked.
   c. The bottom "**Unencrypted**" and "**Encrypted**" lights should be out when there is no traffic and flickering amber when there is traffic.
   d. Neither "Expansion" light should be lit since that port is not used.

2. During normal operations, the **multi-client radio adapter** lights should be as follows:
   a. There are two LEDs built in to the top of the Ethernet port. Figure 3-28
      (1) The right one should be solid green, to indicate the link to the hub.
      (2) The left one will flash to indicate traffic.

   b. The three lights on the top of the radio adapter should behave as follows: Figure 3-29
      (1) The center "**Status**" LED should be steady. (Indicates you are associated with a bridge.
      (2) The top, "**Ethernet**" and bottom "**Radio**" LEDs will blink when there is traffic.

3. **If you are not associated and you know the network is up, either you do not have the right SSID, WEP key, or your radio is not reaching any bridges**.
   a. Ensure physical connections procedures for the module have been performed. Refer to Paragraph 2.33.1 for CCM physical connection procedures.

      Basically, it is connect the SSR notebook to the radio as follows: Disconnect the red crossover Ethernet cable from the back of the encryptor. Connect it to the wired NIC in your SSR notebook. (You can use the RJ-45 Straight-through adapter from the SSR Accessory Kit to extend the cable and make it easier to connect).

   b. Ensure module is receiving power. Refer to Paragraph 3.8.1.
   c. Verify the SSID, WEP and configuration parameters. Refer to TB 11-5895-1691-10, Paragraph 4.4.3.

4. If you still are not associated, check the antenna system IAW procedures outlined in Paragraph 3.8.4.

5. If you are associated and indications are normal, connect your SSR notebook wired NIC to the hub in the CCM and attempt to pass traffic to a distant host that you know is up. Watch the lights. (**Verify your are associated**).

   a. On the hub, the port light for the port that you are connected to should flicker, to indicate that traffic is originating at the hub port.

   b. On the encryptor, the "**Encrypted**" activity light should flicker, in time with the light on the hub, to indicate that there is outbound traffic and that it has been encrypted.

   c. On the radio adapter the lights should conform to the following:

      (1) The amber activity light on the Ethernet port should flicker in time with the light on the encryptor.

      (2) The "**Ethernet Activity**" and "**Radio Activity**" lights should both flicker to indicate that traffic has been received on the Ethernet port and transmitted on the radio port.

   d. If you are receiving a response, on the encryptor the "**Unencrypted**" light will flicker to indicate that traffic has been received and unencrypted. The two activity lights on the encryptor will blink in time with the two activity lights on the radio adapter. On the hub, the port light will also blink on the port to which the encryptor is connected (normally port "1.")

   e. If you are not receiving a response, try communicating with a different distant host. The gateway (usually the NES or a CAISI router) is a good candidate.

6. **If you can communicate with some hosts and not others,** either parts of the network are down or your encryptor is not synchronizing with one or more other encryptors. Cycle power on the encryptor to clear the MAC tables.

7. **If you cannot communicate with any distant host, the problem might be in your encryptor or the radio**. First cycle power on the encryptor and, if that doesn't fix it, cycle power on the radio.

8. **If you still cannot communicate,** refer to TB 11-5895-1691-10, Paragraph 4.4.3 to reset the Access ID on the encryptor and the WEP key on the multi-client radio adapter.

9. **If you still cannot communicate,** follow procedures outlined in Paragraph 4.3.3 of the TB 11-5895-1691-10 to verify the wireless bridge WEP key matches the radio adapters.

10. Check the antenna system IAW procedures outlined in Paragraph 3.8.4 because you apparently have a sufficient signal to associate, but not a sufficient signal to communicate over the radio.

11. **If you still cannot communicate**, perform a complete reset and reconfiguration on both the encryptor and radio adapter. Refer to Paragraphs 2.12 or 3.7 in the TB 11-5895-1691-10 for the multi-client radio adapter configuration utilizing CAISI Admin**.**

3.8.4 Troubleshooting CCM Antenna System

CCM communications are dependent upon the antenna system. It must not be defective, must be properly installed, and must be high enough and properly oriented.

If the radio adapter is not associated (has a blinking status light), check the root node. It might not yet be up, or it might be temporarily down due to an extended power outage or other circumstance.

If the root bridge is up but you are not associated, or if any other troubleshooting indicates that you should check the antenna system, proceed as follows:

1. **Check the antenna installation**.

   a. Verify the entire fiberglass portion (painted OD green) of the omni-directional antenna is outside the camouflage net.

Figure 3-32 Troubleshooting Omni-Directional Antenna

   b. Verify the antenna is clean and free of damage (breaks, cracks, bullet holes).

   c. Verify the antenna is erected as vertical as possible and it is positioned away from metallic objects.

   d. Verify the antenna is erected as high as it should be for the length of the shot.

2. **Check the antenna cable connections**.

   a. Verify they are tight and not cross-threaded. All antenna connections require numerous turns to tighten. If a connector only turns once or twice, it is probably cross-threaded and it will only work intermittently or for very short ranges.

   b. Verify cable connectors are clean and dry.

3. **Test the CCM antenna**.

PROCEDURAL NOTE: In order to perform the following procedures affectively, you must have an additional root radio with the same WEP and SSID. It is best if you separate the two radios and lower their power to a setting where the signal strength and quality are below average. If you don't do this, at close range, and high power, it is very difficult to know if you have a bad antenna.

When testing the suspected antenna compare its results with the known good antenna. **Before disconnecting the suspected antenna from the CBM/CCM chassis, ensure power to the radio is turned off**.

MMCX to N (F)
Adapter Cable

Right Angle
(Double N) adapter

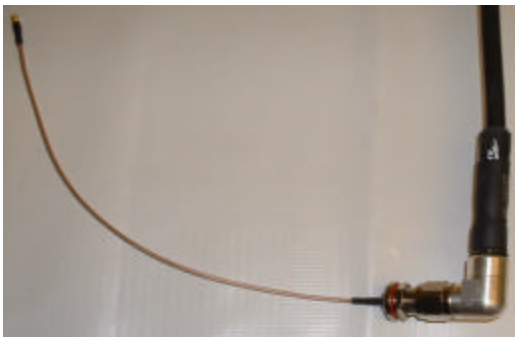


Figure 3-33 Testing 4", 24" or 40" Whip Antenna

a. Connect the MMCX to N (F) adapter cable from the right port on the wireless NIC in the notebook to one side of the right angle (Double N) adapter.

b. Connect the other end of the right angle adapter to the antenna, with the antenna oriented vertically.

c. Use the Link Status Meter (LSM) to compare and check the signal quality. Refer to the TB 11-5895-1691-10, Paragraph 4.4.4.

When finished, disconnect the MMCX cable from the wireless NIC, right angle adapter and the antenna being tested. Reconnect the antenna to the chassis and apply power to the radio.

4. **Test the CCM Antenna and RF Cable.**

PROCEDURAL NOTE: In order to perform the following procedures affectively, you must follow the procedural guidelines noted above for testing the CBM antenna as well as those that follow. When comparing cables, make sure you use the same length of cable. If you use different lengths when comparing, the longer cable will have greater signal losses and therefore will have a lower signal strength and quality.

When testing the suspected cable, compare its results with the known good cable. **Before disconnecting the suspected antenna from the CBM/CCM chassis, ensure power to the radio is turned off**.

a. Disconnect the RF antenna cable from the outside of the CCM lightning arrestor.

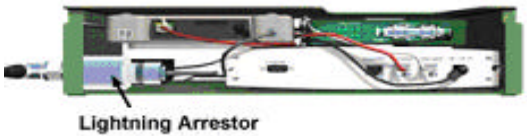


Figure 3-34 Troubleshoot CCM Lighting Arrestor and RF Antenna Cable

b. Disconnect the RF antenna cable from the outside of the CCM lightning arrestor.

c. Connect your MMCX to N (female) to the N (male) antenna cable connector you just disconnected from the lightning arrestor.

d. Connect the other end of your MMCX cable to the right port of the wireless NIC installed in the SSR notebook.

e. Use the LSM to check signal quality IAW procedures outlined in Paragraph 4.4.4 of the TB 11-5895-1691-10.

f. Disconnect the MMCX to N (female) cable from notebook wireless NIC and the N (male) antenna cable.

g. Reconnect all components and cables.

5. **Troubleshoot the CCM Lightning Arrestor**.

a. Disconnect the small RF cable inside the CCM from the inside of the lightning arrestor.

b. Connect the right angle (Double N) adapter to the lightning arrestor.

c. Connect the MMCX to N cable to the right angle adapter.

d. Connect the other end of your MMCX cable to the right port of the wireless NIC installed in the SSR notebook.

e. Use the LSM to check signal quality IAW procedures outlined in Paragraph 4.4.4 of the TB 11-5895-1691-10.

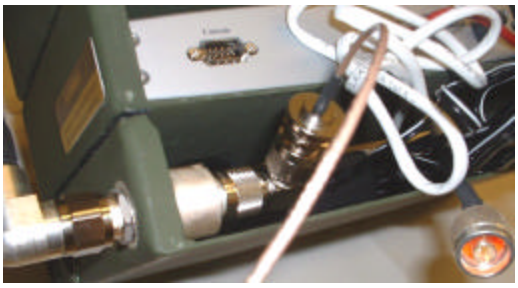


Figure 3-35 Troubleshoot Lightning Arrestor in CCM

f. If there is a substantial difference in signal quality from the previous test, the small RF cable inside the CCM may be defective.

g. Disconnect the MMCX to N cable from the notebook wireless NIC and the right angle adapter.

h. Disconnect the right angle adapter from the lightning arrestor.

i. Reconnect all components and cables.

6. **Troubleshoot the CCM Internal 12” RF cable.**

a. Disconnect the small RF cable inside the CCM from the radio.

b. Connect the MMCX to RPTNC adapter cable from the right port on the notebook wireless NIC to the free end of the 12” cable inside the module.

Figure 3-36 MMCX to RPTNC and 12-inch RF Antenna Cable

c. Use the LSM to check signal quality IAW procedures outlined in Paragraph 4.4.4 of the TB 11-5895-1691-10.

d. If there is a substantial difference in signal quality from the previous test, the small RF cable inside the CCM may be defective.

e. Disconnect the MMCX to RPTNC adapter cable from the right port on the notebook wireless NIC and the 12” cable inside the module.

f. Reconnect all components and cables.

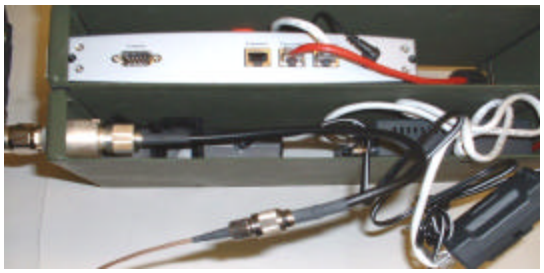


Figure 3-37 Troubleshoot 12” RF Cable in CCM

3.9 TROUBLESHOOTING THE LSA. When troubleshooting the LSA, there are 3 basic faults that will occur with the component. Like most troubleshooting procedures you should first check the LEDs and the connections.

- **Connections**
- **LEDs**
- **If you can not connect**
- **If the client can not connect**

As always first verify the LSA (MSS-100) has operational status. Secondly, check the physical connections and LEDs.

During normal operations, the CAISI LSA LEDs indicate Ethernet, serial links, and traffic. The LSA (MSS-100) has five LEDs to provide status information.

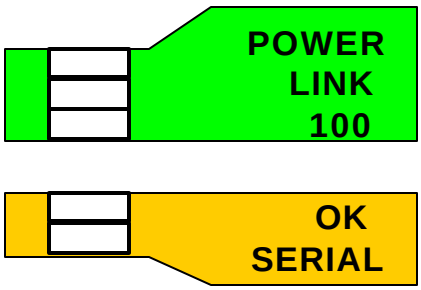


Figure 3-38 LSA LEDs

Table 3-9 LSA LEDs Description

LED	INDICATOR
Power	Indicates power is flowing to the transceiver. It is possible for power to be applied and no lights steadily lit, if there is no wireless card and no CAT-5 connection.
Link	Indicates a link to a hub.
100	If lit, the Ethernet connection is at 100MB. If not lit, the link is 10MB.
OK	If lit, indicates the transceiver has booted properly. It will blink every 2 seconds.
Serial	If lit, traffic is flowing through the transceiver.

The “OK”, “Serial”, and “Link” LED will blink during boot-up, but once booted, the lights will go out. But shortly thereafter, the “OK” LED will come on and blink every two seconds, to indicate that the box is operating normally as it can without a network connection.

If the MSS-100 is not operating normally, perform the following steps for each case:

1. **If you have a rapidly blinking "OK" light,** cycle power (turn the LSA off and then on) to force it to reboot. If it still blinks rapidly, then the unit must be replaced.

2. **If you have a solid red "Serial" or "OK" light or if either is solid red for three seconds followed by a one second of another color**, the unit must be replaced.

3. **If you connect the Cat-5 to an MSS-100 and do not get a Link light,** then the distant end is not yet connected, or there is a problem with the Ethernet cable:

   a. Contact the distant end to ensure the cable is connected.

   b. Check for good connection at each end. The connectors must be firmly seated in the sockets.

   c. Check the cable for shorts, breaks or bad splices. Usually you can detect problems by visual inspection but you may have to do a physical inspection.

   d. If possible, use a network cable test set to check the cable. If the test set is not available, replace the cable.

4. **If there are no lights at all**, the device or its power supply must be replaced.

3.9.1 Advanced Troubleshooting for the LSA. SSR Notebook is required.

1. **If indications are normal, but your STAMIS computer cannot connect**, perform the following:

   a. If you do not get a warning and **TS>** prompt

      (1) Check the serial cable. It must be a null-modem cable and be firmly connected at both ends.

      (2) Cycle power (turn the LSA off then on) to force it to reboot and restart the CAISI VEE program. Then try again to communicate.

      The STAMIS will need to be registered again because registration is lost when power is lost.

      Watch the BLAST screen to ensure that the warning and the **TS>** prompt appear. If it does not, contact the system administrator to remotely attempt to restart the CAISI VEE program in your LSA.

      (3) If you don't see any prompts, replace the cable.

b. If you get a **Boot>** prompt, check the network cable, just as if you have no green link LED (above), then cycle power.

c. If you get a **Login>** prompt, the LSA has been reset and the CAISIVEE program is not running. Reconfigure and restart the LSA just as if it were new. It's possible you might have to reload the HOSTS file, CAISIVEE.CFG file, or the other program files. Refer to the TB 11-5895-1691-10, Paragraph 2.14 for the steps to do this procedure.

d. If you get good Blast messages, but cannot contact the distant end SAMS, SARSS, or other STAMIS host, contact the STAMIS operator at the distant end to ensure that their system is operational and in answer mode.

e. If you still cannot connect, contact the SSR (CSS S6 or other automated support personnel) or network control to ensure that the network is actually up the whole way.

f. You may have to reset and reconfigured the LSA.

The procedure to restore factory default parameters: (**Reset the LSA**)

(1) Complete initial connections.

(2) Remove power to the LSA.

(3) Push the reset button (use pointed end of a paper clip) and **keep the button pressed in**.

(4) Apply power to LSA while also holding in the reset button.

(5) Hold it until the serial lights stop blinking (about 5-10 seconds).

(6) All configuration parameters are set back to factory.

g. If you still cannot communicate, you will need to replace the LSA.

3.10 TROUBLESHOOTING THE ROUTER. In troubleshooting the Router, you have to remember that not only you are affected if it goes down, but you and the clients on both the private and public side of your network are affected. You may have problems when the client cannot connect, you may not be able connect, or the router may not just need rebooting.

During normal operations, the CAISI router LEDs should be as shown in Table 3-10.

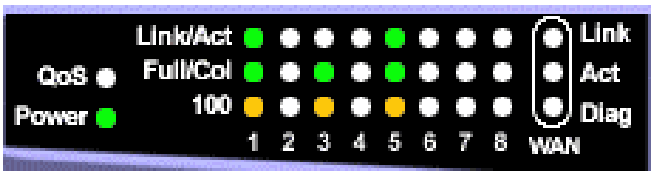


Figure 3-39 Router LEDs

The "Power", "Link" and number 8 "Link/Act" LED will be green during normal operations. All other LEDs should be off.

Table 3-10 Router LEDs Description

LED	INDICATOR
Power	Indicates power is flowing to the router.
100	If lit, the Ethernet connection is at 100MB. If not lit, the link is 10MB.
Full/Col	Indicates Full Duplex/Collision. When lit, the connection is running in full duplex mode. When it flickers, the connection is experiencing collisions. Infrequent collisions are normal.
Link/Act	If lit, it is connected to a device on one of the ports; if the LED is flickering, the router is actively sending or receiving data over the port.
WAN Act	Flickers to show passing traffic.
# 8 Link/Act	Flickers to show passing traffic
Diag	The WAN "Diag" LED lights up when the unit is first powered up, then goes out at the end of the boot cycle. If this LED stays on for a abnormally long period of time, the device is not working properly. Try to re-flash the firmware by assigning a static IP address to the computer and then upgrade the firmware again. If that doesn't help, replace the unit.

If you have connected other computers or equipment to the other router ports, their link lights should also be lit. Their "Full/Col" (Full Duplex/Collision) and "100" (100Base-TX) LEDs may be lit or not, depending on the equipment you connect.

Router is not working correctly when:

1. **If the "Full/Col" light is constantly flickering**, it indicates excessive collisions. They may be anywhere on the network. Briefly pressing the reset will refresh the router's connections, possibly clearing any jammed links.

   Refresh the Router: Insert the reset tool, stiff wire, small screw, paper clip, or similar device into the reset button recess and quickly **press and release** the button. You will be able to feel the button press and release.

CAUTION: Don't hold it. Push it and let go immediately. It only takes about five seconds to reset the router and lose you entire configuration.

2. **If your clients can not connect:**

   a. Remember that clients of the private side of the network can only connect to each other and to servers on the public side. Determine if one client is having connectivity problems or if all are. If only one is having problems, check the configuration of that computer.

   b. **If none of the clients can communicate,** check the router configuration.

      (1) Using the CAISI laptop, connect to the router and make sure that the configuration of the client matches the configuration of the router. Procedures to connect to the router is in Paragraph 2.31.

      Also make sure that the parameters for the WAN (the IP address, subnet mask, default gateway, and DNS server) are correctly set. See the TB 11-5895-1691-10, Paragraph 4.2.2.2 for the steps to do this procedure.

3. **If you cannot connect to the router:**

   a. Check your PC network configuration to ensure that matches the portion of the network to which you are connected and that you are trying to connect to the correct address.

      (1) If you are connected to the private side, you can only connect using the router's private address.

      (2) If you are connected to the public side, you must use the public address and remote management must not be disabled. Connect from the private side and check the "Advanced/Filters" tab.

   b. If you still cannot connect to the router, try rebooting it. Remove the power cable for four seconds and then plug it back in.

c. As a last resort, you may **reset the router**:

(1) Press and hold the reset button for 7 – 10 seconds. This will erase the current configuration, including passwords. The default IP is 192.168.1.1, and the default password is *Admin*. The router will be in the default state, as if it were brand new.

(2) Connect to the router from the private side, and configure it as detailed in the TB 11-5895-1691-10, Paragraph 2.9 (manual) or Paragraph 3.9 (CAISI Admin)

4. **If reconfiguration does not resolve the problem**, the router needs to be replaced.

5. **If you lose the password:**

Check with your security officer to get the password envelope from safekeeping. If you, or whoever originally set it, failed to turn in the password, or if the password envelope is not available, you must set a new one. Without the correct password, you will have to reset the router. Reset and reconfigure the router as above in (4c).

REMEMBER: If you reset and reconfigure the router, be sure to change the password. You do not want to leave the router with the default password.

Once you put in a new password, you must write it down, seal it in an envelope, and turn it in to your security officer for safekeeping.

NOTE: *For more information on configuration of the router, refer to the TB 11-5895-1691-10, Paragraph 2.9 (manual) / Paragraph 3.9 (CAISI Admin).*

Troubleshooting the router, refer to TB 11-5895-1691-10, Paragraph 4.2.2.

3.11 TROUBLESHOOTING THE 10BASE-T TRANSCEIVER. The 10Base-T transceiver is used primarily for connecting to the NES at the MSE van. Few issues arise with the transceiver – it only has two connections and has no power supply – it gets its power from the AUI port.

Below is a description of the LEDs on the transceiver during normal operations. **No special configuration is required**.

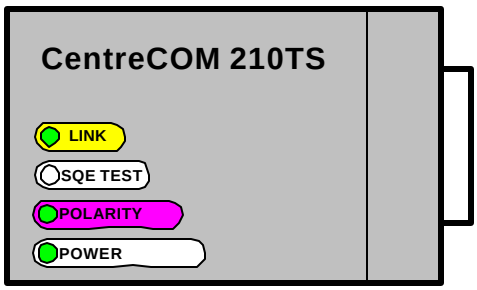


Figure 3-40 10Base-T Transceiver LEDs

Table 3-11 10Base-T Transceiver LEDs Description

LED	INDICATOR
Link	Indicates, when lit, a connection to the destination. Blinks to indicate traffic.
SQE Test	Should not be lit. If it is, replace the transceiver.
Polarity	Should be lit.
Power	Will be lit when power is applied.

The only configuration for the transceiver is to ensure the "heartbeat" is set to "Off". This is done by moving the switch on the side of the LED to the OFF position.

Transceiver is not working properly if:

1. **If the transceiver has no lights,** check the INE or connected equipment to make sure that it is on. (The transceiver receives its power through the AUI port).

2. **If all indications are normal** – you have all the right lights – but your clients can not connect: Check your cables.

   a. Cycle power (unplug the transceiver from the AUI port for about ten seconds, then plug it back it).

   b. Check the "SQE Test" switch. It should be all the way to the left inside the slot.

   c. Cycle power or reboot (as appropriate) the next item in line at each end (switches, hubs, PCs, etc.).

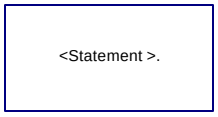
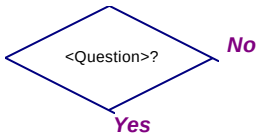
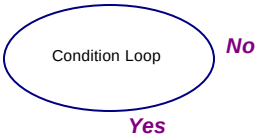
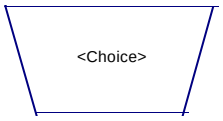
   d. If you still have a problem, replace the transceiver.

3.12 TROUBLESHOOTING THE AB-1244B ANTENNA MAST.

The troubleshooting procedures for the AB-1244B Antenna Mast is in Chapter 4 of the TM 11-5985-357-13, Antenna Group OE-254/GRC.

3.13 TROUBLESHOOTING FLOWCHARTS. The following flowcharts provide summary information on CAISI PMCS, maintenance, and troubleshooting.

Table 3-12 Flowchart Symbols

Flow Chart Item	Description of Flow Chart Item
<Title>	Title of the flow chart will be located on the top of the first page of a flow chart.
	This symbol represents the first statement or Start symbol of a flow chart.
	This symbol represents a statement block in a flow chart.
	This symbol represents a question in a flow chart. This symbol will have a Yes Branch and a No branch.
	This symbol represents a condition loop in a flow chart. This symbol will have a Yes branch and a No branch, and the Yes branch will be followed while the condition statement is True.
	This symbol represents a case command in a flow chart. This symbol is utilized when there are multiple branches available based on the decision made at this intersection.
	This symbol represents a choice statement in a flow chart. This symbol represents available options from a case command.
	This symbol represents a comment or a header of a flow chart.

On the following pages you will find a series of flowcharts that attempt to diagram the process of troubleshooting the CAISI hardware. The flowcharts are designed to provide a step-by-step process to assist the CAISI installer/maintainer in identifying, isolating, and correcting CAISI problems. Included in the steps are references to relevant portions of this manual to be consulted in performing that particular step.

Table 3-13 List of Troubleshooting Flowcharts

Flowchart Title	Figure	Page
Network	3-41	p. 3-60
CAISI Installation – CBM	3-42	p. 3-61
CAISI Installation – LSA	3-43	p. 3-62
CAISI PMCS	3-44	p. 3-63
Troubleshooting Components	3-45	p. 3-64
Troubleshooting Hardware Components:	3-46	p. 3-65
SSR Notebook	3-47	p. 3-66
CBM		
Wireless Bridge	3-48	p. 3-67
Inline Encryptor	3-49	p. 3-68
DSL Bridge	3-50	p. 3-69
Hubs	3-51	p. 3-70
UPS	3-52	p. 3-71
CCM		
Multi-Client Radio Adapter	3-53	p. 3-72
LSA (MSS-100)	3-54	p. 3-73
Linksys Router	3-55	p. 3-74
10Base-T Transceiver	3-56	p. 3-75
CAISI Maintenance Support	3-57	p. 3-76

