
DRAFT

TECHNICAL BULLETIN

SOFTWARE USERS MANUAL (SUM)

**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 07703-5000.

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

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INSERT LATEST CHANGED PAGES, DESTROY SUPERSEDED PAGES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..... 0August 2003

TOTAL NUMBER OF PAGES IN THIS PUBLICATION IS 398
CONSISTING OF THE FOLLOWING:

<u>Page No.</u>	<u>*Change No.</u>
Title.....	0
A.....	0
B Blank.....	0
i - xxi.....	0
1-1 - 1-11.....	0
1-12 Blank.....	0
2-1 - 2-30.....	0
2-31 - 2-42.....	0
2-43 - 2-74.....	0
2-75 - 2-90.....	0
2-91 - 2-108.....	0
3-1 - 3-54.....	0
3-55 - 3-110.....	0
4-1 - 4-55.....	0
4-56 - Blank.....	0
A-1 - A-20.....	0
B-1 - B-12.....	0
C-1 - C-46.....	0
Index-1 - Index-8.....	0 (Index)

THIS PAGE IS INTENTIONALLY LEFT BLANK

TECHNICAL BULLETIN

No. 11-5895-1691-10

**HEADQUARTERS
DEPARTMENT OF THE ARMY
WASHINGTON, D.C., 1 Aug 2003**

SOFTWARE USERS MANUAL (SUM)

**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 DOCUMENT OVERVIEW	1-1
1.3 SOFTWARE INVENTORY	1-3
1.3.1 Software Security	1-5
1.3.2 Software Developer/Maintainers and Support Engineers	1-5
Section II Equipment Description and Data	1-6
1.4 CAISI EQUIPMENT	1-6
1.4.1 CAISI Bridge Module (CBM)	1-7
1.4.2 CAISI Client Module (CCM)	1-8
1.4.3 Legacy Support Adaptor (LSA)	1-9
1.4.4 System Support Representative (SSR) Accessory Kit	1-9
1.5 CAISI CONFIGURATION OVERVIEW	1-10
1.5.1 CAISI Supported Components	1-11
Chapter 2 MANUAL CONFIGURATION	2-1
Section I Notebook Configuration	2-1
2.1 SSR NOTEBOOK	2-1
2.1.1 SSR Notebook Security	2-2
2.2 SSR NOTEBOOK SETUP	2-2