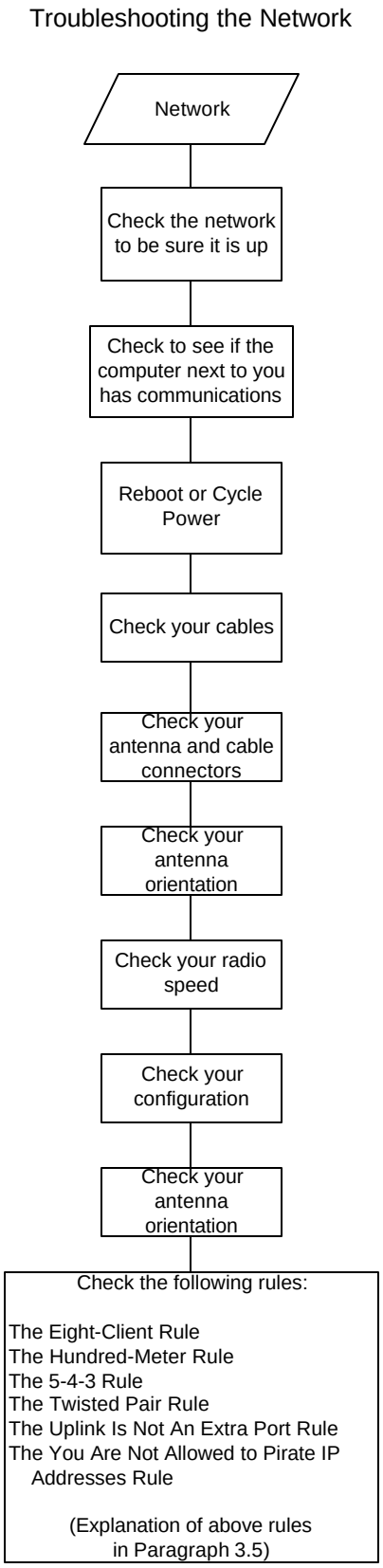


Figure 3-41 Troubleshooting the Network Flowchart

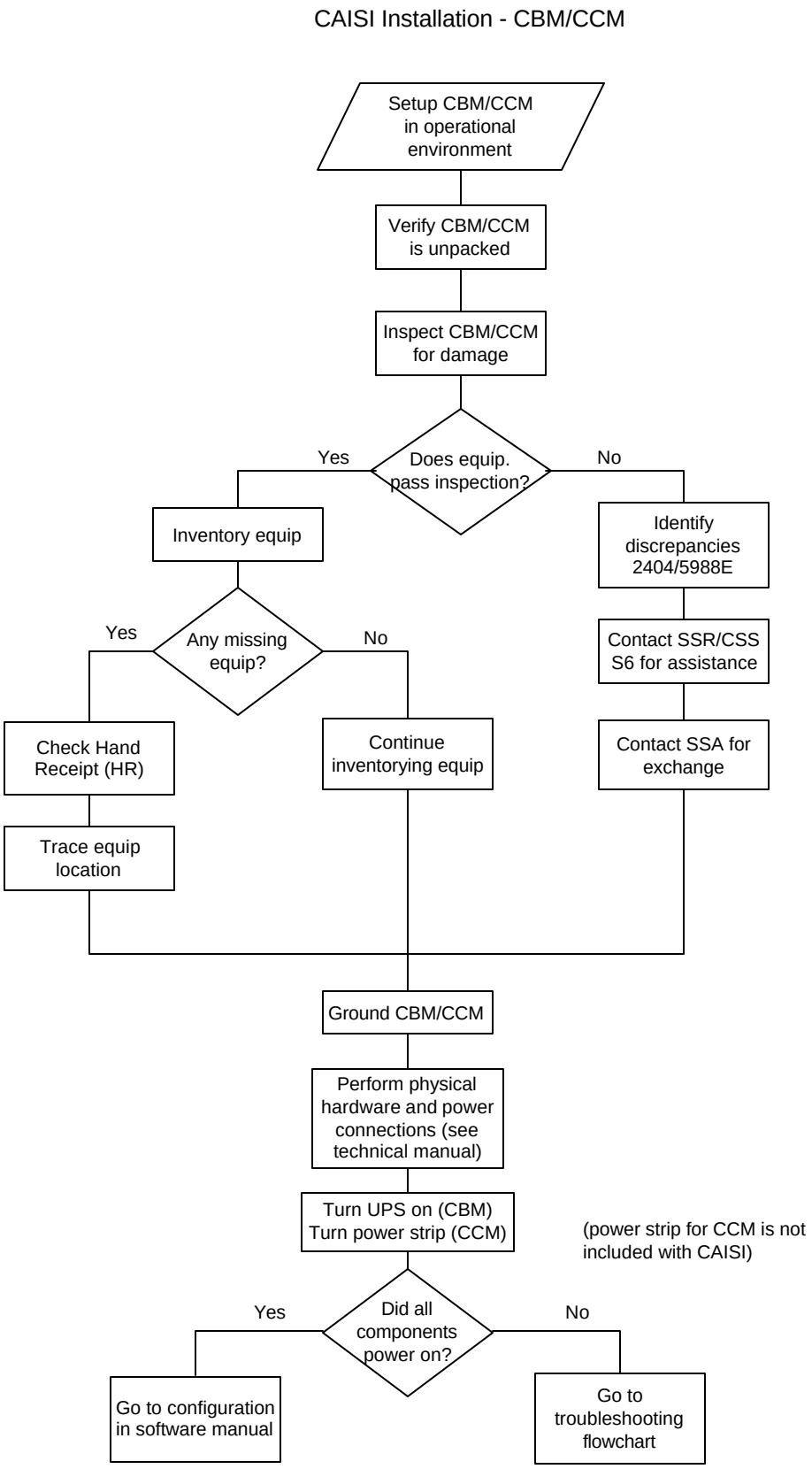


Figure 3-42 CAISI Installation – CBM Flowchart

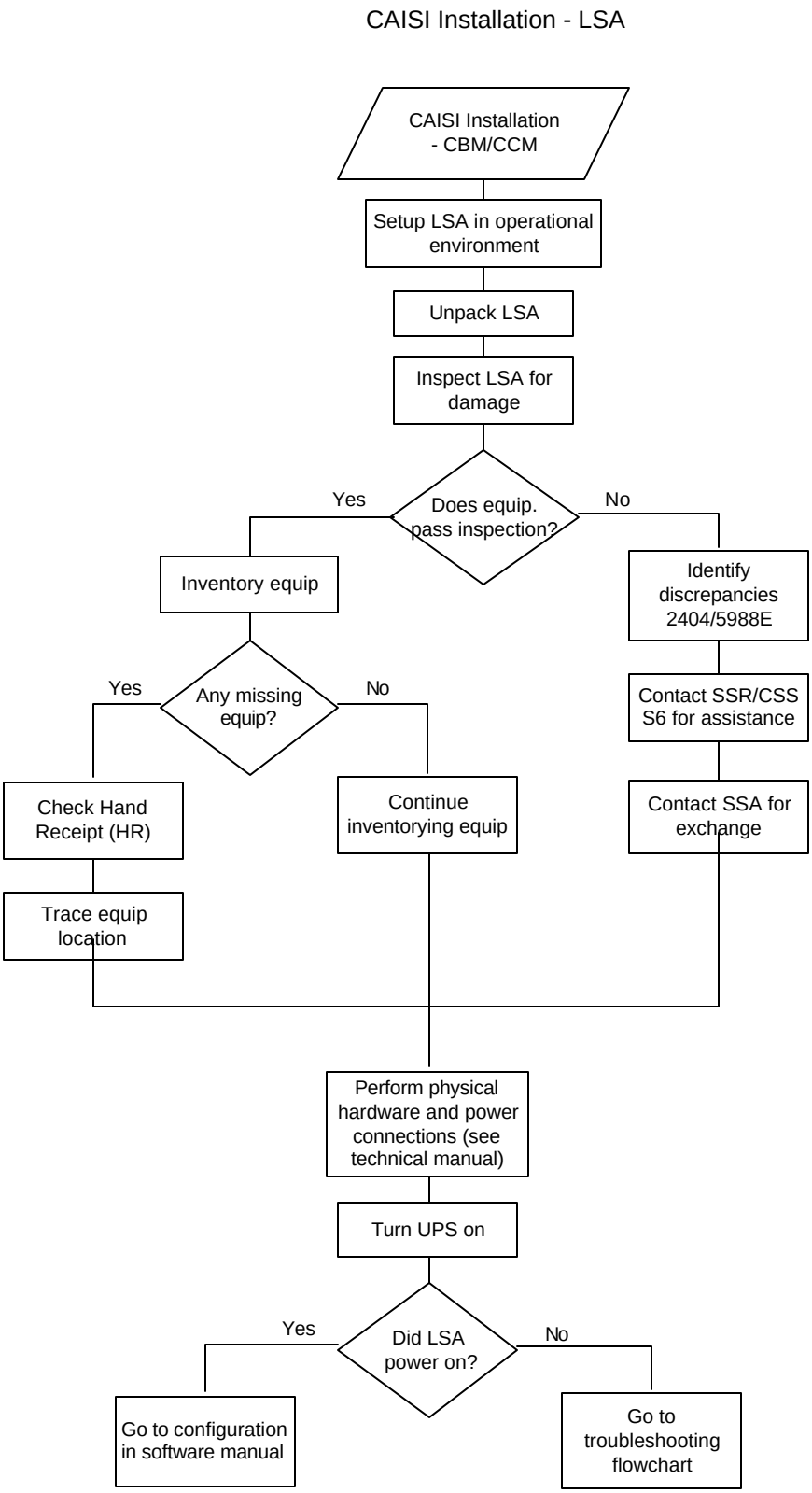


Figure 3-43 CAISI Installation – LSA Flowchart

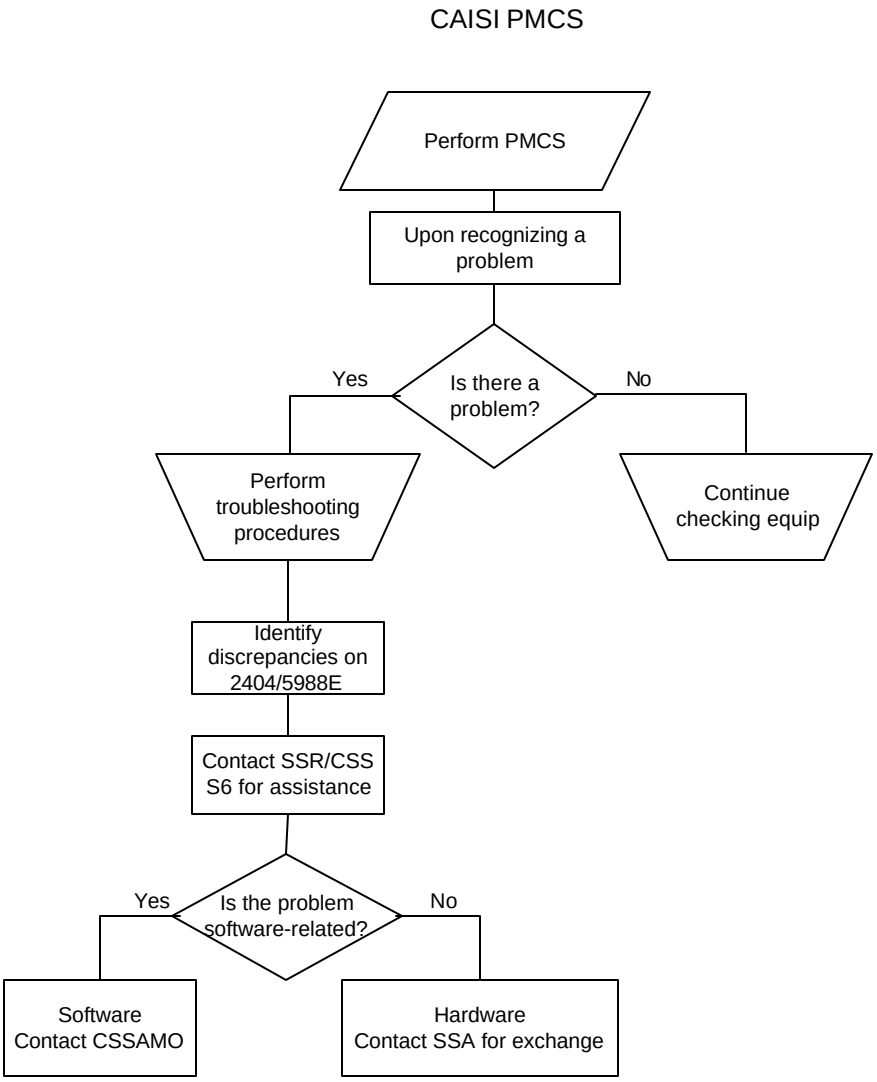


Figure 3-44 CAISI PMCS Flowchart

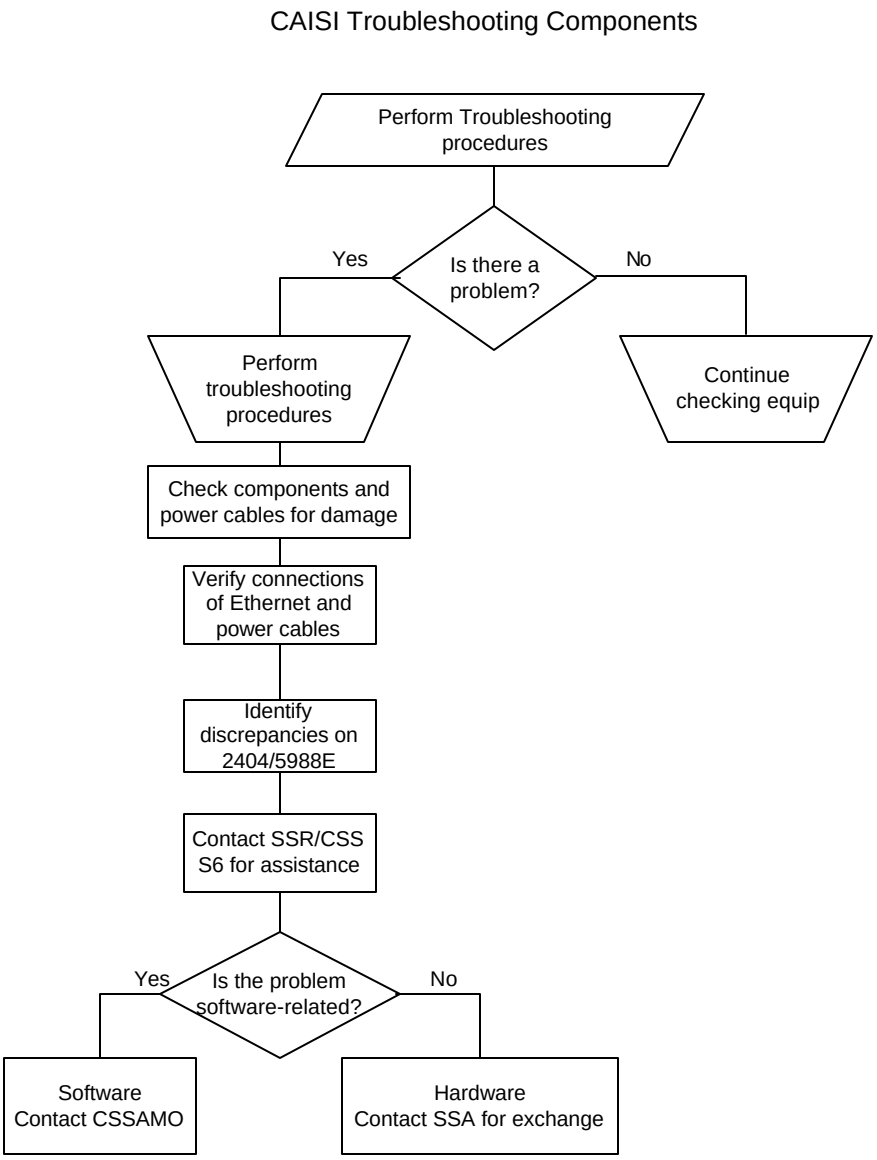


Figure 3-45 Troubleshooting Components Flowchart

Troubleshooting Hardware Components

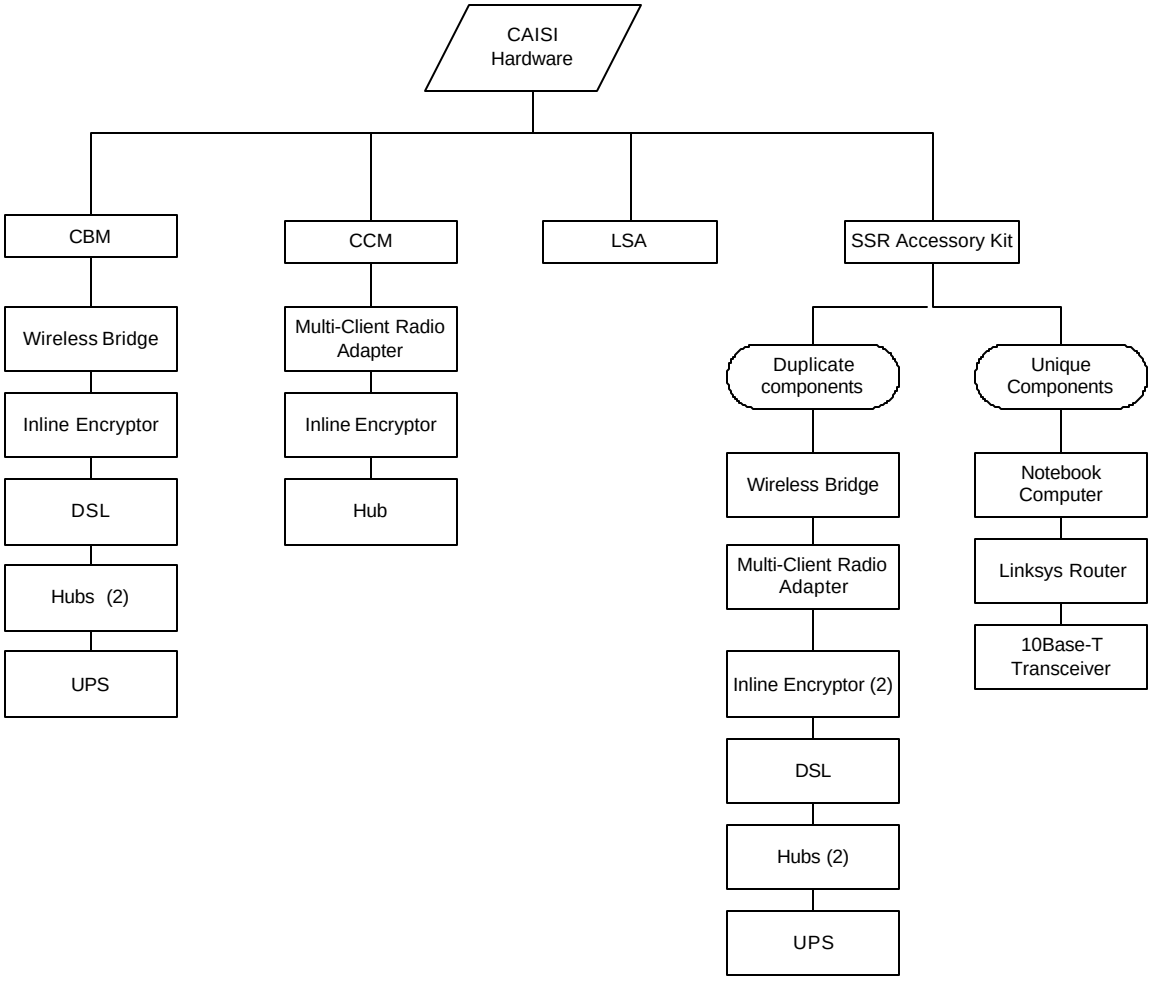


Figure 3-46 Troubleshooting Hardware Components Flowchart

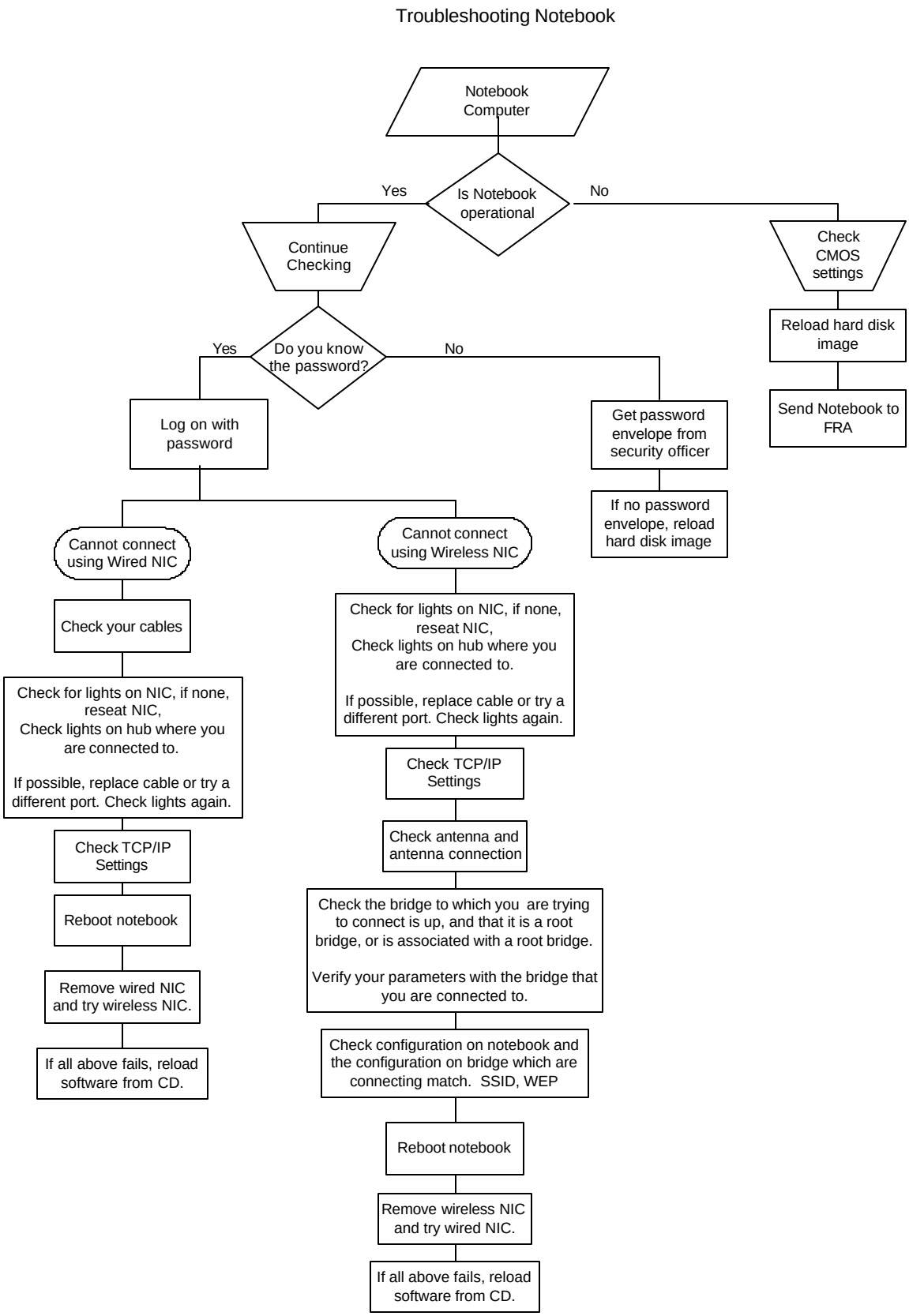


Figure 3-47 Troubleshooting SSR Notebook Flowchart

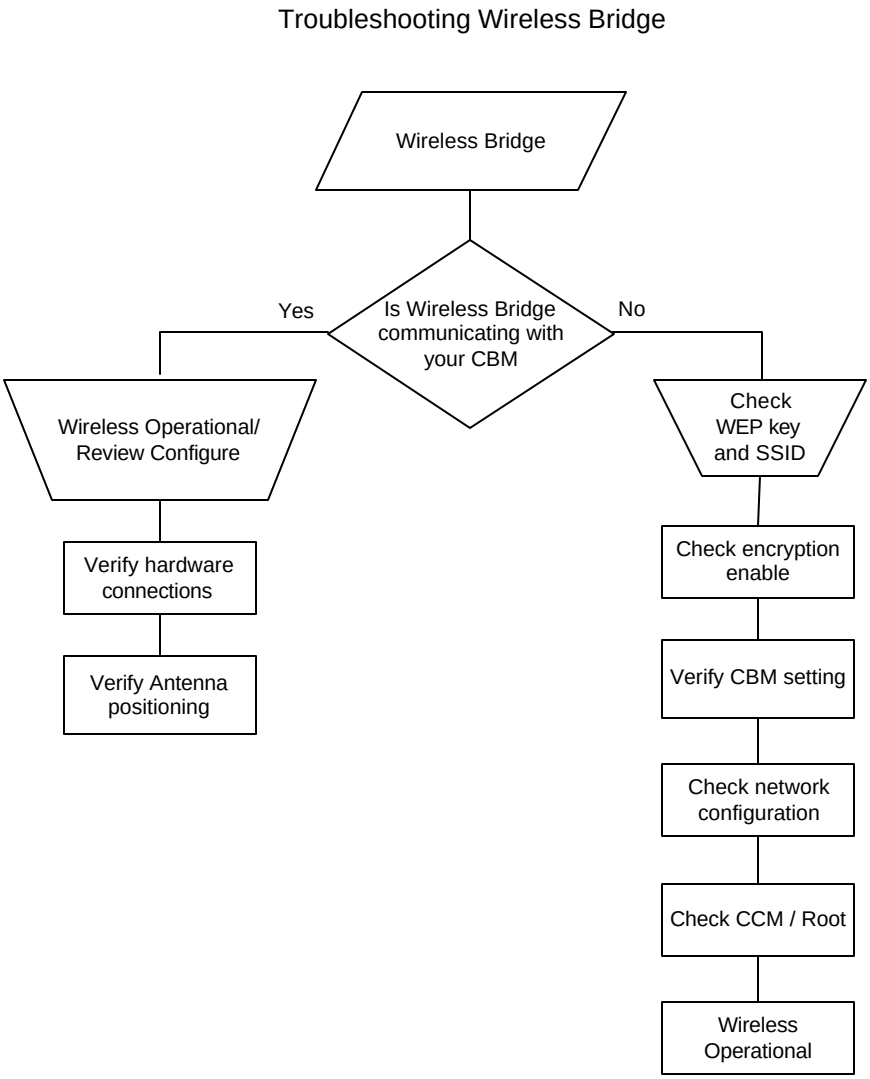


Figure 3-48 Troubleshooting Wireless Bridge Flowchart

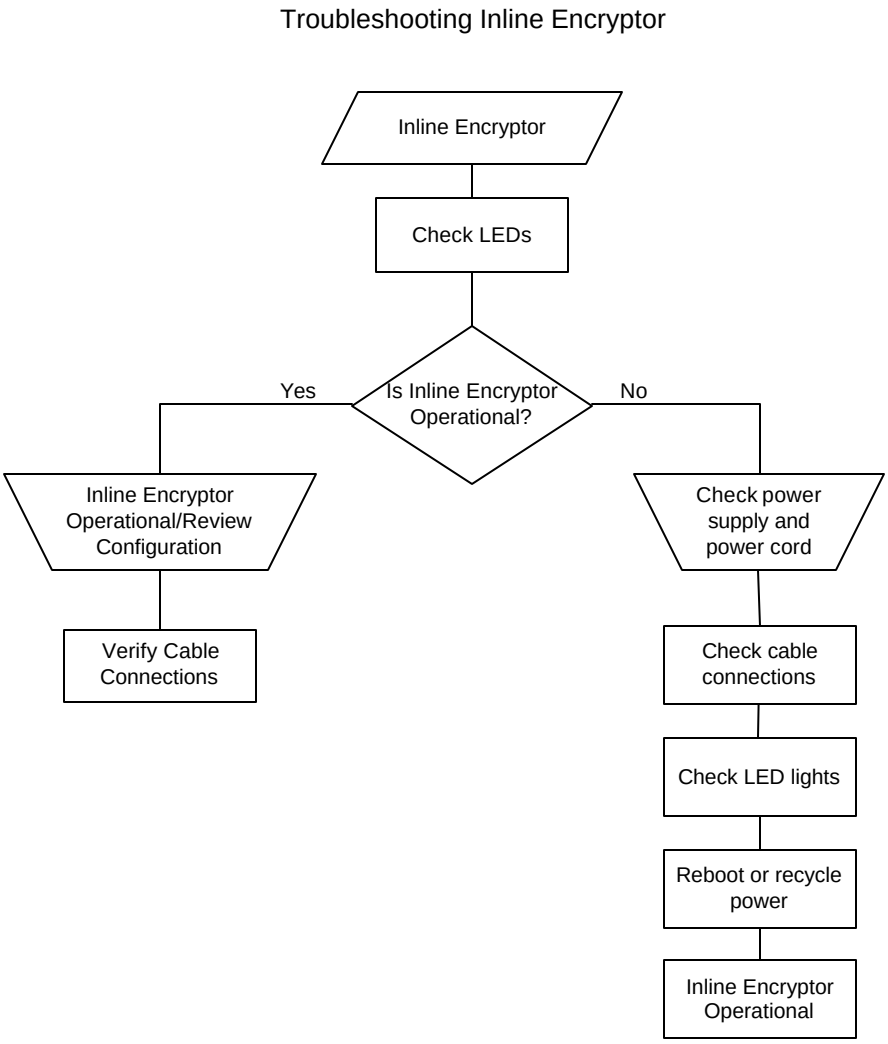


Figure 3-49 Troubleshooting Inline Encryptor Flowchart

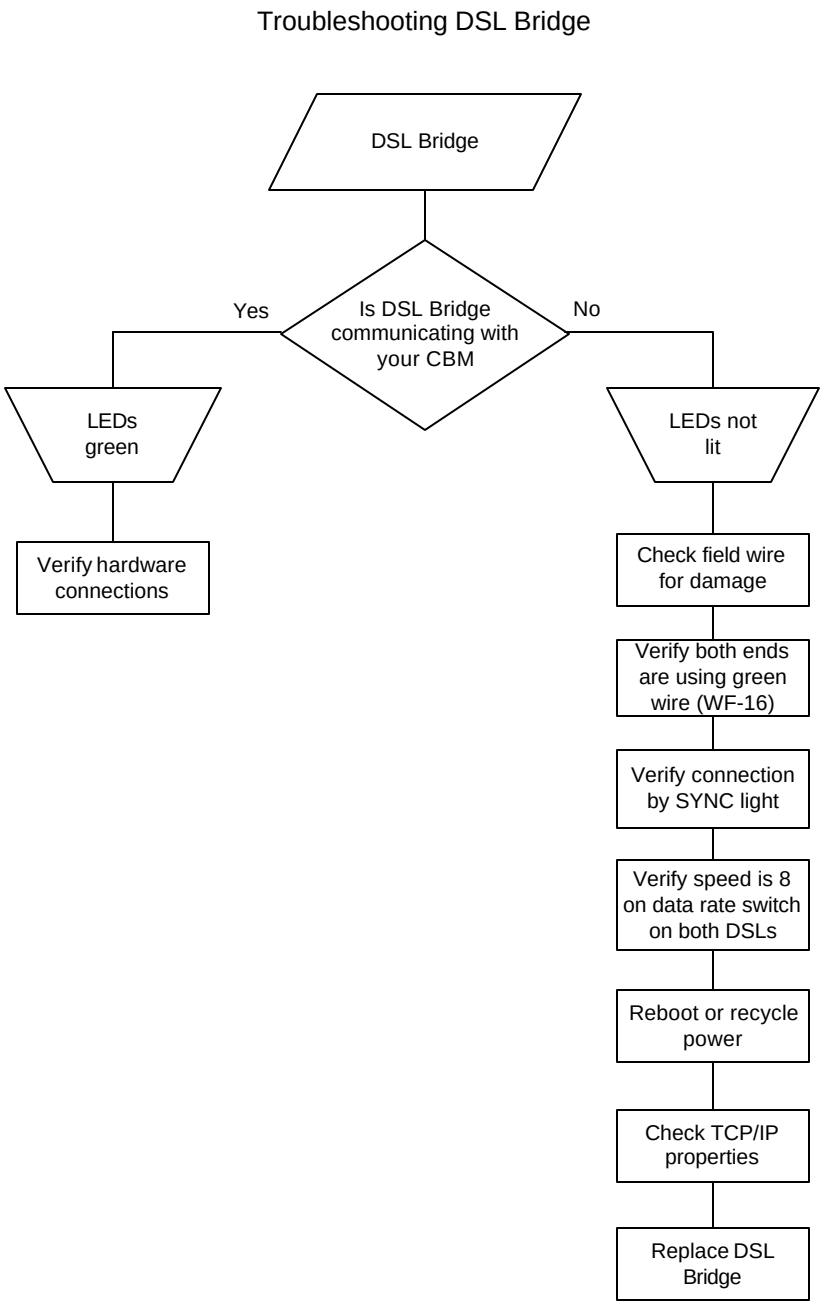


Figure 3-50 Troubleshooting DSL Bridge Flowchart

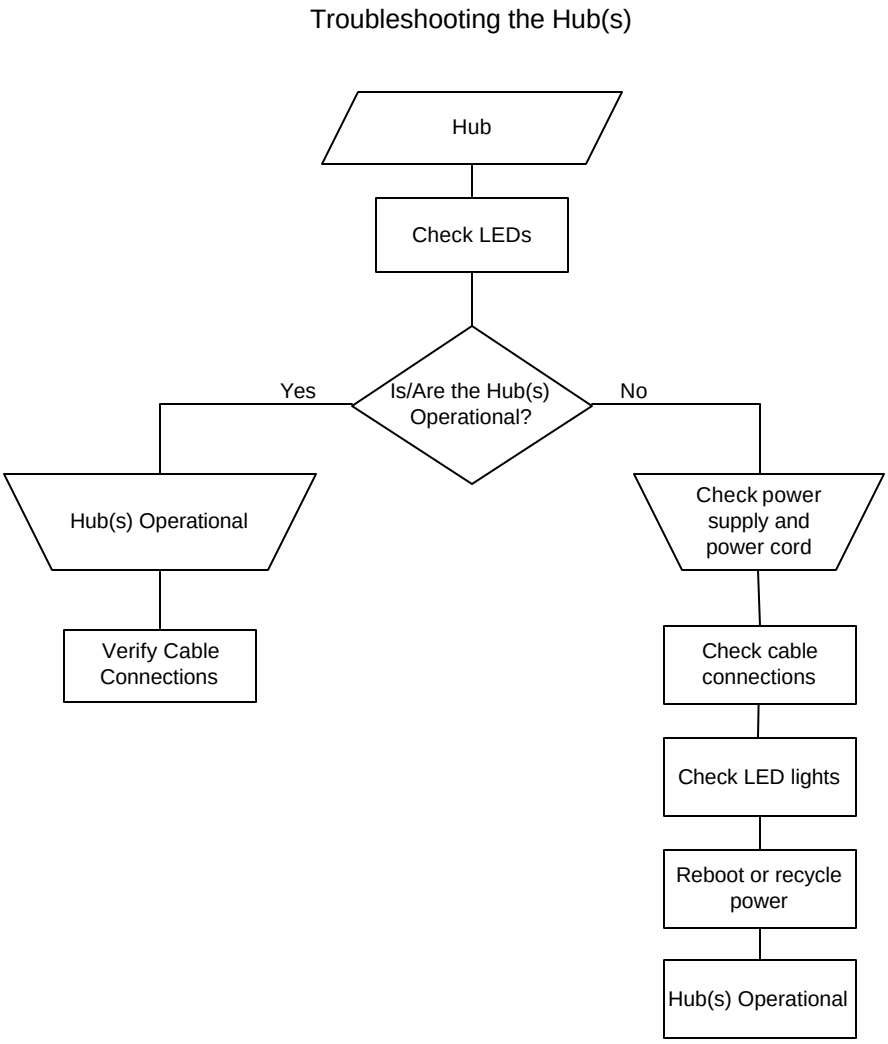


Figure 3-51 Troubleshooting the Hub(s) Flowchart

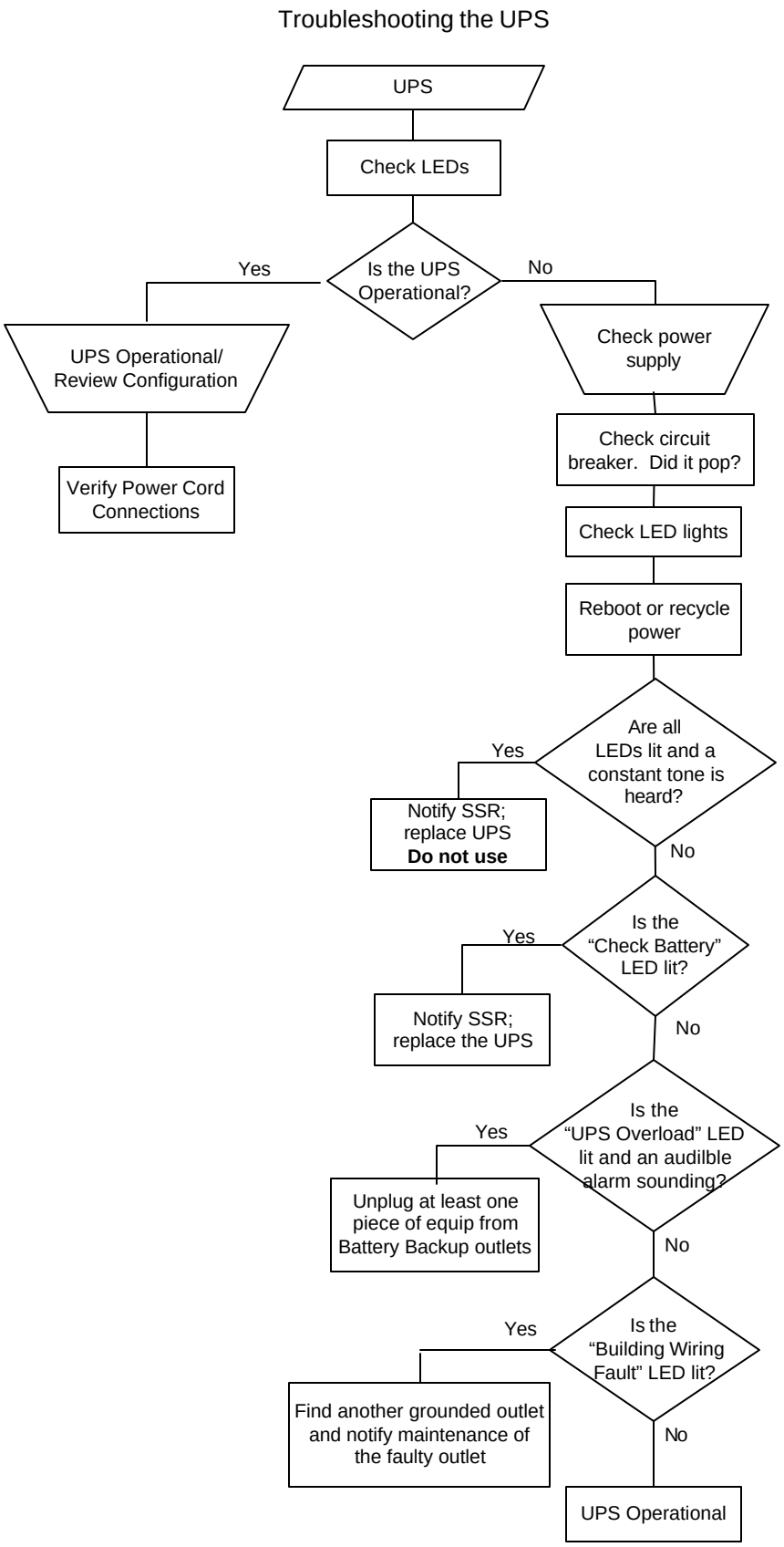


Figure 3-52 Troubleshooting the UPS Flowchart

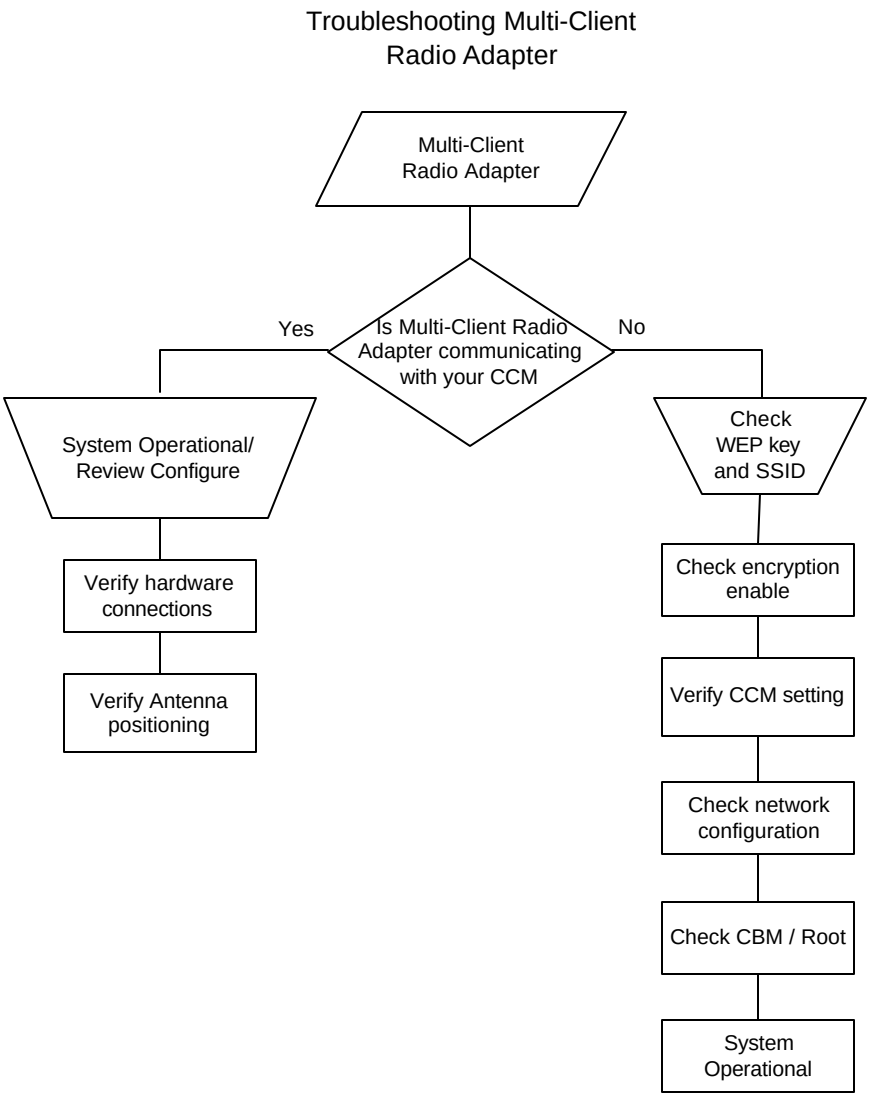


Figure 3-53 Troubleshooting Multi-Client Radio Adapter Flowchart

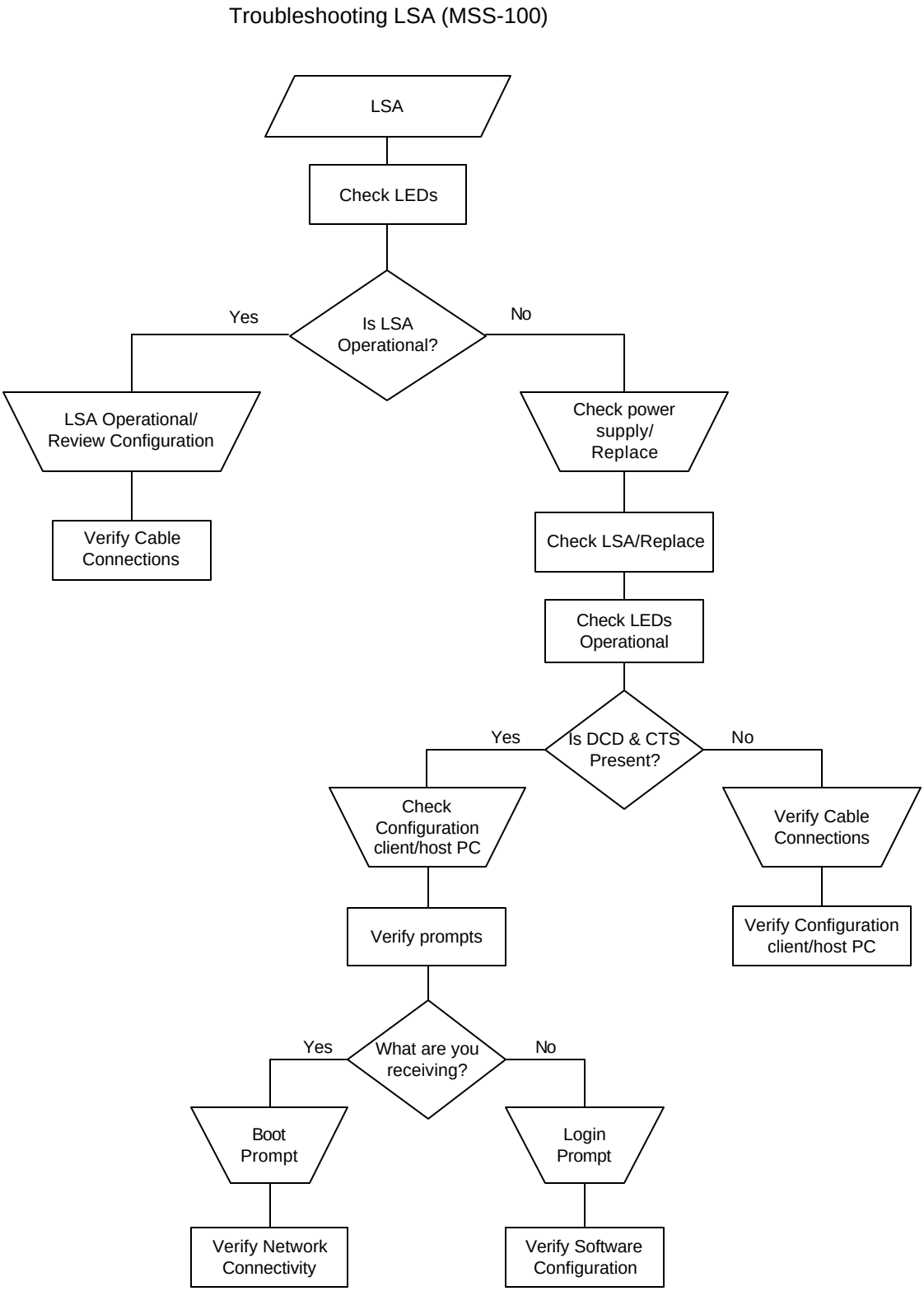


Figure 3-54 Troubleshooting LSA (MSS-100) Flowchart

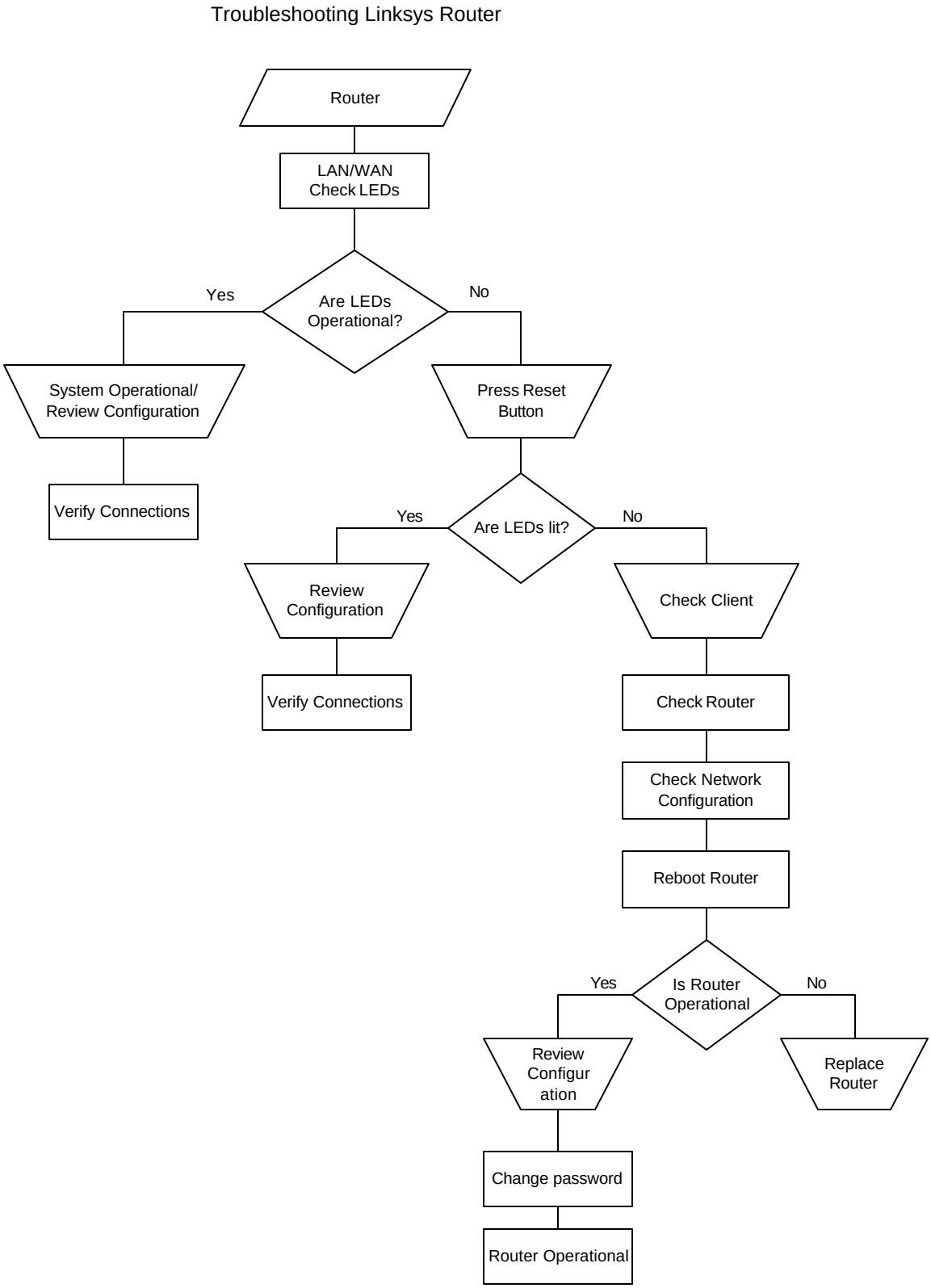


Figure 3-55 Troubleshooting Linksys Router Flowchart

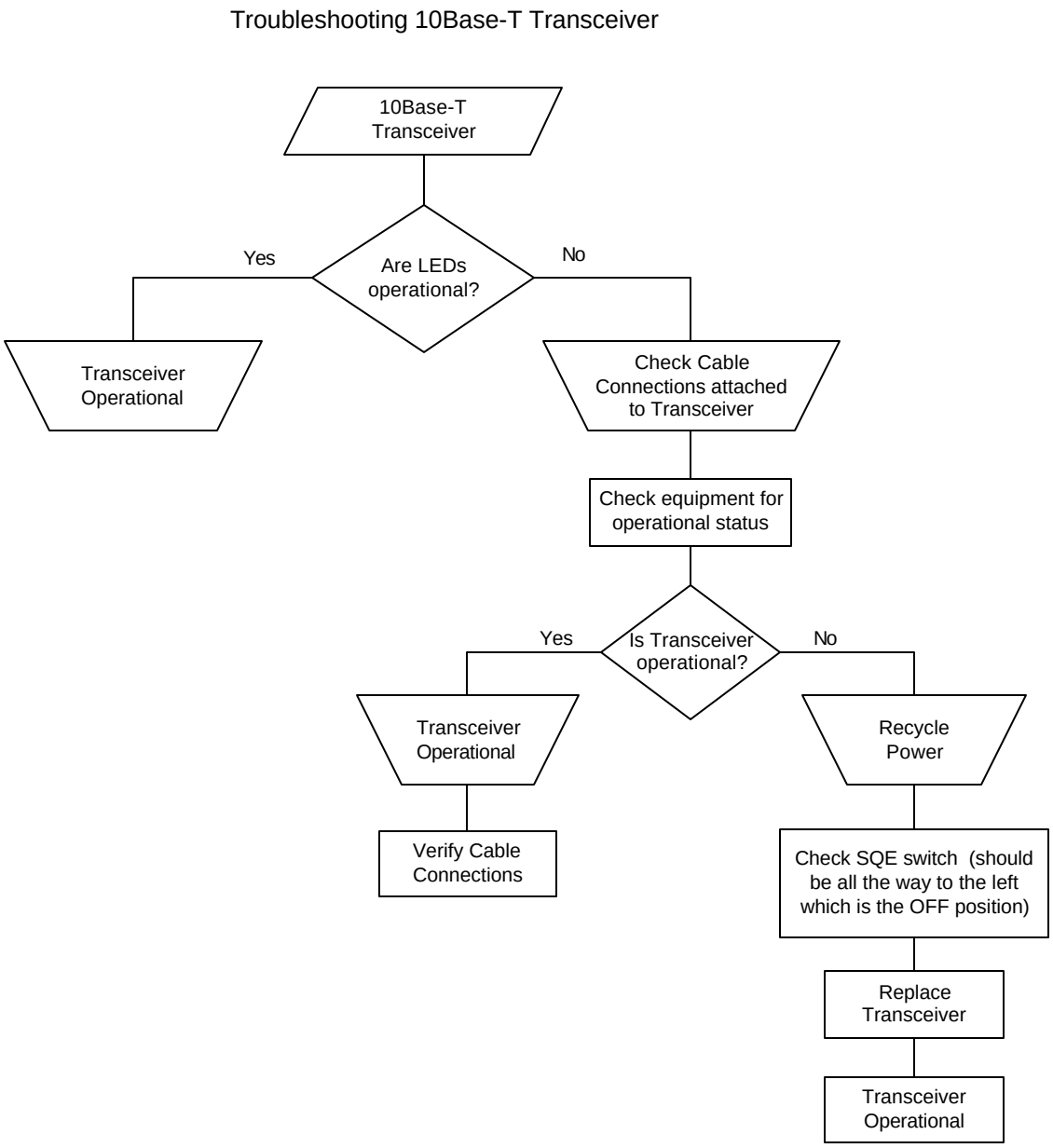


Figure 3-56 Troubleshooting 10Base-T Transceiver Flowchart

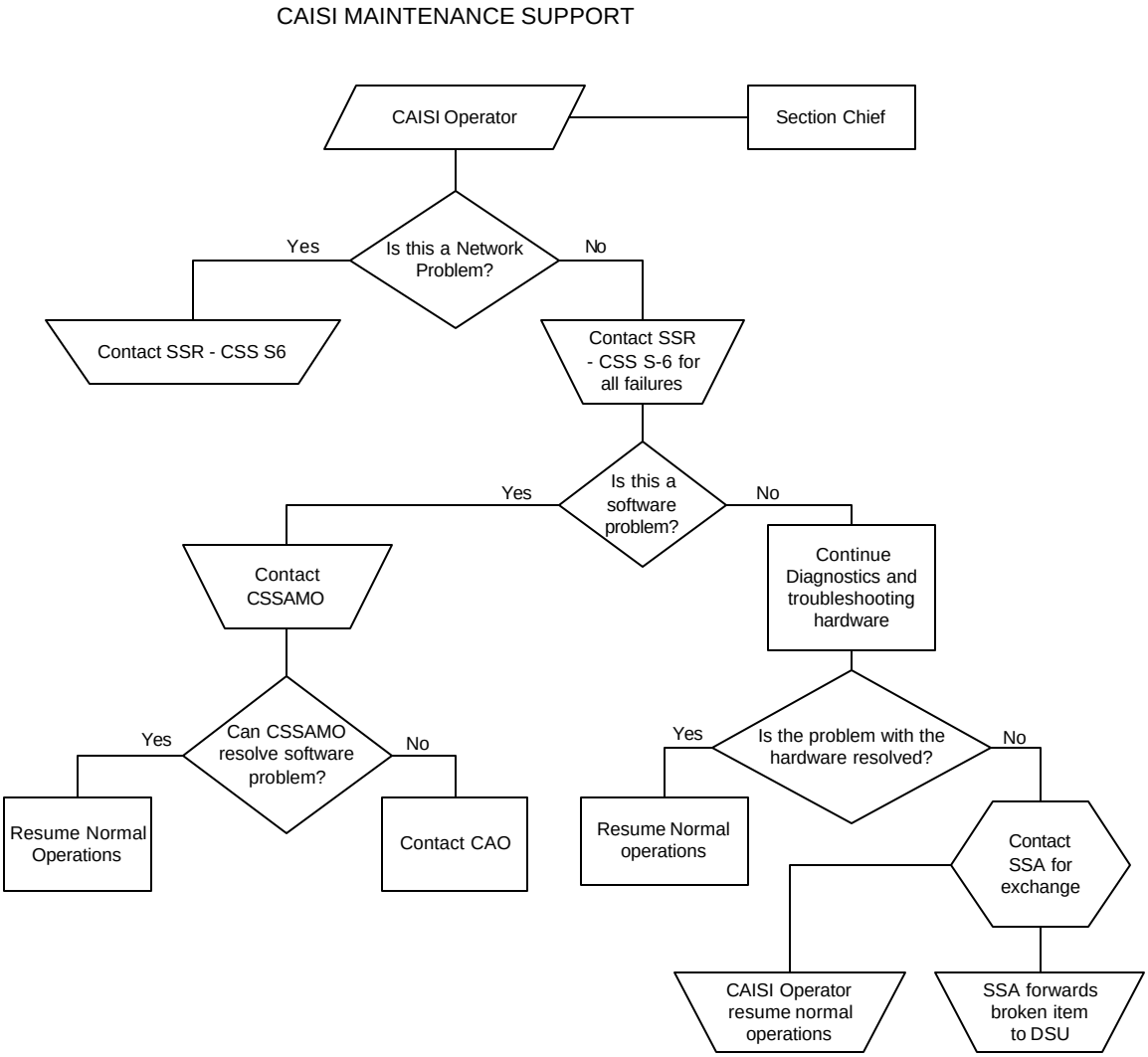


Figure 3-57 CAISI Maintenance Support Flowchart

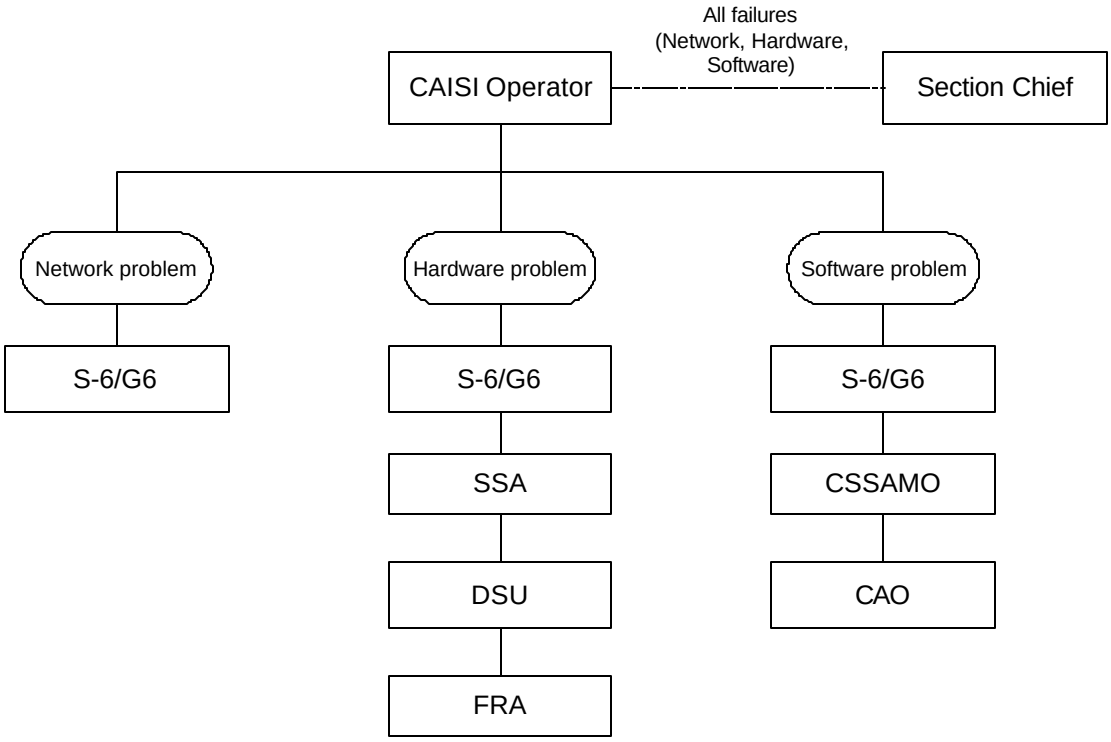


Figure 3-58 CAISI Maintenance Support

Explanation of Figure 3-58: (Flowchart is Figure 3-57).

Table 3-14 CAISI Maintenance Support

	Hardware	Software	Network
CAISI Operator	Section Chief S-6/G-6 SSA	Section Chief S-6/G-6 CSSAMO	Section Chief S-6/G-6
SSA	DSU		
DSU	FRA		
CSSAMO		CAO	

CAISI Operator and Section Chief can be the same person.

Each level tries to solve the hardware, software or network problem first. If the problem can not be resolved then they can call the next higher level. The solution of the problem comes back to the same level that made the contact. FRA talks to DSU not directly to the CAISI operator.

Further detail on each level's responsibilities and duties is in Paragraph 3.14.1.

Section III Operator Maintenance Procedures

3.14 MAINTENANCE

3.14.1 Introduction. The CAISI is designed to operate with minimal user input during normal operations. However, when a problem arises, the unit/operator must be aware of what to do.

The CAISI maintenance concept is a three level maintenance concept: **unit/operator**, **direct support** and **depot**. The following procedures describe the processes that should be followed when requesting CAISI maintenance support or when users are experiencing hardware or software-related problems.

The procedures are in accordance with AR 750-1, Army Materiel Maintenance Policy and Retail Maintenance Operations, Prevention, and Control.

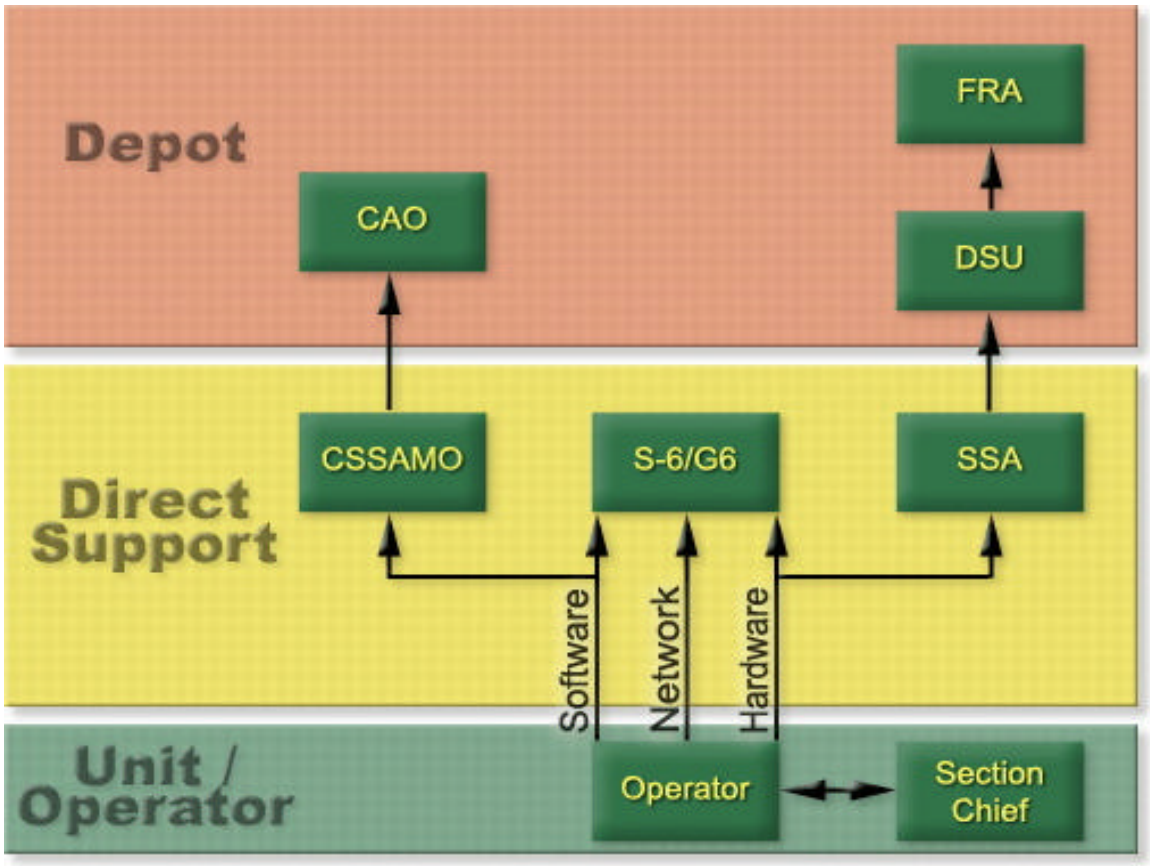


Figure 3-59 CAISI Maintenance Concept

1. **Unit/Operator Level Maintenance**. Maintenance operations for CAISI unit maintenance include the following:

   a. Performance of Preventive Maintenance Checks and Services (PMCS). (Paragraph 2.13)

   b. Conduct of inspections by sight and touch of external and other easily accessible components.

   c. Cleaning, tightening and minor adjustments as authorized.

   d. Upon recognizing that the CAISI component is not functioning properly or is non-operational, the using unit user will perform PMCS and common sense basic troubleshooting:

      (1) Ensure STAMIS communications module is properly configured.

      (2) Troubleshoot the STAMIS computer. If problem is with the STAMIS, contact the supporting Combat Service Support Automation Management Office (CSSAMO).

      (3) Checks connections to the CBM, CCM, LSA.

      (4) Contact the "owner" of the CBM and/or other users connected to the CBM/CCM to see if they have connectivity.

      (5) If the problem is determined not to be the STAMIS, the using unit will further troubleshoot his/her CBM or CCM as well as all other modules attached to determine connectivity.

CAISI LRUs are: Wireless Bridge, Multi-Client Radio Adapter, Inline Encryptor, DSL Bridge, Hubs, Power Supplies, Lightning Arrestors, Router, Notebook Computer, UPS, Antennas and antenna cables.

      (6) Complete DA Form 2404/5988E, Equipment Inspection and Maintenance Worksheet, in accordance with DA PAM 738-750, The Army Maintenance Management System (TAMMS), identifying the faulty condition and the status provided by the operator diagnostics or the failure symptom at the time of failure.

e. In addition to the information outlined in DA PAM 738-750, the following information must be annotated on the DA Form 2404/5988E.

(1) System, i.e., CAISI.

(2) Type of operating system – Not applicable.

(3) Part number and type of Line Replaceable Unit (LRU) (e.g., CBM, CCM, etc).

(4) Manufacturer/Integrator of the failed item, i.e., Tobyhanna Army Depot.

(5) Symptoms of the failure and results of the diagnostics or troubleshooting procedures.

(6) Serial number of the failed component.

f. If your CAISI module is the only unit not receiving connectivity, contact the SSR for assistance in troubleshooting the network and/or communications - related failures.

g. If the SSR, after appropriate troubleshooting and system diagnostics checks, determines that a STAMIS software problem exists, the using unit will be referred to the supporting CSSAMO.

h. If the SSR, after appropriate troubleshooting and system diagnostics checks, determines that a STAMIS hardware problem exists, the SSR will advise the CAISI owner to contact the supporting Supply Support Activity (SSA) or Interservice Supply Support Activity (ISSA). The supporting SSA/ISSA is responsible for maintaining the STAMIS computer exchange (SCX) for CAISI and is authorized to swap out defective modules.

i. After exchanging the LRU at the Class VII SSA/ISSA, the using unit will return to his unit, connect the exchanged LRU and attempt to operate the system. (See Paragraph 3.18.2 for instructions on how to replace a LRU).

2. **System Support Representative (SSR).**

a. The SSR for CAISI is the CSS S6 who oversees the installation and maintenance of the local area network.

b. When the SSR is contacted by the CAISI owner, who is experiencing a problem, the CSS S6 will:

(1) Record the symptoms/problems that the user is experiencing and actions that lead to the problems. Also record any visible damage that the unit operator has noted.

(2) Apply common solutions for common problems that have occurred.

(3) Troubleshoot the system and identify the failure as software or hardware or network/communications related.

(4) Assists the CSSAMO in troubleshooting to determine if the failure is hardware and software or network/communications related.

c. If the SSR, after appropriate troubleshooting and system diagnostics checks, determines that a STAMIS software problem exists, the SSR will advise the CAISI owner to contact the supporting CSSAMO.

d. If the SSR, after appropriate troubleshooting and system diagnostics checks, determines that a STAMIS hardware problem exists, the SSR will advise the CAISI owner to contact the supporting DSU or designated supply support activity (SSA).

3. **Combat Service Support Automation Management (CSSAMO).**

a. If the SSR, after appropriate troubleshooting and system diagnostics checks, determines that a STAMIS software problem exists, the SSR will advise the CAISI owner to contact the supporting CSSAMO.

b. When the CSSAMO is contacted, the CSSAMO will:

(1) Record the symptoms/problems that the user is experiencing and actions that lead to the problems. Also record any visible damage that the unit operator has noted.

(2) If a software problem exists, the supporting CSSAMO will contact the CAISI Software Help Desk (STAMIS Customer Assistance Office (CAO)).

4. **CAISI Software Help Desk**.

The CAISI Software Help Desk at Ft. Lee:

Comm 804-734-1051 Fax Comm: 804-734-2947
DSN: 687-1051 Fax DSN: 687-2947

Email: cao@lee-dns2.army.mil

The Ft. Lee CAO will contact the CAISI Software Team at Ft. Belvoir if they are unable to fix the problem at their level.

b. When the software help desk is contacted by the CSSAMO experiencing a problem, the software help desk will:

(1) Record the symptoms/problems that the user is experiencing and actions that lead to the problems. Also record any visible damage that the unit operator has noted.

(2) Apply common sense solutions for common problems that have occurred.

(3) Provide the technical support necessary to restore the system to an operational condition.

(4) If the problem is software-related, advise the CSSAMO on how to resolve the issue.

(5) If the problem is hardware-related, advise the supporting DSU or designated SSA.

5. **Class VII SSA/ISSA.**

a. The Class VII SSA/ISSA will have the ability to perform basic diagnostics in an attempt to determine which LRU has malfunctioned.

b. Will accept the LRU from the unit with a properly completed DA Form 2765-1, Request for turn in and another DA Form 2765-1, Request for Issue and provide the unit a replacement LRU from the SCX stockage.

c. Will process the turn-in, record the demand, and process the item in accordance with the SCX (reparable exchange) procedures.

d. The Class VII SSA/ISSA personnel will prepare a DA Form 2407/5990E, Maintenance Request in accordance with DA PAM 738-750, TAMMS for the failed LRU describing the failure. (The DA Form 2407/5990E will accompany the LRU through the entire repair process).

e. In addition to the information outlined in DA PAM 738-750, the following information must be annotated on the DA Form 2407/5990E:

(1) System, i.e., CAISI.

(2) Type of operating system – Not applicable.

(3) Part number and type of Line Replaceable Unit (LRU) (e.g., CBM, CCM, etc).

(4) Manufacturer/Integrator of the failed item, i.e., Tobyhanna Army Depot.

(5) Symptoms of the failure and results of the diagnostics or troubleshooting procedures.

(6) Serial number of the failed component.

f. The Class VII SSA/ISSA personnel will forward the failed LRU to the Direct Support Unit (DSU) / Installation Material Maintenance Activity (IMMA).

6. **Depot / Forward Repair Activity (FRA).**

a. The Depot/FRA performs all maintenance actions above the DS level. LRUs are repaired, rebuilt, refurbished, or replaced. The FRA facilitates the distribution and repair of all warranted and non-warranted hardware.

NOTE: *Replacement items may have greater capability (e.g. more RAM (memory), greater speed, etc.) than the returned items, but will always be of the same form, fit, and function.*

b. FRAs are operated by Tobyhanna Army Depot (TYAD).

c. FRAs are staffed with a point of contact (POC) during the Principal Period for Maintenance (PPM) hours.

(1) The continental United States (CONUS) FRAs operate from 0800 to 1600 hours, local time, Monday through Friday (the PPM), excluding federal holidays.

(2) Outside continental United States (OCONUS), the Help-Line operates from 0800 to 1700, local time, Monday through Friday, excluding federal and host nation holidays.

(3) Hours other than PPM are defined as Outside Principal Period for Maintenance (OPPM). FRAs will, at a minimum, provide an answering service to record calls.

d. FRAs may be staffed 24 hours per day, 7 days a week, during contingencies, exercises or in wartime.

e. A Depot/FRA facility is located at Tobyhanna, PA, Colonial Heights, VA, Fort Bragg, NC, Fort Hood, TX, Republic of Germany, Korea, Hawaii, Bosnia and Kosovo. **Table 3-15 lists all of the FRAs i**nformation to include POC, phone numbers, fax numbers, email address and address.

The Depot/FRA is responsible for the disposition instructions as well as warranty guidance, repair or disposal. The Depot/FRA Help-Line operator will do the following:

a. Talks the DSU/IMMA maintenance personnel through a series of questions or diagnostics for the system described. The objective of the telephonic Help-Line is to preclude costly No Evidence Of Failure (NEOF) incidents.

b. Determines the warranty status of the unserviceable LRU, during telephonic contact with the DSU/IMMA maintenance personnel.

(1) If the LRU is under warranty, the Depot/FRA Help-Line operator provides the DSU/IMMA maintenance personnel with the telephone number of the appropriate vendor or the Original Equipment Manufacturer (OEM) for repair action.

(2) If the LRU is not covered under warranty, the Depot/FRA Help-Line operator provides the DSU/IMMA maintenance personnel shipping instructions for the item to be returned.

c. The Depot/FRA Help-Line operator obtains the following information from the DA Form 2407/DA Form 5990-E, Maintenance Request:

(1) Owning unit's Unit Identification Code (UIC).

(2) Owning unit's Department of Defense Activity Address Code (DODAAC).

(3) The owning unit's DSU/IMMA designation.

(4) CAISI CBM, CCM, LSA or SSR Accessory Kit.

(5) Type of operating system (OS).

(6) The part number and type of LRU.

(7) Manufacturer of the failed LRU.

(8) Symptoms of the failure and results of the diagnostics or troubleshooting procedures.

(9) Serial number of the failed LRU.

d. Determination of Class VII SSA/ISSA.

(1) If the LRU is not a Class VII SSA/ISSA SCX stocked item, the FRA prepares and ships a replacement item using a 24-hour shipping service.

(2) If the item is Class VII SSA/ISSA SCX stocked, the FRA prepares and ships a replacement item **within 72 hours** (3 working days) after receipt of the failed item. The FRA attaches a label to the replacement item that reflects the intended UIC, the type software, the OS, and the date loaded.

e. Upon receipt of the faulty item from the DSU/IMMA, the FRA logs the LRU into the FRA database by part number, UIC of the losing unit, and reported fault. The FRA screens LRUs for NEOF.

f. No items covered under a warranty are to be sent to the Depot/FRA **without prior coordination**. Items that are inadvertently forwarded to the FRA will be returned to the unit for processing under the warranty provisions.

7. **Maintenance Contingency Operations**.

a. Program Executive Office Enterprise Information Systems (PEO EIS) provides a rapidly deployable FRA to provide maintenance essential materials, and increased flexible combat service support of commercial off the shelf non-developmental item automated data processing equipment (COTS NDI ADPE) in support of deployed U.S. Forces.

b. The FRA is established as an In-Theater Computer Repair Activity (ITCRA) to meet deployment requirements.

The objective of the ITCRA is to reduce the logistics delay time by minimizing the evacuation of tactical systems from the theater for repair. This reduces the time and distance between point of failure and point of repair.

The ITCRA interfaces with the theater command structure to resolve COTS NDI ADPE issues and problems. This capability is offered to assist the theater in repair of all other COTS systems on a reimbursable basis.

c. PEO EIS has three 36-foot vans and three S-280 shelters pre-positioned at Tobyhanna Army Depot, Tobyhanna, PA. The combination of vans and shelters gives PEO EIS the capability to provide maintenance in four theaters of operation simultaneously.

The ITCRA can be deployed as a standalone configuration, or as part of a Logistic Support Element (LSE). The ITCRA is configured in one of the configurations as follows:

(1) A 36-foot van configured with workstations, small parts storage, and large parts storage.

(2) Three S-280 shelters: a small parts storage shelter, a large parts storage shelter, and a repair/workshop shelter.

d. Operations include repair of PEO EIS COTS NDI ADPE systems, repair of LRUs and system replaceable unit (SRUs), modules, and components, in addition to providing a capability to determine source of repair and disposition of returns (in-theater or retrograde out of theater).

Operations also include repair of all other COTS systems on a reimbursable basis.

Table 3-15 Forward Repair Activity (FRA) Addresses

Location	Mailing Address	Voice & Fax (DSN & Comm)
Tobyhanna, Pennsylvania STAMIS Repair Activity WHS 5, Bay 2, Maintenance 11 Hap Arnold Blvd Tobyhanna, PA 18466-5028	STAMIS Repair Activity WHS 5, Bay 2, Maintenance 11 Hap Arnold Blvd Tobyhanna, PA 18466-5028 Mark For: Special Project "BUY" DODAAC: W25JNE	POC: Leo Yesvetz DSN 795-6747 Comm 570-895-6747 888-278-8281 Fax: DSN 795-6049 Comm 570-895-6049 Email: lyesvetz@tobyhanna.army.mil
Tobyhanna, Pennsylvania Product Management: Cdr, Tobyhanna Army Depot ATTN: AMSEL-TY-MM-P 11 Hap Arnold Blvd Tobyhanna, PA 18466-5028	Cdr, Tobyhanna Army Depot ATTN: AMSEL-TY-MM-P 11 Hap Arnold Blvd Tobyhanna, PA 18466-5028	POC: Luddy Manganiello DSN 795-7605 Comm 570-895-7605 Fax: DSN 795-7796 Comm 570-895-7796 Email: Ludwig.manganiello@tobyhanna.army.mil
Tobyhanna, Pennsylvania FRA Division Chief Tobyhanna Army Depot ATTN: AMSEL-TY-MX-D 11 Hap Arnold Blvd Tobyhanna, PA 18466-5028	Tobyhanna Army Depot ATTN: AMSEL-TY-MX-D 11 Hap Arnold Blvd Tobyhanna, PA 18466-5028	POC: Alex Radkiewicz DSN 795-6479 Comm 570-895-6479 Fax: DSN 795-6947 Comm 570-895-6947 Email: Alex.radkiewicz@tobyhanna.army.mil
Colonial Heights, Virginia Tobyhanna FRA U.S. Army Reserve STAMIS Computer 840C West Roslyn Road Colonial Heights, VA 23834 **NOTE**: Services Army Reserve SCX Center Only.	Tobyhanna FRA Colonial Heights 840C West Roslyn Road Colonial Heights, VA 23834	POC: William Lofton Comm 804-526-6046/6047 Fax: 804-526-6048 Email william.lofton@tobyhanna.army.mil

Table 3-15 Forward Repair Activity (FRA) Addresses (Continued)

Location	Mailing Address	Voice & Fax (DSN & Comm)
Fort Bragg, North Carolina Tobyhanna FRA Bldg. J-2144 Knox Street Complex Fort Bragg, NC 28310	Tobyhanna Army Depot FRA Bldg. J-2144 Knox Street Complex Fort Bragg, NC 28310	POC: Charles Marsala, Ted Pearil DSN 236-3080 Comm 910-396-3080 Fax: DSN 236-5033 Comm 910-396-5033 Email: charles.marsala@tobyhanna.army.mil theodore.pearil@tobyhanna.army.mil
Fort Hood, Texas Location & FEDEX/UPS Address: Tobyhanna FRA Bldg. 4417 Corner of 68th St. & Santa Fe Ave. Fort Hood, TX 76544	Tobyhanna Army Depot FRA PO Box 5430 Fort Hood, TX 76544	POC: Gary Leofsky, Scott Jones DSN 738-5079 Comm 254-288-5079 Fax: DSN 738-0905 Comm 254-288-0905 Email: gary.lefosky@Hood.army.mil
Fort Lewis, Washington Tobyhanna FRA Bldg. 3096 Stryker Ave at S. 20 St. Fort Lewis, WA 98433-9500	ESSC ATTN: Anthony Losito (TYAD FRA) Bldg 3096, MS60, Box 339500 Stryker Ave at S. 20 St. Fort Lewis, WA 98433-9500	POC: Tony Lositio DSN 347-7086 Comm 253-966-7086 Fax: DSN 357-2565 Comm 253-967-2565 Email: lositoa@Lewis.army.mil
Seoul, Korea Tobyhanna FRA SR 595th CS Maint Co DS Songnam, Seoul, Korea KS	Tobyhanna FRA Bldg S606 Songnam, Seoul AB Korea, KS DODAAC WT4KDX	POC: Mike Lucas DSN 315-741-6348 COMM 1-901-182-317-206348 Fax: DSN 315-741-6356 COMM 1-901-182-317-206356 Email: Lucasm@usfk.korea.army.mil

Table 3-15 Forward Repair Activity (FRA) Addresses (Continued)

Location	Mailing Address	Voice & Fax (DSN & Comm)
Friedrichsfeld, Germany Actual Location & Fedex/UPS USAMC Europe Tobyhanna FRA Bldg 1041 Steineugstrasse 19 Friedrichsfeld STG Activity 68229 Mannheim DODAAC W80YW6	HQ, AMC Europe Tobyhanna FRA Unit 29331, Box 293 APO AE 09266 DODAAC W80YW6	POC: Rich Pryor, Dallas Jamison, Laura Tigert DSN 314-375-6075 Comm 011-49-621-4876075 Fax: DSN: 314-375-7199 Comm 011-49-621-4877199 Email: pryorr@hq.hqusareur.army.mil
Schofield Barracks, Hawaii Actual location & Fedex/UPS Tobyhanna FRA Hawaii Bldg. 847 (J-Quad) Schofield Barracks, HI 96857	Ship Large Items to: DOL, HQ USA SCH Storage Branch, Bldg 6037 East Range, HI 96857-5006 ATTN: Official Mail to: Army Logistics Assistance Office, 25th ID ATTN: AMXLS-P-SB Tobyhanna Stop #236 Schofield Barracks, HI 96857-5400	POC: Brian McFeely Comm 808-655-0902 Fax: Comm 808-655-0906 Email:
Comanche Base, Bosnia Task Force Eagle Operation Joint Forge Computer Repair Facility Bldg. 106 Eagle Base, Bosnia	OJF Eagle Base Tuzla, Bosnia Computer Repair Facility Bldg. 106 APO, AE 09789	POC: Rotates DSN 314-762-7544 BDI Fax: 314-762-7543 Email: Lse-b.tobyhanna@email-tc3.5sigcmd.army.mil
Camp Bondsteel, Kosovo Operation Joint Guardian TACMIS/TIER III BLDG 2024L Camp Bondsteel, Kosovo	Computer Repair Facility TF Falcon Bondsteel, Kosovo FSB (AMC) TACMIS/TIER III APO, AE 09340	POC: Rotates DSN 314-781-3100 Email: Christopher.sefchik@bondsteel2.areur.army.mil

Table 3-15 Forward Repair Activity (FRA) Addresses (Continued)

Location	Mailing Address	Voice & Fax (DSN & Comm)
Camp AS-Sayliyah **Qatar** **Actual Location & Fedex/UPS** **Tobyhanna FRA** **Brian Kelly/ATTN: 511** **Armed Forces Stores Depot** **AS-Sayliyah** **United States Armed Forces** **Doha, Qatar**	Freight: WODA AMC SWA/CEB-Qatar Tobyhanna FRA, Brian Kelly APS 5 511 Bldg CR Warehouse Armed Forces Stores Depot AS-Sayliyah Doha, Qatar	POC: Rotates DSN 318-432-2499 Fax: DSN 318-432-2406
Camp Arijan, Kuwait	OPP Alghanim Warehouse 318-825-2118 AL RAI Industrial Area Kuwait 395	POC: Charles Marsala DSN 987-5062 x6626 Email: charles.marsala@tobyhanna.army.mil
Iraq	4th Infantry Division	POC: Craig Jenning 732-532-0565 x8418 craig.jenning@us.army.mil
Iraq	Baghdad International Airport	POC: Bill Price CGS Iridium phone DSN 717-632-6539

3.14.2 Replacing Components within the CBM and CCM.

In accordance with the maintenance concept described above, you will occasionally need to replace a LRU components within the CBM or CCM. CBM Architecture is discussed in Paragraph 1.19.1 and the CCM Architecture is discussed in Paragraph 1.19.2.

1. Remove all power from the unit. Unplug power cables and disconnect them from the unit.
2. Disconnect all other external cables, such as network cables, antenna cables, and the grounding strap.
3. Remove the top cover. Undo the screws and pull up on the cover until the Velcro separates.
4. Disconnect cables from the component to be replaced.
5. Remove the component.
6. Attach the replacement component.
7. Reconnect the cables
8. Reattach the cover.
9. Reattach external cables.
10. Reconnect power cables and apply power.
11. Configure the unit.
12. Test the unit.

For further detailed instructions on the exact placement of components and cables within the CBM and CCM, see the Standard Engineering Installation Package (SEIP).

THIS PAGE IS INTENTIONALLY LEFT BLANK

Chapter 4

UNIT MAINTENANCE INSTRUCTIONS

Section I. Repair Parts, Tools, Special Tools, Test, Measurement, and Diagnostic Equipment (TMDE)

4.1 INTRODUCTION

This section covers repair parts, tools, special tools, and test, measurement, and diagnostic equipment (TMDE) required to support the CAISI suite of equipment.

4.2 COMMON TOOLS AND EQUIPMENT

Refer to the Maintenance Allocation Chart (MAC) in Appendix B for authorized common tools and equipment required for each maintenance function.

4.3 SPECIAL TOOLS, TMDE, AND SUPPORT EQUIPMENT

None Required.

4.4 REPAIR PARTS

No repair parts will be authorized to the unit level.

Section II. Preventive Maintenance Checks and Services

4.5 PREVENTIVE MAINTENANCE CHECKS AND SERVICES

No additional PMCS is authorized at the unit level.

Section III. Troubleshooting

4.6 TROUBLESHOOTING

All authorized troubleshooting procedures are detailed in Chapter 3 of this manual.

Section IV. Maintenance Procedures

4.7 MAINTENANCE PROCEDURES

Unit Level Maintenance for the CAISI is the same as Operator Level Maintenance which was discussed in Paragraph 3.14.

Section V. Preparation for Storage or Shipment

4.8 INTRODUCTION

The transit cases issued with the CAISI components are the only authorized packaging and shipping containers to be used with the CAISI. Follow shutdown and packup procedures detailed in Paragraph 2.36 – 2.46 of this manual.

Appendix A

REFERENCES

A.1 SCOPE

This appendix lists forms and publications that are referenced in this manual.

A.2 FORMS

DA Form 2028-2	Recommended Changes to Equipment Technical Publications
DA Form 2404	Equipment Inspection and Maintenance Worksheet
DA Form 2407	Maintenance Request
DA Form 2765-1	Request for Issue or Turn in
SF 361	Transportation Discrepancy Report (TDR)
SF 364	Report of Discrepancy (ROD)
SF 368	Product Quality Deficiency Report

A.3 PUBLICATIONS

AR 55-38	Reporting of Transportation Discrepancies in Shipments
AR 190-13	The Army Physical Security Program, June 1985
AR 190-51	Security of Army Property at Unit and Installation Level, April 1986
AR 340-17	Release of Information and Records from Army Files
AR 380-5	Department of the Army Information Security Program
AR 381-12	Subversion And Espionage Directed Against The U.S. Army (SAEDA) 15 Jan 1993
AR 381-14(S)	Counterintelligence-Technical Surveillance Countermeasures (U)
AR 380-19	Information Systems Security

AR 380-67	Department of the Army Personnel Security Program, September 1988
AR 735-11-2	Reporting of Item and Package Discrepancies
AR 750-1	Army Maintenance Policy and Retail Maintenance Operations
CTA 50-970	Expendable Items (Except Medical, Class V, Repair Parts, and Heraldic Items
DA Pam 25-30	Consolidated Index of Army Publications and Blank Forms
DA Pam 738-750	The Army Maintenance Management System (TAMMS)
DoDS 5200.28	Department of Defense (DoD) 5200.28-Standard (DoDS), Trusted Computer Security Evaluation Criteria (TCSEC), December 1985
DoDD 5200.40	DoD Directive (DoDD) 5200.40, Defense Information Technology Security Certification and Accreditation Process (DITSCAP), 31 December 1997
FIPS Pub 140-1	Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules, January 1994
FM 11-487-4	Installation Practices; Communications Systems Grounding, Bonding, and Shielding
FM 21-11	First Aid for Soldiers
FM 24-7	Tactical Local Area Network (LAN) Management, October 1999
FM 24-19	Radio Operations Manual, May 1991
MIL-HDBK-419A	Grounding, Bonding, and Shielding for Electronic Equipment & Facilities, Volume 1 & 2
MIL-PRF-81705D	Barrier Materials, Flexible, Electrostatic Protective, Heat Sealable
MIL-STD-129N	Military Marking

MIL-STD-461D(1)	Requirements for the Control of Electromagnetic Interference Emissions, and Susceptibility
NSTSSAM TEMPEST 1-91	National Communications Security Information Memorandum
PPP-B-1672D(1)	Boxes, Shipping, Reusable with Cushioning
SB 746-1	Publications for Packaging Army General Supplies
TB 43-0118	Field Instructions for Painting and Preserving Communications-Electronics Equipment
TB 11-5895-1691-10	CAISI Software User's Manual
TM 750-244-2	Procedures for Destruction of Electronics Material to Prevent Enemy Use (Electronic Command)
TM 11-5985-357-13	Operator's Organizational and Direct Support Maintenance Manual For Antenna OE-254/GRC

A.4 COMMERCIAL MANUALS

DSL Bridge. ADC PairGain Megabit Modem 300SBP Users Guide, LTI DataComm. Not available online.

Encryptor. Air Fortress AF-1100 User's Manual. Not available online.

Hubs. Addtron HUB8CT Ethernet 10Base-T Multi-Port Hub or Farallon Streamline Starlet hub User's Manual. Not available online.

Legacy Support Adapter. Lantronix MSS-100 Universal Thin Server Installation Guide. Available online at http://www.lantronix.com/support/docs/pdf/mss100.pdf. Reference Manual at http://www.lantronix.com/support/docs/pdf/mss_ref.pdf.

Router. Linksys Cable/DSL Router BEFSR81 Users Guide. Available online at ftp://ftp.linksys.com/pdf/befsr81ug.pdf.

Router. Netscreen 5xp. Concepts and Examples Guide, WebUI Reference Manual, Message Log Reference Guide and CLI Reference Guide. Available online at http://www.netscreen.com/support/manuals.html

SSR Notebook. MITAC 7020/MITAC 7251 Installation Manual. Not available online.

Wired Network Interface Card. Xircom RealPort 10/100. Information available online at http://www.xircom.com/dl/detail/0,1306,1-840-1_47Z1-840-1_20-20Z,00.html.

Wireless Bridge. Cisco Aironet 340 Series Bridge Users Guide, Reference Manual, and Reference Manual Addendum. Users Guide available online at http://www.cisco.com/univercd/cc/td/doc/product/wireless/aironet/bridge/ebridge.pdf .

Wireless Bridge. Cisco Aironet 350 Series Bridge Users Guide, Reference Manual, and Reference Manual Addendum. Users Guide available online at http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350brdgs/index.htm .

Wireless Multi-Client Radio Adapter, WGB 342. Cisco Aironet Workgroup Bridge, Hardware Installation Guide and Software configuration Guide. Available online at http://www.cisco.com/univercd/cc/td/doc/product/wireless/aironet/wgbridge/hig/index.htm and http://www.cisco.com/univercd/cc/td/doc/product/wireless/aironet/wgbridge/wgbscg/index.htm .

Wireless Multi-Client Radio Adapter, WGB 352. Cisco Aironet Workgroup Bridge, Hardware Installation Guide and Software configuration Guide. Available online at http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350wgb/350hig/index.htm and http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350wgb/350scg/index.htm .

Wireless Network Interface Card, LMC342, LMC352. Cisco Aironet PCMCIA Client Adapter, Hardware Installation Guide and Software configuration Guide. Available online at http://www.cisco.com/univercd/cc/td/doc/product/wireless/aironet/adapters .

UPS. Owner's Manual, Internet Office 280 UPS System, Tripp Lite, 1998

Appendix B

MAINTENANCE ALLOCATION CHART (MAC)

Section I. Introduction

B.1 THE ARMY MAINTENANCE SYSTEM MAC

a. This introduction provides a general explanation of all maintenance and repair functions authorized at various maintenance levels under the Standard Army Maintenance System concept.

b. The Maintenance Allocation Chart (MAC) in Section II designates overall authority and responsibility for the performance of maintenance functions on the identified end item or component. The application of the maintenance functions to the end item or component will be consistent with the capacities and capabilities of the designated maintenance levels, which are shown on the MAC in column (4) as:

Unit	includes two subcolumns, C (crew/operator) and O (organization/unit) maintenance
Direct Support	includes an F subcolumn
General Support	includes an H subcolumn
Depot	includes a D subcolumn

c. Section III lists the tools and test equipment (both special tools and common tool sets) required for each maintenance function as referenced from Section II.

d. Section IV contains supplemental instructions and explanatory notes for a particular maintenance function.

B.2 MAINTENANCE FUNCTIONS

Maintenance functions are limited to and defined as follows:

a. **Inspect.** To determine the serviceability of an item by comparing its physical, mechanical, and/or electrical characteristics with established standards through examination (e.g., by sight, sound, or feel).

b. **Test.** To verify serviceability by measuring the mechanical, pneumatic, hydraulic, or electrical characteristics of an item and comparing those characteristics with prescribed standards.

c. **Service.** Operations required periodically to keep an item in proper operating condition; e.g., to clean (includes decontamination, when required), to preserve, to drain, to paint, or to replenish fuel, lubricants, chemical fluids, or gases.

d. **Adjust.** To maintain or regulate, within prescribed limits, by bringing into proper position, or by setting the operating characteristics to specified parameters.

e. **Align.** To adjust specified variable elements of an item to bring about optimum or desired performance.

f. **Calibrate.** To determine and cause corrections to be made or to be adjusted on instruments or test, measuring, and diagnostic equipment used in precision measurement. Calibration consists of comparisons of two instruments, one of which is a certified standard of known accuracy, to detect and adjust any discrepancy in the accuracy of the instrument being compared.

g. **Remove/Install**. To remove and install the same item when required to perform service or other maintenance functions. Install may be the act of emplacing, seating, or fixing into position a spare, repair part, or module (component or assembly) in a manner to allow the proper functioning of an item of equipment or a system.

h. **Replace.** To remove an unserviceable item and install a serviceable counterpart in its place. "Replace" is authorized by the MAC and assigned maintenance level is shown as the 3d position code of the Source Maintenance, and Recoverability (SMR) code.

i. **Repair.** The application of maintenance services [1] including fault location/troubleshooting[2], removal/installation and disassembly/assembly[3] procedures, and maintenance actions[4] to identify troubles and restore serviceability to an item by correcting specific damage, fault, malfunction, or failure in a part, subassembly, module (component or assembly), end item, or system.

j. **Overhaul.** That maintenance effort (service/action) prescribed to restore an item to a completely serviceable/operational condition as required by maintenance standards in appropriate technical publications, i.e., DMWR. Overhaul is normally the highest degree of maintenance performed by the Army. Overhaul does not normally return an item to like new condition.

k. **Rebuild.** Consists of those service/actions necessary for the restoration of unserviceable equipment to a like new condition in accordance with original manufacturing standards. Rebuild is the highest degree of material maintenance applied

---

[1] Services - Inspect, test, service, adjust, align, calibrate, and/or replace.

[2] Fault location/troubleshooting - The process of investigating and detecting the cause of equipment malfunctioning; the act of isolating a fault within a system or unit under test (UUT).

[3] Disassembly/assembly - The step-by-step breakdown (taking apart) of a spare/functional group coded item to the level of its least component, that is assigned an SMR code for the level of maintenance under consideration (i.e., identified as maintenance significant).

[4] Actions - Welding, grinding, riveting, straightening, facing, machining, and/or resurfacing.

to Army equipment. The rebuild operation includes the act of returning to zero those age measurements (e.g., hours/miles) considered in classifying Army equipment/components.

SECTION II. Maintenance Allocation Chart

B.3 EXPLANATION OF COLUMNS IN THE MAC, TABLE B-1

a. **Column 1, Group Number.** Column 1 lists functional group code numbers, the purpose of which is to identify maintenance significant components, assemblies, subassemblies, and modules with the next higher assembly.

b. **Column 2, Component/Assembly.** Column 2 contains the names of components, assemblies, subassemblies, and modules for which maintenance is authorized.

c. **Column 3, Maintenance Function.** Column 3 lists the functions to be performed on the item listed in Column 2. (For detailed explanation of these functions, see Paragraph B-2).

d. **Column 4, Maintenance Level.** Column 4 specifies each level of maintenance authorized to perform each function listed in Column 3, by indicating work time required (expressed as man-hours in whole hours or decimals) in the appropriate subcolumn. This work-time figure represents the active time required to perform that maintenance function at the indicated level of maintenance. If the number or complexity of the tasks within the listed maintenance function vary at different maintenance levels, appropriate work-time figures are to be shown for each level. The work-time figure represents the average time required to restore an item (assembly, subassembly, component, module, end item, or system) to a serviceable condition under typical field operating conditions. This time includes preparation time (including any necessary disassembly/ assembly time), troubleshooting/fault location time, and quality assurance time in addition to the time required to perform the specific tasks identified for the maintenance functions authorized in the maintenance allocation chart. The symbol designations for the various maintenance levels are:

C	Crew or Operator maintenance
O	Organization or Unit maintenance
F	Direct support maintenance
L	Specialized Repair Activity (SRA)[5]
H	General support maintenance
D	Depot maintenance

[5] This maintenance level is not included in Section II, column (4) of the Maintenance Allocation Chart. Functions to this level of maintenance are identified by a work-time figure in "H" column of Section II, column(4), and an associated reference code is used in the Remarks column (6). This code is keyed to Section IV, Remarks, and the SRA complete repair is explained there.

e. **Column 5, Tools and Test Equipment Reference Code.** Column 5 specifies, by code, those common tools, sets (not individual tools), common TMDE, and special tools, special TMDE, and special support equipment required to perform the designated function. Codes are keyed to tools and test equipment in Section III.

f. **Column 6, Remarks Code.** When applicable, this column contains a letter code, in alphabetical order, which is keyed to the remarks contained in Section IV.

Table B-1 Maintenance Allocation Chart (MAC) for the CAISI

(1) GROUP NUMBER	(2) COMPONENT/ASSEMBLY	(3) MAINTENANCE FUNCTION	(4) MAINTENANCE LEVEL					(5) TOOLS AND EQUIPMENT	(6) REMARKS CODE
			UNIT		DSU	GSU	DEPOT		
			C	O	F	H	D		
00	CAISI	Inspect	0.3						
		Inspect		0.3					
		Repair	0.3						
		Repair		0.3					
		Repair					X		
01	CAISI Bridge Module (CBM)	Inspect	0.1						
		Inspect		0.1					
		Test	0.3						A
		Test		0.3					B
		Repair					X		C
02	CAISI Client Module (CCM)	Inspect	0.1						
		Inspect		0.1					
		Test	0.3						A
		Test		0.3					B
		Repair					X		C
03	System Support Representative Accessory Kit	Inspe ct	0.1						
		Inspect		0.1					
		Test	0.3						A
		Test		0.3					B
		Repair	0.2						D
		Repair		0.2					D
		Repair					X		C
04	Antenna Group	Inspect	0.1						
		Inspect		0.1					
		Test	0.3						
		Repair		0.2			X		F
05	Mast AB-1244/GRC	Test	0.1						
		Test		0.1					
		Replace		0.3					
		Repair		0.2			X		F

Section III TOOL AND TEST EQUIPMENT REQUIREMENTS

B.4 EXPLANATION OF COLUMNS IN TOOLS AND TEST EQUIPMENT TABLE B-2

a. **Column 1, Tool or Test Equipment Reference Code.** The tool or test equipment reference code correlates with a code used in the MAC, Section II, Column 5.

b. **Column 2, Maintenance Level.** The lowest level of maintenance authorized to use the tool or test equipment.

c. **Column 3, Nomenclature.** Name or identification of the tool or test equipment.

d. **Column 4, National Stock Number.** The National Stock Number of the tool or test equipment.

e. **Column 5, Tool Number.** The manufacturer's part number, model number or type number.

Table B-2 Tools and Test Equipment for CAISI

TOOL OR TEST EQUIPMENT REFERENCE CODE	MAINTENANCE LEVEL	NOMENCLATURE	NATIONAL/NATO STOCK NUMBER	TOOL NUMBER
1	O	Multimeter, Digital AN/PSM-45A	6625-01-139-2512	AN/PSM-45A

Section IV. REMARKS for CAISI

B.5 EXPLANATION OF COLUMNS IN REMARKS, SECTION IV.

a. **Column 1, Remarks Code.** The code recorded in Column 6, Section II.

b. **Column 2, Remarks.** This column lists information pertinent to the maintenance function being performed as indicated in the MAC, Section II.

Table B-3 Remarks for CAISI

REFERENCE CODE	REMARKS
A	System level repair consists of the replacement of the component (Line replaceable unit (LRU))
B	System administrator tests in accordance with system administrator troubleshooting procedures.
C	Test in accordance with unit level maintenance troubleshooting procedures.
D	Unserviceable CBM and CCM are forwarded to the DSU in accordance with AR 750-1. DSU will then forward unserviceable CBM andCCM to the appropriate FRA.
E	PMCS performed by the System Support Representative (SSR) beyond the service capability of the Operator/Unit .
F	Repair of OE-254/GRC antenna mast is in accordance with TM 11-5985-357-13.

Appendix C

COMPONENTS OF END ITEM (COEI) AND BASIC ISSUE ITEMS (BII) LISTS

Section I. INTRODUCTION

C.1 Scope

This work package lists COEI and BII for the CAISI to help you inventory items for safe and efficient operation of the equipment.

C.2 General

The COEI and BII information is divided into the following lists:

a. Components of End Item (COEI). Table C-1. This list is for informational purposes only and is not authority to requisition replacements. These items are part of the CAISI. As part of the end item, these items must be with the end item whenever it is issued or transferred between property accounts. Items of COEI are removed and separately packaged for transportation or shipment only when necessary. Illustrations are furnished to help you find and identify the items.

b. Basic Issue Items (BII). Table C-2. These essential items are required to place the CAISI in operation, operate it, and to do emergency repairs. Although shipped separately packaged, BII must be with the CAISI during operation and when it is transferred between property accounts. Listing these items is your authority to request/requisition them for replacement based on authorization of the end item by the Table of Organization and Equipment (TOE) / Modified Table of Organization and Equipment (MTOE). Illustrations are furnished to help you find and identify the items.

C.3 Explanation of Columns in the COEI List and BII List

a. Illustration. This column is divided as follows:

(1) Figure Number. Indicates the figure number of the illustration on which the item is shown.

(2) Item Number. The number used to identify item called out in the illustration.

b. National Stock Number (NSN). Indicates the National Stock Number assigned to the item and which will be used for requisitioning.

c. Description. Indicates the Federal item name and, if required, a minimum description to identify the item. The part number indicates the primary number used by the manufacturer, which controls the design and characteristics of the item by means of

its engineering drawings, specifications, standards, and inspection requirements to identify the item or range of items. Following the part number, the Federal supply code for manufacturers (FSCM) is shown in parentheses.

d. Location. The physical location of each item listed is given in this column. The lists are designed to inventory all items I one area of the major item before moving on to an adjacent area.

e. Usable on Code. When applicable, gives you a code if the item you need is not the same for different models of equipment. These codes are identified below:

f. Quantity Required (QTY Req'd). This column lists the quantity of each item required for a complete major item.

g. Quantity. This column is left blank for use during an inventory. Under the RCVD (Received) column, list the quantity you actually receive on your major item. The DATE columns are for your use when you inventory the major item.

Table C-1 CAISI Components of End Item (COEI)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-1		5820-01-487-4020 Z53098 OL-701/TYQ	CAISI BRIDGE Module – processor, communications, Gateway A3269821	CBM Transit case	N/A	TBD		
C-1	1		CBM Transit Case Ruggedized Toby-CBM ECS # 11522			1		
			ONE CBM CONSISTS OF:					
C-1	2		One CBM Chassis	Main compartment	N/A			
			CONSISTING OF:					
C-2	1		Wireless Bridge Cisco Aironet AIR-BR352 Cisco #AIR-BR350-A-K9	CBM Chassis		1		

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-2	2		DSL Bridge ADC 300SBP (formerly Pairgain)	CBM Chassis		1		
C-2	3		Hub, Addtron or Farallon, 9-port (8 10Base-T and 1 10Base-2 port) Farallon #PN520/8A-1	CBM Chassis		2		
C-2	4		Inline Encryptor Air Fortress AF-1100	CBM Chassis		1		
C-2	5		Power Supply & Injector for wireless bridge Cisco AIR-PWR 34-1537-01 (Power supply) Injector – Cisco AIR-PWRINJ	CBM Chassis		1		
C-2	6		Power Supply for DSL bridge	CBM Chassis		1		
C-2	7		Power Supply for hubs & encryptor (3-lead) Custom 125PIE02-563W-C7AC	CBM Chassis		1		
C-2	8		"T" Connector AIM27-8140	CBM Chassis		2		
			50-ohm Terminator AIM27-9008	CBM Chassis		2		
C-2	9		18-inch coaxial 10Base-2 Cable	CBM Chassis		1		

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-2	10		Lightning Arrestor Polyphaser PSX	CBM Chassis		1		
C-2	11		12-inch RF Antenna Cable Talley SRCA24GP-1	CBM Chassis		1		
C-2	12		Ethernet Cables (2 red crossover and 2 white straight-through)	CBM Chassis		2 red 2 white		
C-1	3		UPS Tripplite 300 UPS	Main compartment		1		
C-1	4		7-inch Panel Antenna AAI00079	Top compartment		1		
C-1	5		40-inch break-apart Whip Antenna ODN12-2400BA	Top compartment		1		
C-1	6		25-foot RF Antenna Cable Andrew Corp F2A-PNMNR-25-USA	Top compartment		1		
			35-foot RF Antenna Cable Andrew Corp F2A-PNMNR-35-USA	Top compartment		1		

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-1	7		Barrel Connector (Double "N" Cable Adapter) RF Industries RFN-1013-1	Main compartment		1		
C-1	8		Antenna Bracket 7-inch TYAD-F	Top compartment		1		
C-1	9		Grounding Strap TYAD CON 1394	Top compartment		1		
C-1	10		3-prong Power Cord	Top compartment		1		
C-1	11		2-prong Power Cord	Top compartment		2		
C-1	12		Ethernet Cables (1 red crossover and 1 white straight-through)	Top compartment		1 red 1 white		
C-1	13	4010-01-072-4414	42-foot Guy Rope Red-clips SM-D-659410-GP1	Top compartment		4		
C-1	14	8130-00-355-7616	Reel, Assembly RL-28 SC-D-1064	Top compartment		2		
C-5		5820-01-487-4023 Z53056 OL-700/TYQ	CAISI Client Module – Processor, Bridge A3269822	CCM Carrying Case		TBD		
C-5	1		CCM Carrying Case Vinyl Toby-CCM pack			1		
			ONE CCM CONSISTS OF:					

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-5	2		CCM Chassis	Chassis compartment	N/A	1		
			Consisting of:					
C-7	1		Multi-client Radio Adapter – CISCO Aironet WorkGroup Bridge (WGB342R / WGB352R)	CCM Chassis		1		
C-7	2		Inline Encryptor Air Fortress AF-1100	CCM Chassis		1		
C-7	3		Hub, Addtron or Farallon, 9-port (8 10Base-T and 1 10Base-2 port) Farallon #PN520-8A-1	CCM Chassis		1		
C-7	4		Power Supply for Radio, Encryptor & Hub (3-lead) Custom 125PIE02-563W-C7AC	CCM Chassis		1		
C-7	5	5685-00-670-0871	"T" Connector AIM27-8140	CCM Chassis		1		
		5985-01-397-1999	50-ohm Terminator AIM27-9008	CCM Chassis		2		
C-7	6		Lightning Arrestor Polyphaser PSX	CCM Chassis		1		

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-7	7		12-inch RF Antenna Cable Talley SRCA24GP-1	CCM Chassis		1		
C-7	8		Ethernet Cables (1 red crossover and 1 white straight-through)	CCM Chassis		1 red 1 white		
C-5	3		24-inch 9 dbi Omni-directional Whip Antenna ODN9-2400FG	Main compartment		1		
C-5	4		35-foot RF Antenna Cable Andrew Corp F2A-PNMNR-35-USA	Main compartment		1		
C-5	5		Antenna Bracket TYAD-F	Misc compartment		1		
C-5	6		Grounding Strap TYAD CON 1394	Misc compartment				
C-5	7		White Straight-Through Ethernet Cable	Misc compartment		1		
C-5	8		2-prong Power Cord	Misc compartment		1		
C-8		7025-01-487-4021	Legacy Support Adapter – Interface Unit, ADP	LSA Transit Box		TBD		

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
			ONE LSA CONSISTS OF:					
C-8	1		Micro Serial Server 100/10 with 110-220 power supply MSS 100-01	Stored with STAMIS computer		1		
C-8	2		9-to-25 pin Null Modem Cable RS232 Null cable	Stored with STAMIS computer		1		
C-8	3		White Straight-Through Ethernet Cable	Stored with STAMIS computer		1		
C-8	4		Power Supply, 5V	Stored with STAMIS computer		1		
C-8	5		3-prong Power Cord	Stored with STAMIS computer		1		
C-9		5999-01-487-2681 Z00057 MK-2975/TYQ	SSR Accessory Kit, Electronics Equipment A3269820	1 transit case, 1 notebook case and 2 carrying cases: SSR Transit Case SSR Notebook Case SSR Antenna Carrying Case SSR Antenna Mast Carrying Case		TBD		
C-9	1		Transit Case for SSR, Ruggedized, Rolling Toby-SSR Box ECS #11671 SSR Transit case consists of:					
C-9	2		Inline Encryptor Air Fortress, AF1100	Main compartment		1		

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-9	3		UPS Tripplite 300 UPS	Main compartment		1		
C-9	4		Wireless Bridge Cisco Aironet AIR-BR352 Cisco AIR-BR350-A-K9	Main compartment		1		
C-9	5		Multi-Client Radio Adapter – CISCO Aironet WorkGroup Bridge (WGB342R / WGB352R)	Main compartment		1		
C-9	6		DSL Bridge – Digital Subscriber Line Modem bridge ADC 300SBP (formerly Pairgain)	Main compartment		1		
C-9	7		Cable Router / Firewall Network Translator Linksys BEFSR81 (Future version – Netscreen – 5xp, NS-5XP-101, Qty 2)	Main Compartment		1		
C-9	8		Hubs, Addtron or Farallon, 9-port (8 10Base-T and 1 10Base-2 port) Farallon PN520/8A-1	Main compartment		2		

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-9	9		10 Base-T Transceiver AT-210TS	Main compartment		1		
C-9	10		40-inch break-apart Whip Antenna ODN12-2400BA	Top compartment		2		
C-9	11		4-inch Whip Antenna AIR-ANT4941	Top compartment		2		
C-9	12		Lightning Arrestor & Bracket (Lightning Arrestor Assembly) Polyphaser PSX	Top compartment		2		
C-9	13		Grounding Strap TYAD CON 1394	Top compartment		2		
C-9	14		12-inch RF Antenna Cable N (M) to RPTNC (M) Talley SRCA24GP-1	Top compartment		2		
C-9b	15		12-inch RF Antenna Cable N (M) to RPTNC (F) Talley TIMA24HP-1	Top compartment		2		
C-9b	16		Adapter, N (M) to N (M) right angle Federal Custom Cable # A198	Top compartment		2		

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-9b	17		Antenna "Dummy Load" N (M), 50 ohm AIM Electronics Corp # 26-8023	Top compartment		2		
C-9b	18		White Ethernet Straight-through Cables CAT-5 Standard wiring T68B to T68B	Top compartment		4		
C-9b	19		Red Ethernet Cables Crossover Standard wiring T68A to T68B	Top compartment		4		
C-9b	20		Adapter, RJ-45 (F) to RJ-45 (F) Straight-through RJ-45 Line coupler	Top compartment		3		
C-9b	21		Adapter, RJ-45 (F) to RJ-45 (F) Crossover RJ-45 Line coupler	Top compartment		3		
C-9b	22		9-pin Straight-through serial extension cable (M-F) (blue)	Top compartment		1		
C-9b	23		9-pin Crossover Serial Cable (F-F) (beige)	Top compartment		1		
C-9b	24		9-to-25 pin Null Modem Cable RS232 Null cable (only if LSA was issued)	Top compartment		1		

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-9b	25		Reset Tool, 1/16" dia. X 4" min length Pin Punch Enco 240-2054 Mil spec: GGG-P-831E	Top compartment		3		
C-9b	26		Power Supply & Injector for Wireless Bridge Cisco AIR-PWR 34-1537-01 (Power supply) Injector – Cisco AIR-PWRINJ	Main compartment		1		
C-9b	27		Power Supply for DSL bridge	Main compartment		1		
C-9b	28		Power Supply for Linksys Router	Main compartment		1		
C-9b	29		Power Supply, 5V, 3 lead Custom 125PIE02-563W-C7AC	Main compartment		2		
C-9b	30		Power Supply, 5V, 1 lead, Wall style	Main compartment		5		
C-9b	31		2-prong Power Cord	Main compartment		3		
C-9b	32		3-prong Power Cord custom 125PIE02-563W-C7AC	Main compartment		2		
C-9b	33		3-prong, 1-foot Power Cord NEMA 5-15P to NEMA 5-15R	Main compartment		5		

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-12			SSR Notebook Case consists of:					
C-12	1		Transit Case Hardigg Storm IMI2400			1		
C-12	2		SSR Notebook – MITAC 7020 / 7251 Alternate models must be tested by CAISI	Main compartment		1		
C-12	3		Power Supply for Notebook Computer	Main compartment		1		
C-12	4		Power Cord for Power Supply	Main compartment		1		
C-12	5		Wireless NIC 340 Series 11 Mbps DSSS PC Card w/128-bit WEP w/o antenna AIR-LMC342 / LMC352	Main compartment		1		
C-12	6		2.2 dBi Diversity "Rabbit Ear" External Antenna AIR-ANT3342 Telex # 2428AA	Main compartment		1		
C-12	7		Xircom Wired NIC RealPort 10/100 PC-Bus card RealPort CardBus RBE-100BTX	Main compartment		1		

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-12	8		White Ethernet Cable Straight-through CAT-5 Standard wiring T68B to T68B	Main compartment		1		
C-12	9		Red Ethernet Cable Crossover Standard wiring T68A to T68B	Main compartment		1		
C-12	10		Adapter, RJ-45 (F) to RJ-45 (F) Straight-through RJ-45 Line coupler	Main compartment		1		
C-12	11		Adapter, RJ-45 (F) to RJ-45 (M) Crossover RJ-45 Line coupler	Main compartment		1		
C-12	12		9-pin Straight-through serial extension cable (M-F) (blue)	Main compartment		1		
C-12	13		9-pin Crossover Serial Cable (F-F) (beige)	Main compartment		1		
C-12	14		Adapter Cable MMCX to N (F) Talley SRCSP316-12MM9NFB	Main compartment		1		
C-12	15		Adapter Cable MMCX to RPTNC (F) Talley SRCSP316-12MM9TFRP	Main compartment		1		

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-12	16		Adapter, N (M) to N (M) right angle Federal Custom Cable # A198	Main compartment		1		
C-12	17		Antenna "Dummy Load" N (M), 50 ohm AIM Electronics Corp # 26-8023	Main compartment		1		
C-12	18		Reset Tool, 1/16" dia. X 4" min length Pin Punch Enco 240-2054 Mil spec: GGG-P-831E	Main compartment		1		
C-12	19		Baseline CD Version Z13-4B-xx (replace xx's with specific version)	Lid compartment		1		
C-14			SSR Antenna Carrying Case consists of:					
C-14	1		Carrying Case TYAD-SSR Cable pack			1		
C-14	2		50-foot RF Antenna Cable F2A-PNMNR-50-USA	Outer compartments (2 in each)		4		
C-14	3		14-inch Panel Directional Antenna 18 dBi AAI00096	Center compartment		2		

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-14	4		7-inch Panel Antenna Bracket TYAD-F	Outer compartments (1 in each)		2		
C-14	5		14-inch Panel Antenna Bracket TYAD-G	Outer compartments (1 in each)		2		
C-14	6		Double "N" Cable Adapter (Barrel Connector) RF Industries RFN-1013-1	Outside pouch		4		
C-14	7	4010-01-072-4414	42-Foot Guy Rope (Red Clips) (80063) SM-D-659410-GP1	Outer compartment		4		
C-14	8	8130-00-355-7616	Reel Unit For Guy Ropes (Containing Above, Four Guy Ropes Per Reel Unit) RL-28 SC-D-1064	Outer compartments		2		
C-14	9	5985-01-073-6103	Guy Stakes (80063) SM-C-659375	Outer compartments		4		
C-16	1		SSR Antenna Mast Carrying Case consists of:					
C-16		5985-01-072-4339	Carrying Case BG-1244			1		
C-17		5985-01-324-3461	AB-1244B/GRC 30 ft Mast kit (12 poles) A3002867 Consists of:					
C-16		5985-01-324-3463	Upper Mast Section (80063) A3159899	Mast Section		5		
C-16		5985-01-324-3462	Lower Mast Section (80063) A3159892	Mast Section		5		

Table C-1 CAISI Components of End Item (COEI) (Continued)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
C-16		5985-01-326-5533	Upper Mast Adapter Section (Red Ring) (80063) A3159902	Mast Section		1		
C-16		5985-01-327-1448	Lower Mast Adapter Section (Blue Ring) (80063) A3159895	Mast Section		1		
C-16		5985-01-072-4414	36-Foot Guy Rope (Blue Clips) (80063) SM-D-659410-GP2	Mast Section		4		
C-17		4010-01-072-4414	42-Foot Guy Rope (Red Clips) (80063) SM-D-659410-GP1	Mast Section		4		
C-17		8130-00-355-7616	Reel Unit For Guy Ropes (Containing Above, Four Guy Ropes Per Reel Unit) RL-28 SC-D-1064	Mast Section		2		
C-17		5985-01-073-6103	Guy Stakes (80063) SM-C-659375	Pocket Section		4		
C-17		5985-01-072-8018	Mast base assembly (80063) SM-D-659263	Pocket Section		1		
C-17		5985-01-122-3959	Base Plate (80063) SC-B-659275	Pocket Section		1		
C-17		4030-01-072-8017	Base Plate Pins (80063) SC-B-729924	Pocket Section		2		
C-17		4030-01-074-7881 4030-01-072-8126	Guy Rings (One Red, One Blue) (80063) SM-B-659290-1 SM-B-659290-2	Pocket Section		2		
C-17		5975-01-072-4496	Strain Relief Clamp, Electircal Conductor PF-211/G: (80063) SC-DL-142-03	Pocket Section		1		
C-17		5120-00-203-4656	2.5 Pound Sledge Hammer (81348), Type X, Class I, GGG-H-86C	Pocket Section		1		

CAISI Bridge Module

Major Components

All of the below items are located in the CBM Transit Case.

1

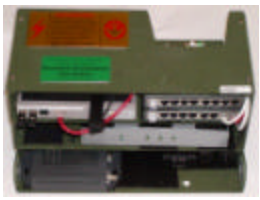
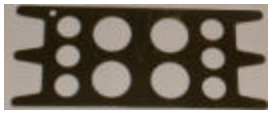
2 CBM Chassis 	3 UPS	4 7-inch Panel Antenna
5 40-inch Break-apart Whip Antenna	6 RF Antenna Cable (25 & 35 feet)	7 Double "N" Cable Adapter (Barrel Connector)
8 Antenna Bracket (7-inch)	9 Grounding Strap	10 3-prong Power Cord
11 2-prong Power Cord (Qty 2)	Ethernet Cables (1 Red Crossover and 1 White Straight-through) 12	Antenna guy rope on reel (42-ft) (red) (Qty 4) (two per reel) 13
14 Reel Unit (RL-28) (Qty 2) 		

Figure C-1 CBM Components of End Item

The **CBM Chassis** includes the following components installed in the chassis.

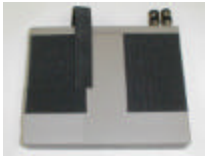
1 Wireless Bridge	2 DSL Bridge 	3 Hub (Qty 2)
4 Inline Encryptor	5 Power Supply & Power Injector for Wireless Bridge	6 Power Supply for DSL Bridge
7 Power Supply for Hubs & Encryptor	8 Terminators & "T" connectors (2 of each)	9 18-inch Coaxial 10Base-2 Cable
10 Lightning Arrestor	11 12-inch RF Antenna Cable	12 Ethernet Cables (2 Red Crossover and 2 White Straight-through)

Figure C-2 CBM Chassis Components of End Item

Figure C-3 CBM Transit Case – Main Compartment

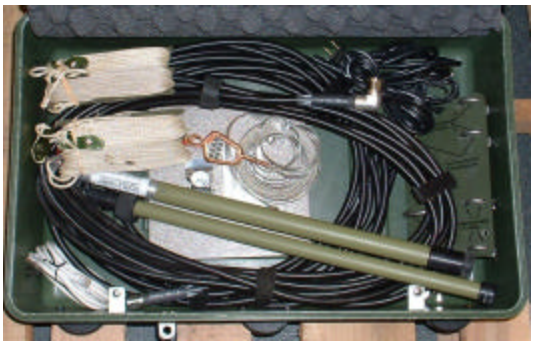


Figure C-4 CBM Transit Case – Top Compartment (Lid Section)

CAISI Client Module

Major components

The below items are components of the CCM and are located in the carrying case.

1

2 CCM Chassis	3 24-inch Whip Antenna	4 35-foot RF Antenna Cable

5 Antenna Bracket (7-inch)	6 Grounding Strap	7 White Straight-through Ethernet Cable	8 2-prong Power Cord

Figure C-5 CCM Components of End Item

Main (Cable and Antenna) Compartment	
Bracket and Misc Compartment	**CCM Chassis Compartment**

Figure C-6 CCM Carrying Case – Compartments

The **CCM Chassis** includes the following components installed in the chassis.

1 Multi-Client Radio Adapter	2 Inline Encryptor	Hub 3
Power Supply for Radio, Encryptor & Hub 4	Terminators (Qty 2) & "T" Connector (Qty 1) 5	Lightning arrestor 6
12-inch RF antenna cable 7	Ethernet Cables (1 Red Crossover and 1 White Straight-through) 8	

Figure C-7 CCM Chassis Components of End Item

CAISI Legacy Support Adapter

LSA Components

1 Legacy Support Adapter MSS-100 	2 9-to-25 Null Modem Cable 	3 White Straight-Through Ethernet Cable
4 Power Supply, 5V 	5 3-prong Power Cord 	

Figure C-8 LSA Components of End Item

CAISI SSR Accessory Kit

Major Components of the SSR Accessory Kit stored in the SSR Transit case.

1

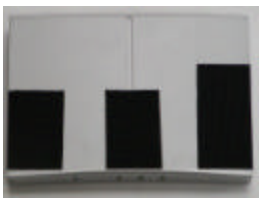
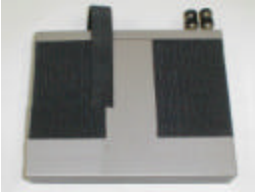
2 Inline Encryptor (Qty 2) 	3 UPS	4 Wireless Bridge
5 Multi-Client Radio Adapter	6 DSL Bridge 	7 Router
8 Hub (Qty 2)	9 10Base-T Transceiver	10 40-inch break-apart Whip Antenna (Qty 2)
11 4-inch whip antenna (Qty 2)	12 Lightning Arrestor Assembly (Qty 2)	13 Grounding Strap (Qty 2)
14 12-inch RF Antenna Cable N (M) to RPTNC (M) (Qty 2)	15 12-inch RF Antenna Cable N (M) to RPTNC (F) (Qty 2)	16 Adapter, Right Angle (N-M to N-M) (Qty 2)

Figure C-9 SSR Accessory Kit – Transit Case Components

50 Ohm, Antenna "Dummy Load" (N-M) (Qty 2) 17 	White Straight-through Ethernet Cable (Qty 4) 18 	Red Crossover Ethernet Cable (Qty 4) 19
RJ-45 Straight-Through Adapter (Qty 3) 20 	RJ-45 Crossover Adapter (Qty 3) 21 	9-pin serial cable, straight (M-F) (blue) 22
9-pin serial cable, crossover (F-F) (beige) 23 	9-to-25 Null Modem Cable 24 	Reset Tool (Qty 3) 25
Power Supply & Power Injector for Wireless Bridge 26 	Power Supply for DSL Bridge 27 	Power Supply for Linksys Router (Version 1) 28
Power supply, 5V, 3 lead (Qty 2) 29 	Power Supply, 5V, 1 lead (Qty 5) 30 	2-prong Power Cord (Qty 3) 31
3-prong Power Cord (Qty 2) 32 	3-prong, 1-foot Power Cable (Qty 5) for use with Power Supply, 5V, 1 lead 33 	**NOTE:** *Power supply for version 2 of the Linksys Router is different. Power supply is the 5V, 1 lead in box 30. With version 2 router, qty for box 30 and box 33 is 6.*

Figure C-9b SSR Transit Case Components - continued

Figure C-10 SSR Transit Case – Main Compartment

Figure C-11 SSR Transit Case – Top Compartment (Lid Section)

CAISI SSR Accessory Kit
Quick Reference Card

SSR Notebook Case

1

The following items are packed in the **SSR Notebook case.**

2 SSR Notebook	3 Power Supply for Notebook Computer	4 2-prong power cord
5 Wireless NIC	6 "Rabbit Ears" Antenna	7 Wired NIC (if issued)
8 White Straight-through Ethernet Cable	9 Red Crossover Ethernet Cable	10 RJ-45 Straight-Through Adapter
11 RJ-45 Crossover Adapter	12 9-pin serial cable, straight (M-F) (blue)	13 9-pin serial cable, crossover (F-F)
14 Adapter Cable, MMCX to N (F)	15 Adapter Cable, MMCX to RPTNC (F)	16 Adapter , Right Angle (M-M)
17 50 Ohm Antenna "Dummy Load" with "N" (M) connector	18 Reset Tool	19 Baseline CD

Figure C-12 SSR Notebook Case Components

Figure C-13 SSR Notebook Case – Main Compartment

CAISI SSR Accessory Kit
Antenna Carrying Case

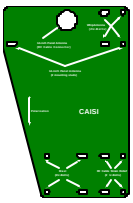
1 Carrying Case	2 50-foot RF Antenna Cable (Qty 4)	3 14-inch Panel Antenna (Qty 2)
4 7-inch panel Antenna Bracket (Qty 2)	5 14-inch Panel Antenna Bracket (Qty 2) 	6 Double "N" Cable Adapter (Barrel Connector) (Qty 4)
7 Antenna guy rope on reel (42-ft) (red) (Qty 4) (two per reel)	8 Reel Unit RL-28 (Qty 2)	9 Antenna guy stake (Qty 4)

Figure C-14 SSR Antenna Carrying Case Components

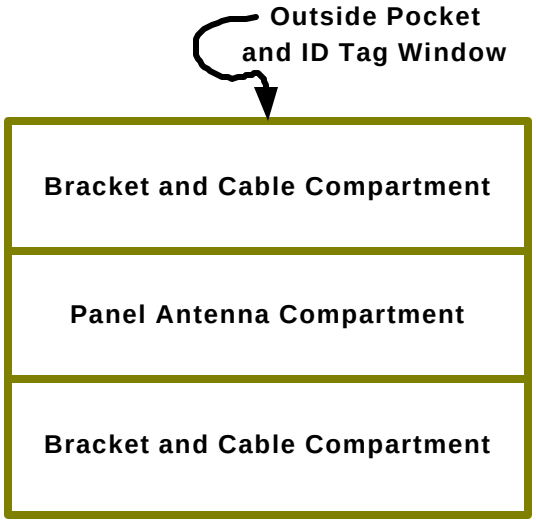


Figure C-15 SSR Antenna Carrying Case Layout

SSR Antenna Mast Carrying Case

Figure C-16 SSR Antenna Mast Carrying Case

The SSR Antenna Mast Carrying Case consists of the Antenna mast sections and the Antenna Mast Kit. This is the AB-1244B/GRC antenna mast. Both are shown below:

Figure C-17 Antenna Mast Sections

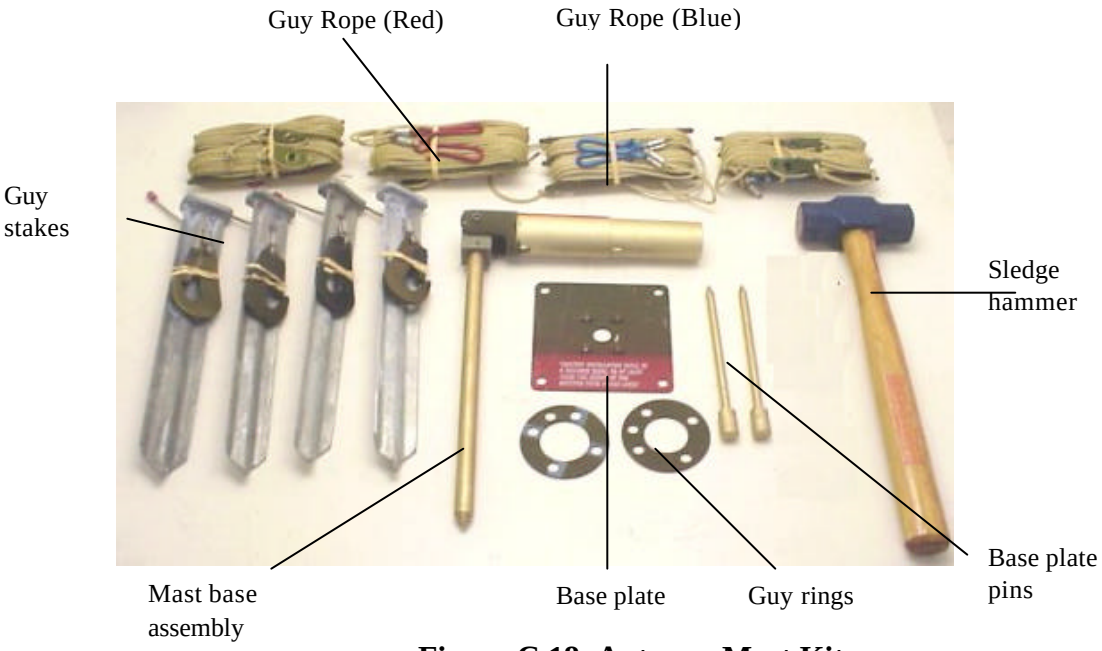


Figure C-18 Antenna Mast Kit

Table C-2 CAISI Basic Issue Items (BII)

(1)		(2)	(3)	(4)	(5)	(6)	(7)	
ILLUSTRATION		NATIONAL	DESCRIPTION	LOCATION	USEABLE	QTY	QUANTITY	
(A)	(B)	STOCK			ON	REQ'D	RCVD	DATE
FIG	ITEM	NUMBER	PART NO. CAGE		CODE			
NO.	NO.							
		5820-01-487-4020 OL-701/TYQ	CAISI Bridge Module (CBM) - Processor, Communications Gateway A3269821		N/A			
		5820-01-487-4023 OL-700/TYQ	CAISI Client Module (CCM) – Processor, Bridge A3269822					
		7025-01-487-4021	Legacy Support Adapter (LSA) – Interface Unit MSS100-01					
		5999-01-487-2681 MK-2975/TYQ	SSR Accessory Kit, Electronics Equipment A3269820					

Appendix D

ADDITIONAL AUTHORIZATION LIST (AAL)

Section I INTRODUCTION

D.1 GENERAL

This appendix lists additional items you are authorized for the support of the CAISI. The items identified herein are not provided with the CAISI and do not have to be turned in with it. These items are authorized by CTA, MTOE, TDA or JTA. **AAL items will be acquired by the gaining Unit if desired and at their expense.**

D.2 EXPLANATION OF COLUMNS IN THE AAL

a. Column (1) – National Stock Number (NSN). Identifies the stock number of the item to be used for requisitioning purposes.

b. Column (2) – Description, CAGE Code, and Part Number. Identifies the Federal item name and, if required, a description to identify the item. The last line below the description is the Commercial and Government Entity (CAGE) Code (in parenthesis), if applicable, and the part number.

c. Column (3) - Unit of Measure (U/M). Indicates the physical measurement or count of the item as issues per the National Stock Number shown in column (2). This measure is expressed by a two-character alphabetical abbreviation (e.g., ea, in, pr).

d. Column (4) - Qty Auth. Indicates the quantity authorized.

Section II Additional Authorization List

Table D-1 Additional Authorization List (AAL)

(1) NATIONAL STOCK NUMBER	(2) DESCRIPTION CAGE CODE, AND PART NUMBER	(3) UNIT OF MEAS	(4) QTY AUTH
5820-01-487-4020 OL-701/TYQ	CAISI Bridge Module (CBM) - Processor, Communications Gateway A3269821		
5820-01-487-4023 OL-700/TYQ	CAISI Client Module (CCM) – Processor, Bridge A3269822		
7025-01-487-4021	Legacy Support Adapter (LSA) – Interface Unit MSS100-01		
5999-01-487-2681 MK-2975/TYQ	SSR Accessory Kit, Electronics Equipment A3269820		
	ACCESSORIES/OPTIONS		
	Camouflage pole		
	Gloves		
4240-00-052-3776	Goggles		
	Grounding Rod		
8470-01-092-7527	Helmet (Kevlar) - Large		
8470-01-092-7528	Helmet (Kevlar) - Small		

Appendix E

EXPENDABLE AND DURABLE ITEMS LIST

Section I INTRODUCTION

E.1 Scope

This appendix lists expendable and durable items that you will need to operate and maintain the CAISI. This list is for information only and is not authority to requisition the listed items. These items are authorized to you by CTA 50-970, Expendable Items(Except Medical, Class V, Repair Parts, and Heraldic Items).

E.2 Explanation of Columns in the Expendable/Durable Items List

a. Column (1) – Item Number. This number is assigned to the entry in the list as is referenced in the narrative instructions to identify the item (e.g., "Use cleaning compound, item 1, App. D").

b. Column (2) – Level. This column identifies the lowest level of maintenance that requires the listed item

C = Operator/Crew

O = Unit/AVUM

F = Direct Support/AVUM

H = General Support

D = Depot

c. Column (3) – National Stock Number (NSN). This is the NSN assigned to the item which you can use to requisition it.

d. Column (4) – Item Name, Description, Commercial and Government Entity (CAGE) Code, and Part Number (P/N). This column provides the other information you need to identify the item.

e. Column (5) – Unit of Measure (U/M). This code indicates the measure used in performing the actual maintenance function. This measure is expressed by a two-character alphabetical abbreviation (e.g., ea, in, pr). If the unit of measure differs from the unit of issue, requisition the lowest unit of issue that will satisfy your requirements.

Table E-1 Expendable and Durable Items List

(1) ITEM NUMBER	(2) LEVEL	(3) NATIONAL STOCK NUMBER	(4) ITEM NAME, DESCRIPTION, CAGE CODE, PART NUMBER	(5) UM
	C		CAT-5 Crossover Cable	
	C		CAT-5 Ethernet Cable (different sizes)	
	C	5640-00-103-2254	Duct Tape (100-mile-n-hour tape)	RL
	C	5970-00-419-4291	Electrical Tape	RL
	O	8010-01-039-5939	Paint, Alkyd, Camouflage, Forest Green, MIL-E-52798	QT
	C	6150-01-281-1058	Power strip, Electrical Outlet, Surge protection	EA
	C		RG-58 Cable	
	C	5120-01-465-9828	Serial Cable – 9 pin to 25 pin	EA
	C	5685-00-670-0871	T-Connectors	EA
	C	5985-01-397-0871	Terminators	
	C		Velcro Straps	
	C		Washer	
	C		Wing Nuts	
	C	5110-01-177-7332	Wire stripper	
	C		Wire ties	
	C		Ziploc storage bags	

Appendix F

CAISI SECURITY AND PRIVACY CONSIDERATIONS

F.1 Security Functions.

Each installation and unit has local security officers who are assigned the responsibility to train and inform users of all the security policies and procedures. They inform higher authority whenever they believe a security violation exists. These are the:

1. Information System Security Manager (ISSM) or Information Systems Security Officer (ISSO).

2. System Support Representative (SSR, CSS S6, or other automated support personnel).

All responsibilities are based on AR 380-19, as brought forth here, as well as implementation of Army Information Security Programs within a given organization.

F.1.1 STAMIS and CSS User Responsibilities.

1. Work only within the STAMIS or approved CSS application software.

2. Operate CAISI components only within the bounds of system documentation.

3. Maintain an inventory of CAISI components under the user's control, and provide site security to ensure physical protection of CAISI as a high dollar item, in accordance with the unit Standard Operating Procedures (SOP).

4. Assume Physical Security responsibility (**main responsibility**) for CAISI components and connected communications cables under their control. Follow security guidelines in accordance with the unit SOP.

5. Immediately report suspected security breaches, and actual security breaches, to the CSS S6.

6. Report any suspicious system activity to the CSS S6 or unit ISSO.

F.1.2 SSR Security Responsibilities.

Unit commanders will designate at least one SSR (CSS S6, CSSAMO or other automated support personnel) for each CAISI. Although they work under the staff supervision of the CSS S6, each SSR must be trained and experienced on the CAISI that they are required to maintain. The SSR must ensure that all components of the CAISI are protected so that the CAISI can effectively and securely operate in the three operational modes: in garrison, in transit, and deployed.

SSR has the following **Security duties**:

1. Network Management

2. System Administration.

3. Troubleshoot LAN problems dealing with hardware and network operating system failures.

4. Information Technology associated with issuing and installing anti-virus software. Maintain the operating system and application software at the most current version. Apply patches immediately upon receipt from the U.S. Army Information Systems Software Command (USAISSC), Tobyhanna Army Depot (TYAD), or Project Officer (PO), CAISI. Check for and apply updates to anti-virus software and data files at least weekly.

5. Assist CSSAMO in troubleshooting hardware/software.

6. Oversees installation and maintenance of LAN supporting Division Support Command (DISCOM), Forward Support Battalion (FSB), Division Support Battalion (DSB), and Aviation Support Battalion (ASB).

7. Coordinates with Signal Division for connectivity.

8. In special circumstances, you will be required to erect an AB-1244B antenna mast using CAISI various antennas.

9. Secure, transport, set up and configure the CBMs, CCMs and LSAs. Supervise the connection of client circuits, and to monitor the CAISI to ensure continuous operations and availability.

SSR has the following **Security responsibilities.**

1. With the assistance of the CSS S6, prepare and obtain approval of site specific Protected Distribution Systems (PDS).

2. Maintain the operating system and application software at the most current version.

3. Maintain an inventory of CAISI components under the SSR's control, and provide site security to ensure physical protection of CAISI as a high dollar item, in accordance with the unit SOP.

4. Authorize access to the operational facility.

5. Destroy equipment prior to capture.

F.1.3 CSS S6 Responsibilities.

The CSS S6 is the overall CAISI administrator. The CSS S6 influences or conducts the interaction between the SSR, the CAISI users, and the security representatives of the command elements. The CSS S6 will often also serve as the unit ISSO or ISSM in this instance they will assume the ISSM or ISSO duties listed in Paragraph F-1.4 in addition to their CSS S6 responsibilities. Additionally, the CSS S6 occasionally assumes the duties of an SSR when the CAISI equipment is directly under his/her control. For a list of these responsibilities refer to the previous paragraph on SSR responsibilities.

The CSS S6 responsibilities are listed below:

1. Verify the requirement for an individual to access CAISI prior to establishing an account for them.

2. Establish and maintain user accounts.

3. Generate and issue passwords. At the time of issuing a password, brief the user on the following:

   a. Password classification and exclusiveness.

   b. Measures to safeguard the password.

   c. Prohibition against disclosure of the password.

   d. Requirement for the user to inform the CSS S6 or unit ISSO of password compromise, loss, or misuse

4. Maintain, review and archive the audit files for each CAISI for detection of possible system penetration, as frequently as time and the tactical situation allow, but at least weekly.

5. Ensure systems are operated in accordance with the Draft CAISI Technical Manual 11-5895-1691-12.

6. Exercise direct staff supervision over CAISI SSR personnel.

7. Report suspected or actual security incidents to the unit ISSO or ISSM.

F.1.4 ISSM or ISSO Responsibilities.

The unit ISSM or ISSO is responsible for the unit's overall information systems security management as well as the security management and security configuration of all Automated Information Systems (AIS), including the CAISI. Personnel should not be appointed ISSO if they have a vested interest in keeping CAISI operational at the expense of security.

The responsibilities of the unit ISSO are listed below:

1. Ensure systems are operated and maintained in accordance with AR 380-19.

2. Ensure managers, system administrators, and users have the appropriate personnel security clearances, authorizations, and need-to-know.

3. Include all personnel associated with the AIS in the system-specific and general awareness security training.

4. Prepare, distribute, and maintain plans, instructions, and guidance, in accordance with the unit SOP concerning security of system operations.

5. Report immediately to the next higher unit or installation ISSO or ISSM any attempt to gain unauthorized access to information, any system failure, and any compromise, which could lead to unauthorized disclosure, loss of integrity, or unavailability of system information.

6. Review and evaluate the security impact of system changes, including interfaces with other AIS.

7. Report security incidents and technical vulnerabilities to the ISSM per AR 380-19, AR 381-14 (S), AR 380-5, and AR 381-12.

8. Prepare or oversee the preparation of the accreditation and certification documentation.

9. Maintain a current network or AIS certification or accreditation statement and initiate re-accreditation and re-certification when changes affecting security have occurred.

10. Establish a procedure for issuing, protecting, and changing system passwords.

11. Oversee the review of system audit trails and resolve security violations or suspected security violations. Maintain access control records and ensure they reviewed at least weekly.

12. Ensure that an SSR is appointed for each workstation or group of workstations.

13. Ensure that foreign nationals have appropriate pre-employment checks prior to accessing CAISI.

14. In addition to item “7.” above, contact APM, CAISI and request intensive auditing of CAISI if malicious activity is suspected.

15. Review all security incident reports, cooperate in the investigation, and advise the commander during the investigation.

F.2 CAISI SSR Security Procedures.

This paragraph applies to CAISI System Support Representatives who are responsible to secure, transport, set up, and configure the CBMs, CCMs, and LSAs. If you are an SSR, or someone performing as an SSR, this paragraph is addressed specifically to you.

F.2.1 Operations Security (OPSEC).

The following activities should be observed to support OPSEC:

1. Operate CAISI only in an environment commensurate with the classification of the data being processed on the CAISI.

2. Orient the computer screen to minimize the possibility of observation by others without a need-to-know.

3. Do not share information obtained from CAISI with other individuals, unless their position requires them to know that information.

4. Do not use CAISI for personal purposes, e.g. personal mail or games.

5. Do not distribute manuals for CAISI to other individuals unless their position requires them to know that information.

6. Do not discuss vulnerabilities of CAISI except as necessary to orient users to protect it.

7. Maintain a security conscious workforce by practicing all available countermeasures, in accordance with the unit SOP.

8. Ensure all personnel having access to CAISI systems are identified and have a legitimate need-to-know.

9. In order to maintain accountability, do not turn over control of the workstation to another user without performing a logoff.

10. Always logoff when leaving the workstation.

F.2.2 Physical Security.

Physical security standards must be based on the following events as they pertain to the specific situation:

1. Wartime or Peacetime criticality.

2. Sensitivity Level of information processed.

3. Value of the information to the unit.

4. Value of the automated equipment.

Based on the considerations above, CAISI should be provided with a high level of physical security. The CAISI hardware is considered to be a high dollar value item and the information that passes through CAISI is critical to the conduct of US combat operations. A firm physical security foundation consisting of barriers and procedures to include structural standards, key control, lighting, lock application, inventory, and accountability will be employed in accordance with (IAW) AR 190-13. (Army Physical Security Program).

1. At a minimum CAISI will be treated and secured as a high value item IAW AR 190-51. (Security of Army Property at Unit and Installation Level).

2. CAISI will be maintained in a locked or guarded area during non-duty hours.

3. Sufficient physical security will be provided to ensure that CAISI is not lost, stolen, modified, damaged or destroyed and that the information that CAISI transmits is not impeded or modified.

4. Physical security will be enforced when transporting CAISI. A copy of the accreditation documentation should always be kept with the CAISI when the CAISI is moved. CAISI, even when not operational, will be provided security commensurate with its status as a high value item.

F.2.3 Software Security.

The CAISI application operates as part of the Trusted Computer Base (TCB). All personnel associated with CAISI will implement the following general security procedures to protect the CAISI against compromise, subversion, or unauthorized manipulation:

1. Public domain, shareware, or other privately acquired software is prohibited from being used on CAISI.

2. Hardware and Software modification will be made only as authorized by Assistant Project Manager (APM) CAISI.

3. Only personnel performing official duties will be allowed access to CAISI.

4. CAISI will only be used IAW documented procedures as described in the Software User's Manual, TB 11-5895-1691-10. Undocumented usage of CAISI must be reported to the CSS S6 to be properly evaluated and to determine if it caused any additional risk to CAISI.

5. To prevent CAISI operations and security from being compromised, the CSS S6 must ensure the software security implementations on the baseline are not modified.

F.2.4 Communications Security.

F.2.4.1 Use of the Inline Network Encryption Device

Though not a part of the CAISI program, CAISI interfaces to the Unclassified Packet Network through In-line Network Encryption (INE) device, either the Network Encryption System (NES) or the TACLANE (not an acronym, a KG-175 cryptographic device named "TACLANE"). The INE insures separation of the unclassified data from the classified data on the classified tactical network. **CAISI must never be connected to the tactical network without the use of an INE.**

F.2.5 Protected Distribution System (PDS).

While CAISI does not process or transmit classified information, it facilitates the exchange of Sensitive But Unclassified (SBU) information. At the present time it is not feasible for the entire CSS community that uses CAISI to utilize a common encryption capability. Therefore, a Protected Distribution System (PDS) will be established locally for the appropriate types of connections. For interfaces not suitable for a PDS the local commander may authorize their establishment after proper review of the relevant risks and countermeasures.

A PDS is a wireline or fiber-optics telecommunications system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.

A PDS must be established in accordance with AR 380-19, as described below. CAISI cannot be operated with a PDS until the PDS has been approved.

F.2.5.1 Cable Connections.

Paragraph 4-5 of AR 380-19 permits the establishment of a PDS so that SBU data can be transmitted on certain lines in clear text. A PDS must be site specific since the physical layout varies based on the situation. As such, it must be approved by the local commander. It is the responsibility of the CSS S6 to acquire a PDS approval.

The establishment of a PDS for CAISI remote digital subscriber line (DSL) bridge modules is appropriate, given the point-to-point nature and limited range nature of such connections. The connection is between two DSL modem bridges that are synchronized by a special protocol. Anyone trying to "tap" into the line would interfere with communications, thus precluding the interception of normal data traffic. In spite of this, however, the line must still be inspected periodically. Traffic could be intercepted with special equipment.

Similarly, the 10Base-T category-5 unshielded twisted pair and 10Base-2 coaxial cable must be protected. The coaxial cable is the most susceptible to interception and must be inspected closely.

The major requirement of a PDS is that it be sufficiently controlled to prevent covert penetration and interception. This requirement is satisfied in most tactical situations by the deployment of CAISI to an area entirely under the control of US forces. To insure that this requirement is met, the CSS S6 must insure that the following conditions are true:

1. The physical location of all cabling is under US control.

2. The cables are periodically inspected along their entire route with specific guidance given to search for illicit taps.

3. The cables are not routed along any conductor that could act as an antenna for stray signals, such as water pipes or electrical lines.

4. The cables are terminated at authorized CAISI connections, and responsibility for the security of the cable at the terminus is assigned to a specific individual.

5. The following cables should be included in your evaluation:

   a. DSL field wire line

   b. Network cables from your computers or LSA to the hubs in the CBMs or CCMs.

   c. The cable from the CAISI to the INE at the MSE node **must** be secured.

F.2.5.2 Wireless Local Area Network.

The CAISI wireless bridges and clients use encryption to ensure wire equivalent privacy (WEP) in accordance with IEEE (Institute of Electrical & Electronics Engineers) **standard 802.11b**. The CAISI bridges and clients use a 128-bit encryption key to protect the radio transmission. The entire packet is encrypted, not just the data load. Although this type of interface is defined as having the same security as the cabled portion of the network, it has been broken and is not sufficient to protect the SBU traffic.

Consequently, CAISI now includes an inline encryptor, the Air Fortress 1100 to protect over-the-air wireless transmissions. It utilizes 3DES (Triple Data Encryption Standard) encryption and is FIPS 140-1 compliant. It is therefore sufficient to protect SBU traffic. As such, it integrates well into the PDS.

The Air Fortress encryptor separates the SBU network from the unencrypted wireless portion of the CAISI network. This keeps intruders from intercepting SBU traffic or intruding onto the SBU network.

Because the Air Fortress protects the wireless segments of the network, it integrates well into the PDS.

NOTE: *The Air Fortress is not intended or certified to protect classified traffic. It is strictly for the SBU CAISI network.*

F.2.5.3 Mobile Subscriber Equipment - Circuit Switch.

At times, two STAMIS devices must communicate, even though they are each connected to a different CAISI, and are separated geographically. For these two STAMIS systems to communicate they require a connection through Mobile Subscriber Equipment (MSE) – Circuit Switch (CS). However, before the data gets onto the MSE tactical communications network, it is encrypted by an In-line Network Encryption (INE) device, currently the Motorola Network Encryption System (NES). SBU data is considered protected if it is encrypted, or if all communication remains in a PDS or if encryption and a PDS are used together. When STAMIS communications are routed through the NES and MSE, the SBU data is properly protected.

Therefore connections from STAMIS to STAMIS via MSE CS over Digital Nonsecure Voice Terminals (DNVT) Digital Subscriber Voice Terminals (DSVT), or Tactical Terminal Adapters (TTA) do not need the SSR to initiate a separate PDS for them. They are part of the MSE system and are included in the MSE PDS.

The CSS S6 is responsible, however, to ensure that the serial cable that connects the DNVT or TTA to the CAISI Legacy Support Adapters (LSA) is secure and not subject to illicit taps. The STAMIS user is responsible for the security of the serial cable from the STAMIS computer to the LSA.
Additionally, the cable from the CAISI to the INE at the MSE node must be secured as part of the CAISI PDS. This is because the information on the wire connecting the CAISI to the INE is part of the unencrypted local area network. The CSS S6 or CAISI System Administrator will periodically inspect the connection.

F.2.6 Commercial Modem Access.

1. **Unprotected commercial modem connection to CAISI is prohibited.**

2. **Encrypted modem connections** are allowed, if the following conditions are met.

   a. The encryption hardware or software is approved by the National Security Agency (NSA) or National Institute of Standards (NIST).

   b. The encryption is built-in to the modem, an in-line encryption device, or socket-level software.

The STAMIS user for this type of connection is responsible for providing the appropriate encryption to support commercial modems. The CAISI Fielding Plan does not include the deployment of NSA or NIST-approved communications security (COMSEC) hardware or software. Therefore, if a STAMIS equipped unit wishes to utilize the public telephone system for their interfaces, they are responsible for providing, maintaining, and the testing of their approved COMSEC equipment with CAISI.

3. **Unencrypted but protected modem connection** is allowed under either of the following conditions.

   a. Connection is over U.S. tactical telephone systems where the system is protected by bulk encryption devices. Generally this means use of a Tactical Terminal Adapter (TTA) connected to the tactical packet network (TPN).

   b. Both ends ***and the entire circuit path*** are over a U.S. military telephone system, and the system is approved by the commander as a protected distribution system (PDS). Generally this means that both ends are on the same physical installation and a military switch provides the telephone service.

Commercial modems connected to a non-US-military-controlled telephone system cannot be protected by a PDS. STAMIS systems that wish to utilize the commercial telephone system but cannot provide NSA or NIST-approved COMSEC **may not do so**.

Knowledge of phone numbers associated with modems connected to commercial networks will be limited to those STAMIS systems requiring that interface.

F.2.7 Security Training.

All personnel who manage, design, develop, maintain, or operate CAISI will undergo a training and awareness program consisting of the following:

1. An initial security training and awareness briefing. This briefing may be generic to Automated Information System (AIS), but must also include specific information tailored to CAISI.

2. Periodic security training and awareness. This may be satisfied by the unit's current security awareness and training policy through the use of Subversion and Espionage Directed Against the U.S. Army (SAEDA) briefings, posters, bulletins or films.

F.2.8 Miscellaneous Provisions.

F.2.8.1 Marking of Output.

All output of CAISI should be initially marked as being SBU until the output can be reviewed. After proper review if the material is deemed not to contain SBU information the output can be administratively downgraded to the proper level. This requirement includes any hardcopy printouts or removable media. Output will be protected as SBU until downgraded or destroyed.

F.2.8.2 Access by Foreign Nationals.

The Commander or unit ISSO will ensure that foreign nationals have appropriate pre-employment checks prior to accessing CAISI. Access to CAISI by foreign nationals will be limited to that described in their Limited Access Authority (LAA). An appropriately cleared US person will supervise all activities of a foreign national on CAISI. The LAA will be reviewed annually.

F.2.8.3 Access by Maintenance Personnel.

Access to SBU information does not require a security clearance. But civilian, military, consultant, and contractor personnel must meet the requirements of an automated data processing (ADP) level I, II or III position (see AR 380-67) to perform maintenance on the CAISI.

1. ADP-I positions include, but are not limited to, positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software. (AR 380-67, Appendix K).

2. ADP-II positions include responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of a higher authority in the ADP-I category (AR 380-67, Appendix K). Basically, this means personnel at ADP-II can perform maintenance on the CAISI, provided an ADP-I position reviews the work.

3. ADP-III positions include all Federal computer activities not addressed in ADP-I and ADP-II. All personnel in ADP-III positions must be observed when performing maintenance on CAISI.

F.2.9 Continuity of Operations.

F.2.9.1 Restoration of Service.

CAISI will maintain continuity of operations by borrowing supplementary equipment from the SSR Accessory Kit to remedy problems as they arise. Only authorized configuration management components will be used in CAISI.

Once the swap occurs the replacement CAISI component will be configured as necessary. Configurations settings are stored in the SSR (CSS S6) notebook. The SSR (CSS S6) may store a backup copy of the configuration settings on floppy disk.

Encryption keys are not stored on either the SA notebook or disk. They must be restored manually. Sealed copies are maintained by the ISSO, CSSAMO, or unit security officer.

F.2.9.2 Restoration of Data.

No provision for restoration of data is required, because the CAISI does not store any data. The CAISI provides network transmission media and VEE protocol conversion only.

F.2.10 Emergency Destruction.

In the event that CAISI is subject to imminent capture, the system must be destroyed IAW your unit's SOP for destruction of electronic, communications, and information processing equipment. The priority for destruction is as follows:

Priority for Destruction

1. Air Fortress encryptors and any notebooks containing Air Fortress client encryption settings.
2. Wireless Bridges, Access Points and Client Devices (containing System ID, encryption settings and configuration data.)
3. Wireless Radios other than bridges (containing WEP settings.)
4. Notebooks (containing System ID, configuration data and possibly, application data – not CAISI data, but other data stored by the users).
5. Legacy Support Adapters (communication equipment containing configuration data.)
6. DSL Bridges (communications equipment)

Figure F-1 Priority for Destruction Chart

F.2.11 CAISI SSR Notebook User Security Procedures.

This paragraph applies to the laptop or notebook computer included in the System Support Representative (SSR) transit case. The terms "laptop" and "notebook" are used interchangeably throughout this document. This laptop is used by the SSR (CSS S6 or other automated personnel).

F.2.11.1 User Interface Description.

The CAISI notebook is a commercial off-the-shelf (COTS) notebook computer running Microsoft Windows 2000. Windows is used in order to take advantage of the built-in security features and provide a robust platform for applications.

CAISI Administration Software Application (CAISI Admin):

1. Appears as an icon on your desktop.

2. It is a government-developed interface designed to help you configure the various CAISI components and perform monitoring as required by regulations.

3. You may have other applications and services running on the CAISI notebook to accomplish your official duties, as long as they do not interfere with the operation or security of the CAISI system. You may, for instance, use the CAISI notebook for official electronic mail (email) or word processing, but may not use it to play Hearts, Doom, or any other games. You may not "surf" the Internet, except as required by your official duties.

   NOTE: *Unofficial use consumes part of the limited communications channels available, and thus impairs operation of the CAISI. It also constitutes a potential security hazard since you might inadvertently touch a hostile web site.*

4. You may personalize the laptop to conform to the way you work, as long as you do not compromise security or make it difficult for others to use the notebook.

   You may, for instance change the color scheme, add shortcuts, or add the official applications you need for your official duties. You may not "save" passwords, remove or rename the standard icons, or add unauthorized software or games.

   Be aware, however, that your personalization will be lost if you ever have to reload the system from disk, because only the standard configuration and software is on the system CD-ROM disk.

F.2.11.2 User Identification and Authentication.

When you first become an SSR, you need to request an account from the CSS S6, in accordance with your local SOP. The CSS S6 will issue your account, which consists of a user identification name (userid), associated password, and a profile that gives you the rights and privileges necessary to login to the machine and do your job.

1. Your userid is unique to you and **must not** be shared. Follow these security procedures:

   a. Do not allow others to use your password, except under your direct supervision.

   b. If a computer repairperson needs to work on your system, you may not allow him or her to use your userid.

(1) In the rare instance that they cannot use their own userid, such as when fixing your profile, you must watch everything they do to ensure that CAISI operations and security are not compromised.

When they are logged in as you, the computer thinks that they **are** you and allows them all of **your** rights and privileges.

c. Additionally, if you share a userid, accountability is lost, since we can no longer tell who did what.

2. There will be other accounts on your machine as well:

a. There will be accounts for any other SSR assigned to your CAISI.

b. There may be CSSAMO accounts.

c. There may be accounts for the STAMIS and CSS users who connect to and through your CAISI.

3. User accounts may be in one of the following groups:

a. **Admin Account:** "Admin" users (the SSR, CSS S6, or their representatives)

b. **Power User Account:** "Operator" users (STAMIS or CSS users who normally use the notebook for monitoring or other users not requiring admin privileges).

c. "**Guest**" users: STAMIS or CSS users who connect through the CAISI and who might occasionally need to log onto your notebook while they are in your facility.

NOTE: *DoD Policy prohibits the use of the "guest" account on an active network. The account is a guest type not a logon name.*

Each of these groups has different privileges to run applications, to create and view files, and to use CAISI services.

F.2.11.3 Passwords.

The following are procedures for password security:

1. You will be issued a password to go with your userid. Without this password, you cannot log in to your account.

2. Under no circumstances are you to tell anyone your password. Your password allows you to control the CAISI, which is passing SBU traffic. Your password must be protected as SBU.

   Memorize the password. You may not write it on slip of paper and put it in your desk drawer, wallet, or purse. If you do write it down, seal it in an envelope and put the envelope in the ISSO's or S-2's safe.

3. The initial password issued to you will be created by the CSS S6 or randomly generated by the CAISI Administration application. Thereafter, you must change it at least once every six months.

   a. Change your password according to Windows 2000 Admin tools.

   b. If you allow your password to expire without changing it, you will need to have the CSS S6 issue you a new one.

      (1) In the meantime, you can no longer logon to CAISI. You will get a message explaining that your password has expired.

   c. If a password is compromised, or suspected compromised, contact the CSS S6 immediately so he or she can assign a new password and assess any potential compromise.

   d. Passwords are case-sensitive.

NOTE: *You will be locked out after three unsuccessful login attempts, therefore, you must be careful when entering your user name and password information. If you get locked out, you must contact the CSS S6 to unlock your account. If the Admin password is lost, you will have to reload the CAISI software.*

F.2.11.4 Screen Saver.

1. A screen saver will be set up on the CAISI notebook and will be activated if there is no keyboard or mouse activity for five minutes.

2. When the screen saver is active, hit any key on the keyboard, or move the mouse. You will be prompted to enter your password.

3. Do **not** deactivate the screen saver.

F.2.11.5 Login Banner.

1. When you logon to the SSR notebook, a DoD security warning banner will be displayed (Figure F-2).

2. Click on the OK button or press the {Esc} key. Clicking on the OK button constitutes that you consent to security monitoring, and gives you access to the CAISI login screen.

3. If you don't wish to consent to monitoring or you decided not to access CAISI, click on the Cancel button or press the {Esc} key when the login screen appears.

4. DoD security warning banner should appear on all of your official computers. It is stored in the NT registry and must not be removed.

WARNING

ATTENTION

THIS IS A DoD COMPUTER SYSTEM. BEFORE PROCESSING CLASSIFIED INFORMATION, CHECK THE SECURITY ACCREDITATION LEVEL OF THIS SYSTEM. DO NOT PROCESS, STORE, OR TRANSMIT INFORMATION CLASSIFIED ABOVE THE ACCREDITATION LEVEL OF THIS SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (INCLUDES INTERNET ACCESS) ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES, BUT IS NOT LIMITED TO, ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING. UNAUTHORIZED USE OF THIS DoD COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES.

Figure F-2 DoD Warning Banner

F.2.11.6 Virus Protection.

1. CAISI runs the DOD-standard Norton Anti-Virus (NAV) with all the standard capabilities including automatic scans of memory and disk drives for viruses, and periodic downloads of new virus definitions. NAV will either eradicate or disinfect the virus and prompt the operator for the action to take.

2. As SSR, you are responsible to keep the anti-virus program and definitions current. Run Norton's Live Update at least weekly to ensure that both the program and virus definition files are up to date.

NOTE: *Immediately notify the CSS S6 if the program reports a virus.*

F.2.11.7 Wireless Network Card

The notebook includes a wireless network interface card (NIC) and Air Fortress remote client encryption software.

The wireless NIC **may not** be used for over-the-air configuration of the CAISI wireless bridges or clients.

The wireless NIC **may not** be used to pass traffic without the remote client encryption software active.

F.2.12 Security Features and Configuration.

As a designated service support representative (SSR), Signal staff (S-6) soldier, or Combat Service Support Automation Management Office (CSSAMO) soldier, ***you are*** responsible to configure the CAISI and implement the security features.

Security features and configuration are not included in the STAMIS and CSS Operators Manual for the CAISI. That manual addresses operators' security responsibilities and the installation, operation, and maintenance of *pre-configured* CAISI components.

This document addresses the CAISI security features. This includes configuration instructions for the CAISI because the security features all require configuration. The STAMIS and CSS operators do not configure the CAISI. Configuration is solely a SSR responsibility.

This appendix expands on the system description in Chapter 1, so that you know how each item of equipment fits into the whole system. Additional general information and planning considerations can be found in Appendix I.

In the field, security encompasses three main areas: confidentiality, availability, and accountability.

1. You ensure **confidentiality** by properly configuring the equipment. Configuration procedures are included in the Paragraph 2.22 for the hardware connections and TB #11-5895-1691-12 for the software. Security planning and reporting, implementing protected distribution systems, and preventing unauthorized or unnecessary access to the system also fall in this category. You also must protect passwords and encryption keys.

2. Operators ensure **availability** by properly installing, operating, and maintaining the equipment. As SSR, or CSSAMO you assist them if the equipment fails or if they are having trouble communicating. Additionally, you will be called upon to operate and maintain the equipment included in the SSR Accessory Kit. Installation, operation, and maintenance procedures are therefore also included in this manual.

3. Owning units and assigned operators are responsible for **accountability**. Again, you may be called upon to assist operators. And, as the assigned operator of the SSR Accessory Kit, you may be responsible for its accountability. You also must account for issued passwords and encryption keys.

F.2.13.1 Component Functions and Relationships

In order to configure the CAISI and implement its security features, you need to understand the functions of the components that make it up. You also need to understand the relationships amongst the components -- how they work together.

What is a hub?

A hub has multiple network ports and acts as a repeater, sending data to all the ports. Hubs are efficient, but dumb. Well, not dumb, just ignorant. Because they can't read, they don't know to whom data is addressed. So they retransmit every packet to every port. Each connected computer therefore sees every packet sent from and to every other. They politely ignore those not addressed to them. But the network segment can become congested. Collisions occur when two or more computers try to communicate at the same time. Hubs do nothing to prevent collisions.

What is a bridge?

Bridges connect one local area network (LAN) or LAN segment to another. They take data packets from their own LAN segment and retransmit them to the remote bridge. And retransmit packets from remote bridges to the local segment. They help reduce collisions by retransmitting only some of the packets. They keep track of the computers to whom the data is addressed, and retransmit only those that need to be retransmitted. Bridges read the Media Access Control (MAC) addresses in the data packets and watch to see where the sending and receiving computers are. Every network component has its own unique MAC address, the physical address built-in by the manufacturer. The bridges store MAC information in "bridge tables" in memory. The next time a packet is sent, the bridge checks its bridge tables and retransmits the packet only if it needs to. If both the sender and receiver are local, or if both are remote, the bridge will not retransmit the packet. If the packet is a broadcast (addressed to everybody) or if the bridge doesn't know where the computers are (the addressee is not in its bridge table), it retransmits the packet. Bridge tables are dynamic. The bridges learn addresses as they pass traffic. If a bridge table becomes full or stale (containing outdated information), it needs to be flushed or reset. The bridge then rebuilds the table.

What is a switch?

Switches are like a cross between a hub and a bridge. They have multiple ports and retransmit packets, but only to the port where the target computer is connected. They also accumulate tables of MAC address in memory and retransmit only those packets that need it. Like a bridge, the switch forwards broadcasts and packets to unknown recipients everywhere. A switch greatly reduces the number of collisions on the network because the packets sent only where they actually need to go, not everywhere.

What is a router?

A router looks at Transmission Control Protocol/Internet Protocol (TCP/IP) addresses instead of MAC addresses. The TCP/IP address is a logical address, identifying the virtual location of the network device. If the addressee is not on the local network, the router forwards the packet to another router, according to rules maintained in "router tables" in memory or on disk. These router tables can be accumulated dynamically, or created manually. Manual fixed routes are known as "static routes." Either way, router tables identify the next router in line for a group of TCP/IP addresses. (As opposed to bridge tables that keep tabs on individual computers by their MAC addresses.) Eventually the packet arrives at the addressee's LAN and is delivered.

How is the CAISI router different?

The CAISI router is not a traditional router. It is actually designed for homes or offices to connect to the Internet using a single IP address. It is a network address translator (NAT) server and divides the network into public (WAN) and private (LAN) segments. Although it provides no services to the public segment, it acts as a traditional router, a firewall, and a dynamic host configuration profile (DHCP) server for the private segment. The CAISI router includes an eight-port switch on the LAN side. It can be used as a switch even when you don't need the router functions. The CAISI router is included in the SSR accessory kit. It is optional -- there if you need it, otherwise leave it in the transport case. An additional, more powerful router will soon be added to the CAISI. It will do everything this router does, but on a larger scale. It will support more addresses, larger more flexible DHCP pools, and additional security and routing functions.

What is wireless?

This seems to be a term that means many different things. To many it means cellular telephones or satellite television. For CAISI, however, it means simply that a computer or bridge in one work center connects to a computer or bridge in another work center by radio instead of by miles of network cables. The data is encrypted for security purposes before it is transmitted over the radio. This provides the same level of protection as though it were on wire instead of radio (as mentioned earlier, the wireless standard optimistically calls this "wired equivalent privacy," or WEP). CAISI supplements WEP with separate encryptors (see "What is an Air Fortress," below).

> **NOTE:** *Within the work centers, short cables connect computers to the CAISI bridge module or CAISI client module. This allows a single CBM or CCM, with a single antenna erected above the camouflage, to provide communications for several computers. If we used no network cables at all ("totally wireless") we'd actually need a lot more cable overall, because every computer would need its own antenna cable and antenna.*

What is a DSL?

A Digital Subscriber Line bridge is actually a kind of modem (a modulator/demodulator) – that is to say, a protocol converter. It takes the network traffic on its LAN port and retransmits it on its DSL port, using a different protocol to allow it to go a long distance over field wire. As a bridge, of course, it retransmits only those packets that it need to. Normally network traffic can only travel about a hundred meters over high quality multi-pair fragile cables (category-5 Ethernet cable) or up to a hundred and eighty five meters over large, heavy coaxial cable. The CAISI DSL bridges can send traffic up to four miles over field wire. And field wire is much easier to deploy, recover, and repair. We would,

of course, prefer not to run any field wire at all. The DSL bridges are included in CAISI for those circumstances where you cannot use the wireless bridges, or where it is easier to use the DSL. The wireless radios use an extremely high radio frequency (and therefore very short radio waves). These microwaves are easily absorbed by obstacles, so they need a pretty clear line-of-sight from one radio to the next. Heavy vegetation, hills, and buildings all hurt the wireless. The DSL bridges give you an alternate means of communications.

NOTE: *Beside the fact that you have to run wire, the DSL bridges have one other major disadvantage when compared to the wireless bridges. They are point-to-point. That is to say, each DSL bridge can be connected to only one DSL bridge. To connect two points you need a pair. To interconnect three work centers, you would need two pairs of DSL bridges. For each additional work center you need an additional DSL* ***pair****, not just one more DSL. The wireless bridges, on the other hand, operate in point-to-multipoint mode. You need only one per work center. The wireless bridges can talk to more than one at a time, and even relay for each other.*

What is an LSA? And what is VEE? Many of the STAMIS applications were designed to communicate through their serial ports, not over the network. The original version of the CAISI, and every version since, has provided a means for these STAMIS applications to use the network to pass their data as though their serial ports were directly connected. The CAISI Legacy Support Adapter (LSA) provides a Virtual-End-to-End (VEE) circuit simulating a direct serial connection. The LSA is a protocol converter, taking the serial data stream and packaging it into network packets addressed to the LSA that is connected to the remote STAMIS computer. The remote LSA turns the packets back into a serial data stream.

What is an Air Fortress? CAISI is a combat service support system. As such, it handles Sensitive Unclassified Information (SUI), also referred to as Sensitive But Unclassified (SBU) data. This traffic must be protected when it traverses the wireless portion of the local network. The Air Fortress is an inline encryptor that uses encryption and authentication techniques that are strong enough to protect this data. The Air Fortress encrypts the IP packet (header and data) prior to transmission. Every other Air Fortress checks the MAC address in the encrypted packet to see if it is for a computer or other network device connected to them. If not, they ignore it. If it is for a connected host, the receiving Air Fortress decrypts and authenticates the packet prior to passing it on to that host. If the packet cannot be decrypted, or if it fails authentication, the Air Fortress drops it.

What is a NES? And what is a TACLANE? The CAISI system is not cleared to pass classified traffic, but the only network that interconnects the field sites is classified SECRET. We use Motorola Network Encryption System (NES) in-line network encryption (INE) devices to connect CAISI to the Mobile Subscriber Equipment (MSE) Tactical Packet Network (TPN) provided by the Signal unit. The NES takes data from the CAISI network, encrypts it and routes it over the TPN to another NES where it is decrypted and handed to the CAISI network there. The TACLANE will soon replace the NES. It is an INE and will accomplish the same functions as the NES, except that the TACLANE is not a router. It needs the routers in the TPN to handle the routing, although future versions of the TACLANE will include a routing function. The TACLANE encapsulates the entire packet and encloses it with a new header to go through the TPN. The end TACLANE discards the duplicate header and allows the original packet to continue on its way. The NES and TACLANE are not interchangeable

or interoperable. It is conceivable that there will be instances where a unit has one of each in use at the same time in order to communicate with two differently equipped distant ends.

How does everything fit together? It's kind of like that old song: "The head bone's connected to the neck bone"...

1. STAMIS applications that require CAISI VEE support are connected to LSAs.

2. LSAs are in turn connected to CCMs or CBMs.

3. CSS computers and STAMIS applications that do not require VEE support connect directly to CCMs or CBMs.

4. CCMs communicate to CBMs.

5. CBMs communicate to other CBMs.

6. The CBM root node is connected to the INE device, which in turn connects to the MSE.

7. MSE is connected to the installation network or the NIPRNET. The NIPRNET is connected to the Internet.

NOTE: *CAISI provides local communications.* ***Only****.*

The Signal unit provides all of the long-haul, inter-site communications.

The NES, TACLANE, and MSE belong to the Signal unit not the CAISI. Network services, such as DNS, are also provided by Signal.

The tactical LAN architecture, on Figure F-3, shows how the clients connect to the CAISI LAN and the CAISI LAN in turn connects to MSE.

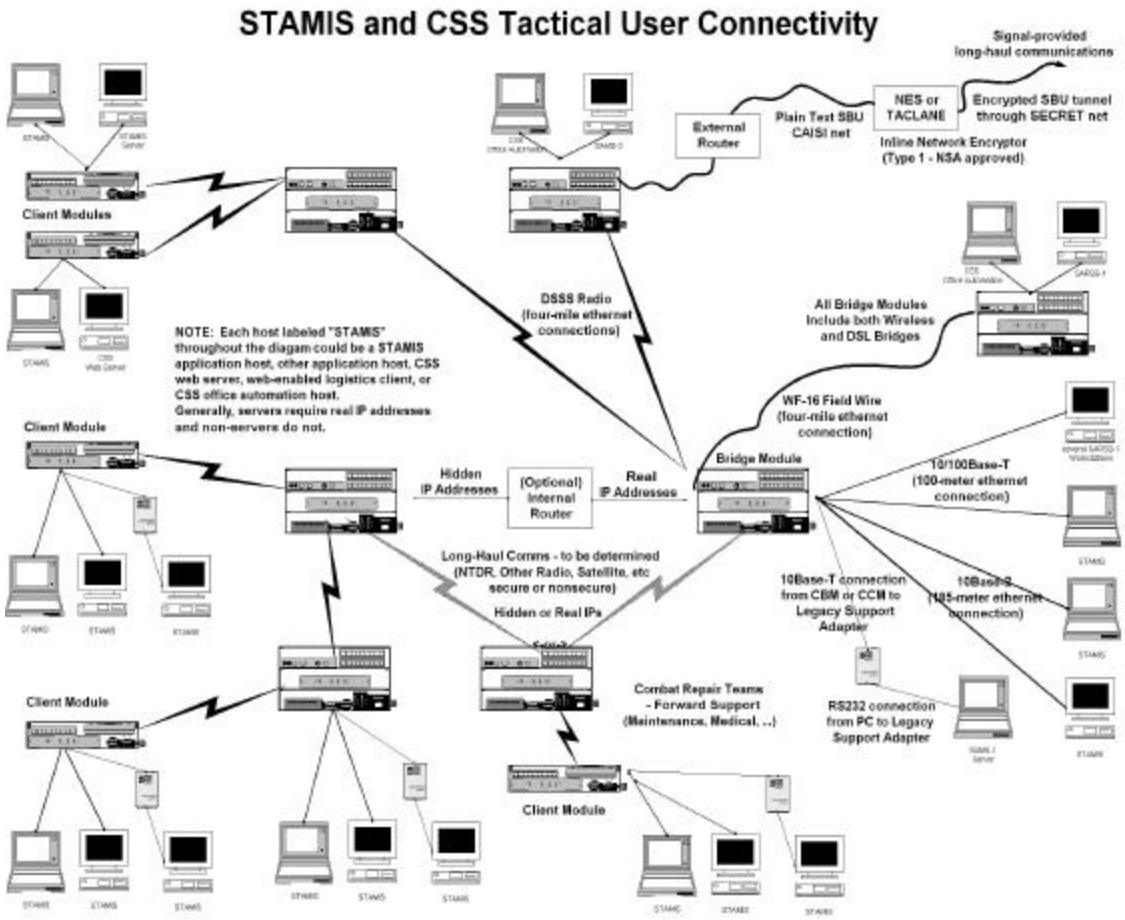


Figure F-3 Tactical CAISI LAN Architecture

Appendix G

Glossary

Glossary of Terms

3DES. Triple Data Encryption Standard. The National Institute of Standards and Technology (NIST) standard for 192-bit encryption

10Base-2. One of several adaptations of the Ethernet (IEEE 802.3) standard for Local Area Networks (LANs). The 10Base-2 standard (also called *Thinnet*) uses 50 ohm coaxial cable (RG-58 A/U) with maximum lengths of 185 meters. This cable is thinner and more flexible than that used for the 10Base-5 standard. The RG-58 A/U cable is both less expensive and easier to place. Cables in the 10Base-2 system connect with BNC connectors. The Network Interface Card (NIC) in a computer requires a T-connector where you can attach two cables to adjacent computers. Any unused connection must have a 50 ohm terminator. The 10Base-2 system operates at 10 Mbps and uses baseband transmission methods.

10Base-T. One of several adaptations of the Ethernet (IEEE 802.3) standard for Local Area Networks (LANs). The 10Base-T standard (also called *Twisted Pair Ethernet*) uses a twisted-pair cable with maximum lengths of 100 meters. The cable is thinner and more flexible than the coaxial cable used for the 10Base-2 or 10Base-5 standards. Cables in the 10Base-T system connect with RJ-45 connectors. A star topology is common with 12 or more computers connected directly to a hub or concentrator. The 10Base-T system operates at 10 Mbps and uses baseband transmission methods.

802.11. The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) wireless LANs.

802.11b. The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5 and 11- Mbps wireless LANs. (Security protocol for CAISI).

Access Control. The process of limiting access to the resources of a system only to authorized programs, processes or other systems (in a network).

Access Point. A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.

Ad Hoc Network. A wireless network composed of stations without Access Points.

AES. Advanced Encryption Standard. This is a cryptographic algorithm for use by U.S. Government organizations to protect sensitive (unclassified) information as specified in the Federal Information Processing Standard (FIPS) Publication. The CAISI Inline Encryptor supports AES 192-encryption.

Associated. A station is configured properly to allow it to communicate wirelessly with an Access Point.

Blocked Asynchronous Transmission (BLAST). A terminal emulation program that runs in DOS mode on the notebook computer. It is used by STAMIS applications for communications and can be used for troubleshooting.

Bridge. A device that connects two LAN segments together. A bridge is inserted into a network to segment it and keep traffic contained within the segments to improve performance. Bridges take data packets from their own LAN segment and retransmit them to the remote bridge, which in turn retransmits them to the local segment. Bridges learn from experience and build and maintain address tables of the nodes on the network. By monitoring which station acknowledged receipt of the address, they learn which nodes belong to that segment.

Brigade Subscriber Node (BSN). An element of Mobile Subscriber Equipment (MSE).

CAISI VEE (Virtual End-to-End). The CAISI VEE software allows data that has been sent to non-network capable STAMIS devices to be passed through the CAISI to a STAMIS that is registered and connected to it. CAISI VEE places the data into packets to be sent over the TPN.

Coaxial (cable). Also known as RG-58. A data transmission medium with a single wire conductor insulated from Electromagnetic Interference/Radio Frequency Interference.

Collision. When two or more stations attempt to transmit on the same wire at the same moment, a data collision will occur. When a collision occurs, each station will wait a randomly selected time period – usually several microseconds – before attempting to transmit again.

Collision Domain. A network configuration on which two nodes transmitting data at the same time will cause a collision.

Combat Service Support (CSS) Computers. Computers hosting various Standard Army Management Information Systems (STAMIS), designed to operate in both a tactical and garrison environment.

Commercial off-the Shelf (COTS). Commercially available items, hardware or software, sometimes modified slightly for Army use.

Decibel (referenced to isotropic radiator) (dBi). It is the gain of the antenna and is described in a mathematical formula, where gain is the ratio of input versus output power. The greater the dBi value, the higher the gain, and the more acute the angle of coverage.

DeMilitarized Zone (DMZ). A middle ground between an organization's trusted internal network and an untrusted, external network such as the Internet. The DMZ is a subnetwork (subnet) that may sit between firewalls or off one leg of a firewall. **CAISI does not use the DMZ port on the inline encryptor at this time.**

Denial of Service. Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose.

Digital Subscriber Line (DSL). A digital subscriber line bridge takes the network traffic on its LAN port and retransmits it onto the DSL port, using a different protocol to allow it to go long distances over field wire. As a bridge, it retransmits only those packets that are necessary.

Domain Name Server (DNS). The DNS is a database that keeps track of the Internet Protocol (IP) addresses of the devices within the site's control or domain. The database contains the IP addresses, names, and locations of every device connected to the network. Provides name to IP address resolution.

Direct Sequence Spread Spectrum (DSSS). A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

Dynamic Host Configuration Protocol (DHCP). A means of restricting the number of IP addresses required. Users are assigned an IP from an available pool of addresses when they connect to the network.

Encryption. The encoding of data for security purposes, by converting it into a proprietary code. It is used to transmit data over a network or to encode data so that it cannot easily be changed.

Ethernet. A protocol (set of rules) for communicating between computers governing format, timing, sequencing, and error control.

Firewall. A way to restrict access to computers. Users outside the firewall cannot, in most cases, initiate contact with users behind the firewall.

Forward Repair Activity (FRA). In several centralized locations, both CONUS and OCONUS, and maintained by Tobyhanna Army Depot, FRAs provide facilities for repair of computer equipment without returning the equipment to the depot.

Gateway. A device that connects two otherwise incompatible networks together.

Hub. A hub has multiple network ports, and acts as a repeater, sending data to all the ports.

IEEE. Institute of Electrical and Electronic Engineers. A professional society serving electrical engineers through its publications, conferences, standards development activities. The IEEE is best known for developing standards for the computer and electronics industry, especially the Ethernet 802.3 and wireless LAN 802.11 specifications.

Infrastructure. The wired Ethernet network.

InLine Encryptor. Air Fortress hardware and remote software client encryptors are included in the CAISI configuration.

a. Hardware encryptors serve as a dedicated security device placed in the Ethernet link between the radios and the hubs in the CBMs and CCMs. The device encrypts (or decrypts, as appropriate) packets. It then forwards the packets out its other interface to another AirFortress inline encryptor.

b. The Air Fortress Remote Client software works exactly like the hardware encryptor, except that it operates on the client computer. It encrypts and decrypts the network traffic as it is passes in and out of the computer. It sits between the computer and the NIC – in the same way that the inline encryptor sits between the hub and the radio.

In-Line Network Encryption (INE) Device. A device collocated with the Small Extension Node (SEN) of the MSE that allows Unclassified Tactical Packet Network (TPN) users to communicate over the TPN while meeting the security requirements of the TPN. The INE device is sometimes referred to as the Network Encryption System (NES).

Internet Protocol (IP) Address. A series of numbers specific to an individual computer that allows other computers on the network to find it and communicate with it. Expressed in terms of four **Octets**, i.e., xxx.xxx.xxx.xxx.

Large Extension Node (LEN). An element of Mobile Subscriber Equipment (MSE).

Legacy Support Adapter (LSA). CAISI LSA MSS100 provides a virtual circuit from one host computer's serial port to another, over the 10Base-T network. The MSS100 makes it easy to communicate through the network for any device with a serial interface.

Line Replaceable Unit (LRU). When a computer system is in need of repair, the LRU is the lowest level the components can be separated and returned for repair.

NOTE: *LRUs for the CAISI are the wireless bridges, multi-client radio adapters, DSL bridges, hub, power supplies, lightning arrestor, router, notebook computer, UPS, antennas, and cables.*

Local Area Network (LAN). A means of connecting computers together to allow them to exchange data among themselves. (A computer network that spans a relatively small area. Most LANs are confined to a single building or a group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN)).

Light Emitting Diodes (LEDs). A tube allowing current flow in one direction, illuminating one end.

Medium/Media Access Control (MAC) Address: A unique 48-bit number that identifies a device and is used to properly direct network traffic to the correct device.

Mobile Subscriber Equipment (MSE). The hardware element of the Tactical Packet Network (TPN). MSE includes Small Extension Nodes (SEN), Forced Entry Switch and Node Center Switch.

Need-to-know. The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

Network Address Translation (NAT). With Network Address Translation, the network is divided into two segments, one "public" and one "private", behind a router. This allows as many as 250 users behind the NAT Server, on the private side, without having to use public, "real" IP addresses.

Network Encryption System (NES). The NES is Motorola's name for a device known as an inline network encryption (INE) device. The NES allows unclassified data to use the secret-high TPN by "tunneling through" the classified network. This method has been implemented to allow unclassified users to use the TPN secret-high network.

NIPRNET. Non-secure Internet Protocol Router Network. The Army's unclassified wide area network. Is also used by Department of Defense.

Node. Any device, including bridges, servers, and workstations, that are connected to the network. Also refers to the point where the devices are connected.

Node Center Switch. An element of **Mobile Subscriber Equipment**.

Null Modem Cable. A type of data transmission cable that retains the pin structure of the sending device. Externally, a null modem cable appears identical to an ordinary RS-232 cable, however, its internal configuration dictates when and how it may be used.

Octet. A numbering system, which is used in one of four segments of an IP address separated by a period. For example, in the IP address 192.172.19.241, 19 is the third octet.

Original Equipment Manufacturer (OEM). The commercial manufacturer of a hardware component.

Packet. A collection of bits comprising data and control information formatted for transmission from one **node** to another.

Point-to-Point Protocol (PPP). An enhanced serial communications package that provides a means of transferring TCP/IP packets over dial-up or direct connections.

Power Surge. A sudden abnormal increase in power flow through a line.

Preventive Maintenance Checks and Services (PMCS). Routine procedures performed on a regularly scheduled basis to maintain equipment readiness and prevent problems from arising.

Protected Distribution System (PDS). A wireline or fiber-optics telecommunications system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.

Repeating. The act of regenerating and amplifying a data signal as it travels along a network. Repeating allows a given data signal to travel a farther distance without compromising data integrity. It is independent of protocol and media.

RF. Radio frequency. A generic term for radio-based technology.

Router. A device that forwards data packets from one local area network (LAN) or wide area network (WAN) to another. Based on routing tables and routing protocols, routers read the network address in each transmitted frame and make a decision on how to send it based on the most expedient route.

> The **CAISI router** is not a traditional router. It is actually designed for homes or offices to connect to the Internet using a single IP address. It is a network address translator (NAT) server and divides the network into public and private segments.
>
> Although it provides no services to the public segment, it acts as a traditional router, a firewall, and a Dynamic Host Configuration Protocol (DHCP) server to the private segment.b.

Sensitive But Unclassified (SBU). Any information, that the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5 United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense foreign policy.

Serial. A means of data transmission where the elements of a character are presented one byte at a time, as opposed to parallel, where the entire character is presented at once. Parallel is faster, but serial data transmission is capable of traveling farther distances with greater data integrity.

Small Extension Node (SEN). An element of the Mobile Subscriber Equipment (MSE) that hosts the INE device.

Sneaker Net. Refers to transferring data from computer to computer by physically carrying disks between the computers instead of using a network connection.

Spread Spectrum. A radio transmission technology that spreads the user information over a much wider bandwidth than otherwise required in order to gain benefits such as improved interference tolerance and unlicensed operation.

Service Set Identification (SSID). This is an unique identifier that bridges and client devices use to associate to other bridges. The network ID for the public or private segment for the CAISI as determined by the SSR, S6 or the Director of Information Management (DOIM).

Strain Relief. The act of tying off any cable prior to making a connection to ensure that if the cable is pulled on it will not break the connection. Strain relief should be used with all cable connections.

SUI. Sensitive unclassified information.

Systems High Security Mode. AIS security mode of operation wherein each user, with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts, has all of the following:

a. Valid security clearance for all information within an AIS

b. Formal access approval and signed non-disclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs)

c. Valid need-to-know for some of the information contained within the AIS.

T-Connector. A T-shaped device with two female and one male BNC connectors.

Tactical Packet Network (TPN). The TPN is the component of the Mobile Subscriber Equipment (MSE) that allows *data packets* to be sent and received. Since the TPN is a secret-high system, unclassified data must be separated from classified. This separation is done through the use of an In-Line-Encryption device or Network Encryption System (NES).

Telnet. A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password.

Terminator. A device placed on the end of a T-Connector to prevent a data signal from attempting to travel in that direction.

Topology. The shape of a Local Area Network (LAN). Basically, is the way computers are connected together to form a network. CAISI topology will deal with the layout of CBMs, CCMs, Antenna(s), DSL(s) and Linksys Router.

Transmission Control Protocol/Internet Protocol (TCP/IP). The most common protocol (set of rules) to allow computers to exchange data. Every device that communicates on the Internet (NIPRNET, the Army's unclassified portion of the Internet) must have an IP address so information can be sent to it.

Troubleshooting. The act of identifying and resolving problems.

Trusted Computer Base (TCB). The totality of protection mechanisms within a computer system, including hardware, firmware and software, the combination of which is responsible for enforcing a security policy.

Uninterruptible Power Supply (UPS). A device used to protect electrical equipment from surges and fluctuations in power. The UPS also contains a battery to provide temporary power in the event of a loss of primary power.

Wide Area Network (WAN). A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Wired Equivalent Privacy (WEP). An 802.11 security protocol for wireless networks. The WEP encryption method is designed to provide the "equivalent" security available in wireline networks.

Wireless. This term has many definitions, however its relevance to CAISI is simply that a computer or bridge in one work center connects to a computer or bridge in another work center by radio instead of by miles of network cables.

Abbreviations and Acronyms

3DES	Triple Data Encryption Standard
A	Amperes
AAL	Additional Authorization List
ACT	Activity
ACU	Aironet Client Utility
ACUS	Area Common-User System
ADP	Automated Data Processing
ADPE	Automated Data Processing Equipment
AES	Advanced Encryption Standard
AIS	Automated Information System
APM	Assistant Project Manager
AR	Army Regulation
ASB	Aviation Support Battalion
AUI	Auxiliary Unit Interface
BII	Basic Issue Items
BIOS	Basic Input/Output System
BLAST	Blocked Asynchronous Transport
BNC	British Naval Connector (could also be Bayonet Navy Connector, Bayonet Naval Connector, Bayonet Nut Connection)
BNC-T	British Naval Connector and Terminator
BSA	Brigade Support Area
BSN	Brigade Subscriber Node
CAGE	Commercial and Government Entity
CAISI	Combat Service Support Automated Information Systems Interface
CAISI Admin	CAISI Administration Software Application
CAISI-MT	Combat Service Support AIS Interface – Mid Term Fix
CAISI-NTF	Combat Service Support AIS Interface – Near Term Fix
CAO	Customer Assistance Office
CAT-5	Category 5 Cable
CBM	CAISI Bridge Module
CCM	CAISI Client Module
CEM	Client Encryption Manager
CLI	Command Line Interface
CMOS	Complementary Metal Oxide Semiconductor
CNR	Combat Net Radio
COEI	Components of End Item
COL	Collision
COMSEC	Communication Security
CONUS	Continental United States
COTS	Commercial Off-The-Shelf
CP	Command Post

CPC	Corrosion Prevention and Control
CPU	Central Processing Unit
CS	Circuit Switch
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSS	Combat Service Support
CSSAMO	Combat Service Support Automation Management Office
DA	Department of the Army
dBi	Decibel
DHCP	Dynamic Host Configuration Protocol
DIAG	Diagnostics
DISA	Defense Information Systems Agency
DISCOM	Division Support Command
DMZ	DeMilitarized Zone
DNS	Domain Name Server
DNVT	Digital Non-secure Voice Terminal
DoD	Department of Defense
DODAAC	Department of Defense Activity Address Code
DOIM	Directorate of Information Management
DOT	Distance, Obstacles, and Terrain
DSA	Division Support Area
DSB	Division Support Battalion
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
DSU	Direct Support Unit
DSVT	Digital Subscriber Voice Terminal
EIA	Electronic Industries Alliance
EIR	Equipment Improvement Recommendations
EIRP	Equivalent Isotropic Radiated Power
ERR	Error
EPLRS	Enhanced Position Location Reporting System
ESC	Escape key
ESD	Electrostatic-Discharge
ETSI	European Telecommunications Standards Institute
FIPS Pub	Federal Information Processing Standards Publication
FM	Field Manual
FMC	Fully Mission Capable
FRA	Forward Repair Activity
FRS	Family Radio Service
FSB	Forward Support Battalion
FSCM	Federal Supply Code for Manufacturers
FTP	File Transfer Protocol

HF	High Frequency
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure (secure web pages)
HyperTerm	HyperTerminal
Hz	Hertz
IAW	In Accordance With
IEEE	Institute of Electrical and Electrical Engineers
IIS	Internet Information Server
IMMA	Installation Material Maintenance Activity
INE	In-Line Network Encryption
IOM	Install, Operate and Maintain
IP	Internet Protocol
IPAA	IP Address Assistant
IPSU	IP Setup
ISSA	Installation Supply Support Activity
ISSM	Installation System Security Manager
ISSO	Information System Security Officer
ISYSCON	Integrated System Control
ITCRA	In-Theater Computer Repair Activity
JTRS	Joint Tactical Radio System
LAA	Limited Access Authority
LAN	Local Area Network
LED	Light Emitting Diode
LEN	Large Extension Node
LOS	Line of Sight
LRU	Line Replaceable Unit
LSA	Legacy Support Adapter
LSE	Logistic Support Element
LSM	Link Status Meter
MAC	Media Access Control
MAR	Margin of Error
MB	Megabyte
Mbps	Megabits per second
MCS	Maneuver Control System
MDI	Media Dependent Interface
MDI-X	Media Dependent Interface - crossover
METT-T	Mission, Enemy, Terrain, Troops and Time Available
Mhz	Megahertz
MIL-HDBK	Military Handbook
MILNET	Military Network
MIL-STD	Military Standard
MISC	Miscellaneous

MMCX	Multimedia Communication Exchange
MOS	Military Occupational Specialty
MSE	Mobile Subscriber Equipment
MSRT	Mobile Subscriber Radiotelephone Terminal
MTOE	Modified Table of Organization and Equipment
mW	Milli-Watt
NAT	Network Address Translation
NAV	Norton Anti-Virus
NDI	Non-developmental Item
NEOF	No Evidence of Failure
NES	Network Encryption System
NIC	Network Interface Card
NIPRNET	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards
NOC	Network Operations Center
NSA	National Security Agency
NSN	National Stock Number
NTDR	Near Term Digital Radio
OCONUS	Outside Continental United States
OEM	Original Equipment Manufacturer
OPPM	Outside Principal Period for Maintenance
OPSEC	Operations Security
OS	Operating System
PAM	Pamphlet
PCMCIA	Personal Computer Memory Card International Association
PDF	Portable Document Format
PDS	Projected Distribution System
PEO EIS	Program Executive Office Enterprise Information Systems
PMCS	Preventive Maintenance Checks and Services
PO	Project Officer
POC	Point of Contact
PPM	Period for Maintenance
PPP	Point-to-Point Protocol
PWR	Power
QoS	Quality of Service
QTY	Quantity
RAU	Radio Access Unit
RCVD	Received
REC	Receive
RECM	Recommended
RF	Radio Frequency

ROD	Report of Discrepancy
RPTNC	Reverse Polarity TNC
RSVD	Reserved
RX	Receive
SA	System Administrator
SAEDA	Subversion and Espionage Directed Against the U.S. Army
SAMS	Standard Army Maintenance System
SAMS-1	Standard Army Maintenance System Level 1
SAMS-2	Standard Army Maintenance System Level 2
SARSS	Standard Army Retail Supply System
SARSS-1	Standard Army Retail Supply System Level 1
SARSS-2	Standard Army Retail Supply System Level 2
SBU	Sensitive But Unclassified
SCX	STAMIS Computer Exchange
SDSL	Single-pair Digital Subscriber Line
SEIP	Standard Engineering Installation Package
SEN	Small Extension Node
SIDPERS-3	Standard Installation/Division Personnel System-3
SINCGARS	Single Channel Ground and Airborne Radio System
SIPRNET	Secure Internet Protocol Router Network
SMR	Source, Maintenance and Recoverability
SOP	Standard Operating Procedures
SPBS-R	Standard Property Book System - Redesign
SQE	Signal Quality Error
SRA	Specialized Repair Activity
SRU	System Replaceable Unit
SSID	Service Set Identification
SSA	Supply Support Activity
SSH	Secure Shell (used in Unix)
SSR	System Support Representative
STAMIS	Standard Army Management Information Systems
SUI	Sensitive Unclassified Information
SUM	Software User Manual
SW	Software
SYNC	Synchronize
TACCS	Tactical Army Combat Service Support Computer System
TACCS-E	Tactical Army Combat Service Support Computer System - Enhanced
TAMMS	The Army Maintenance Management System
TB	Technical Bulletin
TCB	Trusted Computer Base
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDA	Table of Distribution and Allowance
TDR	Transportation Discrepancy Report

TFSA	Task Force Support Area
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TM	Technical Manual
TMDE	Test, Measurement and Diagnostic Equipment
TNS	Tactical Name Service
TOC	Tactical Operations Center
TOE	Table of Organization and Equipment
TPN	Tactical Packet Network
TRI-TAC	Tri-services Tactical
TTA	Tactical Terminal Adapter
TX	Transmit
TYAD	Tobyhanna Army Depot
UCPN	Unclassified Packet Network
UIC	Unit Identification Code
ULLS	Unit Level Logistics System
UPS	Uninterruptible Power Supply
USAISEC	U.S. Army Information Systems Engineering Command
USAISSC	U.S. Army Information Systems Software Command
USERID	User Identification Name
UTP	Unshielded Twisted Pair
UUT	Unit Under Test
U/M	Unit of Measure
VA	Volt Amperes
VAC	Voltage Alternating Current
VDC	Voltage Direct Current
VEE	Virtual End-to-End
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
XMT	Transmit

Appendix H

SAFE GROUNDING OF COMMUNICATIONS–ELECTRONICS EQUIPMENT IN THE FIELD

H.1 PURPOSE AND SCOPE

This appendix describes earth ground systems and how to install them. Grounding helps protect personnel and equipment from faulty power systems and from lightning strikes. Grounding also reduces circuit noise and other transmission interference in communications systems. These instructions will help you set up a safe ground system for your equipment or shelter.

H.2 THE EARTH GROUNDING SYSTEM

a. Theory. An earth grounding system helps keep the electrical potential on metal surfaces at the same level as the surrounding earth. Earth grounding also provides a discharge path for externally generated electrical surges, including lightning. An earth ground is made by electrically connecting a generator, shelter, or structure to a buried metal conductor that is in contact with moist subsoil or reaches into the underground water table. The type of ground conductor and method of installation you use depend on the climate and soil conditions of the site.

b. Ground rods and plates. A ground rod is generally the most effective conductor. You may get a good ground by connecting to a buried metal object already at the site, such as a metal pipe or a steel building frame. In the desert or other places where ground conductivity is poor, a ground plate or several ground rods connected together will be better than a single ground rod.

c. Soils. Some types of soil make a better electrical ground than others. Use the type of ground conductor that works best for the soil in your location, as shown in table H–1. Under very poor or poor conditions, take special steps, as explained in paragraphs H.5, H.7, and H.8.

Table H–1 Ground Conductor for Various Soil Types and Qualities of Ground

TYPE OF SOIL	QUALITY OF GROUND	GROUND CONDUCTOR
Fine sand with high moisture content	Very good	Ground rod
Clay, loam, or shale	Good	Ground rod or ground plate
Clay, loam, or shale mixed with gravel or sand, or gravel, sand, or stone	Poor and Very poor	Buried metal object, or a ground plate, or several ground rods electrically connected together

H.3 SELECTING A GROUND ROD

a. **Moist Soil Conditions.** In moist soil, select either the 8–foot ground rod NSN 5975–00–296–5324 or the 6–foot ground rod NSN 5975–00–224–5260. Both are single–section rods with a built–in driving head and a thumbscrew coupling for connecting to a ground strap, as shown in figure H-1.

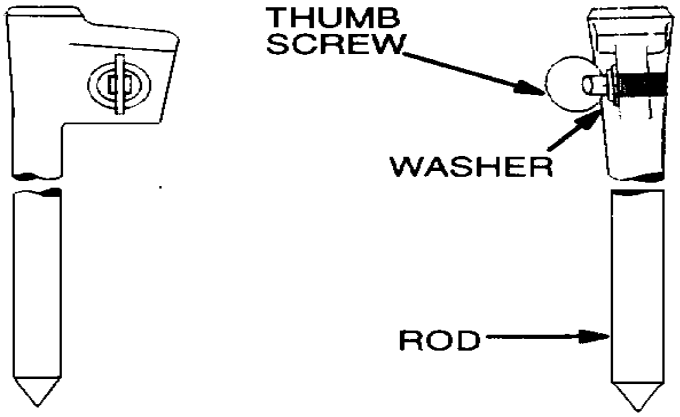


Figure H-1 Single-Section Ground Rod

b. **Dry Soil Conditions.** In dry soil, select a multiple–section rod, such as NSN 5975–00–627–1552 or NSN 5975–00–878–4868, as shown in figure H–2. Drive the rod deep enough to reach moist subsoil. If there is no moist subsoil or the soil won't allow deep penetration, drive the rod as deeply as you can, then apply salt and water as explained in paragraph H.5. See paragraphs H.7 and H.8 for other ways to improve grounding when soil conductivity is poor.

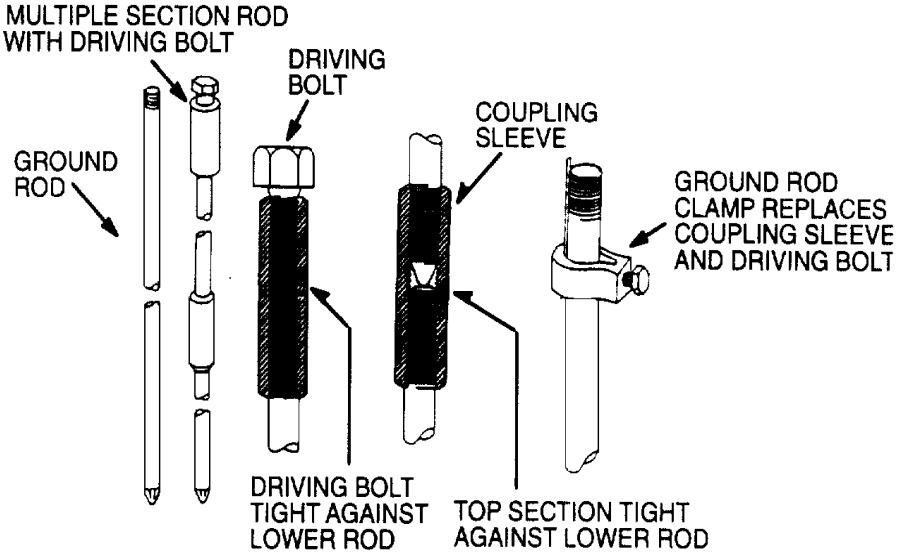


Figure H-2 Multiple-Section Ground Rod

H.4 HOW TO INSTALL GROUND RODS

a. Clean the rod to remove all grease, oil, or paint. Wear gloves to protect your hands from sharp metal, as shown in figure H-3.

Figure H-3 Proper Cleaning of Ground Rod

b. Dig a hole at least 12 inches deep and 36 inches across.

c. Drive the rod through to moist subsoil. To install a multiple–section ground rod, use a driving hammer as shown in figure H-4. Allow about 3 inches of the rod to protrude above the bottom of the hole.

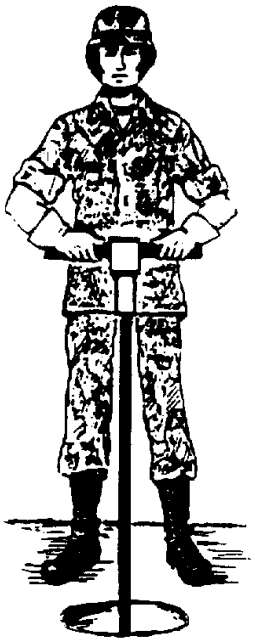


Figure H-4 Proper Method to Drive a Ground Rod

d. Connect the rod to the equipment or shelter using a ground strap. If you don't have a ground strap, use a piece of the heaviest gauge wire you can find, #6 AWG or larger, preferably copper.

e. Connect the ground strap to the ground rod.

(1) Use the terminal screw on the ground rod. If it is missing or broken, connect the ground strap (or heavy wire substitute) with a tight–fitting clamp as shown in figure H–5.

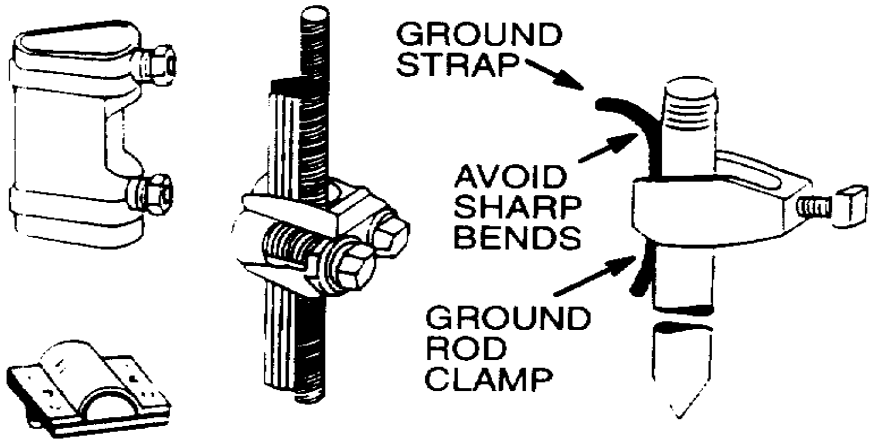


Figure H-5 Proper Method to Connect Ground Strap to Ground Rod

NOTE: ***DO NOT TIE*** *the ground strap (or heavy wire substitute) to the rod or loop it around the rod. A knot or loop will greatly reduce the effectiveness of the ground. The strap must be connected by the terminal screw, a clamp or bound with wire to the rod.*

(2) If you can't find a clamp, bind the ground strap (or heavy wire substitute) to the ground rod with at least 24 turns of stripped telephone wire or other bare wire as shown in figure H–6. Tightly twist the ends of the wire together. Tape the connection to block out moisture.

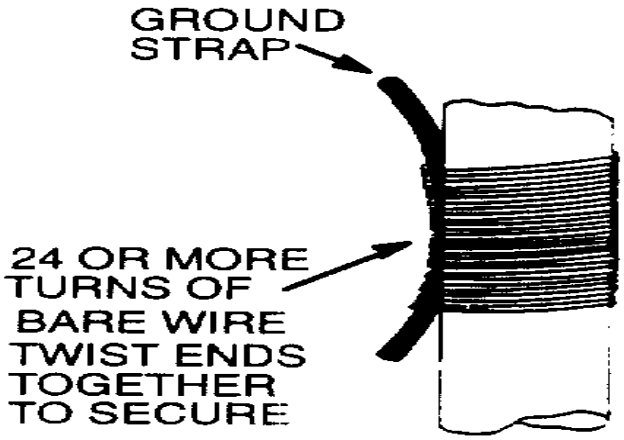


Figure H-6 Substitute Method for Ground Strap Binding

f. After you connect the ground strap (or heavy wire substitute) to the ground rod, connect the other end to the ground lug on the shelter or equipment. Keep the strap or wire as short and straight as possible and make sure there are no loops or knots. Make sure all connections are clean and tight. Figure H–7 shows a complete earth ground system.

g. Fill the hole with water and let it soak in. Then fill the hole with soil. Add water as often as needed to keep the soil moist around the ground rod, at least once a day if it doesn't rain.

h. Check the ground strap every day. Make sure the wire connections are clean and tight.

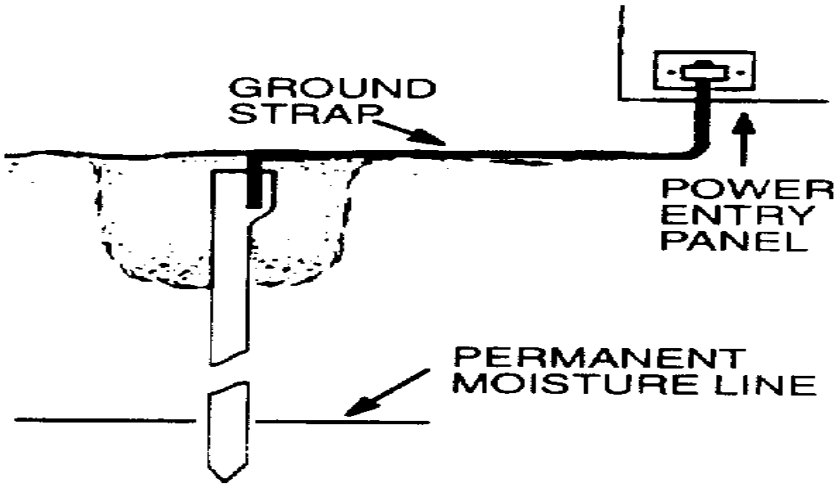


Figure H-7 Complete Earth-Ground System

H.5 IMPROVING SOIL CONDUCTIVITY

Increase soil conductivity by adding salt and water as shown in figure H–8. Use one pound of salt per gallon of water. Replace salt that leaches into the soil by mixing salt with the water at least once a week for the first four weeks of use. Then add the mixture of salt and water at least once a month.

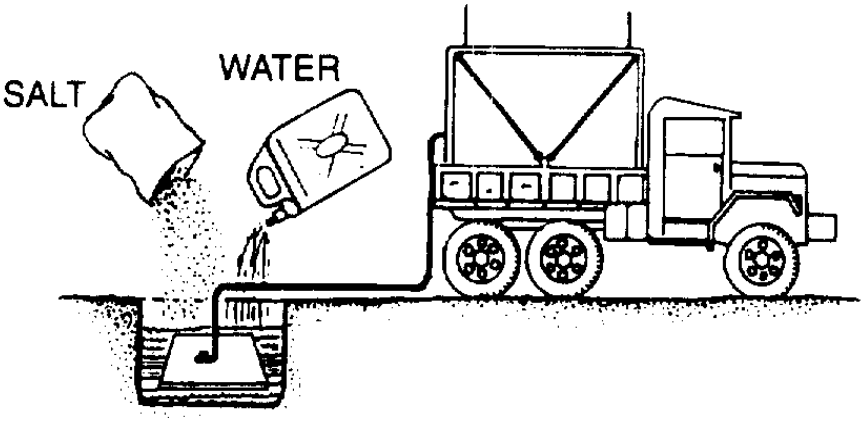


Figure H-8 Improving Soil Conductivity with Salt and Water

H.6 GROUNDING WITH UNDERGROUND OBJECTS

WARNING; DO NOT ATTACH GROUND TO ANY PIPE OR CONTAINER USED FOR GASOLINE OR OTHER FLAMMABLE GASSES OR LIQUIDS.
Metal objects buried at least six feet underground, such as pipes, steel building frames, metal poles, and storage tanks, provide excellent grounding. Connect the ground strap to the underground metal object with a clean, solid connection. Do not wrap or tie it on; avoid sharp bends. Figure H–9 shows examples of good connections to buried objects.

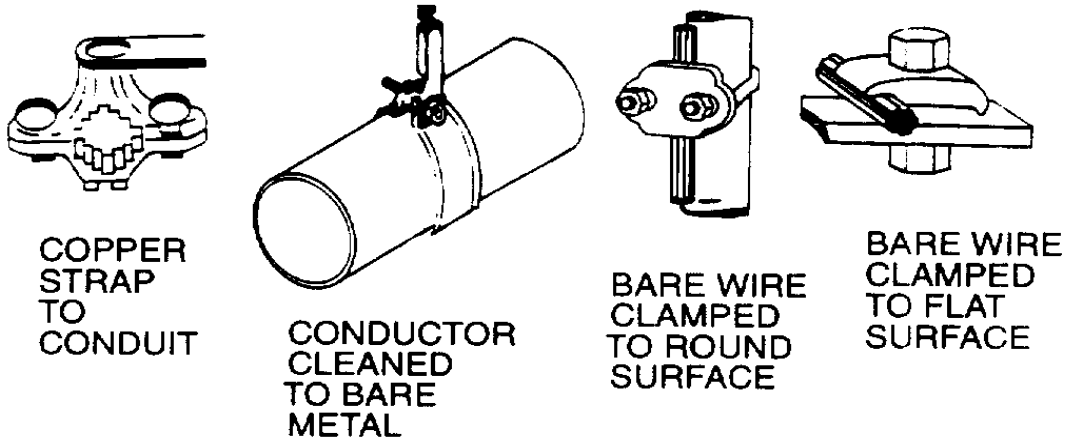


Figure H-9 Examples of Good Ground Connections to Buried Objects

H.7 GROUNDING IN POOR SOIL

When your site does not have fine topsoil, clay, loam, or shale, you must compensate for poor electrical conductivity as described in paragraphs H.7.a through H.7.e and H.8.

a. Desert.

1. In the desert, a ground plate may work better than a ground rod. Use a clean, bare metal plate or sheet at least 3 feet square and at least 1/8 inch thick. Select a metal bolt, nut and lock washer, and then drill a hole in the center of the plate just large enough for the bolt. Fasten a ground strap to the plate as shown in figure H–10. Make sure the connection is clean and tight. Bury the plate at least four feet underground. Apply salt and water as described in paragraph H.5.

2. Make a clean, tight connection to your equipment or shelter and check it every day.

3. If necessary, install several rods or ground plates and connect them together as described in paragraph H.8.

b. Sandy soils, gravel, stones, and soils mixed with gravel or sand.

For ground rods, dig a hole 1-foot deep and 36 inches in diameter. For ground plates, dig a hole at least 4 feet deep, large enough to install the plate horizontally. Install the rod or plate as described in paragraphs H.4 and H.7.a. Keep the soil around the rod or plate moist and use salt to improve conductivity as described in paragraph H.5.

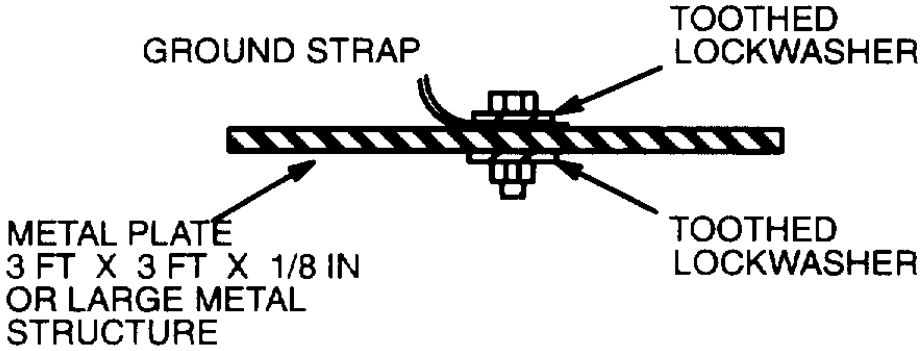


Figure H-10 Desert Ground System

c. Mountains.

It may be impossible to penetrate to moist soil or a water table in many mountainous areas. To properly ground your equipment, you must find a site where a ground rod can be installed. Streambeds are usually the best locations. (See figure H–11.) If you cannot drive a rod to its full length, install additional rods as described in paragraph H.8.

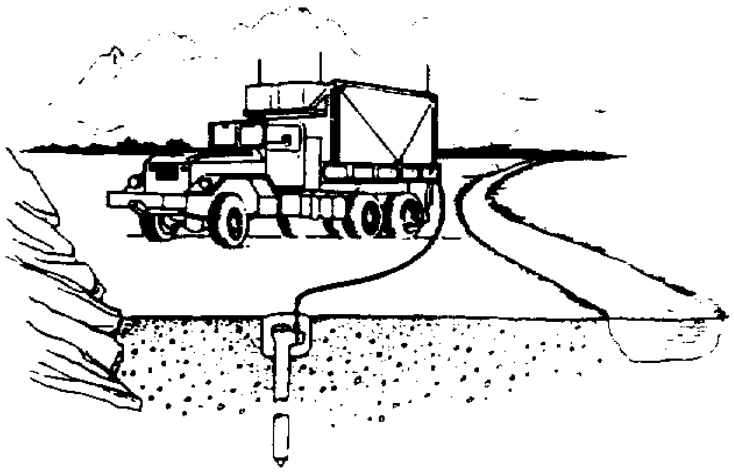


Figure H-11 Streambed Ground System

d. Tropics.

Install the ground rod as in paragraph H.4. Because of the humidity, take care to keep the strap connections clean and dry. Cover the connection to the ground rod with waterproof tape and check it every day.

e. Arctic.

Try to connect to a buried metal object such as an underground pipe or a building frame. Otherwise, drive in several ground rods as deeply as possible. Space them at least two-rod lengths apart and connect them with #6 AWG or larger bare copper cable or braid. Connect the ground lug on the power entry panel of the shelter to the closest ground rod. Treat the soil with salt and water as described in paragraph H.5. Figure H–12 shows some possible ground rod layouts.

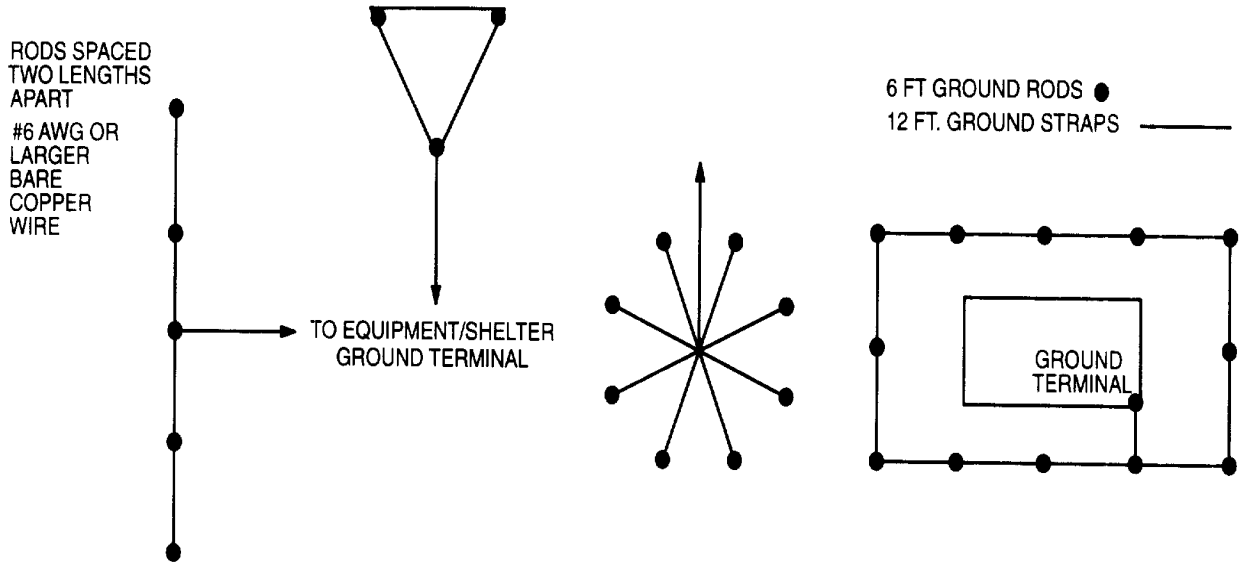


Figure H-12 Possible Ground Rod Layouts to Improve Ground

H.8 HOW TO IMPROVE YOUR GROUND

When a single ground rod provides a poor ground, drive in extra rods as shown in figure H–12. If you can, use 8 or more rods. The more rods you use, the better the electrical connection to the earth. Install rods around the perimeter of your shelter or equipment spaced 2-rod lengths apart. Connect all rods together and connect the closest rod to the shelter's power entry panel ground connector using the heaviest wire you can find, preferably #6 AWG or larger bare copper cable. If possible, connect other perimeter rods to other points on the shelter. Treat the soil around each ground rod with salt and water as explained in paragraph H.5. If a perimeter installation is impractical, install the rods in one of the other layouts shown. Connect the center rod to the shelter and treat the soil with salt and water as explained in paragraph H.5.

H.9 SHELTERS AND NEARBY EQUIPMENT

WARNING; DURING THUNDERSTORMS, LIGHTNING FLASHOVER OR ARCING CAN OCCUR BETWEEN TWO OR MORE UNCONNECTED OR POORLY CONNECTED ADJACENT METAL STRUCTURES. FLASHOVER CAN CAUSE LETHAL VOLTAGE ON THE GROUND IN THE VICINITY OF THESE OBJECTS.

To avoid lightning flashover, separate equipment shelters, antenna masts, and other metal structures by at least 6 feet or connect them with heavy copper cable. Cables should be as short and straight as possible. Connect all structures and objects located within 25 ft of each other to a common ground as shown in figure H–13. This will help prevent dangerous voltages between shelters and reduce signal interference from stray (or common mode) ground currents.

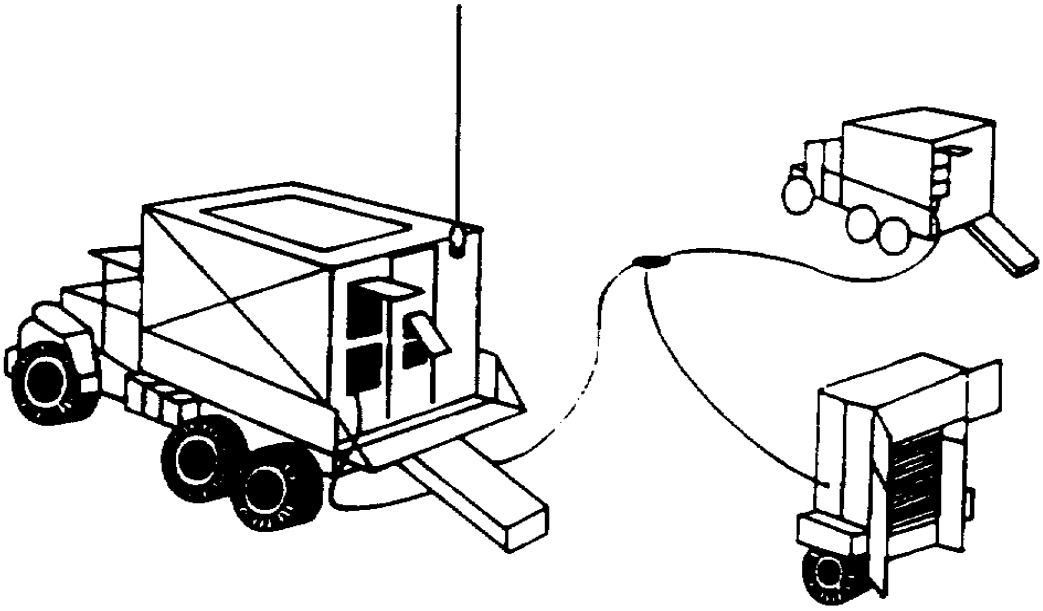


Figure H-13 Prevent Lightning Flashover by Grounding

WARNING; LIGHTING WARNING FOR STAND-ALONE EQUIPMENT WHEN THUNDERSTORMS THREATEN, DISCONNECT POWER FROM STANDING ALONE EQUIPMENT THAT IS NOT SHELTERED BY SEPARATE LIGHTNING PROTECTION SYSTEM. THEN SEPARATE ALL SUCH EQUIPMENT BY AT LEAST 6 FEET OR BOND THEM TOGETHER WITH HEAVY COPPER CABLE.

NEED MORE INFORMATION?

See FM 11–487–4 and MIL–HDBK–419A, Vol. II. For help, contact your local safety office or your CECOM Logistics Assistance Representative or the CECOM Safety Office. You may call CECOM Safety at DSN 992–0084 or (732) 532–0084, or write to:

Commander, US Army CECOM
ATTN: AMSEL–SF–SE
Fort Monmouth, NJ 07703–5024

THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX I

CAISI Planning

I.1 General

CAISI provides local area networks (LANs) for combat service support (CSS). To do this, CAISI offers two services: data transmission and protocol conversion. Each CAISI LAN connects to the Area Common-User System (ACUS). This allows Standard Army Management Information System (STAMIS) and CSS computers to exchange data locally and throughout the battlespace.

Although CAISI provides communications, it belongs to the CSS units, not to Signal. In this respect it is similar to the unit's combat net radios (CNR). The Signal staff (S-6), Integrated Systems Control (ISYSCON), and Combat Service Support Automation Management Office (CSSAMO) staff provide overall supervision and assistance where necessary. But users install, operate, and maintain (IOM) the CAISI equipment. The CAISI is used in conjunction with unit computers and has no separate dedicated installers, operators, or maintainers. CAISI is not a single, central nexus; it consists of numerous components, distributed amongst the users.

I.2 Networking

In Information Technology, a network is a series of points or nodes interconnected by communication paths. Networks can be characterized in terms of spatial distance as LANs or Wide Area Networks (WANs).

I.2.1 What is a Local Area Network?

In the simplest of terms, a local area network (LAN) is a collection of computers and network devices connected by a shared path, or medium, usually cables. The usual symbol for a LAN, shown to the right, reflects this concept of sharing. In some LANs, such as the CAISI, radio links replace or supplement the cables. It is the sharing of common transmission medium that defines the network as local. Obviously, a computer at the Corps Support Command or Division Support Command is not "local" to a computer at one of the Brigade Support Areas. They do not share a common cable and therefore cannot be in the same LAN, even though they communicate frequently.

LANs, to include the CAISI, are generally classified as "base band" networks. This means that all or a part of the transmission medium can carry only one signal at a time. Even if portions of the network, such as the radios, can carry multiple simultaneous signals, the network overall can only handle one.

Communications among the computers, and the way they share the network medium, are governed by protocols. CAISI is an Ethernet network. As such, there are standards for the way data is packaged, addressed, and controlled. Ethernet uses a media access control (MAC) mechanism called Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to control the traffic. This means that everybody listens before talking, and if two devices try to talk at the same time (resulting in a collision), both of their signals are cancelled. To avoid a second collision, they each wait a random period of time before trying again.

The more we can segment the LAN into separate physical networks, the fewer collisions there will be and the more traffic you can pass. Segmentation is a major factor you must take into account when laying out your network.

In order to simplify wiring the LAN and to reduce the amount of cable needed, a LAN usually contains one or more hubs, as shown on Figure I-1. The computers are each connected to the hub. The hub retransmits the packets to the other computers. In order to segment the LAN, switches are often substituted for the hubs. Switches retransmit packets only down the paths needed to reach the destination, not down all paths.

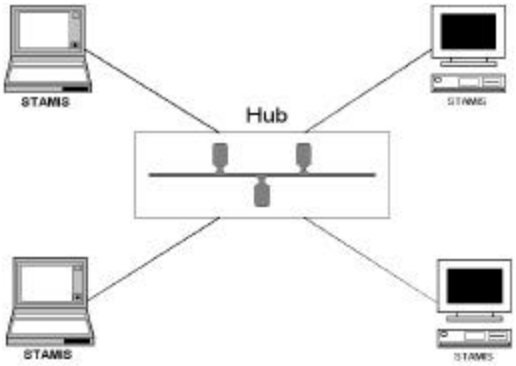


Figure I-1 The Local Area Network (LAN)

So that no one device monopolizes the LAN, the traffic is divided into packets and the packets are transmitted separately. The packets have a standard size header and variable size data loads. Each packet contains addressing and accounting information so that they can be reassembled into a complete, properly sequenced message by the receiving computer or device.

Within the CAISI LAN, there are a number of different network media, each with its own protocols, capabilities and limitations: serial cables, coaxial cables, unshielded twisted pair (UTP) cables, digital subscriber link (DSL) field wires, and wireless links (radio). All are connected together into a single virtual medium, that is to say, a LAN.

I.2.2 What is a Wide Area Network?

Again in the simplest of terms, a wide area network (WAN) consists of two or more LANs connected by one or more long-distance communications links. Routers are required at each end to control the traffic between the LANs. The symbol for a WAN is usually a cloud, because a WAN normally includes numerous long distance links and the route taken by one packet may be different than the route taken by the next packet, even if it is from the same source and going to the same destination.

Signal units provide the long-haul communications (communications between tactical LANs). A small extension node (SEN) or large extension node (LEN) at the field site is connected to the line-of-sight (LOS) radio van that connects to the next LOS van in the communications network. The SEN, LEN, and LOS vans are parts of Signal's mobile subscriber equipment (MSE) system. MSE provides tactical voice and data communications, the ACUS. The data portion is the tactical packet network (TPN). Data travels over the TPN. The SEN and LEN vans contain packet switches (along with other Signal magic) to control the traffic. Each collection of computers is a separate segment of the network.

Because MSE radios are encrypted, MSE is cleared for SECRET traffic. All operators, connected computers, and users must be cleared. This presents a problem for CAISI, because CAISI is used by soldiers and computers not cleared for SECRET. STAMIS and CSS traffic is Sensitive Unclassified Information (SUI), formerly known as Sensitive But Unclassified (SBU). So an inline network encryption (INE) device called a Network Encryption System (NES) is placed between CAISI and the packet switch at each site. The NES encrypts the data flowing from and to the CAISI LAN. Computers connected to the TPN cannot read CAISI traffic and computers connected to the CAISI cannot read secret TPN traffic. The NES also serves as the required router to connect the CAISI LANs together into a WAN.

A Domain Name Service (DNS) server, to translate computer names into addresses, is provided by Signal. It is separate from the Tactical Name Service (TNS) server because the TNS cannot be used by CAISI or CAISI-supported computers. The TNS is on the classified portion of the network. The DNS is on the SBU portion. The Wide Area Network, including CAISI LANs and the TPN, is shown on Figure I-2.

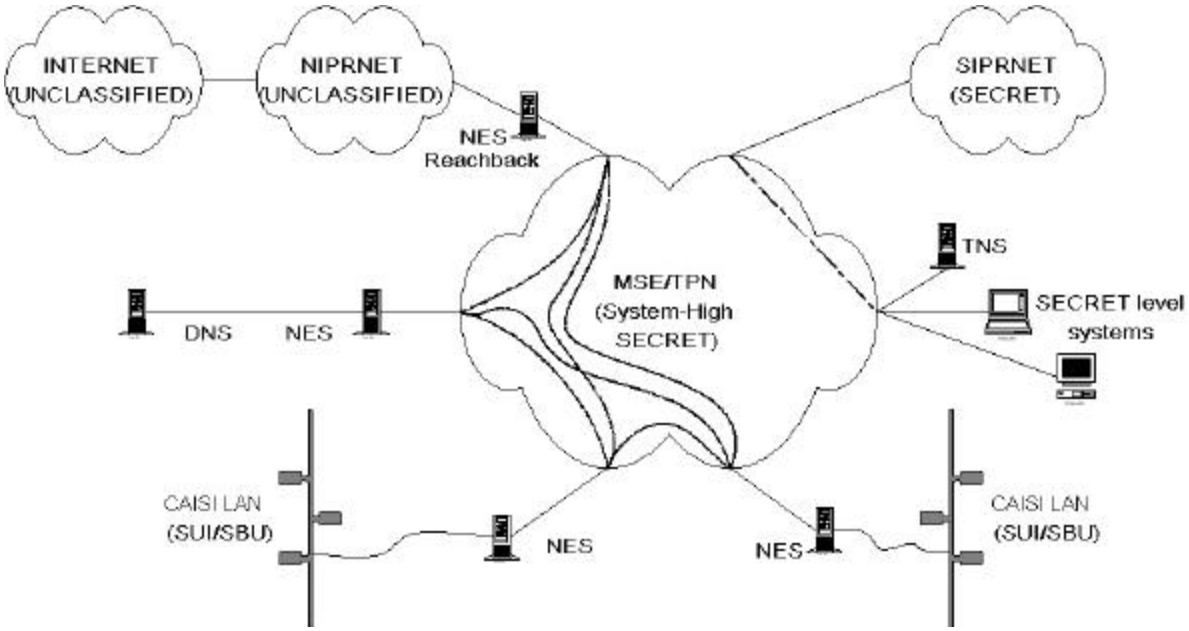


Figure I-2 The Wide Area Network (WAN)

A new generation of INE devices will soon be fielded to replace the NES. The TACLANE will work a little differently. Instead of acting as a router, the TACLANE will allow the routers within the TPN to control the traffic. Additionally, the TACLANE will act as a DNS proxy, taking DNS requests from the CAISI side and going to the TNS for a response, which it will relay back to the CAISI side. Thus a separate DNS server will no longer be required.

A number of networking issues, particularly addressing, will arise as TACLANE replaces the NES. The TPN and SBU portions of the network will, for instance, no longer be allowed duplicate IP addresses. Signal, however, will handle this. CAISI needs only to be prepared to use the addresses provided by Signal. And possibly to supplement them with additional "private" addresses behind the optional network address translation (NAT) routers provided in the CAISI system support representative (SSR) Accessory Kit.

I.2.3 What is Wireless Networking?

There are two basic categories of wireless networks – for simplicity, we'll call them "local" and "cellular." Wireless networks are related in much the same way as local and cellular wireless telephones.

You may have a wireless handset in your house and a cell phone in your pocket. Your low-power local wireless handset has a very short range, and is tied to your low-power local base station connected to the wall jack. The wall jack is in turn wired to the telephone central office, which is connected to the big telephone network. Your cell phone, on the other hand, is higher powered and connects to high-power towers scattered across the countryside. Your cell phone can connect to any compatible tower, and as you move, your call might be handled by different towers, each serving a geographical area,

or "cell." Your tactical digital non-secure voice terminal (DNVT) or digital subscriber voice terminal (DSVT) desk phone is a "local" telephone, wired to the tactical version of the central office, the MSE switch. Your mobile subscriber radiotelephone terminal (MSRT) is a tactical version of the "cell" phone, connecting to the nearest radio access unit (RAU), the tactical version of the cell tower.

Cellular wireless data networks work the same way as cellular phones. The computer uses a modem connected to a radio (either in a single modem/cell phone unit in the computer, a modem card in the computer connected to a cell phone, or even a browser built into the phone itself) to dial in to a service provider to access the network. Just like you use a modem in your home computer connected to your home phone to dial in to the Internet. The difference is that you use a cell phone instead. Your speed is also very limited, in fact usually even more limited than from your home phone.

Local wireless networks like CAISI, on the other hand, are an expansion of the capabilities of traditional local area networks. Your network interface card connects, via radio, to an access point connected to the local network. The CAISI wireless gives you about the same speed as when you are directly connected to a 10MB wired LAN, and relies upon MSE to connect the LAN to the TPN for wide area network access. As the MSE backbone improves, as it is scheduled to do, your WAN access will improve.

I.2.4 What are TCP/IP Addresses?

As mentioned earlier, packets are actually delivered within the LAN based on MAC addresses. Every network device, including the network interface card (NIC) in a STAMIS or CSS computer, has a unique MAC address. But MAC addresses are based on who built the devices, not where they are located. Sending data based on MAC addresses would be like trying to mail you a letter based on your Social Security account number. What we need is the data equivalent to a street address, city, state, and zip code. The Transmission Control Protocol/Internet Protocol (TCP/IP) address it is. Each TCP/IP address is composed of a network portion and a host portion. The host portion is the street number, and the network portion is the street name, city, state, and zip. Routers along the way read the TCP/IP address and send the packets to the next router in line based on where it is going. In much the same way that mail is forwarded from your local post office to a regional one, to another regional one, to a local office, and finally to a carrier to deliver to your house. Only the postal carrier at the far end needs to know exactly where your house is.

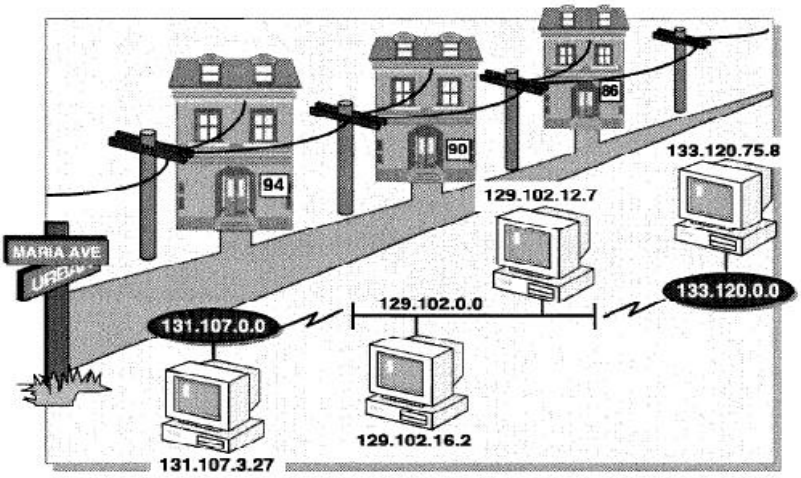


Figure I-3 IP Address vs. House Address

1. **Overview of TCP/IP**. Networks can also be characterized by the type of data transmission technology in use on it, for instance a TCP/IP network.

a. TCP/IP, which stands for Transmission Control Protocol/Internet Protocol, actually refers to a suite of protocols that facilitate the passing of data between computers on a network.

b. TCP/IP is supported on almost all modern computer systems and it has therefore become the most commonly accepted protocol available. It is the protocol of the Internet and is used to communicate on a global basis.

c. The TCP in TCP/IP provides the end-to-end reliable connection; IP is the addressing scheme (the data equivalent to a street address, city, state, and zip code) that allows data to be routed through multiple networks to its final destination.

(1) Each TCP/IP address is composed of a network portion and a host portion.

(2) The host portion is the street number, and the network portion is the street name, city, state, and zip.

2. **IP Network (Packets).**

a. With an IP network, an Internet-connected computer breaks data down into packets for transmission across the network. The Internet Protocol prepares the packets with an address so that they can be routed to their destination. The use of Transmission Control Protocol (TCP) ensures that all data sent is received at the destination computer.

b. What is included in an IP packet? Each packet contains a header that indicates its origin and an IP address of its destination.

c. IP Address. Consists of the following:

(1) Consists of four octets – xxx.xxx.xxx.xxx

(2) Each octet can be from 0 – 255. 0 and 255 are reserved for special use. Example is 192.168.1.3.

(3) Parts of the address will be used to identify the network being used (first three octets) known as the network id and part of the address is being used to identify the computer (last octet) known as the host id.

An example of this is a network behind a NES.

(a) The first 3 octets will display the network being used.

(b) The final octet displays the unique address of the individual device on the network. Example 192.168.1.3

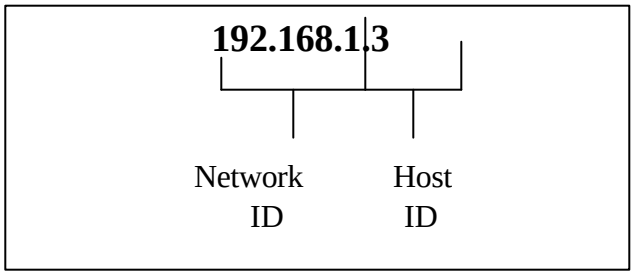


Figure I-4 IP Address

(4) Divided into 5 classes: A, B, C, D and E. (Table I-1)

(a) Class A. The first octet can be 1 – 126 as the network id. Other three octets are used for the host id. (Large organizations – 126 networks, 16,777,214 users per each network id – 1, 2 ..126.)

(b) Class B. First octet can be 128 – 191. Network id is the first two octets. Network id can range from 128.0 through 191.254. The remaining two are the host-id. (Medium size organizations – 16,384 networks, most commonly used – 64,516 user per each network id – 128.0, 129.0, etc..)

(c) Class C. First octet can be 192 – 223. Network id is the first three octets. Network ids can range from 192.0.0 through 223.254.254. Last octet is for the host id. (Small organizations – 2,097,152 networks, only 254 users network id – 192.0.0, 193.0.0, etc..).

(d) Class D. First octet can be 224 – 239. Used for multicasting. Limited use. A multi-cast address is a unique network address that directs packets with that destination address to predefined groups of IP addresses.

(e) Class E. First octet can be 240 – 255. Reserved for research.

Table I-1 IP Addresses for Network Classes

Class	Network ID Ranges		Number of Networks	Users per Network ID
	(xxx's denote the Host ID)			
	to			
A	1.xxx.xxx.xxx	126.xxx.xxx.xxx	126	16,777,214
B	128.0.xxx.xxx	191.255.xxx.xxx	16,384	64,516
C	192.0.0.xxx	223.255.255.xxx	2,097,152	254
D	224.xxx.xxx.xxx	239.255.255.xxx	n/a	n/a
E	240.xxx.xxx.xxx	255.255.255.xxx	n/a	n/a

3. **Standard TCP/IP users on the CAISI**.

a. Use Transmission Control Protocol/Internet Protocol.

b. True network connections.

(1) Connected by RG-58 (Coaxial).

(2) These users have minimal impact on the CAISI.

NOTE: *Most STAMIS users that use the RG-58 are non-network capable. These individuals must register with the DNS in order to communicate with others.*

An example is the STAMIS servers SARSS or SAMS. The SARSS and SAMS must be in the DNS for an ULLS to contact and communicate with them.

4. **Network Characterized by the Physical Links.** A network can be connected in a variety of ways. There are four types of physical links. They are listed below and explained in Table I-2.

Table I-2 Networks Characterized by Physical Links

Physical Link	Characteristics
1. Coaxial Cable	RG-58 only
	Maximum Length is 185 meters
	Unless a repeater is used - total length includes from beginning to end of the segment. Even with multiple TCP/IP connectors.
	Avoid crossing generator power lines
	Avoid using barrel connectors
2. WF-16 Field Wire	Maximum Length – Tested to 4 miles using DSL
	Avoid splices, if practical
3. CAT-5 Cable	RJ-45 Connector
	10Base-T with 100 meters range
4. Wireless Networks	LOS up to but not limited to 4 miles

I.2.5 What is DNS?

The DNS is a database that keeps track of the Internet Protocol (IP) addresses of the devices within the site's control or domain. The database contains the IP addresses, names, and locations of every device connected to the network. Provides name to IP address resolution.

DNS translates names into addresses. Again, just as when using the post office, we need a way to look up your name to find your address. DNS is that. And because names are not unique, we need a way to differentiate among the many people named John Smith.

The domain name is that. A "fully qualified domain name" is the combination of the hostname (the computer or device name) and the domain name. *JohnQSmith.CompanyC.252FSB.52MechDiv.Army.Mil* is pretty unique. To look you up, I could call the military directory office that would ask the Army directory office and they would in turn ask the 52nd Mechanized Infantry Division, who would ask the 252nd Forward Support Battalion to ask Charlie Company. The company clerk would look your address up, and the response would wend its way back to me. If someone else asked the same question soon, the query might not have to all the way down to Charlie Company.

Someone along the way might remember the address. But you wouldn't want them to remember it forever, because you might have moved in the meantime.

So DNS servers cache query responses, but only for a specified short period of time. And not every query needs to go down to Charlie Company every time anyway. If your clerk sends an address change card into the regional post office when you arrive and anytime you move, the query need go no lower. DNS again works the same way.
The Army has a multi-tier DNS system to minimize query traffic. Some addresses are never submitted to the higher DNS system, however, if only locals need to look them up.

I.2.6 What are the Differences Between a Bridge and a Router?

Bridges interconnect pieces of the same LAN and routers interconnect different LANs, as shown on Figure I-5. Bridges and routers both direct traffic. Bridges do it on a computer-by-computer basis, using MAC addresses. Routers do it on a more general network basis, using TCP/IP addresses.

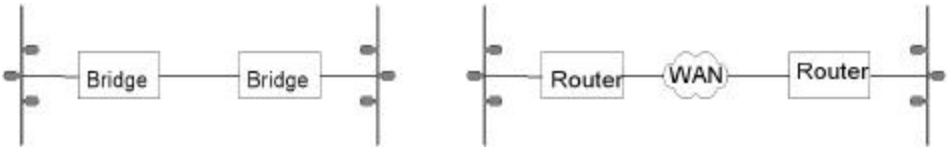


Figure I-5 Bridges vs. Routers

Bridges watch the MAC addresses embedded in the data packets and learn where the computers are. Traffic addressed from one computer to another on the same LAN segment is not relayed by the bridge. Traffic addressed to a computer on the other segment is relayed. Broadcast messages and traffic addressed to unknown computers are also relayed. Broadcast messages are usually requesting network services, such as DHCP. They are sent to a special address that goes to everybody on the local network because you don't know who is providing the service.

Routers do not relay broadcasts. If they did, the entire TPN and Internet would be immediately flooded. They direct traffic based on the destination TCP/IP address. Routers take traffic addressed to them and decide where to send it based on routing tables. Routers are smarter than bridges. The routing tables can be either static (manually built by an administrator) or dynamic (learned, based on exchanging information with other routers).

Notice that routers handle only traffic addressed to them. The computers on the LAN make the initial determination whether the traffic is local or not. If not, then the traffic is addressed to the router to be relayed. Each computer determines if the packet is addressed to another computer on the same LAN or to a computer on a different LAN by comparing the destination network address to its own network address. If the two don't match, then it must be going to a different LAN and the packet is sent to the router to be relayed. The computer uses the subnet mask in its own network configuration (parameters) to determine if the network addresses match or not.

I.2.7 What is a Subnet Mask?

The computer does a logical comparison between the subnet mask and its own IP address. It then does a similar comparison between the subnet mask and the destination address. If the two results match, then the destination is local. Otherwise the packet is sent to the router.

The subnet mask allows you to tell the network part of the address from the host part. It masks, or hides, the network part of the address. Whatever is left is the host part. But there is a more practical way to look at it. All you really want to do is to see how many bits make up the network part of the address. Then you compare that many bits of the source and destination addresses.

Since IP addresses are composed of four eight-bit numbers separated by dots, so are subnet masks. On most networks, for instance, the subnet mask is 255.255.255.0. 255 is the largest number you can make from eight bits. To use the subnet mask, convert it and your addresses to binary. The subnet mask becomes 11111111.11111111.11111111.00000000. The first twenty-four of the thirty-two bits are set (ones). If the first twenty-four bits in the source address match the first twenty-four bits in the destination address, then the networks are the same and the destination is local.

Subnet masks are always built left-to-right. All the ones are on the left and all the zeros are on the right.

To convert address numbers to binary, use the chart to the right as follows, working from left to right.

128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	1

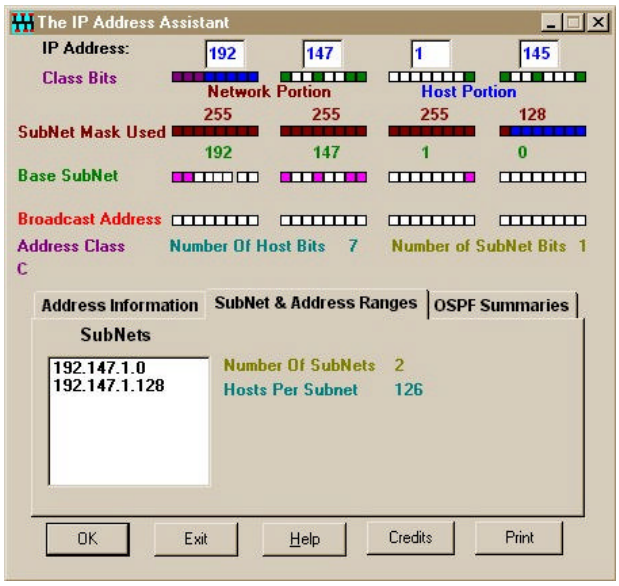
1. If the number is equal to or bigger than the first digit (128) then set the first bit and subtract 128 from the number, otherwise set the first digit to zero.

2. If the number (or remainder) is equal to or bigger than the next digit next digit (64) then set the second bit and subtract 64 from the number.

3. Repeat for each remaining bit.

4. Example: 145 converts as follows:

145 > 128 so subtract 128 and set the first bit	1
17 < 64 so the next bit is zero	10
17 < 32 so the next bit is zero	100
17 > 16 so the next bit is one	1001
1 < 8 so the next bit is zero	10010
1 < 4 so the next bit is zero	100100
1 < 2 so the next bit is zero	1001000
1 = 1 so the last bit is one	10010001



The IP Address Assistant (IPAA) tool, shown to the right, is helpful in doing these comparisons.
Choose it from the CAISI Toolbox on your SSR notebook.

- On the top line you see the address, converted to decimal (in this example, the address is 192.147.1.145).
- On the second line you see the subnet mask (in this case it is 255.255.255.128). The first twenty-five bits are set. So if the first twenty-five bits of the source and destination match, the destination is local.
- For an explanation of the rest of this screen, select “IPAA Help” or “IPAA Manual” from your CAISI Toolbox.

I.3 CAISI Network Topology

Topology is a way of doing things. It is commonly used to discuss the properties of various types of networks. Network topology refers to the way computers are connected together to form a network.

CAISI provides Local Area Networks (LAN) for Combat Service Support (CSS) Computers. When deployed, CAISI is part of a larger Army network that includes other voice and data communications, communications over radios as well as transmissions over data cables.

CAISI Network topology will deal with the layout of LSAs, CBMs, CCMs, Antenna(s), DSL(s) and Linksys router.

I.3.1 CAISI Network Components

The primary CAISI components are CAISI Bridge Modules (CBM) and CAISI Client Modules (CCM). They have been described in detail earlier in this manual. This paragraph tells how they are used and answers the following questions.

a.	How do you connect them?	Paragraph I.3.2
b.	How do you use the wireless bridge?	Paragraph I.3.3
c.	When do you use a LSA? (Legacy STAMIS vs. Network Capable STAMIS)	Paragraph I.3.4
d.	What is the network connectivity?	Paragraph I.3.5
e.	Where to place the root CBM? (Strategic location)	Paragraph I.3.6
f.	When do you use the DSL?	Paragraph I.3.7
g.	What antennas and antenna cables do you use	Paragraph I.3.8
h.	When do you use the Router	Paragraph I.3.9
i.	How do you use the Inline Encryptor?	Paragraph I.3.10

I.3.2 How are CAISI Clients Connected?

Wireless clients communicate with each other in one of two modes: ad hoc and infrastructure. In ad hoc mode, also known as peer-to-peer mode, clients communicate directly. Each client talks directly to each other client. In infrastructure mode, clients talk to an access point and the access point relays the transmission to the other client, as shown on Figure I-6.

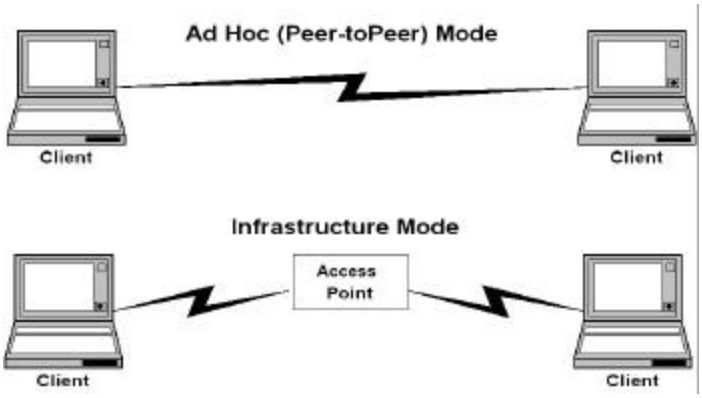


Figure I-6 Wireless Communication Modes

If all of your clients were in the same room, you'd want to use ad hoc mode. But if any client is out of range of any other, you need to use infrastructure mode. Since your STAMIS and CSS client computers in the field are miles apart and in metal vehicles and under camouflage nets (that scatter radio signals in order to defeat radar surveillance)

your clients are almost never in range of each other. Consequently CAISI operates in infrastructure mode. A CAISI LAN has more than access point (actually bridges acting as access points), as shown on Figure I-7, thus the total range of the LAN is extended.

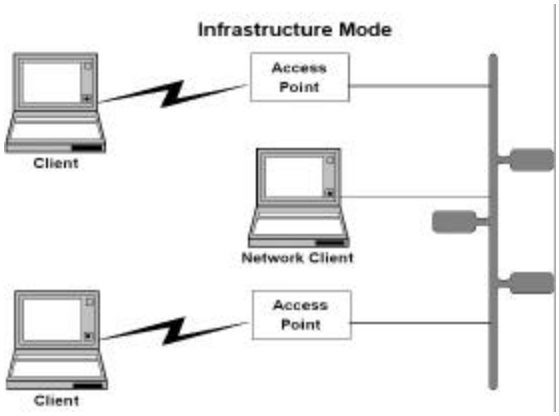
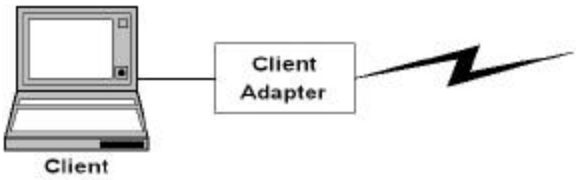


Figure I-7 Wireless Communication With Multiple Access Points

The clients are depicted in the previous two figures as computers with built-in wireless network interface cards. In fact, this will almost never be the case, for two reasons. First, the STAMIS would have to be programmed to use the wireless NIC, and none of them are. Second, every computer would need its own antenna protruding above the camouflage net.

So that the STAMIS software applications can function without change, CAISI needs to be invisible to the STAMIS. The usual wired NIC is left in the STAMIS computer (tower, desktop, or laptop) and connected to an external client adapter.



This configuration would still require one antenna per computer, so a client adapter that can support up to eight computers was selected and packaged with a hub. Now one client adapter, with one antenna, can support many computers in one work center. A work center is some number of computers in a single vehicle or under one camouflage net. That package is called a CAISI Client Module. If you have more than eight clients in a work center, use a CAISI Bridge Module instead.

NOTE: *CSS computers generally are running office automation, mail-enabled clients and web-enabled clients in a Microsoft Windows environment.*

Your unit may elect to acquire wireless network cards for these computers. But if you do, you are back to the requirement to install an antenna for every client.

You may find, however, that wireless clients located in a tent under the same camouflage net as a CBM may work OK on their small rabbit-ears antennas if they are within about 50 feet of the CBM. There is usually enough signal spillover at the lightning arrestor to connect to close-by clients. It has to be a CBM, not a CCM, because CCMs only support clients connected to their Ethernet ports. If your unit wants to try this, you will need to

use your SSR notebook to experiment to find where your best communications are within the tent.

I.3.3 How are Wireless Bridges Used?

To spread the LAN out over the ground occupied by a logistics support area in the field, we use wireless bridges to connect LAN segments, shown on Figure I-8.

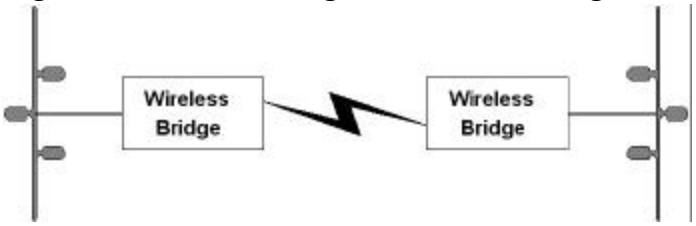


Figure I-8 Wireless Bridges Connecting LAN Segments

But the CAISI bridges are capable of acting as bridges and access points at the same time. And clients can be directly connected by wire as well. So the CAISI LAN now looks like the one shown on Figure I-9. Each CBM includes two hubs, with a total of fourteen available ports. Each bridge communicates with every other bridge in range; they are not paired up as limited point-to-point circuits. They even relay for each other throughout the network through a series of "hops", where necessary. Wireless bridge supports both 10Base2 and 10BaseT users. One wireless bridge/CBM is designated as the "root" and connects at the entry point to MSE. Each CCM must establish communication with a CBM.

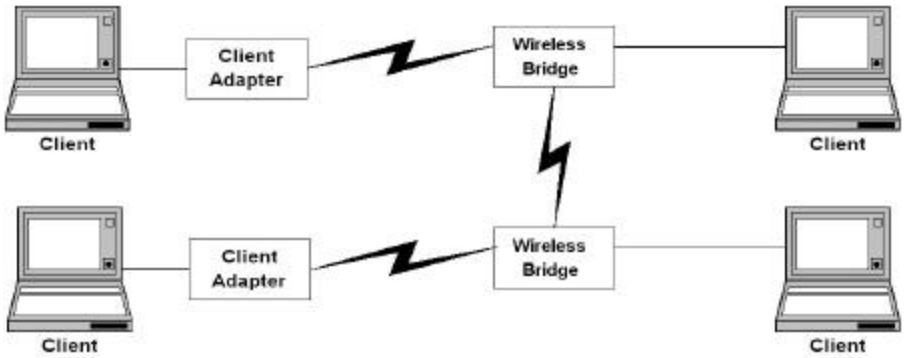


Figure I-9 Wireless Bridges Connecting LAN Segments and Clients

I.3.4 Legacy STAMIS vs. Network Capable STAMIS.

The SSR must know before hand how many LSAs, Network compatible users (TCP/IP) and STAMIS clients that require both. This is essential in structuring the network and is needed before the SSR (CSS S6) can configure each of the CAISI components. These are the questions that you need to answer:

a. Where will you need a LSA? (On STAMIS system where TCP/IP is not supported - SAMS, SPBS-R).

b. Where will you need 10BaseT/10Base2? (On a network capable STAMIS).

c. Where might you need both? (On a STAMIS server that supports both Legacy and Network Capable systems - SARSS is capable of both).

I.3.5 Network Connectivity and the CSS Community.

CAISI provides several means of extending network connectivity to the CSS community. Examples include: CBM, CCM, and DSL. Below are some considerations of each.

a. Distance considerations for the location and usages of CBMs and CCMs.

(1) Less than 100 meters use 10Base-T. (RJ-45)

(2) Less than 185 meters use 10Base-2. (RG-58)

(3) For longer distances (185 meters or more) operate in wireless mode or use DSL.

(i) Line of Sight (LOS) for CBM/CCM (up to 4 miles).

(ii) Use DSL in highly vegetative areas, around large obstacles and/or other terrain impedances. (up to 4 miles).

b. Conduct a site survey for planning purposes.

(1) Try to make a diagram of the local CSS community and centrally locate the root CBM within other wireless remotes.

(2) The object is to use more CBMs/CCMs beyond the 185 meter constraint and fewer DSL bridges.

(3) As CBMs/CCMs increase in distance from the root CBM, there is a is a thresh-hold where the bandwidth may decrease.

(i) If a CCM or CBM is attempting to communicate with the root CBM by relaying through another CBM, the bandwidth will suffer.

Figure I-10 below summarizes the various means of connectivity to the wireless CAISI:

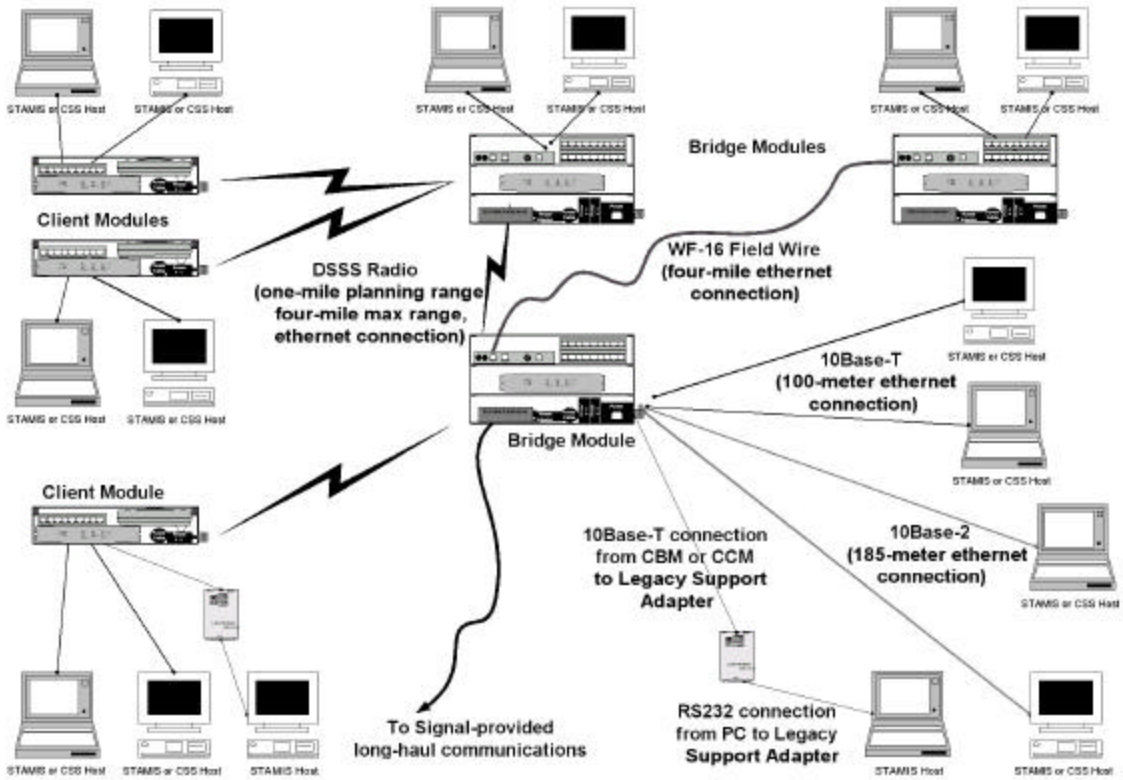


Figure I-10 CAISI Connectivity

1. STAMIS Connections to the CCMs. Most STAMIS computers will connect to the nearest CCM, using 10BaseT, 10Base2, or the LSA. These connections will be determined based on distance, STAMIS capabilities, and local SOP.

2. CCM Connectivity to a CBM. As depicted in the top center of the above diagram, each CCM must establish connection with a CBM. It is important to note, as depicted above, more than one CCM can establish radio connectivity with the same CBM.

3. CBM Connectivity to a CBM. Each CBM must be able to establish radio contact with at least one other CBM. Each CBM will also support direct STAMIS connections. The CBMs provide the "relay" function of the network, ensuring that the data continues along the network to its ultimate destination.

4. DSL Bridge Connection. In the upper right of the above diagram, there is depicted a DSL connection to the root CBM, using WF-16 field wire. Note that it is not necessary for the DSL Bridge to connect to the root Bridge, any CBM will work.

5. Root CBM to MSE. Again, remember that the root CBM does not have to be the CBM that connects to MSE, however it is often depicted that way for the sake of simplicity.

6. STAMIS to Root CBM. The root CBM is identical to the other CBMs in that it will accept all STAMIS connections as the other CBMs. The same limitations of data cable length apply.

7. CCM to Root CBM. Multiple CCMs may also connect to the Root CBM, using the radios. The Root CBM will provide the same relay functionality through the network as the other CBMs.

I.3.6 CAISI Root CBM.

Regardless of the complexity of the fielded network, the importance of the root CBM cannot be overemphasized. One CBM must always be designated as the "root" CBM. It is not essential to do so, but an easy way to keep track of the root is by designating the CBM that makes the connection to MSE at the INE device as the root, and configure it accordingly.

Strategic location of the root CBM.

a. Centrally locate the root CBM within other wireless remotes.

b. Minimize the number of hops/repeats back to the root CBM.

c. Minimize the distance of field wire (WF-16/WD1), if utilization is required.

Remember when configuring the network that each CCM must be able to establish radio contact with at least one CBM, and each CBM must be able to establish radio contact with at least one other CBM. The CBMs provide the "relay" function of the network, ensuring that the data continues along the network to its ultimate destination.

I.3.7 When Do You Use DSL Bridges?

Each CBM also includes a DSL bridge that can be used instead of or in addition to the wireless bridge. DSL bridges use wires, which we would normally prefer to avoid. So most of the time, the DSL bridges will not be used. But they are included in the CBM because they can sometimes work where the wireless cannot. They are there to help you overcome problems with METT-T factors (Mission, Enemy, Terrain and weather, Troops and support available, Time available), primarily terrain.

NOTE: *Refer to Paragraph 2.19.1 for connecting procedures of the DSL.*

Normal employment is illustrated below. The DSL bridge in a CBM is connected to the DSL bridge in another. STAMIS or CSS network clients are connected to the hubs in the CBMs.

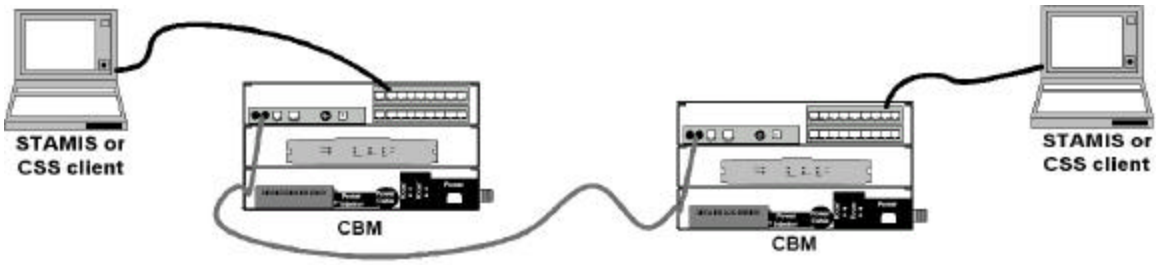


Figure I-11 Normal DSL Bridge Employment

Wireless communications can be impaired or even stopped by obstacles such as hills, heavy vegetation, or urban areas. Even your own vehicles and camouflage nets can sometimes have an impact, stopping or scattering the radio signals. In Figure I-12, part of the logistics support area is separated from the rest by an obstacle, such as a heavy forest. This is known as split node operations.

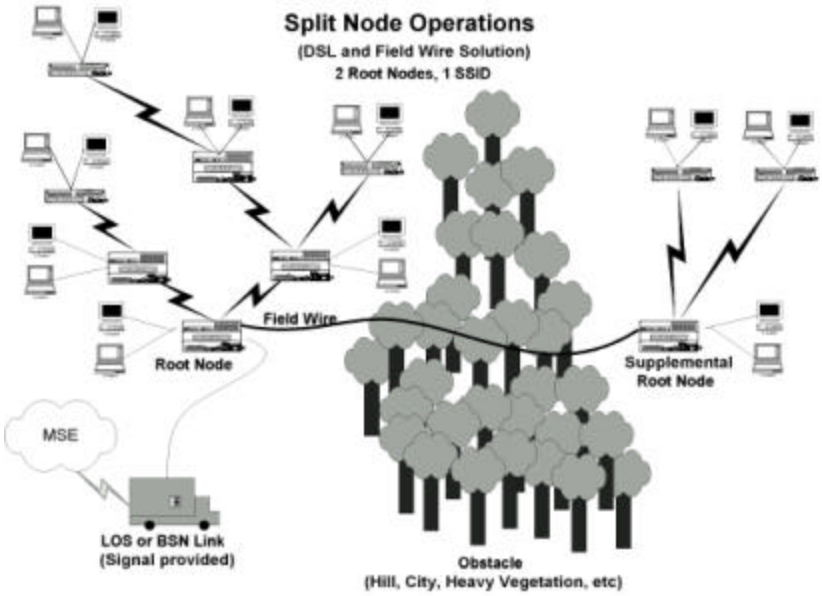


Figure I-12 Using DSL Bridges with Field Wire

In the above picture, vegetation prevents the establishment of line of sight connectivity between the root bridge and the CBM and CCMs located on the right of the diagram. In this case, a DSL Bridge is used to provide connectivity to the root node, thereby extending the network.

Notice that both the wireless and DSL bridges are in use in the two CBMs connected by field wire. Each wireless bridge is a root node for its portion of the wireless network and the two are interconnected by field wire, creating a single network segment. The DSL bridges transmit the traffic, but not the radio control commands, so each half of the network requires its own root radio.

In other cases, you might want to avoid radio emissions so as to hide your command post from the enemy. Two additional methods of splitting the node are shown in Figure I-13 and Figure I-14. In Figure I-13, you see the command post separated from the rest of the logistics support area. This gets the CP away from your local wireless LAN.

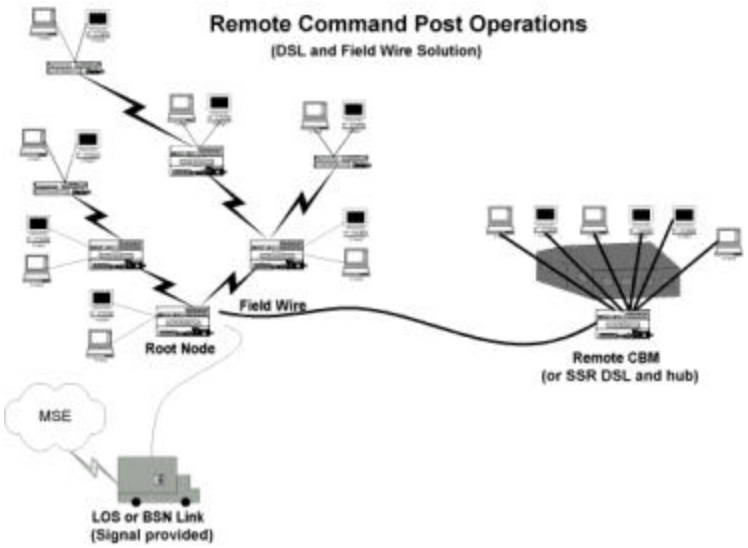


Figure I-13 DSL and Field Wire Solution – Remote Command Post Operations

In Figure I-14, you see the high-power Signal van up on a hill, far away from the support area.

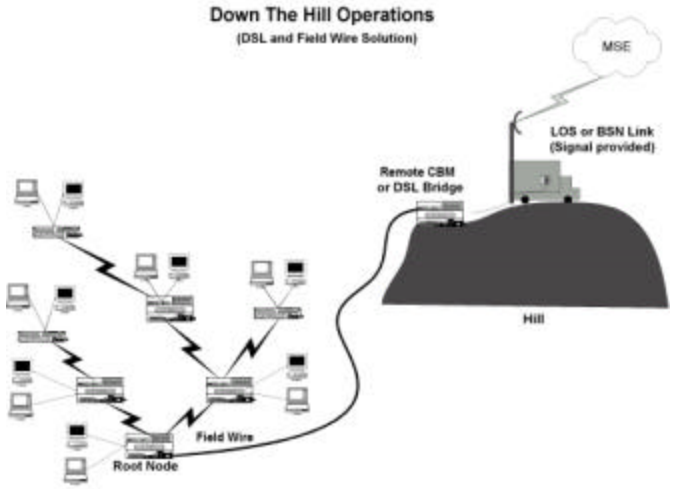


Figure I-14 DSL and Field Wire Solution – Down the Hill Operations

You might also want to use the DSL bridges, instead of wireless clients, to support areas like the ammunition supply point or the rearming and refueling point where radios are sometimes discouraged. Check with your unit safety officer.

NOTE: *Regardless of the reason for using the DSL bridges, it is essential that the speed setting on each is identical. If this is not the case, the bridges will not be able to communicate.*

I.3.7.1 Main Points of the DSL

Antennas do not work well in heavy vegetation or hills. DSL Bridges contained in the CBMs provide a solution to this problem.

a. A DSL Bridge in a CBM is connected to DSL in another CBM using WF-16 field wire. (WD1 or WD1A field wire can be used also).

b. Once connectivity is established, data from a STAMIS device connected to the first CBM may then be sent to the STAMIS device connected to the second CBM (its destination).

c. DSL Bridges are also useful in areas where radio communication is prohibited, such as an ammunition supply point. In addition, when mission requirement may prohibit radio traffic.

d. Regardless of the reason for using the DSL bridges, it is essential that the speed setting on each is identical. If this is not the case, the bridges will not be able to communicate.

I.3.8 Antennas and Radio Frequency (RF) cables

Antennas and radio frequency (RF) cables are provided with each CBM and CCM. Choice of wireless antenna(s) is based on Distance, Obstacles and Terrain (DOT). (An overview of all antennas and RF cables is in Table I-3).

There are two basic types of antennas: directional "panels" and omni-directional "whips". Both antennas are made of ruggedized fiberglass and have standard female "N" – type connectors.

a. Omni-directional "whips" are used on most CBMs/CCMs and come in two sizes:

(1) The forty inch whips are issued with the CBMs.

(2) The twenty-four inch whips are issued with the CCMs.

Omni (whip) antennas are easy to set up and need not be aimed, however they must be mounted vertically.

The taller the whip, the flatter the signal and the more effective power. This effect is called "gain". The more gain, the greater the range. However, there is a trade-off. Because the signal is flat, the two ends have to be at the same elevation.

Otherwise the signals will pass over each other. This is explained in more detail in Paragraph I.5.2.

b. Directional antennas "panels" are used for special circumstances and come in two sizes: Seven and fourteen inches square.

The large directional antennas (14-in) are furnished in the SSR Accessory Kit for special circumstances.

(1) Low gain - Used for short distance.

(2) High gain - Used for longer distances or harder shots.

The panel antennas concentrate all the radio output in a "beam" – in one direction. The bigger the panel, the tighter the beam, and the more gain. The more gain, the greater the range. However, there is a trade-off. As the gain increases, aiming the beam becomes more difficult.

Table I-3 Location of Antenna and Antenna Ancillary Components

Location	**Antenna/Ancillary Component**
CBM	40-inch Whip break-away antenna (omni-directional)
	7-inch Directional Panel antenna
	7-inch Antenna bracket
	25-ft RF antenna cable
	35-ft RF antenna cable
CCM	24-inch Whip antenna
	7-inch Antenna bracket
	35-ft RF antenna cable
SSR Transit Case	40-inch Whip break-away antenna (omni-directional) (Qty: 2)
SSR Antenna Carrying Case	14-inch Directional Panel antenna (Qty: 2)
	7-inch Antenna bracket (Qty: 2)
	14-inch Antenna bracket (Qty: 2)
	50-ft RF antenna cable (Qty: 4)

NOTE: *Before running the field wire to connect the DSL Bridge, you may wish to attempt to establish connectivity using the panel antennas fielded with the SSR Accessory Kit.*

The wireless bridges in the CBMs and SSR Accessory Kit can also be used to extend the network over a wider geographic area. A pair of bridges using powerful directional antennas can sometimes span distances or obstacles that would normally keep you from communicating.

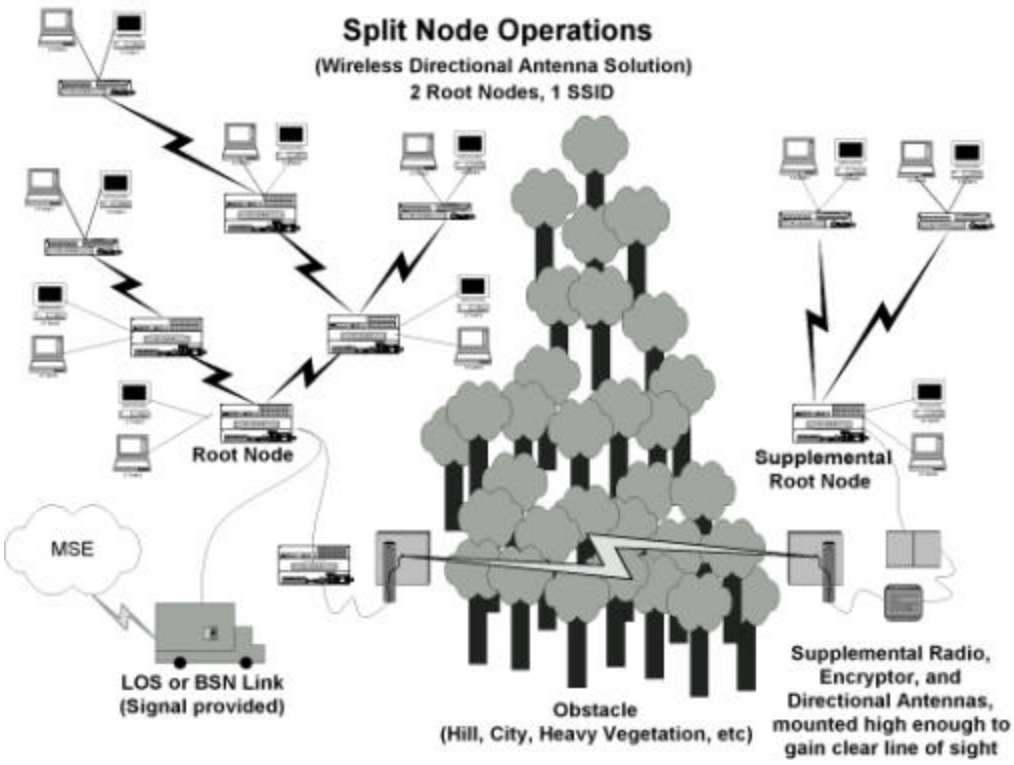


Figure I-15 Using Wireless Bridges with Directional Panel Antennas

Notice that in Figure I-15, there is an extra CBM or wireless bridge (and encryptor) at each end. This allows them to use the directional antennas without having to worry about connecting to local CBMs and clients.

You will need to configure the wireless bridge in the supplemental node as a root. You do not need to change the SSID, as long as the radios are out of range of the bridges in the main portion of the network. If you do change the SSID in the supplemental root, then you also must change the SSID of every client that will connect to it.

One of the two radios for the extension link must also be configured as a root node. A separate SSID should be used to prevent the extension link radios from associating with the others. There are actually three different root nodes in Figure I-15.

You will need to configure the wireless bridge in the supplemental node as a root. You do not need to change the service set identification (SSID), as long as the radios are out of range of the bridges in the main portion of the network. If you do change the SSID in the supplemental root, then you also must change the SSID of every client that will connect to it.

I.3.9 When Do You Use The Router?

The router can be used to divide the network into "public" and "private" segments, as well as to provide security to STAMIS clients connected to the private side, behind the firewall. The router serves as a Firewall, DHCP server, and gateway for the clients on the private side, minimizing the number of "real" IP addresses required for the network. It also acts as a traditional router for outbound traffic from the private segment. Figure 2-41 depicts a simplified version of the network configuration using the router:

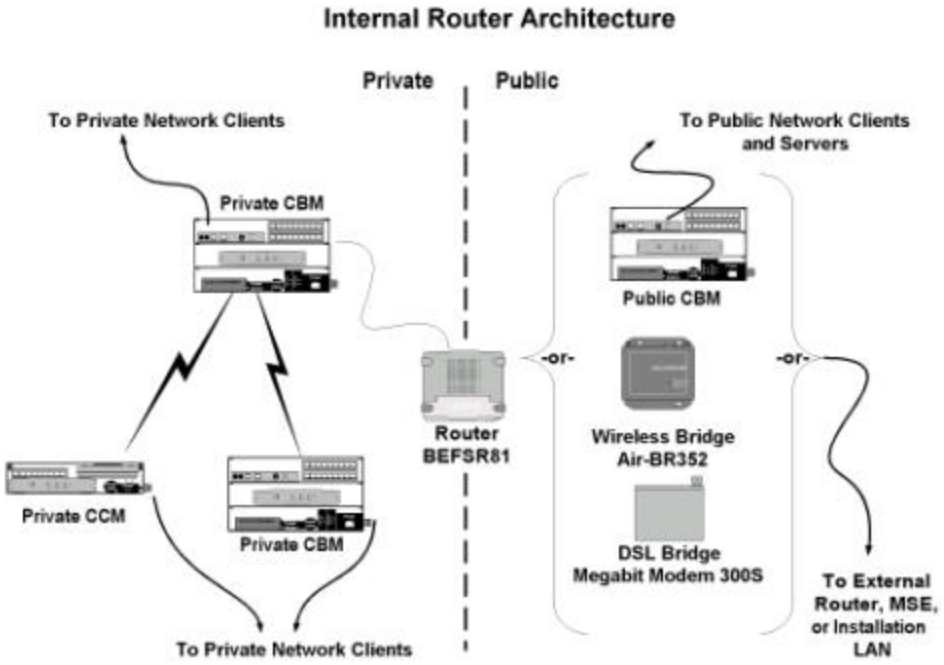


Figure I-16 Using the Router

Remember that users on the private side may connect with each other and with clients on the public side, but clients on the public side may not initiate contact with clients on the private side. Good initial planning is essential when implementing a firewall as part of a network.

The router effectively limits the number of hosts that need to appear on the Public segment to a relatively small number of servers that require connection from clients at other sites or that require DNS entries for their clients to find them.

Segmentation of the network addresses is illustrated on Figure I-16. The figure shows a limited number of STAMIS servers attached to the public segment, the right side of the picture.

> This segment has IP addresses controlled by Signal or by the Director Of Information Management (DOIM) in garrison – usually the S-6 or network operations center. Each host required an assigned static or dynamic IP registered with the Domain Name Service (DNS) server.

In many cases the legacy STAMIS software, Standard Installation/Division Personnel System-3 (SIDPERS-3) for instance, requires static IP addresses for servers. In other cases these addresses could be dynamic, but only if registered in DNS. If dynamic DNS is not available, then all servers require static IP addresses.

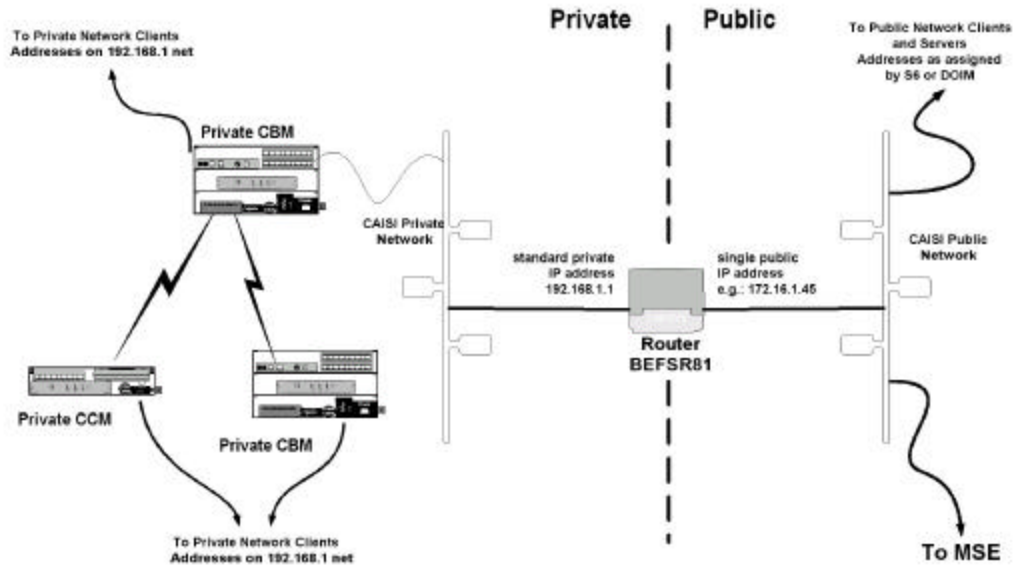


Figure I-17 Segmented Network Addresses

Figure I-17 also shows some number of STAMIS clients connected through the bridges on the private segment, the left side of the picture. These hosts actually constitute the vast majority of the connected computers. They do not consume Signal-provided IP addresses -- because they are behind a router/firewall, they use non-routable addresses assigned by the CAISI system administrator or automatically assigned by the router. The router needs one Signal-assigned address to represent up to 250 clients behind the firewall. These clients can connect to any host with a public address (on the TPN, MILNET, or Internet) as well as those within the same private segment.

The router can be used in three different situations: between two CBMs, connected to a wireless bridge or DSL, or between a CBM and Wireless Bridge.

1. Router between Two CBMs:

Connection of the router is extremely simple. Two network cables are all that are used, as illustrated on Figure I-18.

a. The Public CBM is connected to the WAN port on the Router with a standard gray or white straight-through CAT-5 cable.

b. The Private CBM is connected to any of the eight LAN ports on the Hub with a red crossover CAT-5 cable. If you prefer, you can use a straight-through cable, as long as one end or the other is connected to an uplink port.

Table I-4 explains Figure I-18 in a table format. IP addresses shown are the default IPs. (The numbers in the table corresponds to the numbers in the figure).

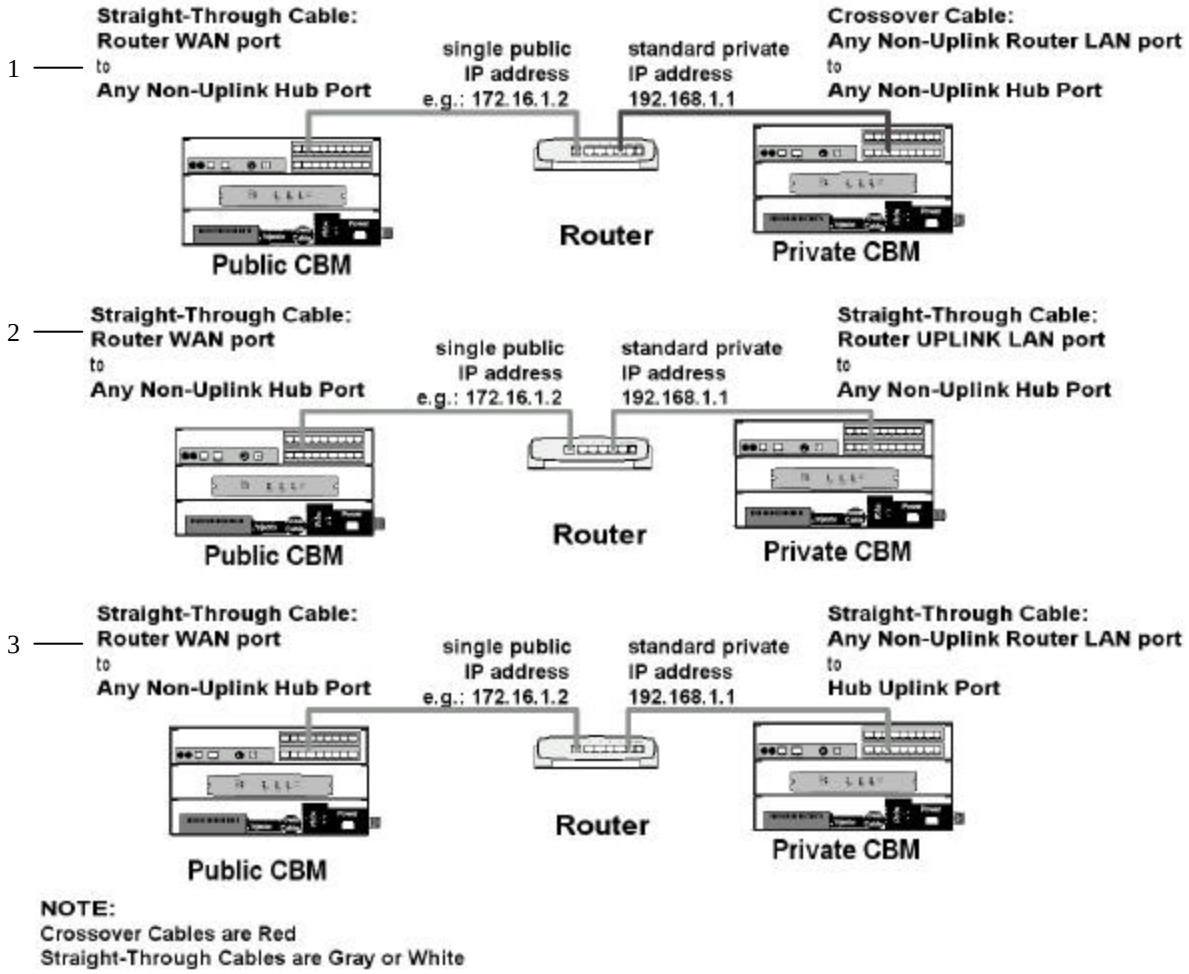


Figure I-18 Router Between Two CBMs

Table I-4 Cable Connections Between Router and Hub

#	Type of Cable	From ROUTER	To HUB
1	Straight-through	Router WAN port	Any Non-Uplink Hub Port
	Crossover	Any Non-Uplink Router LAN port	Any Non-Uplink Hub Port
2	Straight-through	Router WAN port	Any Non-Uplink Hub Port
	Straight-through	Router Uplink LAN port	Any Non-Uplink Hub Port
3	Straight-through	Router WAN port	Any Non-Uplink Hub Port
	Straight-through	Any Non-Uplink Router LAN port	Hub Uplink Port

2. Router Connected to a Bridge (Wireless or DSL)

You might also connect the router to a stand-alone wireless bridge or DSL bridge, as shown on Figure I-19. Four different combinations are shown.

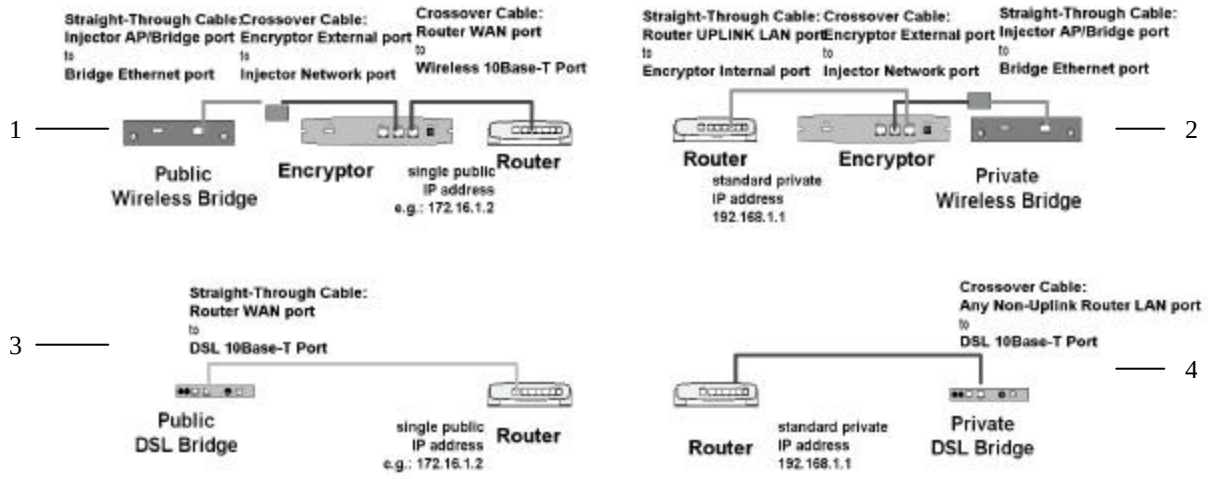


Figure I-19 Router Connected to a Bridge (Wireless or DSL)

2a. Router to the DSL Bridge: Notice that connecting a DSL bridge is still simple. Use a white cable if you are connecting to the (public) WAN port and a red cable if you are connecting to one of the (private) LAN ports. The router can only be configured over the network.

NOTE: ***No encryptor*** *is needed with the DSL bridge.*

2b. Router to the Wireless Bridge: Connecting a wireless bridge is a little more complicated. You need three cables to interconnect a total of four components: the router, the inline encryptor, the bridge power injector, and the wireless bridge. But there are rules.

a. Always use a straight-through cable to go from the bridge to the injector.

When you connect to the injector make sure to connect to the port labeled "AP/Bridge." This is the port where power for the radio is injected.

b. Always use a red crossover cable to go from the injector to the encryptor.

When you connect to the injector, make sure to connect to the port labeled "Network." This port is not powered. If you connect to the wrong port on the injector, you can damage the encryptor. When you connect the other end of the red cable to the encryptor, connect to the "External/Encrypted" port. This is the encrypted "untrusted" port. If you connect to the wrong port on the encryptor, nothing will be damaged, but you will not be able to communicate.

c. Always use a straight-through cable to go from the encryptor to the router.

Connect to the plain-text "internal/unencrypted" port the encryptor. Connect to the "WAN" port of the router for a public connection and to a "LAN" port on the router for a private connection.

Table I-5 Cable Connections Between Router and Wireless Bridge/DSL

#	Type of Cable	From **Wireless Bridge**	Power Injector	Encryptor	To **Router**
1	Straight-through	Ethernet Port	AP/Bridge port		
	Cross-over		Network Port	External / Encrypted Port	
	Cross-over			Internal / Unencrypted Port	Router WAN port
2	Straight-through	Ethernet Port	AP/Bridge Port		
	Crossover		Network Port	External / Encrypted Port	
	Straight-through			Internal / Unencrypted Port	Router Uplink LAN port
	Type of Cable	From **DSL**			To **Router**
3	Straight-through	10Base-T port			WAN port
4	Cross-over	10Base-T port			Any Non-Uplink LAN port

Your most common connection will be placing the router between two CBMs, but you may, of course, combine the two previous diagrams and connect a router between a CBM and a bridge. Pick the appropriate pieces from each diagram and hook it up.

3. Router Between CBM and SSR Wireless Bridge. Your next most common situation will be placing the router between a private CBM and a public bridge that is in turn connected to MSE or the installation LAN. Figure 2-45 shows a public bridge and a private router.

Notice that an encryptor is installed between the router and the wireless bridge. **Remember, a wireless bridge or multi-client radio adapter can never be used without an encryptor.**

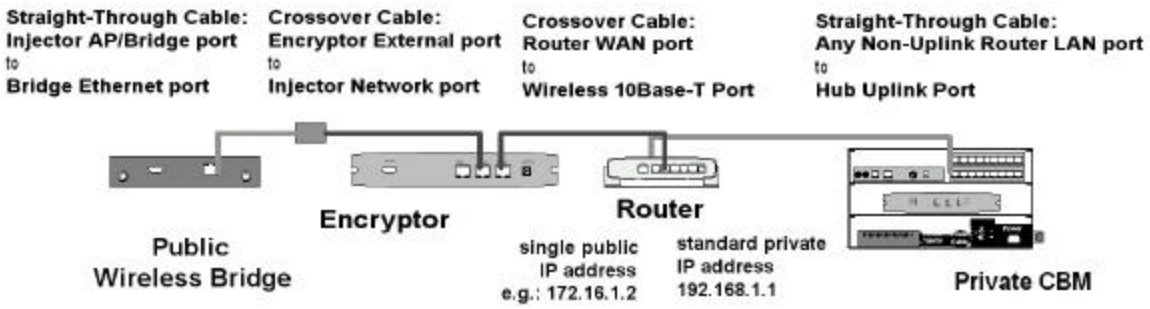


Figure I-20 Router Between CBM and Bridge

Table I-6 Cable Connections for Router Between CBM and Wireless Bridge

#	Type of Cable	From **Wireless Bridge**	Power Injector	Encryptor	**Router**	To CBM
1	Straight-through	Ethernet Port	AP/Bridge port			
	Crossover		Network Port	External / Encrypted Port		
	Crossover			Internal / Unencrypted Port	Router WAN port	
	Straight-through				Any Non-Uplink Router LAN port	Hub Uplink Port

There is no special setup required. The router is a pre-configured component of the SSR Accessory Kit. You, as the SSR, S6, or CSSAMO are responsible for that pre-configuration. Procedures for pre-configuration or field changes are identical.

Configuration will be required only if the public IP address must be changed when the equipment is moved from garrison to the field or from one field site to another. In that case you are likely to need to change four parameters: the IP address, subnet mask, default gateway, and DNS server.

There are no procedures required for normal operation of the router. Once configured, operation is fully automatic and requires no user intervention.

NOTE: *Refer to Paragraph 2.31 for physical steps involved in configuring the router.*

I.3.9.1 Main Points of a Router:

The SSR must determine how many IPs are given to them from the Signal unit for the support of the CSS community. If there is a shortage of real IPs, CAISI has the ability to use 253 non-routable (also known as private) IPs for one real IP by setting up a private network behind the router in the SSR Accessory Kit.

IP Considerations:

a. Public IP Considerations

(1) There are usually not enough "real" IP addresses for all users.

(2) Different addresses are used in the field

(i) Without the router, all users must change IP addresses.

(ii) With the router, only public users need to change IP addresses.

(a) Router assigns IP Address to each user behind it.

(b) Private users may also assign their own address.

b. Private IP Considerations

(1) The private segment of the network serves users who may transmit data but not receive – ex. ULLS.

(2) It also serves as a firewall between the public and private side.

(3) Approximately 253 users can connect to the private segment through a single public IP address.

(4) Addresses are usually assigned dynamically (DHCP), choosing from a pool of available addresses when users connect.

(5) First 50 IP addresses usually reserved for users who assign their own IP address.

c. Typical Network Configuration (Figure I-16).

(1) Users on the Private side may talk to each other and send data to users on the public side.

(2) Users on the public side, however, may not transmit to the users on the private side.

The router is not, however, the only tool you have to segment the network. The bridges in the CBMs also help segment the network. Although they do forward broadcasts and unknown addresses, they do not forward traffic where both the source and destination are on the same side of the bridge. Not only are the public and private segments in separate collision domains, they are in separate IP address domains. The router does not forward broadcasts.

The new router to be added to CAISI will be used to separate the entire CAISI LAN from the WAN, as shown on Figure I-21. This router will have the additional capability to listen for more than one IP address. It will accept traffic addressed to STAMIS servers' public addresses and forward it to their actual (private) address on the CAISI network. This will allow you to put the entire CAISI LAN on a single subnet with a subnet mask like "255.255.0" or "255.255.192.0" and free up the Linksys router to leave behind at the installation for any portion of the unit that does not deploy.

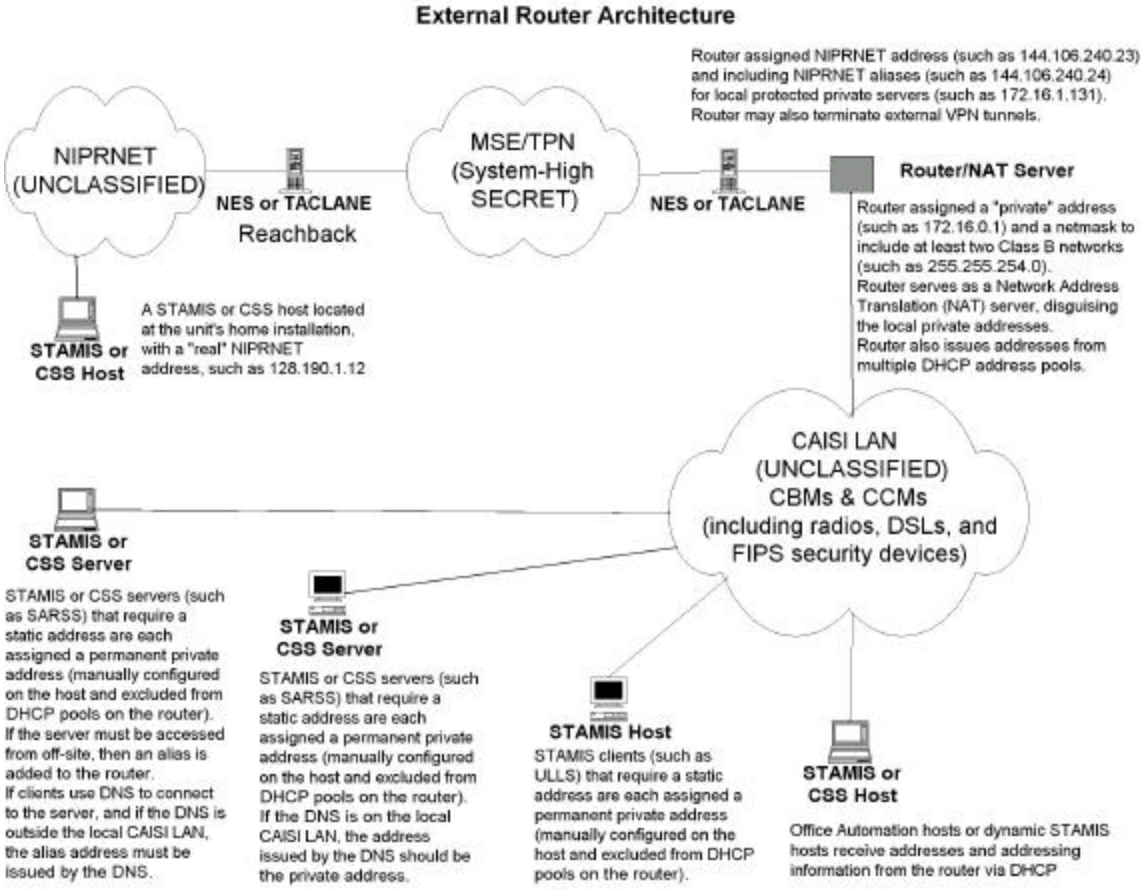


Figure I-21 CAISI External Router Architecture

I.3.10 How do you use the Encryptors?

The Air Fortress encryptors do not require any special deployment planning. Just follow one simple rule: **every radio gets an encryptor.**

a. Radios in a CBM or CCM will have an encryptor pre-wired in it.

b. PCs with wireless NICs must have the AirFortress remote software client. These PCs turn encryption on when using wireless NICs and turn it off when using wired NICs.

c. Radios in the SSR accessory kit also have encryptors. There is wireless bridge (BR-352) and a multi-client radio adapter (WGB-342 or 352), and two AF-1100 encryptors.

The encryptors divide the CAISI LAN into two security zones – trusted and untrusted.

a. The STAMIS and CSS computers are all in the "trusted" zone, along with all the interfaces. This architecture allows your deployed STAMIS and CSS hosts to communicate securely with the servers back at the home station.

b. The radios are in the "untrusted" zone. You cannot communicate to a CAISI radio from anywhere in the trusted zone.

NOTE: *The untrusted wireless network is also sometimes known as a demilitarized zone, because all communications in the zone are encrypted and are therefore safe for exposure to non-military listeners.*

In the illustration on Figure I-22, both the CAISI LAN cloud and the MSE/TPN cloud are untrusted. The AirFortress encryptors separate our clients from the CAISI radios. And the NES encryptors separate us from the MSE TPN. The NIPRNET is trusted, as are the local connections to the CBMs and CCMs in the field.

The AirFortress encrypts, decrypts, and authenticates all traffic. If unencrypted traffic arrives at the external port (the encrypted side), it is ignored. So is any traffic that fails decryption or authentication.

As you can see in Figure I-22, all traffic is plain text (unencrypted) at all interface points, such as routers and the NES. If it were encrypted, those devices could not read the IP headers and route the traffic. It is also in plain text (unencrypted) at the hubs in the CBMs and CCMs.

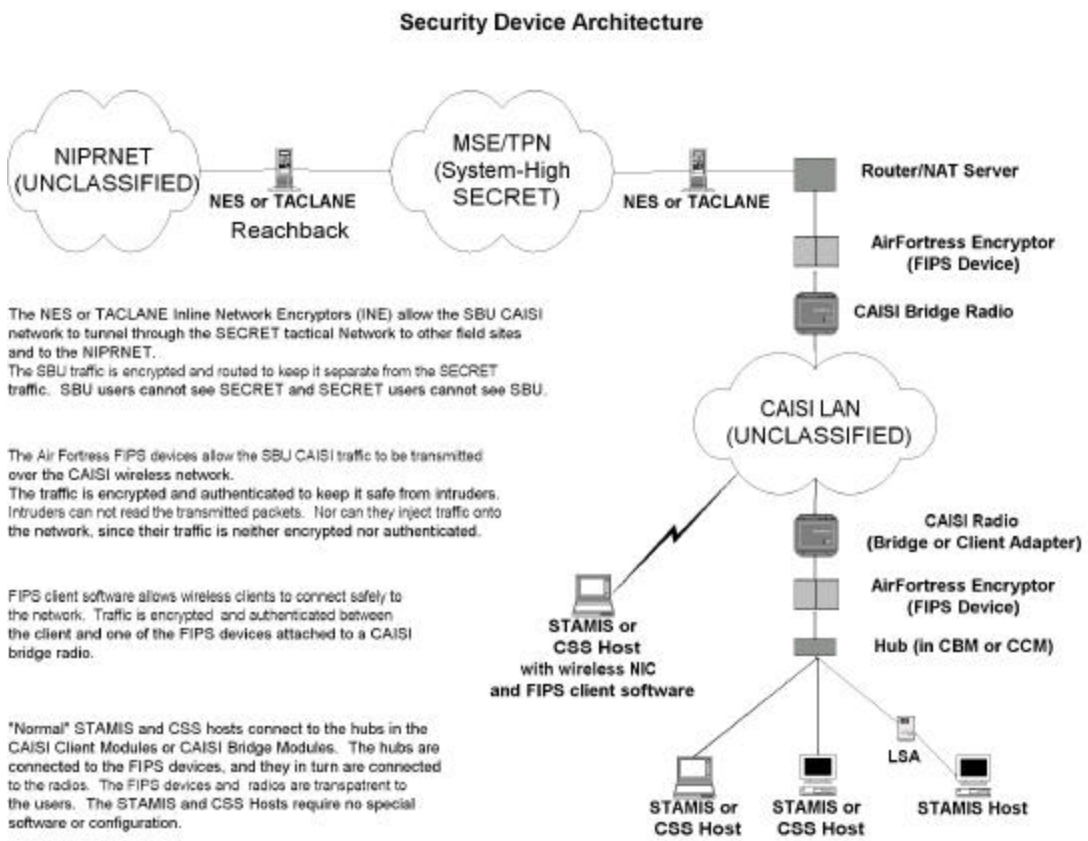


Figure I-22 CAISI Security Device Architecture

You cannot communicate to a CAISI radio from anywhere in the trusted zone. To configure or troubleshoot the radios, you must connect a red Ethernet crossover cable from your SSR notebook directly into the radio, and turn encryption off on your SSR notebook. This prevents anyone from intercepting your configuration commands and passwords. They never go over the network at all – neither over the air nor over the trusted local network.

The AirFortress Remote Client puts the encryptor function on your computer. Your computer combines the functional application (your STAMIS, web browser, mail client, etc), the encryption (the AirFortress Remote Client), and the radio (the Cisco LMC-342 or 352 wireless NIC), as shown on Figure I-23.

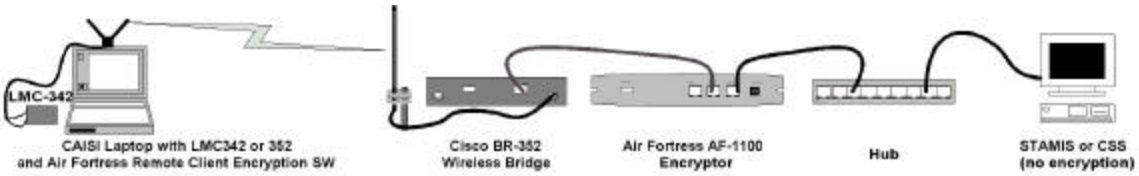


Figure I-23 Air Fortress Remote Client Employment

REMEMBER

Never operate in non-secure mode when your wireless NIC is installed, except to perform antenna alignment and troubleshooting. You should never, under any circumstances, pass traffic in non-secure mode when your wireless NIC is installed.

I.4 ARMY NETWORK TOPOLOGY

CAISI is a part of a larger Army network that includes other voice and data communications – communications over radios as well as communications over data cables. The Army Network Topology includes Mobile Subscriber Equipment (MSE), Tactical Packet Network (TPN), Network Encryption System (NES), Domain Name Server (DNS), and a reachback-router.

a. MSE - The hardware element of the TPN. MSE includes Small Extension Nodes (SEN), Forced Entry Switch and Node Center Switch.

b. TPN - is the component of the MSE that allows *data packets* to be sent and received. Both classified and unclassified data exist on the same physical network. Since the TPN is a secret-high system, unclassified data must be separated from classified. This separation is done through the use of an InLine Encryption device or the NES.

c. NES Gateway - Both classified and unclassified exist on the same physical network, but never see each other. NES separates the unclassified users from the classified user side of the network. In Figure I-24, the cloud with dotted lines around the NES's represents the tunnel effect from NES's to NES's.

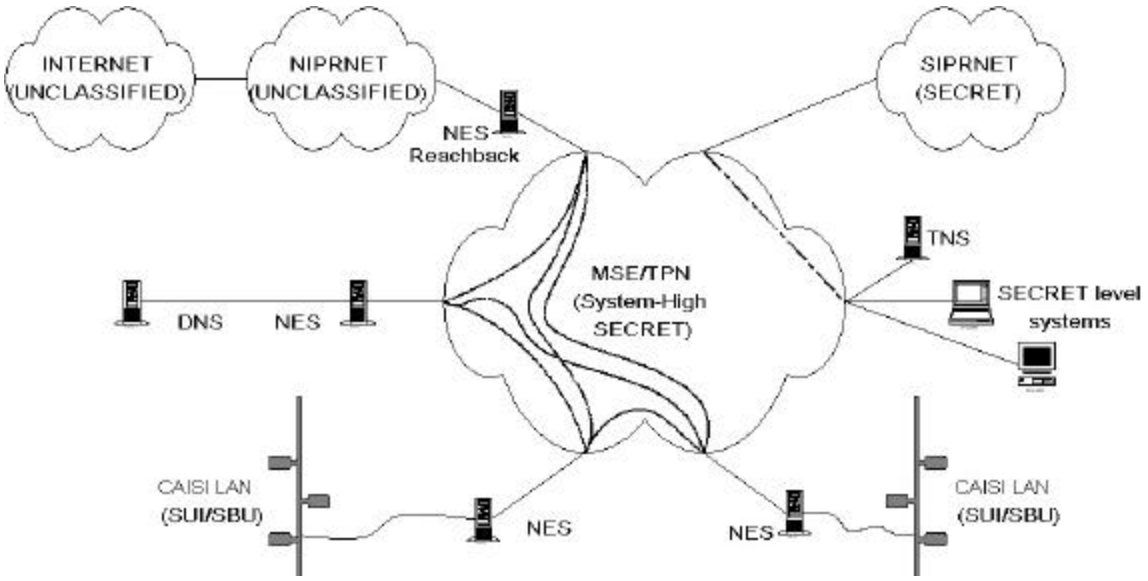


Figure I-24 NES Gateway

NES presents the unclassified data to the CAISI and its subordinate systems (STAMIS devices). NES accomplished this by tunneling the unclassified through the classified. NES tunnels through the TPN to every other NES. NES's are within the security boundary – everything outside is unclassified.

The NES has two IP addresses, one for classified and one for unclassified network interface. CAISI users will only be able to see the unclassified IP address. Unclassified side is available for running tests and pinging.

The NES can act as a router. – the NES routes between itself and other NES's in its group.

CAISI cannot access the TPN without being connected to a NES. Establishing a habitual relationship between a CAISI Root node, NES, and SEN will provide a stable environment for setting up the CAISI. If the same SEN, NES, and CAISI are used to support a particular unit, IP address can remain somewhat constant. Unless the SEN, NES, and CAISI are deployed or moved to a different domain.

All NES systems must perform a form of internal maintenance called, "crypto-resync" once every twenty-four hours. This is a built-in required function. Crypto-resync will cause the system to be unusable to the CAISI for approximately seven minutes.

The crypto-resync time can either be set by the NES operator or it will automatically occur in twenty-four hour increments, based on the last reboot of the NES.

NOTE: *It is recommended that all NES's should be set to go down at the same time each day. This will make the outage period predictable and users can prepare for it.*

d. DNS - A system containing a database of IP addresses and their associated host/domain names that translates names into addresses. A "fully qualified domain name" is the combination of the hostname (the computer or device name) and the domain name. Example: belvoir.eis; belvoir is the hostname, eis is domain name.

e. Reachback – Router - A router is a device used to connect networks together, such as a base LAN infrastructure into the NIPRNET. This allows the STAMIS user to leave the local environment to access any other computer beyond the boundaries of the host.

The router may be under the control of the DOIM (Directorate of Information Management), DISA (Defense Information Systems Agency) or some other agency. It connects the tactical network to NIPRNET. It uses IP addresses to route packets.

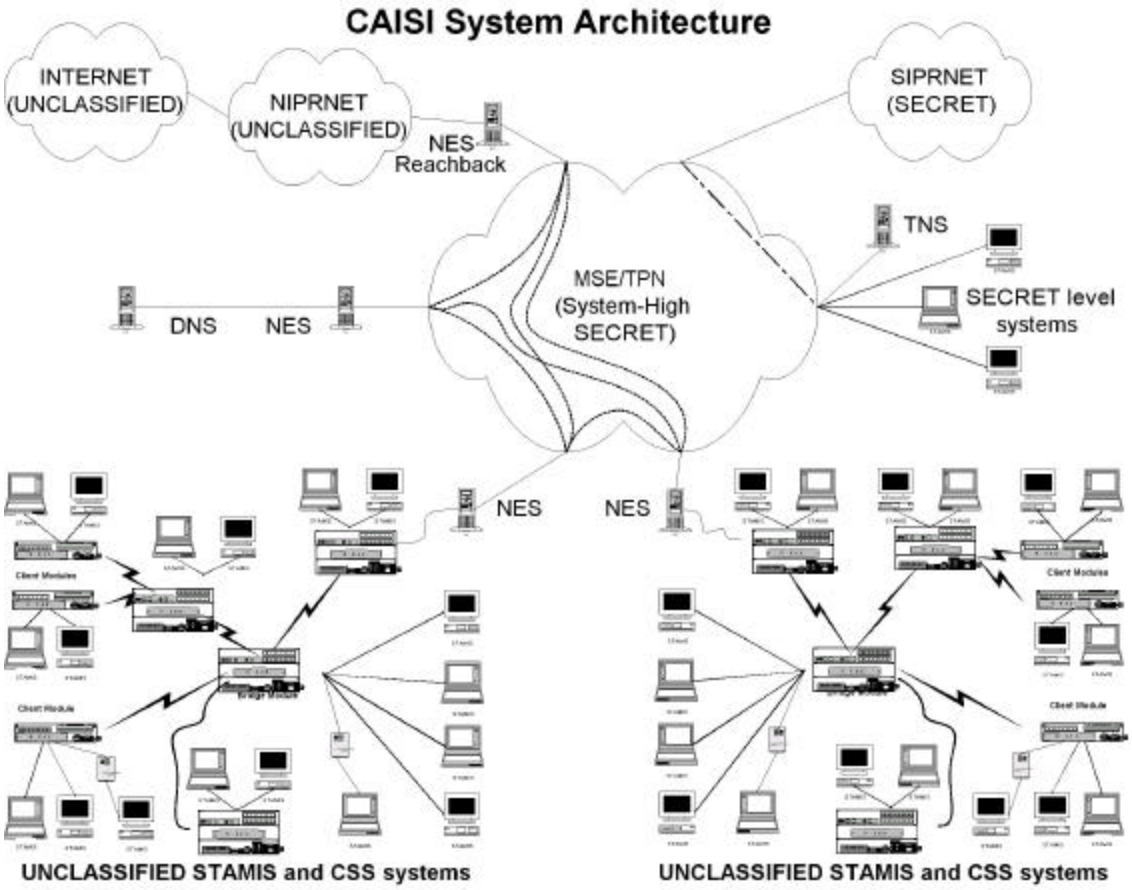


Figure I-25 CAISI System Architecture

I.5 Planning for Deployment

To begin with, there is no one right answer or "school solution" to the question of how to deploy. Every unit has its own methods, but rarely does it the same twice in a row. Your unit Standing Operating Procedures (SOP) provides standard rules and principles, but implementation on the ground is always different from time to time. You rarely deploy to the same spot with the same mix of units and equipment. Even when you go to the same place the terrain often will have changed. Roads may have washed out, for instance, or trees may have grown (or lost) leaves since your last visit.

The only wrong answer, a bad deployment, is one that doesn't provide support to everyone who needs it.

Factors to consider in planning for deployment:

a. Number of Users to be supported.

b. Capability of Users – TCP/IP, Non TCP/IP, or both.

c. Location of Users.

d. Unique Requirements.

e. Inability to use radios.

f. Type of Terrain where deployed.

g. Location of Signal Support.

NOTE: *All of the above factors to consider in planning for deployment will have a tremendous impact on the actual deployment. Once these factors are determined, a deployment plan can be developed –*

a. Mapping out locations of CAISI components and the STAMIS clients to be supported

b. IP addresses can be assigned

c. Components can be configured

d. Equipment can be prepared for the field.

Good advance planning ensures a smooth transition from the garrison to the field.

I.5.1 What Goes Where?

A logistics support area in the field is not evenly distributed. There are bubbles or clusters scattered throughout the area. Some of the clusters are unit headquarters and some are functional centers. All of them contain STAMIS or CSS computers.

Figure I-26 shows a typical support area, with the command post (CP) or tactical operations center (TOC) near the center. It actually can be anywhere. The Signal vans are usually set up close by. The SECRET part of the network uses thin-net coaxial cable so the SEN, LEN, or BSN (Brigade Subscriber Node) van must be within 185 meters of the CP or TOC. In some units, the coaxial cable has been replaced with high-speed fiber optic cable, so the signal van may be farther away.

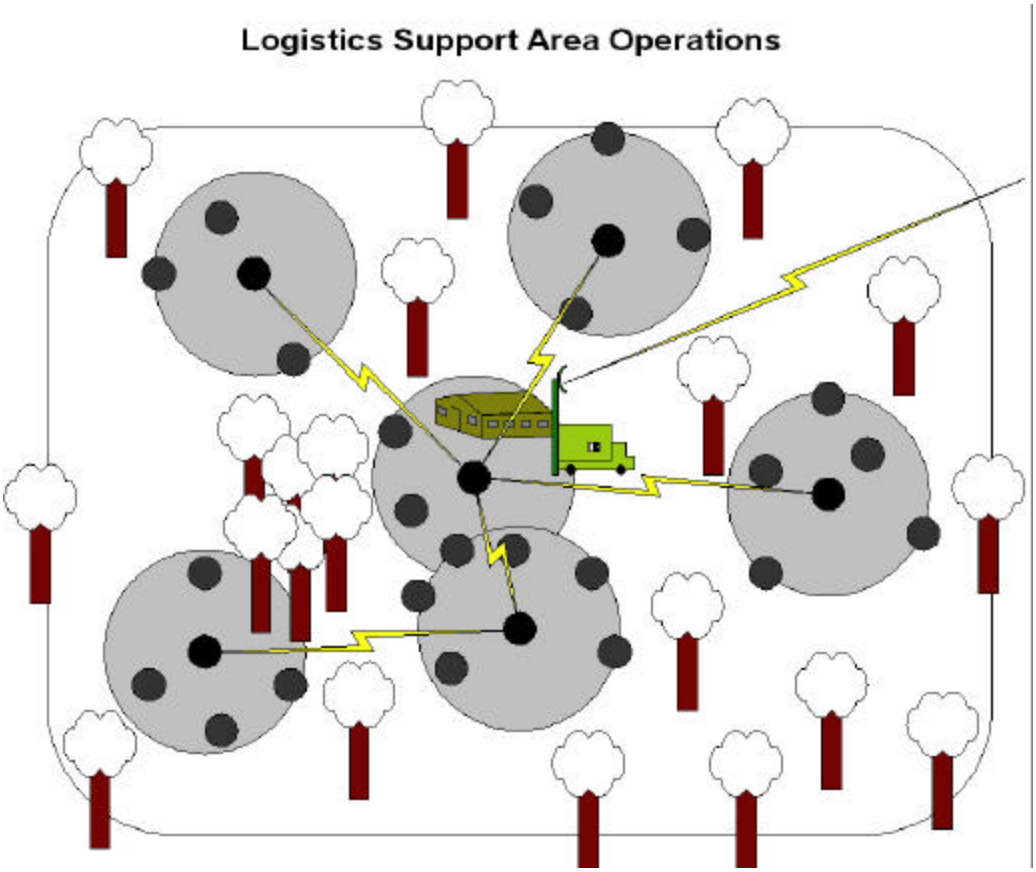


Figure I-26 Logistics Support Area

The overall area can be up to seven kilometers (about four miles) square. And contain large numbers of people, vehicles, and stockpiles of war materials. The gray areas that look like chocolate chip cookies are the functional clusters. Within each are work centers, represented by the chocolate chips. At the center of each functional cluster, we find a CBM. In each work center we find a CCM. Each CBM and CCM supports all the STAMIS and CSS computers in the work center. Everything in the same vehicle or under the same camouflage net connects to it. The CBMs talk to each other. Each CCM talks to the nearest CBM.

The gray circle around each CBM represents the range from which a CCM can communicate to it. **The planning range for CCM to CBM communications is one-quarter mile with good line-of-sight (LOS), so the circles are one-half mile across**. Depending on terrain and vegetation, these circles can be up to two miles across, but we can't count on it.

Because the CBMs have larger antennas and higher transmit power, they can be farther apart. **The planning range for CBM to CBM is one mile, but they can be up to four miles apart, if they have a good LOS**. If they don't, then the range will be much shorter. The good news, however, is that microwaves can follow roads. A typical logistics support area is cut by many roads and clearings. Without them, we could not get our trucks in and out. And we have a lot of vehicles in and out of a logistics support area. The radio signals tend to bounce off the leaves on the trees to the sides of the roads, and can thereby go places we might not otherwise expect them to go. The bad news, it that there is no science to predicting where they will or won't go. You will, however, get a pretty good feel for it over time. The more experience you get, the better you'll be able to predict where you will be able to communicate. Remember too, that you don't need to put your tent in the road. Putting your antenna at the side of the road will do. That's why you have a long antenna cable. And there are extra long ones in the SSR Accessory Kit.

As you can see, there may be areas in the logistics support area that are not inside the gray circles. If you put a client there, you will probably not be able to communicate, although if you use one of the SSR Accessory Kit antennas, you may be able to. Again, experience will help you predict success. Your SSR notebook/laptop and wireless NIC will also help. Go to the spot where you'd like to put a client and try to communicate. Try moving the antenna or using another antenna if you cannot. If you still cannot, then inform the user that if they intend to set up there, they will need to revert to the old sneaker net. If the user is important enough (like the TOC?), you might use the DSL in a CBM to support them.

The areas outside the bubbles also may contain elements not requiring wireless network access. These may include landing zones, storage areas, motor parks, mess halls, sleeping tents, and defensive positions.

I.5.2 What is the Range of the Radios?

Wireless radio planning range is dependent upon power, antennas, antenna cable, antenna height, and intervening obstacles.

Being able to see the antenna at the other end (having a visual line of sight) is good, but is not necessarily sufficient. The way radio waves travel through the air can keep you from communicating, even if you can see the distant antenna.

The curvature of the earth, vegetation, terrain features, buildings, or other objects in the path can block the visual line of sight. Achieving visual line of sight is the first step, although you may not actually be able to see the other antenna from your vantage point on the ground.

If you do have a visual line of sight, the Fresnel effect must also be taken into account. The Fresnel zone is a lens shaped zone that must also be clear of obstacles. The size and shape of the lens depends on the radio frequency. The higher the frequency, the larger the Fresnel zone.

Figure I-27 illustrates the line of sight factors.

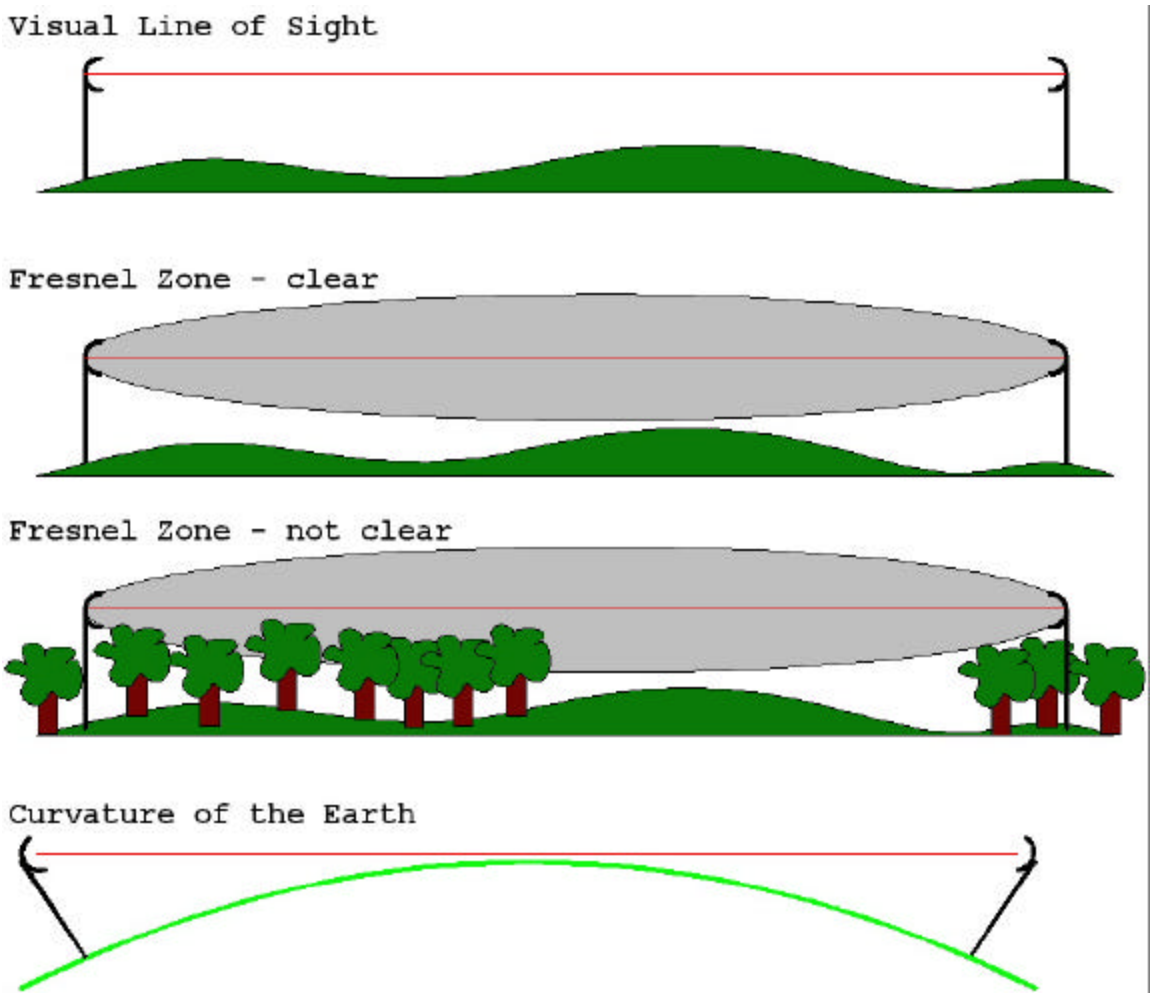


Figure I-27 Line of Sight Factors

For very short ranges, we can ignore the curvature of the earth. It's less than a foot at one mile and only about three feet at four miles.

But the Fresnel zone is much larger. At ¼ mile, the Fresnel zone is about 6 feet. At ½ mile, it's a little less than 10 feet. At one mile, it's over 13 feet. And at four miles it's more than 26 feet. This means that for a four-mile radio link, your antennas must be about 30 feet above the tallest intervening obstacle. Including trees. A few are OK, but the more obstacles in the zone, the more damage they do to your communications.

At longer ranges we also have less power to blast through the trees, because radio waves spread out and get weaker as they travel farther. So as the link gets longer, having Fresnel zone clearance becomes more important.

The following table gives you some common values for the antenna heights required at various ranges at the 2.4GHz wireless frequency. As you can see, distances beyond 4 miles are impractical except under special circumstances, usually involving communications from one hilltop to another. Your SSR Accessory Kit includes a 30-foot mast. To achieve 4 miles, you'll need to borrow another – you need one at each end.

Table I-7 Antenna Heights

Wireless link distance End-to-end		Approx Value "F" (60% Fresnel Zone) Feet at 2.4 GHz	Approx Value "C" (Earth Curvature) Feet at **each end**	Approx Value "H" (Mounting Ht.) (F+C) Total feet at **each end Above obstructions**
Miles	KM			
1	1.6	13	<1	13
2	3.2	19	<1	19
3	4.8	23	2	25
4	6.4	26	3	29
5	8	30	4	34
6	9.6	33	6	39
7	11.2	35	8	43
8	12.8	38	11	48
9	14.4	40	13	53
10	16	42	17	59
15	24	51	37	89
20	32	59	67	126
25	40	66	104	170

Cautions

- Do not attempt to go above 19 feet with camouflage poles.
- Do not mount a 14-inch panel on camouflage poles – it's too heavy.

We also have limitations on range because the wireless radios are extremely low powered. The chart above does not take path loss into account. Path loss is the dissipation of power over distance. You can only listen to your favorite AM or FM radio station for a little while as you drive away from town, because the signal fades out as you get farther away. The wireless radio signal also fades over distance.

The Cisco Aironet BR-352 wireless bridges produce only 100 mW of output power. This is about one-fifth of the power of your little family radio service (FRS) walkie-talkie. The WGB-342 client adapters have even less power: 30 mW.

By putting bigger antennas on the radios, we can get more transmission range. The larger whip antennas flatten out the radio signal, so more goes out the sides and less out the top and bottom. The taller the whip, the flatter the signal and the more effective power. This effect is called "gain." The more gain, the greater the range. However, there is a trade-off. Because the signal is flat, the two ends have to be at about the same elevation.

Otherwise the first one is going over the head of the second. And the second is going into the ground before it gets to the first.

We can get even more gain by using directional antennas. The CAISI panel antennas concentrate all the radio output power in a "beam" -- in one direction. The bigger the panel, the tighter the beam, and the more gain. Again, the more gain, the greater the range. And again, there is a trade off. As gain goes up, aiming the beam becomes more difficult. Elevation differences are less of a factor than with the whip antennas, but you must aim the flat side of the panel antenna toward the distant end. Use a map to determine the direction and compass to aim the antenna if you cannot see to the distant end or very accurately estimate its direction.

Figure I-28 illustrates antenna gain. The longer whip has a flatter signal that extends farther from the antenna. The larger panel has a tighter beam. It also extends farther from the antenna.

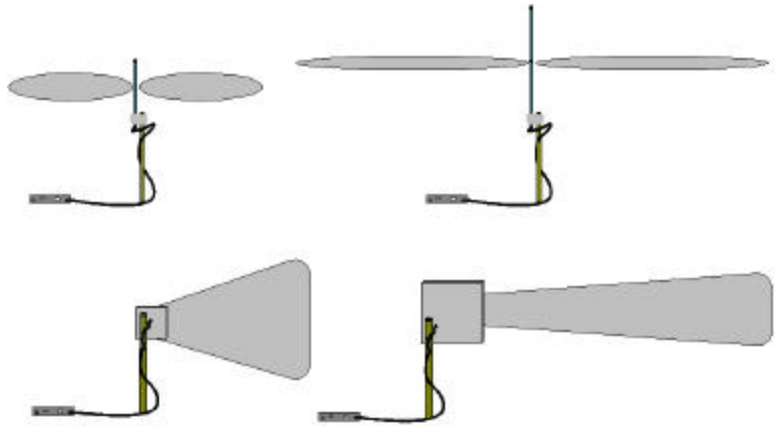


Figure I-28 Antenna Gain

Figure I-29 illustrates compensating for elevation differences. The antennas in the top diagram are not communicating because of the elevation differences. The antennas in the bottom diagram have been tilted to compensate for the elevation differences. Notice, however, that they may not be able to communicate with other nearby radios because of the tilted signals. They not only may miss other antennas, but also will be slightly out of polarity because of the tilt. Avoid tilting antennas any more than you absolutely have to.

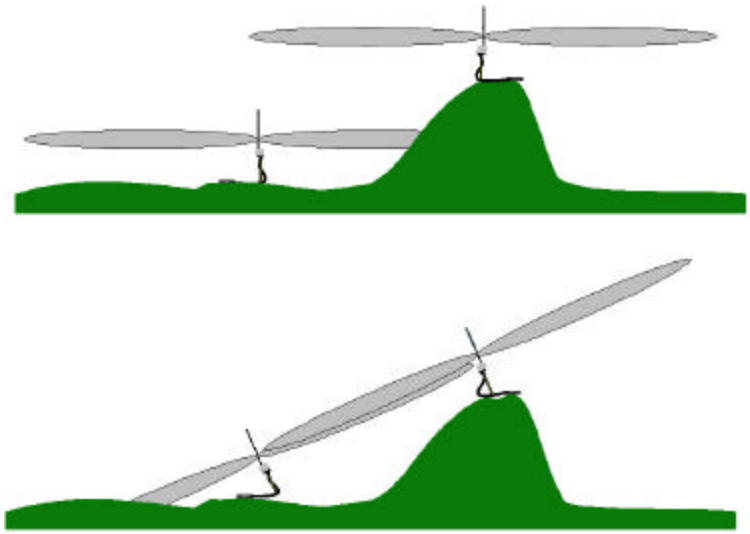


Figure I-29 Compensating for Elevation Differences

Now, some bad news. **We lose some power in the antenna cable. The higher the frequency, and the longer the cable, the greater the loss**. We lose about a quarter of the radio's power in a 35-foot cable. If you combine cables up to a hundred feet, you take away about ¾ of the radios power.

Combine all of the preceding factors to determine the range you can expect from your radios.

The planning ranges that follow are approximate. They are from the listed radio and antenna to a CBM with a 40-inch whip antenna 13 feet above ground level, through light vegetation as is typical in a logistics support area. If your line of sight is better, your range may be greater. If your line of sight is worse (denser vegetation, for instance), your range may be shorter.

Table I-8 Planning Ranges for Antennas

CCM, 24-inch whip, 35-foot cable, 13-foot mast (top of the camouflage net)	¼ mile
CBM, 40-inch whip, 25-foot cable, 13-foot mast (top of the camouflage net)	½ mile
CBM, 7-inch panel, 25-foot cable, 13-foot mast (top of the camouflage net)	½ mile
CBM, 40-inch whip, 35-foot cable, 19-foot mast (well above the camouflage)	1 mile
CBM, 7-inch panel, 35-foot cable, 19-foot mast (well above the camouflage)	1 mile
CBM, 40-inch whip, 50-foot cable, 30-foot mast (from the SSR kit)	2 miles
CBM, 7-inch panel, 50-foot cable, 30-foot mast (from the SSR kit)	2 miles
CBM, 14-inch panel, 50-foot cable, 30-foot mast (from the SSR kit)	4 miles

I.5.3 How are CBMs and CCMs connected in the Support Area?

Figure I-30 shows a Division Support Area (DSA) or other large Logistics Support Area with a CAISI deployed. There are usually more CCMs (up to 30) and users (up to 336) than are depicted, but the figure gives you a pretty good idea what the support area might look like. (CBM has 14 10Base-T ports, CCM has 7 10Base-T ports. Total breakdown is CBM 14 * 9 = 126, CCM 7 * 30 = 210; 126 + 210 = 336)

> **NOTE:** *As mentioned earlier, the actual number of CBMs and CCMs belonging to a CAISI will vary. A "standard" CAISI is defined as 9 CBMs, 30 CCM, and 1 SSR Accessory Kit, however, the number issued to a unit will be specified in the fielding plan. And, the number of modules directly interconnected will vary, even within a standard CAISI.*
>
> *As will be seen in the following diagrams, the entire complement of CBMs and CCMs is usually deployed in a single LAN in a DSA, while the CAISI may be split into several different LANs when in support of a brigade.*

DSA: 9 CBM, 30 CCM (336 ports)

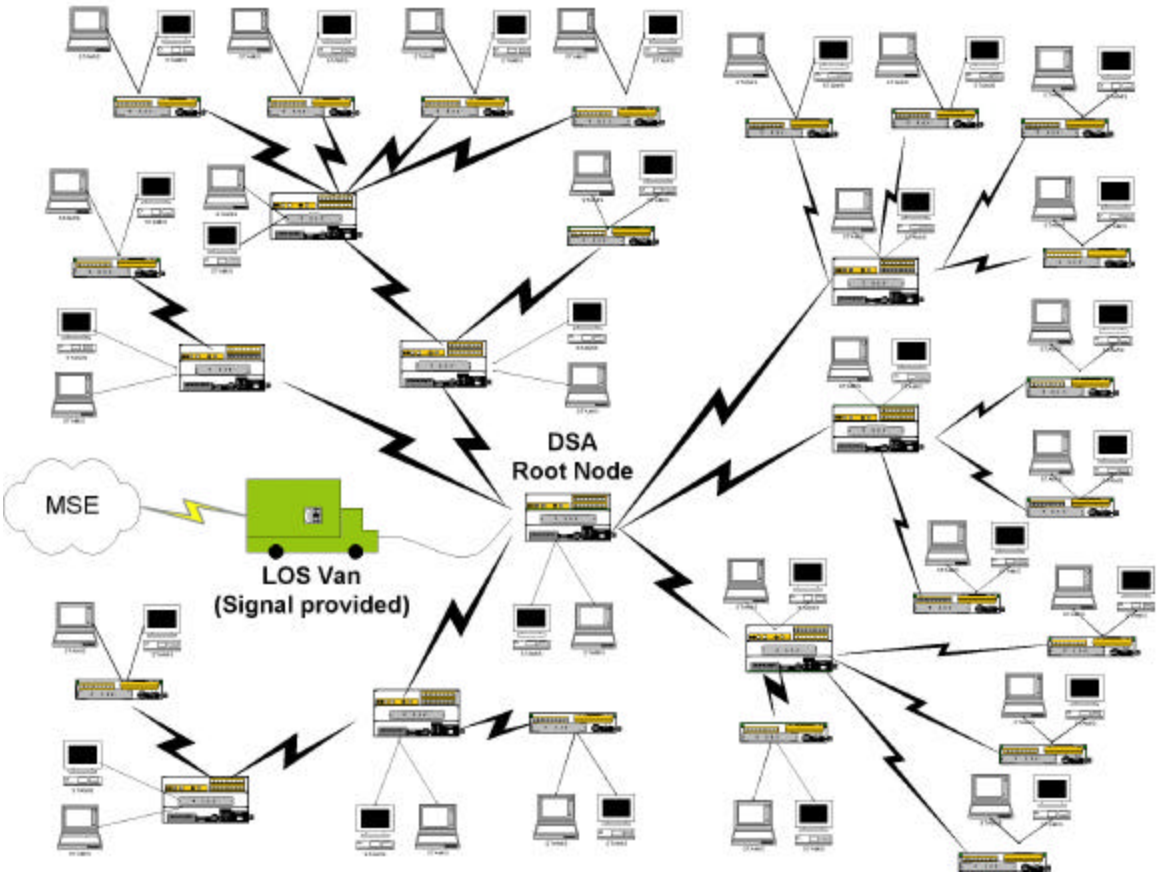


Figure I-30 CAISI in a DSA or Other Large Logistics Support Areas

Figure I-31 shows a CAISI in support of a Brigade. Six of the CBMs and 24 of the CCMs are in the Brigade Support Area (BSA). Three CBMs and six CCMs are deployed forward to the Task Force Support Areas (TFSA).

> **NOTE:** *Again, the numbers of CBMs and CCMs may vary. The unit will deploy the CBMs and CCMs as required to support the situation. This means that not every deployment will be the same. As task force organizations, the terrain, the enemy situation, or the mission change, so will the CAISI deployment.*

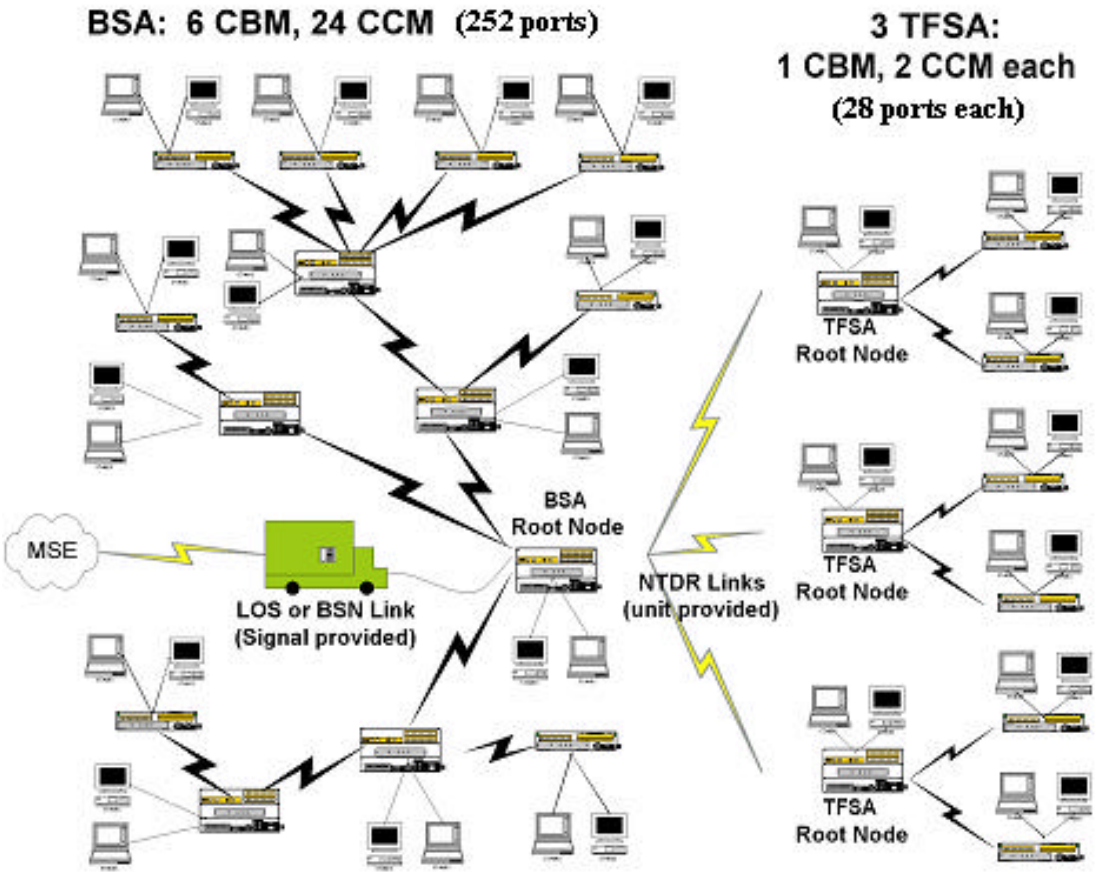


Figure I-31 CAISI in a BSA and TFSA

The figure above shows the TFSAs connected to the BSA through Near Term Digital Radio (NTDR) links. There is not a separate NTDR net for use by SBU CSS systems. The NTDR net is part of the TPN and operates at the SECRET level. So an NES or TACLANE INE is required at the TFSA, as shown on Figure I-32. The INE isolates the CAISI traffic from the SECRET traffic while allowing it to cross through the TPN, just like the INE that separates CAISI from the SEN, LEN, or BSN van.

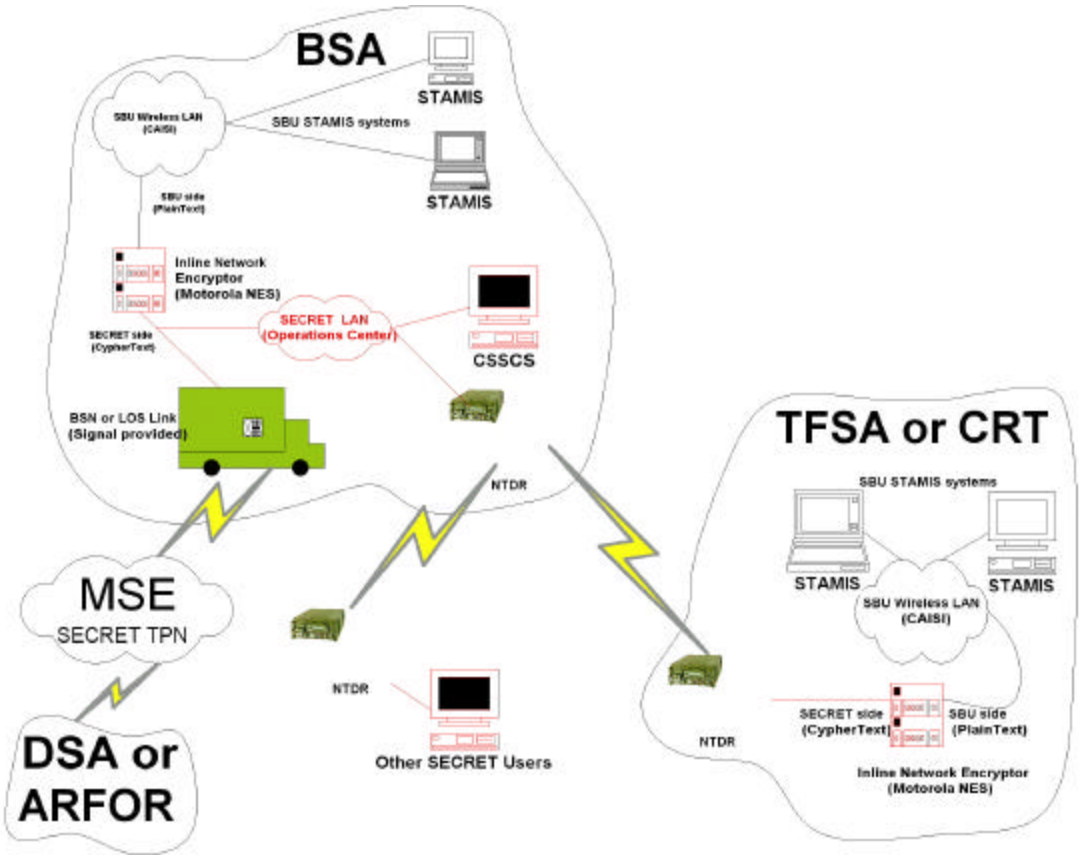


Figure I-32 Using the NTDR to extend the CAISI

The NTDR is representative of a solution that has not yet been finalized into doctrine or the Army Architecture. Other alternatives, such as satellite links and High Frequency (HF) radio, are also being explored. If the NTDR is employed to connect the TFSAs, it will eventually be replaced by the Joint Tactical Radio System (JTRS).

I.5.4 Who Gets the CBMs and CCMs?

STAMIS and CSS users get them based on METT-T factors.

The primary factor as to who gets CBMs is the mission. The next most important factor is the terrain. There are six CBMs available for use in a BSA and nine for use in a DSA.

1. The first CBMs should be allocated to STAMIS users with servers, such as SARSS, SAMS, SIDPERS, etc. This minimizes the possibilities of losing communications because someone else goes down. (CCMs are dependent upon CBMs to connect through). If possible, the root node should be near the MSE van, but this is not critical.

2. The next few CBMs should be allocated based on the physical characteristics of the Logistics Support Area. They should be positioned to act as relays to ensure full coverage of the area. Distances, vegetation, and physical topography must all be considered.

3. The remaining CBMs may be allocated to work centers containing more than eight clients. If there are not enough CBMs to cover all the large work centers, the work centers can be supported by multiple CCMs.

The primary factor as to who gets CCMs is also the mission. There are twenty-four CCMs available for use in a BSA and thirty in a DSA. Keep in mind, the terrain.

1. Every STAMIS or CSS server that doesn't have a CBM should have a CCM.

2. Every work center that includes one or more STAMIS clients should have a CCM. If there are multiple STAMIS users in the work center, only one gets a CCM, the other users will connect to that CCM. The unit will decide which.

3. Every other work center containing a CSS computer needing network access should have a CCM.

If there are not enough CCMs to support every such work center, those that have the "most important" users should be supported, followed by those with the most users, followed by the rest.

Unit SOPs will determine who gets what.

I.5.5 How Do You Use Service Set Identifications (SSIDs) to Segment the Network?

Usually you don't. The gain is not worth the pain. Use SSIDs to control, which CCMs belong to which group of CBMs, but don't get too concerned about using them for segmentation. To use SSIDs for segmentation would require extra CBMs.

The SSID serves two purposes:

1. First, it serves as a security measure. It is a unique identifier that client devices use to associate with the Access Point . It is both a network name and a password. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity. Clients that do not have a matching SSID are not part of the same network. This is especially important if two different units, each with a CAISI, locate close to each other. This can happen if the field, for instance, near the edges of Brigade boundaries. It also happens a lot in garrison, where units are very close together on post.

2. Second, it can serve to segment the network. Each different SSID represents a different collision domain. But there must be a separate root node for every SSID. And the second domain must be somehow connected to the first one. This means that you need to locate two CBMs very close together (so you can connect them by Ethernet or coaxial cable), or you need to connect them with DSL bridges, or you need to use your spare wireless bridge to connect the second root CBM to the first.

NOTE: *In split node operations, with either DSL or wireless remote links, separate SSIDs keep clients from accidentally joining the wrong segment if conditions change. The SSID forces them to remain associated with the correct root node. It does, however impose an administrative burden, since a CBM and some of the CCMs have to be reconfigured to use the second SSID.*

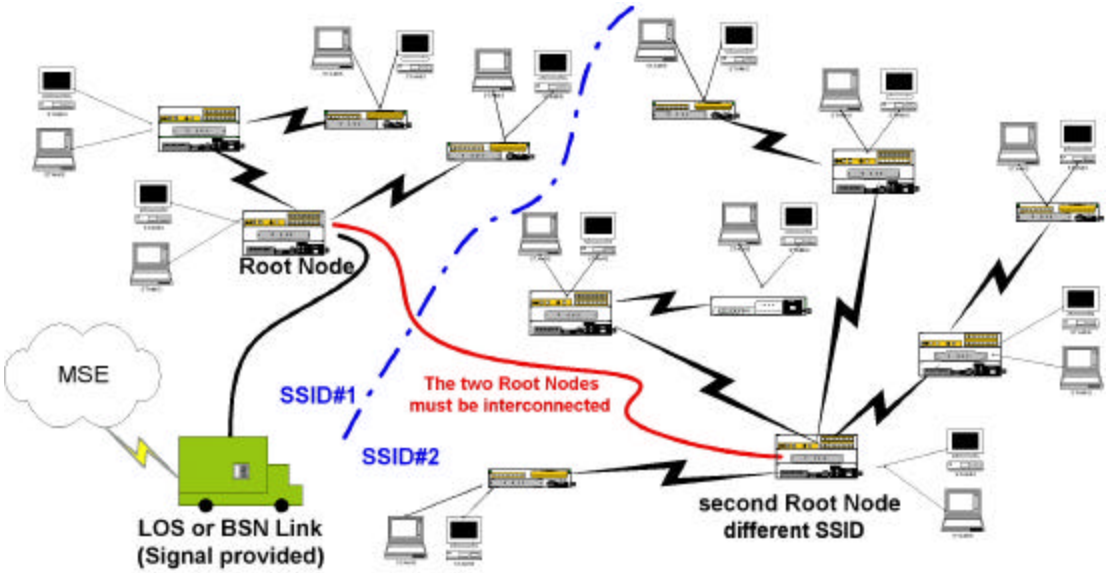


Figure I-33 Using Multiple SSIDs for Segmentation

You will need to decide how to make up SSIDs. You can use any text string up to twenty characters. **SSIDs are case sensitive**. Words and names are easier to use and manage. Random strings are more secure. But, remember that you don't want to make it so secure that you can't use it. One of the many aspects of security is availability. If you go to a CCM to troubleshoot it and can't remember the SSID, then you can't fix it if the configuration gets reset. Use the same principles that guide you in selecting passwords. Use a mix of letters, numbers and characters, but make it memorable. "F1rst_Bde_296fsb" might, for instance, make a good SSID.

I.5.6 Can You Use Multiple Root Radios with the same SSID?

You can, but usually you don't. In this case we are talking about having two root radios in the same area, attached to the same backbone, with the same SSID. Normally, each CAISI will have only one root node per SSID in a physical area, such as the BSA. This is because root nodes cannot talk to each other by radio. They can only communicate through their Ethernet ports.

Advantages for setting up multiple roots.

1. They provide segmentation and an automatic rollover to the other if one goes down.

2. Collisions are minimized because the CBMs have two roots to talk to – two segments – instead of one.

3. If one goes down, because its generator ran out of gas for instance, the other can take over and control the entire network by itself. If there is only one root node and it goes down, the entire network goes down – anarchy reigns because no one is in charge and no radio traffic can be passed until the root is restored.

Disadvantages for setting up multiple roots.

1. Must be connected to each other by wire.

   (a) You might have to position them closer to each other than you normally would, in order to interconnect them by Ethernet or coaxial cable.

   (b) Or you would need to run field wire (WF-16) to interconnect their DSLs.

2. If the interconnection breaks, the two halves of the network cannot talk to each other. And there is some administrative overhead in configuring the second root.

3. You may also need to configure the other bridges to assign their preferred parent (which root CBM do they connect to).

You will have to determine if the advantages outweigh the disadvantages for you. Your primary determining factor should, of course, be mission accomplishment – providing reliable communications to all your customers.

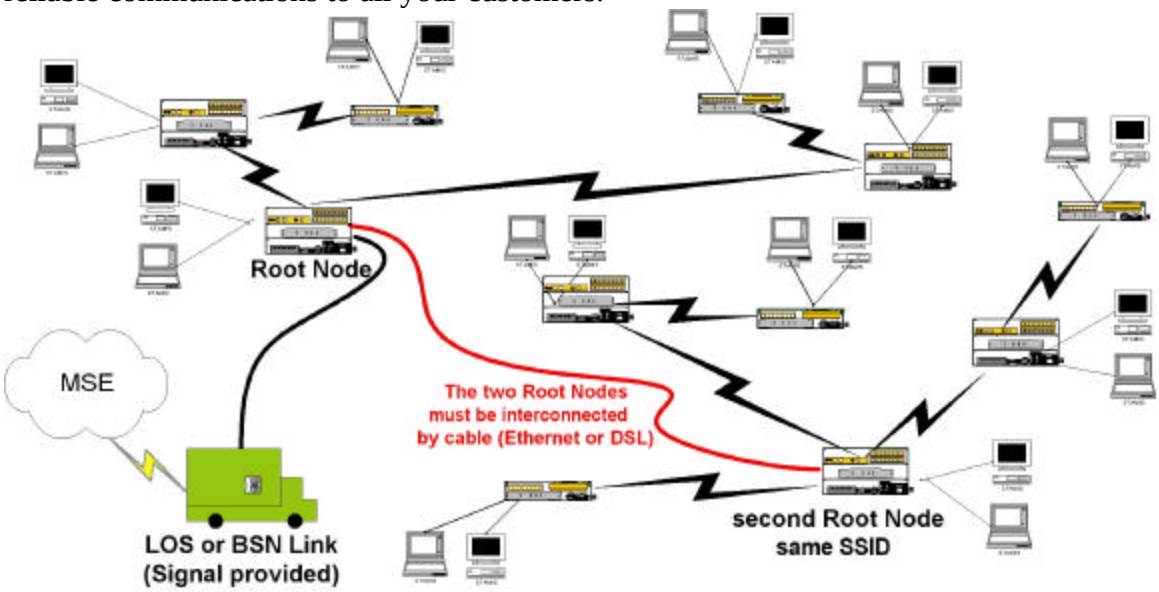


Figure I-34 Multiple Root Radios

Notice that this diagram is similar to Figure I-33. The major difference is that if one root CBM goes down, there is still an operational root. The other CBMs can associate with it and will continue to operate. The entire network remains up. If you have two separate SSIDs and one root goes down, that half of the network goes down since there is no root to control it. The other half of the network remains up.

I.5.7 How Do You Use Wired Equivalent Privacy (WEP) Keys to Secure the Network?

WEP keys are also manually generated and entered into all your devices. WEP keys must match in order to communicate.

> There is currently no way to automatically distribute key changes like you do for your combat net radios (CNR) such as the Single Channel Ground and Airborne Radio System (SINCGARS), the Enhanced Position Location Reporting Systems (EPLRS), or the NTDR. Cisco does plan to add remote key management to the Aironet product line eventually. But not any time soon.

You can use any twenty-six character hexadecimal string for a WEP key. **WEP keys are case sensitive**. That sounds so easy, but isn't. Hexadecimal characters include the numbers 0 through 9 and the letters A through F, only. And you **must have twenty-six characters**. No more, no less.

Tobyhanna Army Depot sets a default key when a CAISI is built, but you need to change it before you deploy. **The default training key is "0123456789ABCDEF0123456789**." That's way too easy to remember. Nor should you use all ones or all zeros.

The more random the better, but you do need to be able to remember it. Try converting some of your favorite phrases to hexadecimal. Thirteen text characters become twenty-six hexadecimal ones. A string like "**296*FSB_(pub)**" becomes "**3239362A4653425F2870756229**." Now that's easy to remember. Well, pretty secure anyway. Do your best. There is probably not good way to make it memorable unless you carry a chart like the following.

Table I-9 Character-to Hex Conversion

CHAR.	HEX.		CHAR.	HEX.		CHAR.	HEX.
space	20		@	40		`	60
!	21		A	41		a	61
"	22		B	42		b	62
#	23		C	43		c	63
$	24		D	44		d	64
%	25		E	45		e	65
&	26		F	46		f	66
'	27		G	47		g	67
(	28		H	48		h	68
)	29		I	49		I	69
*	2A		J	4A		j	6A
+	2B		K	4B		k	6B
,	2C		L	4C		l	6C
-	2D		M	4D		m	6D
.	2E		N	4E		n	6E
/	2F		O	4F		o	6F
0	30		P	50		p	70
1	31		Q	51		q	71
2	32		R	52		r	72
3	33		S	53		s	73
4	34		T	54		t	74
5	35		U	55		u	75
6	36		V	56		v	76
7	37		W	57		w	77
8	38		X	58		x	78
9	39		Y	59		y	79
:	3A		Z	5A		z	7A
;	3B		[	5B		{	7B
<	3C		\	5C		|	7C
=	3D		]	5D		}	7D
>	3E		^	5E		~	7E
?	3F		_	5F			

NOTE: *If you procure wireless equipment from some other vendor, you may need to enter the WEP key as characters. Some use thirteen alpha characters instead of sixteen hexadecimal characters. Some will go either way.*

I.5.8 How Do You Use Multiple SSIDs and WEP Keys?

It is possible to use multiple simultaneous SSIDs and WEP keys, however to prevent situations where you automatically shift to an incompatible network and to simplify configuration, you should avoid this procedure.

I.5.8.1 Multiple SSIDs

The standard rule is that you normally use only one SSID at a time, and you only use WEP key number 1. As you change areas and need to communicate with a different CAISI, change your SSID and WEP key when you arrive. Then get or set a new IP address.

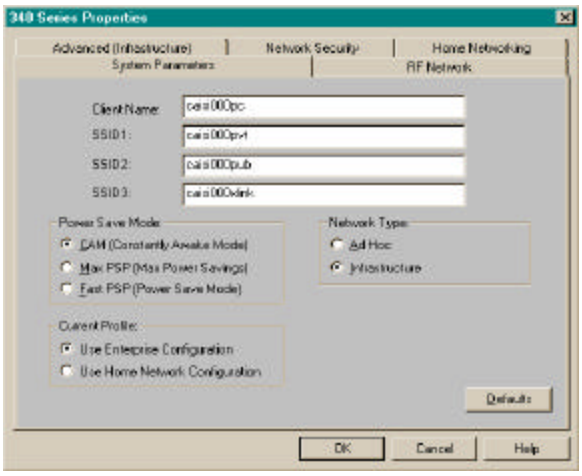
Normally each CAISI will have its own SSID. Each CBM and CCM can have only one SSID. But your CAISI includes numerous CBMs and CCMs. As noted in the previous paragraphs, a CAISI might have some radios with one SSID and others with another SSID.

1. You might be using one public and one private in conjunction with the router.

2. Or you might be using two to achieve segmentation.

3. Or you might be using two to support a split node configuration

You can enter more than one SSID into the Aironet Client Utility (ACU) on your CAISI laptop, as shown to the right.



However the radio will use only one at a time. It will attempt to associate with a bridge using SSID1 and will attempt to use the other SSIDs only if that fails. If it does associate using SSID2 or SSID3, it will periodically check for bridges using the higher priority SSIDs and will switch networks if it finds one.

The unfortunate consequence of this is that you might be left holding a bad IP.

If you are associated with the public segment and switch to the private segment, your IP address will be incompatible and you will be unable to communicate. If this happens do the following:

1. If you are using DHCP to acquire an address, select "**winipcfg**" from your CAISI toolbox to release your old address and get a new one without rebooting.

2. If you have a static address, you would need to manually change it and reboot. So there is not much percentage in automatically switching network segments by entering multiple SSIDs in the ACU tool

I.5.8.2 Multiple WEP keys:

You can enter more than one WEP key into the CBMs and CCMs, as well as your CAISI laptop.

As with SSIDs, the radios can only transmit on one WEP key at a time. And the key number (1 through 4) is part of the key. In order to communicate, the key number and key value must both match. And both radios must have the same selected transmit key.

If you enter the First Brigade's WEP key into WEPkey1 on your laptop and enter Second Brigade's key into WEPkey2, you would still be unable to associate with Second Brigade's CAISI. You cannot communicate even if you select key2 as your transmit key when you enter Second Brigade's area. To make this work, the entire Second Brigade would have to be using key2 instead of key1. Only then when you switched SSIDs and transmit keys, could you communicate. Normally this confusion is not worth the effort.

Yes, it is possible to use multiple simultaneous SSIDs and WEP keys. But you shouldn't. **To simply configuration and to avoid situations where you automatically shift to an incompatible network, it is recommended that you use only one SSID at a time and use WEP key number 1.**

As you change areas and need to communicate with a different CAISI, change your SSID and WEP key when you arrive. Then get or set a new IP address.

NOTE: *Your AirFortress AF-1100 encryptors in the CBMs and CCMs, and the Air Fortress remote encryptor software client on your laptop can only hold one key at a time. If you use different Access IDs in support of each radio SSID, then you will also need to change the AirFortress Access ID every time you change radio nets.*

I.6 Operations In Exceptional Circumstances

Most of the information contained in this manual has addressed the "normal" setup and employment of the CAISI. This Paragraph addresses some of the special situation or circumstances in which you might find yourself. It is not intended to be a complete list of every possible situation and configuration, but should give you ideas as to how to approach whatever approaches you.

I.6.1 When Do You Use Those "Extra" Items in the SSR Accessory Kit?

Your CAISI includes enough CBM and CCMs to support even a large Logistics Support Area. However sometimes you will encounter situations where there are not enough CBMs and CCMs or they don't contain the right components for the situation. Generally you need to use the SSR Accessory Kit components to supplement to CBMs or CCMs when they are having trouble communicating.

Table I-10 Special Circumstances

Situation	Solution	Paragraph
Extra users	Use the wireless bridge or radio adapter in the SSR Accessory Kit to support the extra work center(s).	Paragraph 2.32.1.1/ 2.33.1.1
	Use the hubs to provide extra ports behind the existing CBMs. (Not behind CCMs, however. They support only eight nodes, no matter how many you connect.)	Paragraph I.6.1.1
	Use the router as a switch to provide extra ports behind the existing CBMs. (This you can do, because the CCM will see only the single public address of the router.)	Paragraph 2.31
Simplify installation	Use the wireless bridge to connect to the MSE van. If you use SSR wireless bridge and encryptor, you don't need to waste an entire CBM for a single connection. **NOTE:** *If you connect by coax cable, be sure to configure the radios Ethernet Port setting to support it. The default setting is "10BaseT" (RJ-45).*	Paragraph 2.34.1
	Use the DSL bridge to connect to the MSE van eliminating the need for antennas. Sometimes it's easier to run a short WF-16 run than to install antennas. You may also choose this solution if your wireless bridge is not available.	Paragraph 2.34.2

Situation	Solution	Paragraph
Hard shots	Use the large antennas to replace those issued with the CBM or CCM. Use the long antenna cables (50 ft) to move the antennas to better locations. Use the mast kit to achieve line of sight. Use the extra wireless bridge as a relay	Paragraph 2.28.2 / 2.29 Self-explanatory Paragraph 2.32.1.1
Limit exposure (Avoid the threat)	Use the directional antennas to orient the radio beams to avoid detection or interference. Use DSL to avoid using radio.	Paragraph 2.19.2 / 2.28.2 Paragraph 2.19.1 / Paragraph I.6.1.3

I.6.1.1 Connect one of the SSR Hubs to an existing CBM/CCM.

There might be a time when you want to add an additional hub to a CBM/CCM so that you can have up to 7 more users on the network. You can connect a hub of your own to a CCM but remember that you can have only eight clients connected to a CCM. So, if you have several computers in each of two tents close together, you can put the CCM in one tent and your hub in the other, interconnecting.

Procedure to do this is the following:

1. You will need one of the SSR hubs, a white 10BaseT straight through cable, a 5V power supply with one lead and a two-prong power cord. (Figure I-35)

Hub

White 10Base-T Straight through Cable

Power Supply, 5V, 1 lead

2-prong Power Cord

Other cables that can be used instead of the straight through cable are the crossover cable and the RG-58 cable (does not come with CAISI).

RG-58 Coax Cable

Red Crossover Cable

Figure I-35 Adding an Additional Hub Components

2. Connect one end of the straight through cable to the uplink port on a hub in the CBM or CCM.

3. Connect other end of the straight through cable to one of the 10Base-T ports on the SSR hub.

4. Connect the 2-prong power cord to the power supply adapter. Plug the lead into the power outlet on the hub. Connect the 2-prong power cord to a power source – (if connected to CBM, the UPS, if connected to a CCM, the power strip).

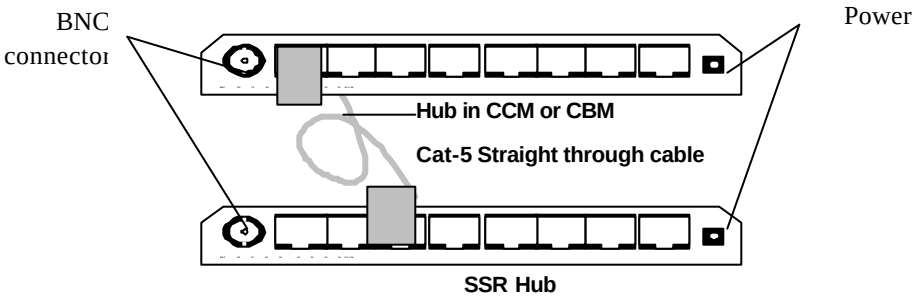


Figure I-36 Connection of Hubs via Cat-5 Straight Through Cable

NOTE: *The BNC connectors are on the front of the hubs to simplify the connection in this picture. In reality, the connector is on the rear of the hub.*

Connecting two hubs with RG-58 cable or with a crossover cable is the same procedure as above accept for steps 2 and 3.

RG-58: (Requires a T-connector, get one from CSSAMO)

1. Connect one end of the RG-58 cable to the hub in the CCM or CBM using a T-connector. Connect the other end to the SSR hub with a T-connector. Remember both ends still need a terminator.

In the following figure, the word NIC is representing a STAMIS computer. Up to 15 devices can be connected using the daisy-chain technique. The last device on the line must have a terminator on it.

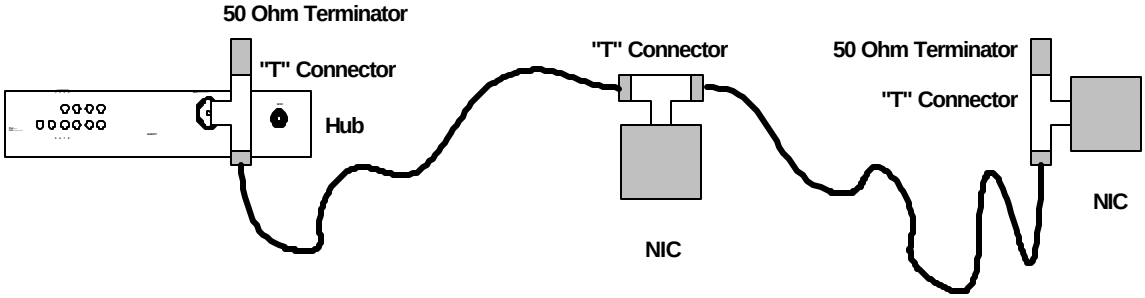


Figure I-37 Daisy-Chain Technique

Crossover Cable:

1. Connect one end of the crossover cable to the Uplink port of a hub in the CBM or CCM. Connect the other end to the uplink port of the SSR hub. Remember, port # 8 can not be used at the same time as the uplink port.

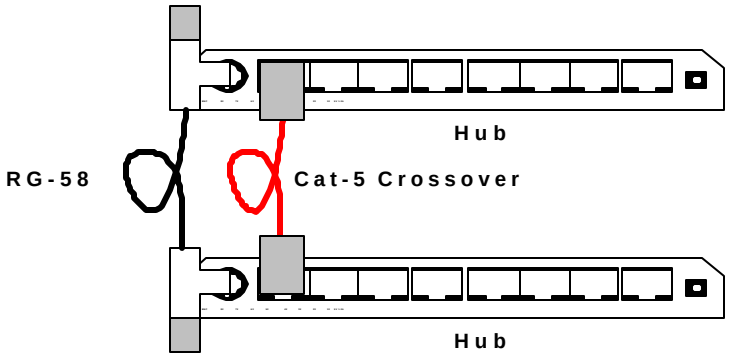


Figure I-38 Connection of Hubs via Cat-5 Crossover Cable/RG-58 Cable

NOTE: *More information concerning the connection of another hub is in Paragraph 2.35.2.*

I.7 How Do You Set up in Garrison?

CAISI is a tactical system, designed and intended to provide communications in the field. Obviously it will also work in garrison, but you will need to coordinate with the DOIM to ensure that it does not interfere with the installations communications.

A frequency request will have been submitted as part of the fielding effort when you received your CAISI, but you still need to let the DOIM know if you plan to operate full-time in garrison. Training should not normally be a problem.

In the field there will be relatively little interference from other equipment in the same frequency band. Although more and more commercial 2.4GHz equipment is coming on the market, it all has a fairly short range and there is not much located in or near your field site. CAISI extends the range by substituting more powerful antennas for those that traditionally come with this equipment, but there should still be relatively little other equipment in range. But in garrison there can be numerous other equipments close by. They can interfere with you and you with them.

To reduce the probability of mutual interference, always set your frequency to "Auto." This will allow CAISI to choose the best available frequency, and to move to a different one later if the conditions change.

When you operate in garrison you will become part of the installation LAN when you connect one or more of your modules "to the wall."

Your connection to the installation LAN becomes your "reach back" connection. To avoid loops that can cause broadcast storms and excessive collisions, be sure that

there is no more than one connection for any SSID. Otherwise the packets can travel in circles forever.

Work out an IP address plan with the DOIM and S-6. Your IP addresses must be legal for use and must be routable by the garrison's routers. You can use your router to get "extra" addresses if required, or to simplify deployment by allowing your clients to use the same addresses in the field as in garrison.

Set your CAISIVEE.CFG hosts lookup parameter to go to DNS then the hosts file (**#define HOSTS_LOOKUP "dns files"**). And put the tactical addresses for your servers in your HOSTS file. In garrison the DNS server will always be available and will provide the garrison IP address for the STAMIS servers.

When you deploy, the DNS will be updated to provide the field addresses. And if it's not available, the LSAs will look in their HOSTS file and find the field IP addresses.

If any clients that were connected behind the router remain in garrison when the router deploys, they will be left hanging without a valid IP address. You need to provide for them.

If any CCM clients remain in garrison when you deploy they will lose connectivity unless a CBM or bridge remains for them to connect to. There must be at least one CBM or bridge configured as a root node.

WARNING

Never connect to any garrison LAN without full operational security, even for training. If you connect to any garrison LAN without implementing proper SSID and WEP key security, you could provide a "back door" into the LAN, bypassing the routers and firewalls that protect the garrison.

The AirFortress encryptors provide sufficient security, in accordance with the Federal Information Processing Standard (FIPS), to protect SBU traffic. Because the encryptors separate the radio portion of the wireless LAN from the installation LAN, they serve to segregate the radios into an isolated demilitarized zone (DMZ) and protect both the fixed and mobile portions of the LAN.

The diagram on Figure I-39 shows two CAISI routers. One is labeled "external" and the other "internal." At this time, CAISI includes only a single router. The routers are not critical to connection to the installation LAN. They are there to simplify addressing. As long as no radio connects to the installation LAN except through an Air Fortress encryptor, the installation will remain secure and no "back doors" will exist.

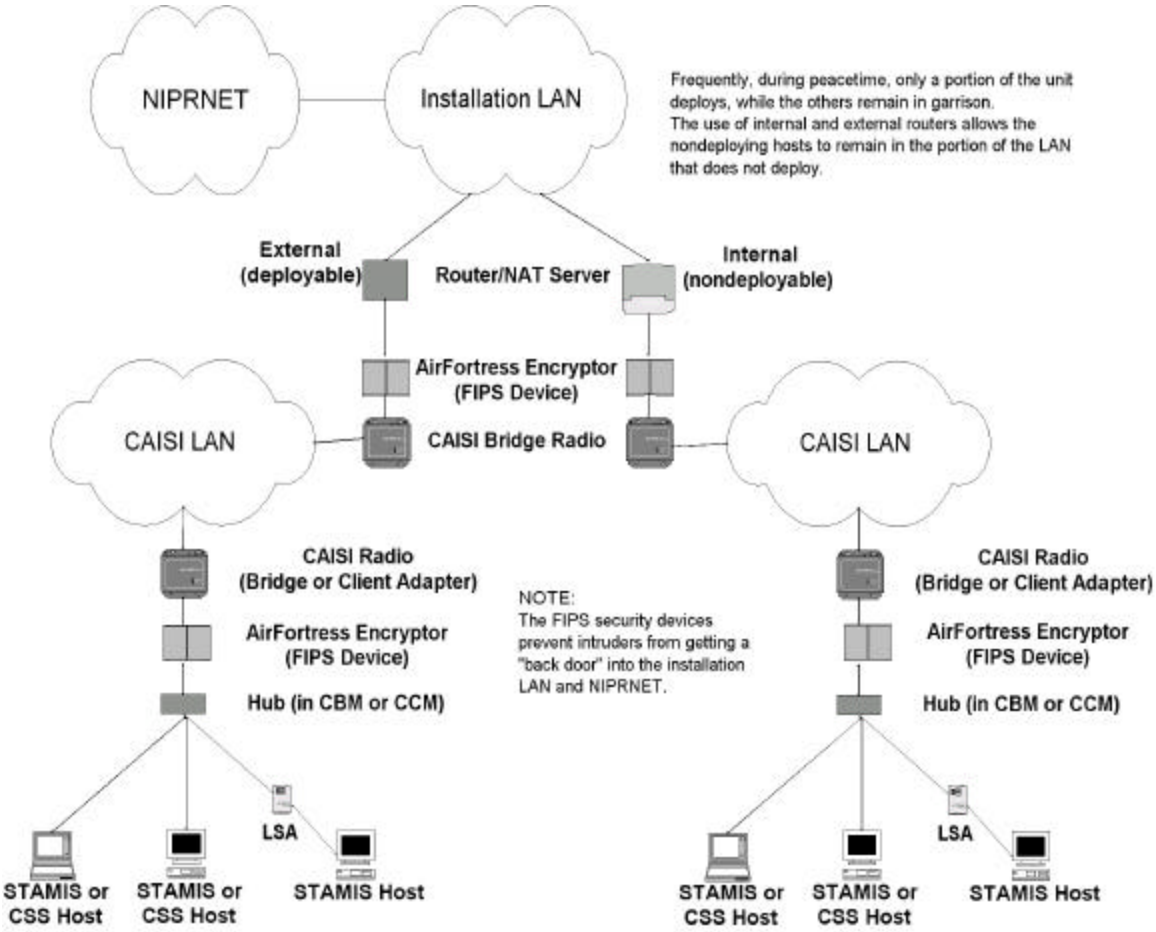


Figure I-39 Garrison LAN Connectivity

I.8 What About Using CAISI OCONUS?

If you are stationed outside of the continental United States (OCONUS), a frequency request will have been submitted as part of the fielding effort when you received your CAISI, but you may still need host nation approvals to operate away from your local training areas. Contact the Frequency Management office.

You will normally only use CAISI in the country where you are stationed. If you deploy elsewhere you need to ensure that you can use CAISI when you arrive. This includes OCONUS units deploying elsewhere in or out of theater.

Prior to deployment, if possible, contact the U.S. Signal staff or Frequency Management office in the destination country. A list of countries with Cisco host nation approvals is at **http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html**. You will still need military approval, and possibly site approvals.

NOTE: *In rare circumstances, your destination may be a friendly nation but one for which we do not have permission to operate the US radios in your CAISI. In this case you will need to take extraordinary measures prior to deployment.*

You will need to acquire host nation approved radio cards for every root bridge.

Install those cards in your root bridges. You may need assistance from Cisco, USAISEC, or your FRA.

Ensure that every other radio's "World Mode" parameter is enabled. This is the CAISI default, but not the factory default, so you need to check. This will make the rest of the radios conform to the host nation parameters in the root radio.

If you are not in world mode, you need to set your power levels and select appropriate antennas for your destination. Whether you are in world mode or not, you need to select appropriate antennas for your power.

A list of Maximum Power Levels and Antenna Gains is at **http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350cards/pc350rn/pc350rn.htm** and is reproduced below. An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. The following table indicates the maximum power levels and antenna gains allowed for each regulatory domain.

The EIRP is the power actually radiated at the antenna.

You can use your short whip antenna where the chart specifies 8.5 dBi.

You can use your long whip or small panel where the chart says 12 dBi.

And you can use your large 18 dBi panel where the chart says 21 dBi.

With 35 feet of cable, subtract 2 dBi.

With 100 feet of cable, subtract 6 dBi.

Subtract cable loss from antenna gain, to compute the net antenna gain. This means that you could, for instance, use the large 18 dBi panel with 100 feet of cable where the chart says 12 dBi.

Table I-11 World-Wide Transmit Power Limitations

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
North America (4 watts EIRP maximum)	0	100
	2.2	100
	5.2	100
	6	100
	8.5	100
	12	100
	13.5	100
	21	5
ETSI (100 mW EIRP maximum) **NOTE:** ***Mexico is now included in the ETSI regulatory domain. However, only channels 9 through 13 can be used in Mexico. Users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of Mexico.***	0	100
	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
	21	1
France/Singapore (100 mW EIRP maximum)	0	100
	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
	21	1
Israel (100 mW EIRP maximum)	0	100
	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
	21	1
Japan (10 mW/MHz EIRP maximum)	0	50
	2.2	30
	5.2	30
	6	30
	8.5	n/a

Table I-13 World-Wide Transmit Power Limitations (Continued)

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
	12	n/a
	13.5	5
	21	n/a

As mentioned above, world mode makes it easier for you to follow the rules. "World Mode" forces the clients and bridges to take on the channel set and other regulatory parameters of the root radio. If you have an ETSI-compliant root radio, every other radio in the network will become ETSI-compliant. So, if possible, borrow or trade a radio with a local unit upon arrival. Make it your root and enable "world mode" on it and every other radio. Your entire network will become locally compliant.

As indicated by the chart above, you may still have to turn down the power levels on your radios to comply with local regulations. Even if you have ETSI radios for use in Germany, for instance, you can only use a maximum 30mW of power with your 9dbi antenna and 50 feet of cable (with 50 feet of cable, your 9 dbi antenna becomes 6dbi).

There may be additional limitations not shown here. Contact the Frequency Manager.

I.9 How do you connect to adjacent units?

You will normally only use CAISI within a local area. Connect to the adjacent unit outside of your support area through the TPN provided by Signal. If units come into your support area, you can integrate them into your network.

If they have CAISI CBMs or CCMs, configure them to join your network. Specifically, configure their WEP keys and SSID to allow them to join the network.

If they don't have CAISI CBMs or CCMs, you can loan them your supplementary items or use the hubs in the SSR Accessory Kit.

I.9.1 What if they have CAISI-MT instead of wireless CAISI?

You will normally only use CAISI with other wireless CAISI. The problem that ensues is not a network problem, but a CAISI-VEE problem. CAISI-VEE in the LSAs is not compatible with CAISI-VEE on the notebooks that are part of the CAISI-MT.

If you have a unit join you and they do not have LSA's you will need to lend them some.

If you cannot lend them LSAs, use floppy disks to transfer the files. Or set up the STAMIS to use floppies, then ftp (File Transfer Protocol) the files to the server and notify them to copy them back to floppy and process them.

No special procedures are required for the network capable STAMIS (non-VEE communications). Your network and theirs are compatible. Just have the S-6 assign IP addresses and add them to the DNS and routing tables if required.

I.10 How Do You Change the SSID or WEP While You are Deployed?

You will normally configure everything before you deploy. Then in the field you need only handle whatever problems arise out of maintenance and troubleshooting.

Remote on-the-fly reconfiguration of some components is possible, but has been disabled to prevent intruders from hacking the configurations. Some other items have no remote configuration capabilities.

Encryptors and notebooks with PCMCIA cards (and towers or desktops with PCMCIA, PCI, or ISA cards) cannot be changed remotely. Encryptors can only be configured through their local ports. Notebooks must be done in person because you have to enter the SSID and WEP key through tools on the desktop.

The bottom line is that you either need to go to the radios, or the radios need to come to you to get reconfigured. Your unit policies and the current situation will prevail.

THIS PAGE IS INTENTIONALLY LEFT BLANK

APPENDIX J

QUICK REFERENCE GUIDE AND INVENTORY CARDS

J-1. GENERAL.

Quick Reference Guides and Inventory cards are provided herein. They are also to be included in the modules when packed at Tobyhanna Army Depot (TYAD) for fielding

They are also for use by TYAD personnel during Quality Assurance Testing.

Extra sets of cards are to be provided to PO CAISI for use by the new equipment training teams during fielding.

J-1.1 Quick Reference Guides.

Quick Reference cards picturing the components of each module and detailing setup and teardown procedures are provided. They are to be reproduced, laminated, and packed with the appropriate modules.

The SSR Accessory Kit has four cards, because it has so many components.

J-1.2 Inventory Cards.

Inventory cards are also provided. They are not to be laminated.

The backs of the CBM, CCM, and LSA cards are identical to the fronts. The SSR cards are two-sided.

These cards are also to be reproduced and ***two of each*** packed with the appropriate module.

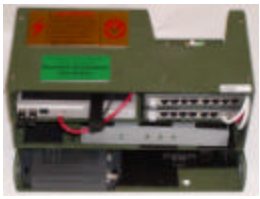
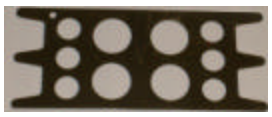
THIS PAGE IS INTENTIONALLY LEFT BLANK

CAISI Bridge Module
Quick Reference Card

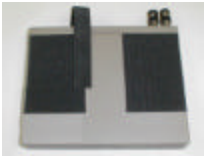
The root CBM is the central distribution point that extends the network within the Division Support Area (DSA), Brigade Support Area (BSA), or other Logistics Support Area. Each other CBM connects, directly or indirectly, back to the root. The wireless bridges in each CBM simultaneously serve as access points (connecting clients), as bridges (connecting other bridges), and as radio relays.

Major Components

The following items are packed in the transit case.

CBM Chassis 	UPS	7-inch Panel Antenna
40-inch break-apart Whip Antenna	RF Antenna Cable 25 & 35-feet	Double “N” Cable Adapter (Barrel Connector)
Antenna Bracket (7-inch)	Grounding Strap	3-prong Power Cord
2-prong Power Cord (Qty 2)	Ethernet Cables (1 Red crossover and 1 White straight-through)	Antenna guy rope on reel (42-ft) (red) (Qty 4) (two per reel)
Reel Unit RL-28 (Qty-2) 		

The CBM Chassis includes the following components installed in the chassis.

Wireless Bridge	DSL Bridge 	Hub (Qty 2)
Inline Encryptor	Power Supply & Power Injector for Wireless Bridge	Power Supply for DSL Bridge
Power Supply for Hubs & Encryptor	Terminator & "T" Connector (2 of each)	18-inch coaxial 10Base-2 Cable
Lightning Arrestor	12-inch RF Antenna Cable	Ethernet Cables (2 Red crossover and 2 White straight-through)

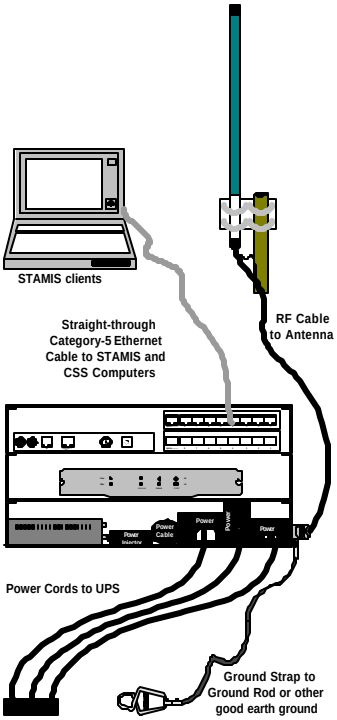
Setup and Teardown

Setup Procedure:

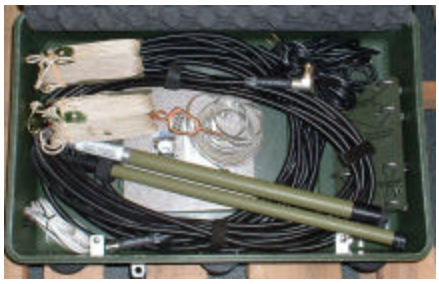
1. Unpack the items you are going to need.
2. Locate the CBM chassis and UPS in a clean, dry location up off the ground. You can use the transit case as a table.
3. Connect the grounding strap from the CBM chassis to a good earth ground. Your generator ground rod is best if it is in reach.
4. Connect the RF cable to the antenna and bracket.
5. Connect the bracket to a camouflage pole and erect it. Make sure the entire antenna above the brass section protrudes above the net.
6. Connect the RF cable to the CBM chassis.
7. Connect the power cables to the CBM chassis and plug them into the UPS, plug the UPS into 110VAC power. Turn the UPS on.

Teardown Procedure:

1. Turn the UPS off and unplug it from the power source.
2. Unplug the power cords and disconnect them from the CBM chassis.
3. Disconnect the RF cable from the CBM chassis.
4. Teardown and disassemble the antenna, bracket, and cable.
5. Disconnect the grounding strap from the CBM chassis
6. Pack everything back into the transit case.
7. Inventory the items to be sure you haven't forgotten anything.



CAISI Bridge Module Inventory Checklist



Component	Quantity	Date						
Transit Case	1							
CBM Chassis	1							
UPS	1							
7-inch Panel Antenna	1							
40-inch break-apart Whip Antenna	1							
25-feet RF Antenna Cable	1							
35-feet RF Antenna Cable	1							
Double “N” Cable Adapter (Barrel Connector)	1							
Antenna Bracket for whip or 7-in panel With U-bolts	1							
Grounding Strap	1							
3-Prong Power Cable	1							
2-Prong Power Cable	2							
White Straight-Through Ethernet Cable	1							
Red Crossover Ethernet Cable	1							
42-Foot Guy Rope (Red Clips)	4							
Reel Unit For Guy Ropes (Containing Above, Two Guy Ropes Per Reel Unit)	2							

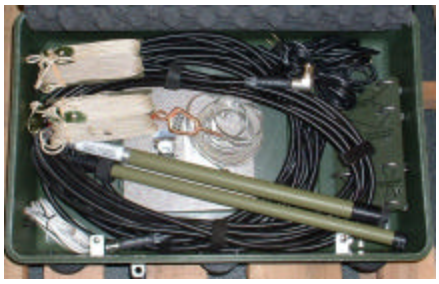
NOTES:

The above inventory reflects the major components of the CBM. All are packed into the transit case. The items are pictured on the laminated Quick Reference Card.

The CBM chassis includes thirteen items installed in the chassis. They are pictured on the reverse of the laminated Quick Reference Card. Do not remove these items for inventory purposes. Make sure the CBM chassis is complete before you initial it on the inventory sheet.

This card is identical front and back. Use up one side before you start on the other. This card is locally reproducible.

CAISI Bridge Module Inventory Checklist



Component	Quantity	Date						
Transit Case	1							
CBM Chassis	1							
UPS	1							
7-inch Panel Antenna	1							
40-inch break-apart Whip Antenna	1							
25-feet RF Antenna Cable	1							
35-feet RF Antenna Cable	1							
Double “N” Cable Adapter (Barrel Connector)	1							
Antenna Bracket for whip or 7-in panel with U-bolts	1							
Grounding Strap	1							
3-Prong Power Cable	1							
2-Prong Power Cable	2							
White Straight-Through Ethernet Cable	1							
Red Crossover Ethernet Cable	1							
42-Foot Guy Rope (Red Clips)	4							
Reel Unit For Guy Ropes (Containing Above, Two Guy Ropes Per Reel Unit)	2							

NOTES:

The above inventory reflects the major components of the CBM. All are packed into the transit case. The items are pictured on the laminated Quick Reference Card.

The CBM chassis includes thirteen items installed in the chassis. They are pictured on the reverse of the laminated Quick Reference Card. Do not remove these items for inventory purposes. Make sure the CBM chassis is complete before you initial it on the inventory sheet.

This card is identical front and back. Use up one side before you start on the other. This card is locally reproducible.

CAISI Client Module
Quick Reference Card

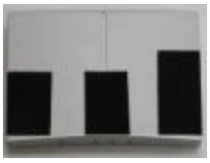
The CAISI Client Module is the distant-end extension for the CAISI Bridge Module. The client module connects your STAMIS or CSS computer to the Sensitive Unclassified Information segment of the tactical packet network.

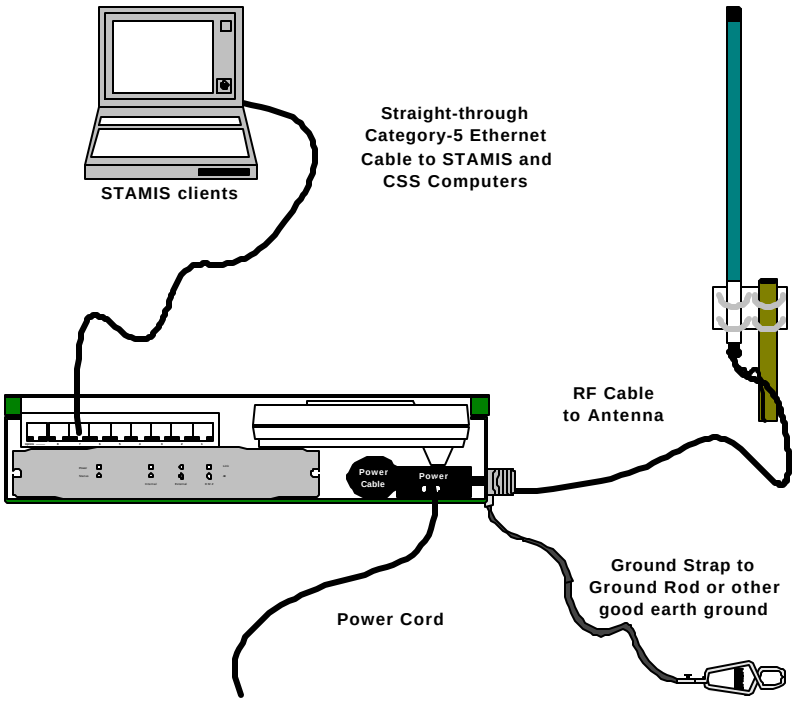
Major Components

The following items are packed in the carrying case.

CCM Chassis	24-inch Whip Antenna	35-feet RF Antenna Cable	
Antenna Bracket (7-inch)	Grounding Strap	White Straight-through Ethernet Cable	2-prong Power Cord

The CCM Chassis includes the following components installed in the chassis.

Multi-Client Radio Adapter	Inline Encryptor 	Hub
Power Supply for Radio, Encryptor & Hub	Terminators (Qty 2) & “T” Connector (Qty 1)	Lightning Arrestor
12-inch RF Antenna Cable	Ethernet Cables (1 Red Crossover and 1 White Straight-through)	



Setup and Teardown

Setup Procedure:

1. Unpack the items you are going to need.
2. Locate the CCM chassis in a clean, dry location up off the ground.
3. Connect the grounding strap from the CCM chassis to a good earth ground. Your generator ground rod is best if it is in reach. If there is no earth ground in reach, go get a ground rod of your own and use it.
4. Connect the RF cable to the antenna and bracket.
5. Connect the bracket to a camouflage pole and erect it. Make sure the entire antenna above the brass section protrudes above the camouflage net.
6. Connect the RF cable to the CCM chassis.
7. Connect the power cable and plug it into 110VAC.

Teardown Procedure:

1. Unplug the power cord and disconnect it from the CCM chassis
2. Disconnect the RF cable from the CCM chassis.
3. Teardown and disassemble the antenna, bracket, and cable.
4. Disconnect the grounding strap from the CCM chassis
5. Pack everything back into the carrying case.
6. Inventory the items to be sure you haven't forgotten anything.

CAISI Client Module Inventory Checklist

Component	Quantity	Date						
Carrying Case	1							
CCM Chassis	1							
24-inch Whip Antenna	1							
35-feet RF Antenna Cable	1							
Antenna Bracket for whip or 7-in panel with U-bolts	1							
Grounding Strap	1							
White Straight-through Ethernet Cable	1							
2-Prong Power Cord	1							

NOTES:

The above inventory reflects the major components of the CCM. All are packed into the carrying case. The items are pictured on the laminated Quick Reference Card.

The CCM chassis includes eight items installed in the chassis. They are also pictured on the laminated Quick Reference Card. Do not remove these items for inventory purposes. Make sure the CCM chassis is complete before you initial it on the inventory sheet.

This card is identical front and back. Use up one side before you start on the other.
This card is locally reproducible.

CAISI Client Module Inventory Checklist

Component	Quantity	Date						
Carrying Case	1							
CCM Chassis	1							
24-inch Whip Antenna	1							
35-feet RF Antenna Cable	1							
Antenna Bracket for whip or 7-in panel with U-bolts	1							
Grounding Strap	1							
White Straight-through Ethernet Cable	1							
2-Prong Power Cord	1							

NOTES:

The above inventory reflects the major components of the CCM. All are packed into the carrying case. The items are pictured on the laminated Quick Reference Card.

The CCM chassis includes eight items installed in the chassis. They are also pictured on the laminated Quick Reference Card. Do not remove these items for inventory purposes. Make sure the CCM chassis is complete before you initial it on the inventory sheet.

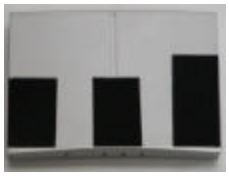
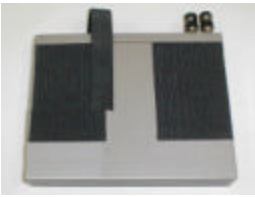
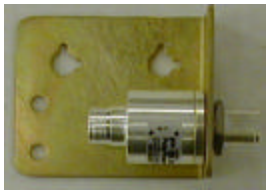
This card is identical front and back. Use up one side before you start on the other. This card is locally reproducible.

CAISI SSR Accessory Kit
Quick Reference Card

Each CAISI will include one Service Support Representative (SSR) Accessory Kit, with a notebook for configuration and monitoring, spare components, and items for use in special circumstances. It is packaged in three containers – one transit case and two carrying cases. The transit case holds the notebook, spares, and special-use components. The first carrying case contains large panel antennas, brackets, and cables. The other carrying case contains an antenna mast system.

Major Components

The following items are packed in the **SSR Transit Case**.

Inline Encryptor (Qty 2) 	UPS	Wireless Bridge
Multi-Client Radio Adapter	DSL Bridge 	Router
Hub (Qty 2)	10Base-T Transceiver	40-inch break-apart Whip Antenna (Qty 2)
4-inch whip antenna (Qty 2)	Lightning Arrestor Assembly (Qty 2) 	Grounding Strap (Qty 2)
12-inch RF Antenna Cable N (M) to RPTNC (M) (Qty 2)	12-inch RF Antenna Cable N (M) to RPTNC (F) (Qty 2)	Adapter, Right Angle (N-M to N-M) (Qty 2)

SSR Transit Case (Continued)

Antenna "Dummy Load" (N-M) (Qty 2)	White or Gray Straight-through Ethernet Cable (Qty 4)	Red Crossover Ethernet Cable (Qty 4)
RJ-45 Straight-Through Adapter (Qty 3)	RJ-45 Crossover Adapter (Qty 3)	9-pin Straight-through Serial Cable, (M-F) (blue)
9-pin Crossover Serial Null Modem Cable (F-F) (beige)	9-to-25 null modem cable (optional – included only if this CAISI includes LSA)	Reset Tool (Qty 3)
Power Supply & Power Injector for Wireless Bridge	Power Supply for DSL Bridge	Power Supply for Linksys Router (version 1)
Power supply, 5V, 3 lead (Qty 2)	Power Supply, 5V, 1 lead (Qty 5) (Qty is 6 with version 2 router)	2-prong Power Cord (Qty 3)
3-prong Power Cord (Qty 2)	3-prong, 1-foot Power Cable (Qty 5) for use with Power Supply, 5V, 1 lead	(Qty is 6 with version 2 router for the 3-prong, 1-foot power cable)

NOTE: *The contents of the notebook case, antenna carrying case and antenna mast carrying case are pictured on separate cards.*

CAISI SSR Transit Case Inventory Checklist

Component	Quantity	Date						
Transit Case	1							
Inline Encryptor, Air Fortress 1100	2							
UPS	1							
Wireless Bridge, CISCO BR-352	1							
Multi-Client Radio Adapter (Workgroup Bridge) Cisco WGB-342 or 352	1							
DSL Bridge, Pairgain 300SBP	1							
Router, Linksys BEFSR81	1							
Hubs, Addtron or Farallon 9-port	2							
10Base-T Transceiver	1							
40-inch break-apart whip antenna	2							
4-inch whip antenna	2							
Lightning Arrestor Assembly – Lightning Arrestor mounted on bracket	2							
Grounding Strap	2							
12-inch RF cable N (M) to RPTNC (M)	2							
12-inch RF cable N (M) to RPTNC (F)	2							
Adapter, Right Angle, N (M) to N (M)	2							
Antenna “Dummy Load” N (M)	2							

(Continued on reverse)

SSR Transit Case Inventory (continued from front side)

White Straight-Through Ethernet Cable	4							
Red Crossover Ethernet Cable	4							
Adapter, RJ-45 (F) to RJ-45 (F) Straight-through	3							
Adapter, RJ-45 (F) to RJ-45 (F) Crossover	3							
9-Pin Straight-Through Serial Extension Cable (M-F) (blue)	1							
9-Pin Crossover Serial Null Modem Cable (F-F) (beige)	1							
9 to 25-Pin Null-Modem Serial Adapter Cable (For use with LSA)								
Reset Tool	3							
Power Supply and Power Injector, 48V, for Wireless Bridge	1							
Power Supply, 5V, DSL	1							
Power Supply, 5V, Router (version 1)	1							
Power Supply, 5V, 3 Leads (for each encryptor) (Can simultaneously power a hub and radio or for two hubs)	2							
Power Supply, 5V, 1 Lead, Wall style (for each router, each hub and the radio adapter) Qty is 6 with version 2 router	5							
Power Cable, 2-Prong	3							
Power Cable, 3-Prong	2							
3-Prong, 1-foot Power Cable for use with power supply, 5V, 1 lead Qty is 6 with version 2 router	5							

NOTES:

The above inventory reflects the major components of the SSR Accessory Kit. All are packed into the SSR Transit Case. The items are pictured on the laminated Quick Reference Card.

This card is locally reproducible.

CAISI SSR Accessory Kit
Quick Reference Card

The following items are packed in the **SSR Notebook Case**.

SSR Notebook	Power Supply for Notebook Computer	2-prong power cord
Wireless NIC	"Rabbit Ears" Antenna	Wired NIC (if issued)
White Straight-through Ethernet Cable	Red Crossover Ethernet Cable	RJ-45 Straight-Through Adapter
RJ-45 Crossover Adapter	9-pin Straight-through Serial Cable, (M-F) (blue)	9-pin Crossover Serial Null Modem Cable, (F-F) (beige)
Adapter Cable, MMCX to N (F)	Adapter Cable, MMCX to RPTNC (F)	Adapter, Right Angle (N-M to N-M)
Antenna "Dummy Load" with "N" (M) connector	Reset Tool	Baseline CD

NOTE: The contents of the SSR Transit Case and the SSR antenna carrying cases are pictured on separate cards.

Using Your SSR Notebook Case to Test Antennas and Cables:

- To test an antenna.
  1. Connect the MMCX-to-N (F) cable from the wireless NIC in the notebook to the Right angle adapter.
  2. Connect the Right angle adapter to the antenna, with the antenna oriented vertically.
  3. Use the Link Status Meter (LSM) to check signal quality.
- To test an antenna and cable.
  1. Connect a 25' or 35' cable to the antenna and erect it.
  2. Connect the MMCX-to-N (F) cable from the antenna cable to your notebook.
  3. Use the LSM to check signal quality.
- To align a directional antenna.
  1. Connect a 25' or 35' cable to the directional antenna and erect it.
  2. Connect the MMCX-to-N (F) cable from the antenna cable to your notebook.
  3. Point the plain flat side of the antenna in the general direction of the root or relay CBM.
     a. Use the LSM to check signal quality.
     b. Watch the meter for about 15 seconds, then turn the antenna a little bit to the left or right. Recheck the signal quality.
     c. Repeat the above until signal quality is maximized.
     d. Use the guy ropes to make sure the antenna will neither turn nor blow over.
- To check CBM or CCM antenna components
  1. Disconnect the antenna cable from the outside of the CBM or CCM lightning arrestor. Connect your MMCX-to-N (F) cable. Check the antenna, as above. Reconnect everything.
  2. Disconnect the small antenna cable inside the CBM or CCM from the inside of the lightning arrestor. Connect your Right angle adapter and MMCX-to-N cable to the lightning arrestor. Check the antenna, as above. Reconnect everything.
  3. Disconnect the small antenna cable inside the CBM or CCM from the radio. Connect your MMCX-to-RPTNC (F) cable to the small antenna cable inside the module. Check the antenna, as above. Reconnect everything.
- To check CBM or CCM link status
  1. With the wired NIC in your laptop, use a white straight-through Ethernet cable and connect to the hub in the CBM or CCM.
  2. Open a web browser and log on to the radio in the module, in accordance with the Technical Bulletin, use the LSM screen built in to the radio to check the link to the root or relay CBM.
- **NOTE:** *Ensure that all antenna and cable connections are tight, dry, and not cross-threaded. All antenna connections require numerous turns to tighten. If a connector only turns once or twice, it is probably cross-threaded and will only work intermittently or for very short ranges.*

REMEMBER: You should never operate in non-secure mode when your wireless NIC is installed, except to perform antenna alignment and troubleshooting as described above.

CAISI SSR
Notebook Case
Inventory Checklist

Component	Quantity	Date						
Transit Case	1							
SSR Notebook computer	1							
Power Supply for Notebook Computer	1							
Power Cord for Notebook Power Supply	1							
Wireless NIC, Cisco LMC-342 or 352	1							
“Rabbit Ears” Antenna	1							
Wired NIC (if issued)	1							
White Straight-Through Ethernet Cable	1							
Red Crossover Ethernet Cable	1							
Adapter, RJ-45 (F) to RJ-45 (F) Straight-through	1							
Adapter, RJ-45 (F) to RJ-45 (M) Crossover	1							
9-Pin Straight-Through Serial Extension Cable (M-F) (blue)	1							
9-Pin Crossover Serial Null Modem Cable (F-F) (beige)	1							
Adapter Cable, 12 inch, MMCX to N (F)	1							
Adapter Cable, 12 inch, MMCX to RPTNC (F)	1							
Adapter, Right-Angle, N (M) to N (M)	1							
Antenna “Dummy Load” N (M)	1							
Reset Tool	1							
Baseline CD	1							

NOTES:
The above inventory reflects the major components of the SSR Notebook Case. All are packed into the transit case. The items are pictured on the laminated Quick Reference Card.
This card is identical front and back. Use up one side before you start on the other.

This card is locally reproducible.

CAISI SSR Notebook Case Inventory Checklist

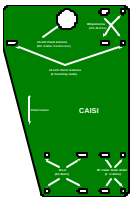
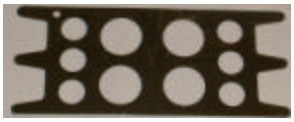
Component	Quantity	Date						
Transit Case	1							
SSR Notebook computer	1							
Power Supply for Notebook Computer	1							
Power Cord for Notebook Power Supply	1							
Wireless NIC, Cisco LMC-342 or 352	1							
“Rabbit Ears” Antenna	1							
Wired NIC (if issued)	1							
White Straight-Through Ethernet Cable	1							
Red Crossover Ethernet Cable	1							
Adapter, RJ-45 (F) to RJ-45 (F) Straight-through	1							
Adapter, RJ-45 (F) to RJ-45 (M) Crossover	1							
9-Pin Straight-Through Serial Extension Cable (M-F) (blue)	1							
9-Pin Crossover Serial Null Modem Cable (F-F) (beige)	1							
Adapter Cable, 12 inch, MMCX to N (F)	1							
Adapter Cable, 12 inch, MMCX to RPTNC (F)	1							
Adapter, Right-Angle, N (M) to N (M)	1							
Antenna “Dummy Load” N (M)	1							
Reset Tool	1							
Baseline CD	1							

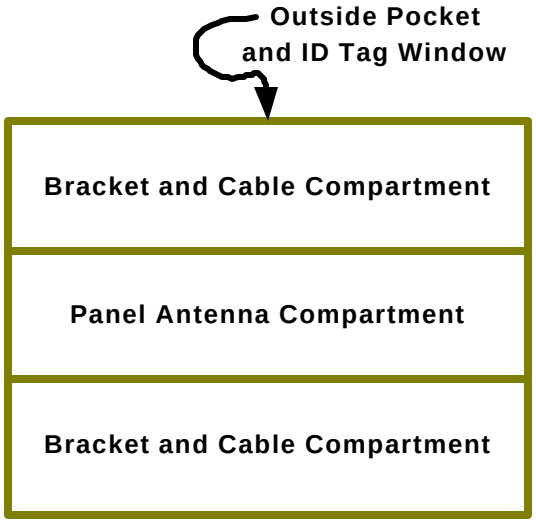
NOTES:
The above inventory reflects the major components of the SSR Notebook Case. All are packed into the Notebook Case. The items are pictured on the laminated Quick Reference Card.

This card is identical front and back. Use up one side before you start on the other.
This card is locally reproducible.

CAISI SSR Accessory Kit
Quick Reference Card

The following items are packed in the **SSR Antenna Carrying case**.

Carrying Case	50-feet RF Antenna Cable (Qty 4)	14-inch Panel Antenna (Qty 2)
7-inch Panel Antenna Bracket (Qty 2) (with U-bolts, washers and wing-nuts)	14-inch Panel Antenna Bracket (Qty 2) (with U-bolts, washers, and wing-nuts) 	Double "N" Cable Adapter (Barrel Connector) (Qty 4)
Antenna guy rope on reel (42-ft) (red) (Qty 4) (two per reel)	Reel Unit RL-28 (Qty 2) 	Antenna guy stake (Qty 4)

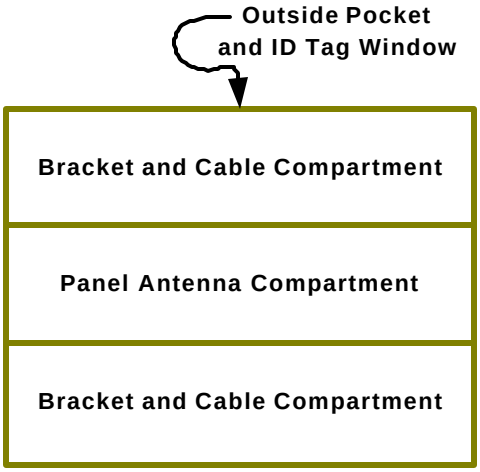


THIS PAGE IS INTENTIONALLY LEFT BLANK

CAISI SSR Accessory Kit
Antenna Carrying Case Inventory Checklist

Component	Quantity	Date						
Carrying Case	1							
14-inch Panel Antenna (store in center section)	2							
50-Foot RF Antenna Cable (store in the two outer sections)	4							
Bracket for 7-inch Panel Antenna (with U-bolts, washers, and wing nuts) (store in one outer section with cables)	2							
Bracket for 14-inch Panel Antenna (with U-bolts, washers, and wing nuts) (store in other outer section with cables)	2							
Double-N Adapter (Barrel Connector) (store in outer pocket)	4							
42-Foot Guy Rope (Red Clips) (store in outer section with cables)	4*							
Reel Unit For Guy Ropes (Containing Above, Two Guy Ropes Per Reel Unit) (store in outer section with cables)	2*							
Guy Stakes (store in outer section with cables)	4*							

* The initial 48 systems may be issued without these components until they become available. Units that do not receive these components initially will receive them when they become available.



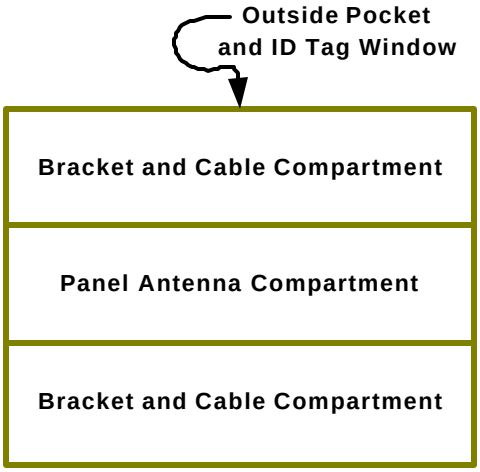
The above inventory reflects the major components of the SSR Antenna Carrying Case. The items are pictured on the laminated Quick Reference Card.

This card is identical front and back. Use up one side before you start on the other. This card is locally reproducible.

CAISI SSR Accessory Kit
Antenna Carrying Case Inventory Checklist

Component	Quantity	Date						
Carrying Case	1							
14-inch Panel Antenna (store in center section)	2							
50-Foot RF Antenna Cable (store in the two outer sections)	4							
Bracket for 7-inch Panel Antenna (with U-bolts, washers, and wing nuts) (store in one outer section with cables)	2							
Bracket for 14-inch Panel Antenna (with U-bolts, washers, and wing nuts) (store in other outer section with cables)	2							
Double-N Adapter (Barrel Connector) (store in outer pocket)	4							
42-Foot Guy Rope (Red Clips) (store in outer section with cables)	4*							
Reel Unit For Guy Ropes (Containing Above, Two Guy Ropes Per Reel Unit) (store in outer section with cables)	2*							
Guy Stakes (store in outer section with cables)	4*							

* The initial 48 systems may be issued without these components until they become available. Units that do not receive these components initially will receive them when they become available.



The above inventory reflects the major components of the SSR Antenna Carrying Case. The items are pictured on the laminated Quick Reference Card.

This card is identical front and back. Use up one side before you start on the other. This card is locally reproducible.

CAISI SSR ACCESSORY KIT
QUICK REFERENCE CARD

The SSR Accessory Kit also includes one standard AB-1244B/GRC antenna mast kit, packed in the **SSR Antenna Mast Carrying Case**. This is the same mast system used with the standard OE-254/GRC radio antenna. It is made up of two parts: antenna mast sections and the antenna mast kit.

The **Antenna Mast Sections** includes five lower sections, 5 upper sections, one lower adapter section and one upper adapter section.

Antenna Mast Sections

The **Antenna Mast Kit** includes four 36 foot guy ropes, four 42 foot guy ropes, four guy stakes, a mast base assembly, a base plate, two base plate pins, two guy rings, and a 2.5 pound sledge hammer.

Antenna Mast Kit

The following is extracted from Field Manual (FM) 24-19, Radio Operators Manual, May 1991. See the FM for complete instructions.

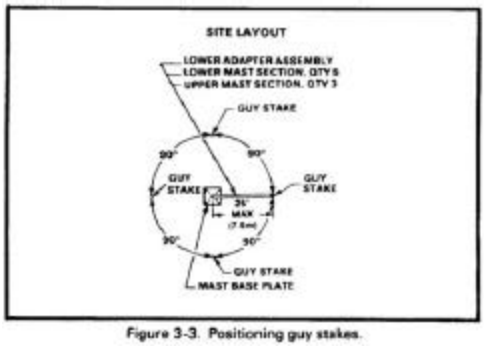


Figure 3-3. Positioning guy stakes.

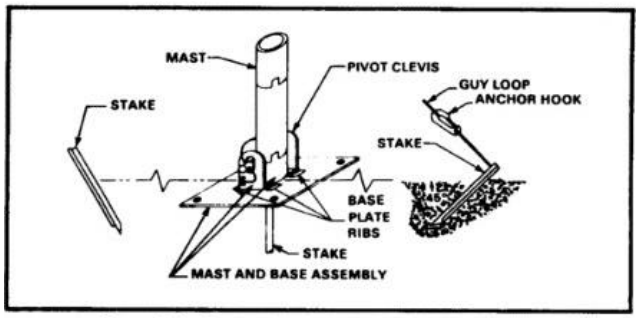


Figure 3-4. Ground anchor/pivot clevis alignment.

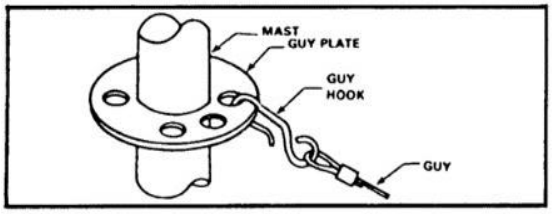


Figure 3-5. Attaching guy hooks to guy plate.

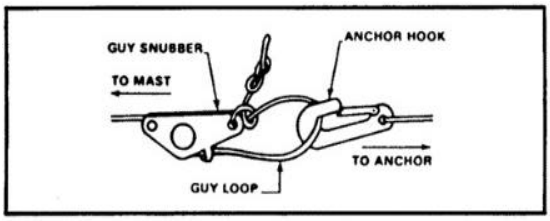


Figure 3-6. Attaching guy loops to ground anchor.

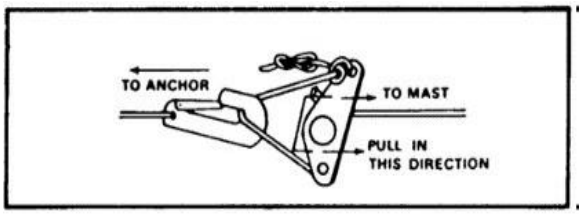


Figure 3-7. Pulling guy rope taut.

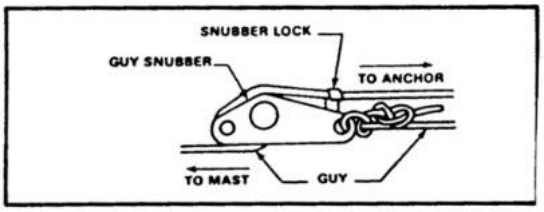


Figure 3-8. Securing guy with snubber lock.

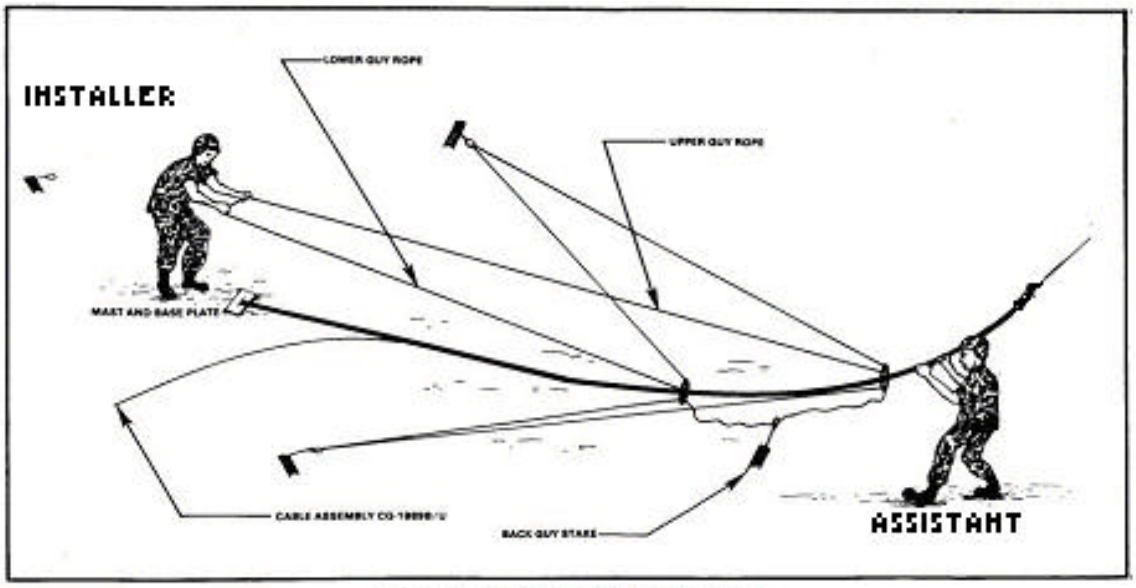


Figure 3-14. Erecting antenna group OE-254/GRC.

CAISI SSR Accessory Kit
Antenna Mast Carrying Case Inventory Checklist

Component	Quantity	Date						
Carrying Case	1							
Upper Mast Section (Mast section assembly (upper))	5							
Lower Mast Section (Mast section assembly (lower))	5							
Upper Mast Adapter Section (Red Ring) (Adapter assembly) (upper))	1							
Lower Mast Adapter Section (Blue Ring) (Adapter assembly) (lower))	1							
36-Foot Guy Rope (Blue Clips)	4							
42-Foot Guy Rope (Red Clips)	4							
Reel Unit For Guy Ropes (Containing Above, Two Guy Ropes Per Reel Unit)	4							
Guy Stakes (Stake assembly)	4							
Mast base assembly	1							
Base Plate	1							
Base Plate Pins (Base plate stakes)	2							
Guy Rings (One Red, One Blue) (Guy plates)	2							
2.5 Pound Sledge Hammer	1							

NOTES:
(Words in parenthesis are the component nomenclature that is in the Technical Manual #11-5895-357-13, Operator's Organizational Direct Support Maintenance Manual for Antenna Group OE-254/GRC).

This card is identical front and back. Use up one side before you start on the other.
This card is locally reproducible.

CAISI SSR Accessory Kit
Antenna Mast Carrying Case Inventory Checklist

Component	Quantity	Date						
Carrying Case	1							
Upper Mast Section (Mast section assembly (upper))	5							
Lower Mast Section (Mast section assembly (lower))	5							
Upper Mast Adapter Section (Red Ring) (Adapter assembly) (upper))	1							
Lower Mast Adapter Section (Blue Ring) (Adapter assembly) (lower))	1							
36-Foot Guy Rope (Blue Clips)	4							
42-Foot Guy Rope (Red Clips)	4							
Reel Unit For Guy Ropes (Containing Above, Two Guy Ropes Per Reel Unit)	4							
Guy Stakes (Stake assembly)	4							
Mast base assembly	1							
Base Plate	1							
Base Plate Pins (Base plate stakes)	2							
Guy Rings (One Red, One Blue) (Guy plates)	2							
2.5 Pound Sledge Hammer	1							

NOTES:

(Words in parenthesis are the component nomenclature that is in the Technical Manual #11-5895-357-13, Operator's Organizational Direct Support Maintenance Manual for Antenna Group OE-254/GRC).

This card is identical front and back. Use up one side before you start on the other.
This card is locally reproducible.

CAISI Legacy Support Adapter Quick Reference Card

The CAISI Legacy Support Adapters provide connectivity to legacy STAMIS computers that can only communicate through their serial ports. It connects your serial port to another STAMIS computer's serial port via a virtual-end-to-end (VEE) circuit over the tactical network.

LSA Components

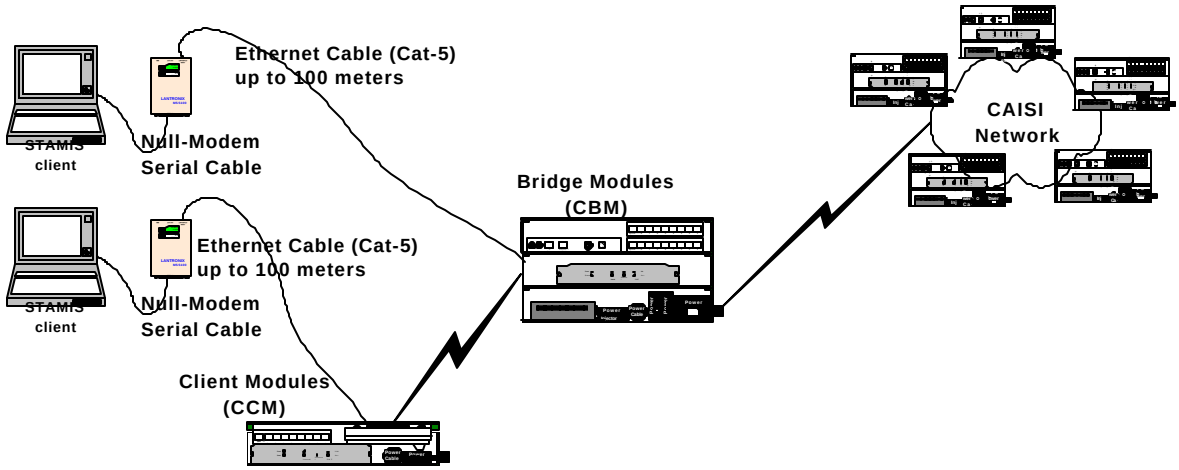
The following items are included.

Legacy Support Adapter MSS-100	9-to-25 Null Modem Cable	White Straight-Through Ethernet Cable
Power Supply, 5V	3-prong Power Cord	

The cover of the MSS-100 might look like either of the two photos above. One has blue trim and the old logo. The other has blue, green, and yellow trim and the new logo. They are exactly the same inside, only the cover is changed. The newer ones have the green and yellow labels next to the LEDs, but the LEDs are the same on both versions.

The LSA is originally issued with a short Ethernet cable. You will probably replace it with a longer one. The short one is fine if your STAMIS computer is right next to a CBM or CCM. If you are on the other side or other end of the tent or truck, you will need a longer cable. Get one from your communications support, S-6 or CSSAMO.

The Legacy Support Adapter does not require a transport case or bag. The LSA components are to be packed with your STAMIS computer in its transit case. Keep this card and the inventory card with the LSA.



Setup and Teardown

Setup Procedure:

1. Unpack the items.
2. Locate the LSA in a clean, dry location up off the ground next to or on your STAMIS computer.
3. Connect the null modem serial cable from your computer's 9-pin serial port to the LSA's 25-pin serial port.
4. Connect the Ethernet cable from the LSA's 10Base-T port to any available 10Base-T port on the nearest CBM or CCM.
5. Connect the power supply to the LSA's 5V power input. Connect the power cable to the LSA and plug it into 110VAC.

Teardown Procedure:

1. Unplug the power cord and disconnect it from the power supply. Disconnect the power supply from the LSA.
2. Disconnect the Ethernet cable from the CCM or CBM. Disconnect the other end from the LSA.
3. Disconnect the null modem serial cable from the STAMIS computer. Disconnect the other end from the LSA.
4. Pack everything back into the transit case.
5. Inventory the items to be sure you haven't forgotten anything.

CAISI Legacy Support Adapter
Inventory Checklist

Component	Quantity	Date						
Legacy Support Adapter, MSS-100	1							
9 to 25-pin Null Modem Cable Adapter	1							
White Straight-Through Ethernet Cable	1							
Power Supply	1							
3-Prong Power Cord	1							

Component	Quantity	Date						
Legacy Support Adapter, MSS-100	1							
9 to 25-pin Null Modem Cable Adapter	1							
White Straight-Through Ethernet Cable	1							
Power Supply	1							
3-Prong Power Cord	1							

NOTES:
This card has two inventory blocks per side. Use up the top one before you use the bottom.

This card is identical front and back. Use up one side before you start on the other.
This card is locally reproducible.

CAISI Legacy Support Adapter
Inventory Checklist

Component	Quantity	Date						
Legacy Support Adapter, MSS-100	1							
9 to 25-pin Null Modem Cable Adapter	1							
White Straight-Through Ethernet Cable	1							
Power Supply	1							
3-Prong Power Cord	1							

Component	Quantity	Date						
Legacy Support Adapter, MSS-100	1							
9 to 25-pin Null Modem Cable Adapter	1							
White Straight-Through Ethernet Cable	1							
Power Supply	1							
3-Prong Power Cord	1							

NOTES:
This card has two inventory blocks per side. Use up the top one before you use the bottom.

This card is identical front and back. Use up one side before you start on the other.
This card is locally reproducible.

Index

Subject	Paragraph	Page
10Base-2 Cable (RG-58)		
Connect CBM to INE using RG-58	2.18.8	2-76
Connect to CAISI Using 10Base-2	2.35.1	2-170
Troubleshooting	3.5	3-7
10Base-T Cable (RJ-45)		
PMCS	2.14.5	2-34
Description	2.17.2; 2.20.2	2-62; 2-88
Straight-through/Crossover Cabling	2.17.2	2-64
MDI/MDI-X	2.17.2	2-65
Connect to CAISI Using 10Base-T	2.35.2	2-172
Troubleshooting	3.5	3-7
How to make 10Base-T cables?	3.5	3-13
10Base-T Transceiver		
Controls and Indicators (LEDs)	2.12	2-25
PMCS	2.14.5	2-39
Description	2.24.2	2-101
Connecting to CBM using 10Base-T Transceiver	2.34	2-163
Connecting to SSR Wireless Bridge using 10Base-T Transceiver	2.34.1	2-165
Connecting to SSR DSL using 10Base-T Transceiver	2.34.2	2-167
Disconnect from INE	2.36.2	2-178
Troubleshooting	3.11	3-57
802.11b	2.17.2; F.2.5.2	2-60; F-8
Acronyms	Appendix G	G-9
Additional Authorizations List (AAL)	Appendix D	D-1
Administrative Instructions	1.1 – 1.11	1-1
Antennas		
Omni-Directional vs. Directional	1.17	1-16
Planning Ranges	1.17	1-16
Set up 40-inch Whip Antenna	2.18.2 – 2.18.4	2-69
Set up 7-inch Panel Antenna	2.19.2	2-80
4-inch Whip Antenna	2.24.2	2-105
Troubleshoot CBM Antenna System	3.7.4	3-32
Troubleshoot CCM Antenna System	3.8.4	3-47
Uses	I.3.8	I-21
Heights	I.5.2	I-41
Basic Issue Items (BII)	Appendix C	C-30
Barrel Connector	2.17.1	2-63
Connections	2.19.2	2-82

Subject	Paragraph	Page
CAISI		
Background	1.12.1	1-5
Mid-Term	1.12.1	1-5
Near Term Fix (NTF)	1.12.1	1-5
Purpose	1.12.2	1-6
System Design Requirements	1.12.3	1-8
Power Requirements and Physical Dimensions Data	1.18	1-18
Architecture	1.19	1-22
Connectivity	2.15.1.1	2-50
Configuration	2.30.1	2-137
Operation Under Unusual Conditions	2.47	2-202
Extreme Heat or Desert Conditions	2.47.1	2-202
Extreme Cold or Artic Conditions	2.47.2	2-202
High Humidity or Tropical Conditions	2.47.3	2-202
Security	Appendix F	F-1
Component Functions and Relationships	F.2.13	F-18
Network	I.3.1	I-13
CAISI Bridge Module (CBM)		
Overview	1.13	1-9
Power Requirements and Physical Dimensions Data	1.18.1	1-18
Architecture	1.19.1	1-24
Controls and Indicators (LEDs)	2.2 – 2.7	2-1
Wireless Bridge	2.3	2-3
Inline Encryptor	2.4	2-7
DSL	2.5	2-9
Hubs	2.6	2-12
UPS	2.7	2-14
Preventive Maintenance Checks and Services	2.14	2-31
Root CBM	2.15.1.1; I.3.6	2-49; I-18
Unpack	2.17	2-52
Components	2.17.2	
Wireless Bridge	2.17.2	2-57
Inline Encryptor	2.17.2	2-60
DSL	2.17.2	2-58
Hubs	2.17.2	2-60
UPS	2.17.2	2-64
Inventory Checklist Card	2.17.3; J-1.2	2-67; J-5
Setup Procedures	2.18	2-68
Connect to INE using RG-58	2.18.8	2-76
Connect to INE using 10Base-T (RJ-45)	2.35.2	2-172
Configuration	2.32	2-150
Wireless Bridge	2.32.1	2-150

Subject	Paragraph	Page
CAISI Bridge Module (CBM) (Continued)		
Inline Encryptor	2.32.2	2-156
Disconnect and Packup Procedures	2.36 – 2.37	2-177
Troubleshooting	3.7	
General	3.7.1	3-23
Hubs	3.7.2	3-26
Inline Encryptor and Wireless Bridge	3.7.3	3-29
Antenna System	3.7.4	3-32
DSL	3.7.5	3-36
UPS	3.7.6	3-38
Quick Reference Card	J-1.1	J-3
CAISI Client Module (CCM)		
Overview	1.14	1-11
Power Requirements and Physical Dimensions Data	1.18.1	1-19
Architecture	1.19.2	1-26
Controls and Indicators (LEDs)	2.8 – 2.9	2-17
Multi-Client Radio Adapter	2.9	2-18
Inline Encryptor	2.4	2-7
Hubs	2.6	2-12
Preventive Maintenance Checks and Services	2.14	2-34
Unpack	2.20	2-83
Components	2.20.2	
Multi-Client Radio Adapter	2.20.2	2-85
Inline Encryptor	2.20.2	2-85
Hub	2.20.2	2-86
Inventory Checklist Card	2.20.3; J-1.2	2-88; J-7
Setup Procedures	2.21	2-89
Security Considerations	2.30.2.1	2-139
Configuration	2.33	2-157
Multi-Client Radio Adapter	2.33.1	2-157
Inline Encryptor	2.33.2	2-162
Disconnect and Packup Procedures	2.38 – 2.39	2-187
Troubleshooting	3.8	3-40
General	3.8.1	3-40
Hub	3.8.2	3-43
Inline Encryptor and Multi-Client Radio Adapter	3.8.3	3-45
Antenna System	3.8.4	3-47
Quick Reference Card	J-1.1	J-9
Components of End Item (COEI)	Appendix C	C-1
Continuity of Operations	F.2.9	F-11
Deployment Planning	I.5	I-37
Diagnostic Features/Procedures	3.3 – 3.4	3-1

Subject	Paragraph	Page
Domain Name Server (DNS)	I.2.5	I-9
DSL		
Controls and Indicators	2.5	2-9
PMCS	2.14.5	2-32; 2-38
Description	2.17.2	2-58
Connecting DSL	2.19.1	2-77
Connect to INE	2.34.2	2-167
Troubleshooting	3.7.5	3-36
When to use DSL	I.3.7	I-18
Use in conjunction with Router	I.3.9	I-27
Electrical Cautions/Procedures	Intro	a-d
Exceptional Circumstances (Special)	I.6	I-54
Expendable and Durable Items List	Appendix E	E-1
External Router	I.3.9	I-31
Flowcharts	3.13	3-58
Forward Repair Activities (FRA)	3.14.1	3-87
Garrison (How to set up in)	I.7	I-57
Glossary of Terms	Appendix G	G-1
Grounding Strap		
Description	2.17.2	2-62
Connection to CBM	2.18.1	2-68
Connection to CCM	2.21.1	2-89
Disconnect from CBM/CCM	2.36.4.6	2-183
Safe Grounding of Communications – Electronic Equipment	Appendix H	H-1
Hubs		
Controls and Indicators (LEDs)	2.6	2-12
PMCS	2.14	2-38
Description	2.17.2	2-60
Use with SSR Wireless Bridge	2.32.1.2	2-154
Use with SSR Multi-Client Radio Adapter	2.33.1.3	2-161
Troubleshooting	3.7.2; 3.8.2	3-26; 3-43
How to connect for extra users	I.6.1.1	I-54
Inline Encryptors (AirFortress)		
Controls and Indicators (LEDs)	2.4	2-7
PMCS	2.14	2-37
Description	2.17.2	2-60
Use with SSR Wireless Bridge	2.32.1.2	2-154
Use with SSR Multi-Client Radio Adapter	2.33.1.3	2-161
Configuration	2.32.2	2-156

Subject	Paragraph	Page
Inline Encryptors (AirFortress) (Continued)		
Troubleshooting	3.7.3; 3.8.3	3-29; 3-45
How to use	I.3.10	I-32
In-Line Network Encryption (INE)		
Connecting to CBM with RG-58	2.18.8	2-76
Connecting to CBM using 10Base-T Transceiver	2.34	2-163
Connecting to SSR Wireless Bridge using 10Base-T Transceiver	2.34.1	2-165
Connecting to SSR DSL using 10Base-T Transceiver	2.34.2	2-167
Disconnect from INE	2.36.2	2-178
Local Area Network (LAN)	I.2.1	I-1
Legacy Support Adapter (LSA)		
Overview	1.15	1-12
Power Requirements and Physical Dimensions Data	1.18.1	1-19
Architecture	1.19.3	1-26
Controls and Indicators (LEDs)	2.10	2-20
PMCS	2.14	2-35
Unpack	2.22	2-91
Connections	2.35.3	2-174
Configuration	2.35.4	2-176
Disconnect & Packup	2.40 – 2.41	2-189
Troubleshooting	3.9	3-51
Maintenance Allocation Chart (MAC)	Appendix B	B-1
Maintenance Procedures	3.14	3-65
Replacing Components inside CBM/CCM	3.14.2	3-77
Mobile Subscriber Equipment (MSE)	2.15.1; I.4	2-49; I-34
Circuit Switch	F.2.5.3	F-9
Monitoring Procedures	2.35.5	2-174
Multi-Client Radio Adapter		
Controls and Indicators (LEDs)	2.9	2-18
PMCS	2.14	2-38
Description	2.19.2	2-85
Configuration	2.33.1	2-157
Reset	2.33.1.1	2-159
Physical Connection of SSR Multi-Client Radio Adapter for Configuration	2.33.1.2	2-160
Physical Connection of SSR Multi-Client Radio Adapter for Operation	2.33.1.3	2-161
Troubleshooting	3.8.3	3-45

Subject	Paragraph	Page
NES Gateway	I.4	I-34
Network		
Overview	I.2	I-1
Local Area Network (LAN)	I.2.1	I-1
Wide Area Network (WAN)	I.2.2	I-3
Wireless Networking	I.2.3	I-4
Physical Links	I.2.4	I-9
Components	I.3.1	I-13
Connectivity and CSS Community	I.3.5	I-16
Army Network Topology	I.4	I-34
Operation Under Unusual Conditions	2.47	2-202
Extreme Heat or Desert Conditions	2.47.1	2-202
Extreme Cold or Artic Conditions	2.47.2	2-202
High Humidity or Tropical Conditions	2.47.3	2-202
Planning your CAISI Setup	Appendix I	I-1
General	I.1	
Networking	I.2	I-1
LAN	I.2.1	I-1
WAN	I.2.2	I-3
Wireless Networking	I.2.3	I-4
TCP/IP Addresses	I.2.4	I-5
Domain Name Server (DNS)	I.2.5	I-9
Differences Between a Bridge and a Router	I.2.6	I-10
Subnet Mask	I.2.7	I-11
CAISI Network Topology	I.3	I-12
CAISI Network Components	I.3.1	I-13
How are CAISI Clients Connected?	I.3.2	I-13
How are Wireless Bridges Used?	I.3.3	I-15
Legacy STAMIS vs. Network Capable STAMIS	I.3.4	I-16
Network Connectivity and CSS Community	I.3.5	I-16
CAISI Root CBM	I.3.6	I-18
When do you use DSL Bridges?	I.3.7	I-18
Antennas and Radio Frequency (RF) Cables	I.3.8	I-21
When do you use the Router?	I.3.9	I-24
How do you use the Encryptors?	I.3.10	I-32
Army Network Topology	I.4	I-34
Planning for Deployment	I.5	I-37
What goes Where?	I.5.1	I-38

Subject	Paragraph	Page
Planning your CAISI Setup (Continued)		
What is the Range of the Radios?	I.5.2	I-39
How are CBMs and CCMs connected in the Support Area	I.5.3	I-44
Who gets the CBMs and CCMs?	I.5.4	I-47
How do you use Service Set Identifications (SSIDs) to Segment the Network?	I.5.5	I-48
Can you use Multiple Root Radios with the same SSID?	I.5.6	I-49
How do you use Wired Equivalent Privacy (WEP) Keys to Secure the Network?	I.5.7	I-50
How do you use Multiple SSIDs and WEP Keys?	I.5.8	I-52
Operations in Exceptional Circumstances (Special)	I.6	I-54
When do you use Those “Extra” Items in the SSR Accessory Kit?	I.6.1	I-54
Use of SSR Wireless Bridge	2.32.1.1	2-153
Use of SSR Multi-Client Radio Adapter	2.33.1.2	2-160
Connect SSR Hub to an existing CBM/CCM	I.6.1.1	I-55
Use of the Router	I.3.9	I-24
Connect to INE with SSR Wireless Bridge	2.34.1	2-165
Connect to INE with SSR DSL	2.34.2	2-167
Use of Larger Antennas	2.28.2 / 2.29	2-129 / 2-131
Use of Long Antenna Cables	2.19.3; I.6	2-82; I-55
Use of Directional Panel Antennas	2.19.2; 2.28.2	2-80; 2-129
Use of DSL to avoid using radios	2.19.1	2-77
How do you set up in Garrison?	I.7	I-57
What about using CAISI OCONUS?	I.8	I-59
World-Wide Transmit Power Limitations Table	I.8	I-61
How do you connect to Adjacent Units?	I.9	I-62
What if they have CAISI-MT instead of wireless CAISI?	I.9.1	I-62
How do you Change the SSID or WEP while you are Deployed?	I.10	I-63

Subject	Paragraph	Page
PMCS	2.14	2-28
User PMCS Table	2.14	2-31
Organizational PMCS Table	2.14	2-37
Quick Reference Guide and Inventory Cards	Appendix J	J-1
CBM		J-3; J-5
CCM		J-7; J-9
SSR Transit Case		J-11; J-13
SSR Notebook Case		J-15; J-17
SSR Antenna Carrying Case		J-19; J-21
SSR Antenna Mast Carrying Case		J-23; J-25
LSA		J-27; J-29
References	Appendix A	A-1
Router, Linksys		
Controls and Indicators (LEDs)	2.11	2-22
PMCS	2.14	2-37
Description	2.19.1	2-100
Configuration	2.31	2-149
Troubleshooting	3.10	3-54
Use of a Router	I.3.9	I-24
Router Between Two CBMs	I.3.9	I-25
Router Connected to SSR Wireless Bridge or SSR DSL	I.3.9	I-27
Router Between CBM and SSR Wireless Bridge	I.3.9	I-28
Security	Appendix F	F-1
Security Measures for Electronic Data	1.11	1-4
CBM Security Considerations	2.30.2.1	2-139
CCM Security Considerations	2.30.2.2	2-140
STAMIS and CSS User Responsibilities	F.1.1	F-1
SSR Security Duties and Responsibilities	F.1.2	F-1
CSS S6 Responsibilities	F.1.3	F-3
ISSM or ISSO Responsibilities	F.1.4	F-3
SSR Security Procedures	F.2	F-5
OPSEC Security	F.2.1	F-5
Physical Security	F.2.2	F-5
Software Security	F.2.3	F-6
Communications Security	F.2.4	F-7
Use of the INE	F.2.4.1	F-7
Protected Distribution System (PDS)	F.2.5	F-7
Cable Connections	F.2.5.1	F-7
Wireless Local Area Network	F.2.5.2	F-8

Subject	Paragraph	Page
Security (Continued)		
Mobile Subscriber Equipment – Circuit Switch	F.2.5.3	F-9
Commercial Modem Access	F.2.6	F-9
Security Training	F.2.7	F-9
Miscellaneous Provisions	F.2.8	F-10
Marking of Output	F.2.8.1	F-10
Access by Foreign Nationals	F.2.8.2	F-11
Access by Maintenance Personnel	F.2.8.3	F-11
Continuity of Operations	F.2.9	F-11
Restoration of Service	F.2.9.1	F-11
Restoration of Data	F.2.9.2	F-12
Emergency Destruction	F.2.10	F-12
SSR Notebook User Security Procedures	F.2.11	F-12
User Interface Description	F.2.11.1	F-12
User Identification and Authentication	F.2.11.2	F-13
Passwords	F.2.11.3	F-15
Screen Saver	F.2.11.4	F-15
Login Banner	F.2.11.5	F-16
Virus Protection	F.2.11.6	F-16
Wireless Network Card	F.2.11.7	F-17
Security Features and Configuration	F.2.12	F-17
Component Functions and Relationships	F.2.13	F-18
Service Set Identification (SSID)		
Description		
How to use to segment network?	I.5.5	I-48
Can you use Multiple Root Radios with the same SSID?	I.5.6	I-49
How to use Multiple SSIDs?	I.5.8.2	I-52
How do you Change the SSID or WEP while you are Deployed?	I.10	I-63
SSR Accessory Kit		
Overview	1.16	1-13
Duplicate Components	1.16	1-14
Unique Components	1.16	1-15
Power Requirements and Physical Dimensions	1.18.1	1-20
Unpack	2.23	2-93
Inventory Checklist Card	2.24.3	2-109
Quick Reference Card	J.1.1	

Subject	Paragraph	Page
SSR Antenna Carrying Case		
Overview	1.16	1-13
PMCS	2.14	2-44
Unpack	2.26	2-120
Inventory Checklist Card	2.26.3	2-124
Packup	2.45	2-197
Quick Reference Card	J.1.1	J-19
SSR Antenna Mast Carrying Case		
Overview	1.16	1-13
PMCS	2.14	2-46
Unpack	2.27	2-126
Inventory Checklist Card	2.27.3	2-128
Set up Antenna Mast Equipment	2.28	2-129
Set up Antenna Mast	2.29	2-131
Teardown	2.42	2-190
Packup	2.46	2-200
Quick Reference Card	J.1.1	J-21
SSR Notebook Case		
Overview	1.16	1-13
Power Requirements and Physical Dimensions Data	1.18.1	1-21
PMCS	2.14	2-42
Unpack	2.25	2-112
Inventory Checklist Card	2.25.3	2-120
Configuration	2.30.2	2-138
Using with Wired NIC	2.30.4	2-144
Using with Wireless NIC	2.30.5 – 2.30.6	2-145
Packup	2.44	2-195
Troubleshooting	3.6	3-19
SSR Notebook User Security Procedures	F.2.11	F-12
User Interface Description	F.2.11.1	F-12
User Identification and Authentication	F.2.11.2	F-13
Passwords	F.2.11.3	F-15
Screen Saver	F.2.11.4	F-15
Login Banner	F.2.11.5	F-16
Virus Protection	F.2.11.6	F-16
Wireless Network Card	F.2.11.7	F-17
Security Features and Configuration	F.2.12	F-17
Quick Reference Card	J.1.1	J-15
SSR Transit Case		
PMCS	2-14	2-37
Unpack	2.23	2-93
Inventory Checklist Card	2.24.3	2-109

Subject	Paragraph	Page
SSR Transit Case (Continued)		
Packup	2.43	2-189
Quick Reference Card	J.1.1	J-11
TCP/IP	I.2.4	I-9
Troubleshooting		
Procedures	3.1	3-1
Flowcharts	3.13	3-58
UPS		
Controls and Indicators (LEDs)	2.7	2-14
PMCS	2.14	2-32
Description	2.17.1	2-64
Connection	2.18.6	2-74
Troubleshooting	3.7.6	3-38
Wired Equivalent Privacy (WEP)		
How do you use WEP Keys to Secure the Network?	I.5.7	I-50
How do you use Multiple SSIDs and WEP Keys?	I.5.8	I-52
How to use Multiple WEPs?	I.5.8.2	I-53
How do you Change the SSID or WEP while you are Deployed?	I.10	I-63
Wireless Bridge		
Controls and Indicators (LEDs)	2.3	2-3
PMCS	2.14	2-38
Description	2.17.1	2-57
Power Supply and Power Injector	2.17.1	2-61
Configuration	2.32.1	2-150
Physical Connection of SSR Wireless Bridge for Configuration	2.32.1.1	2-153
Physical Connection of SSR Wireless Bridge for Operation	2.32.1.2	2-154
Connect SSR Wireless Bridge to INE/NES	2.34.1	2-162
Troubleshooting	3.7.3	3-29

NOTES

NOTES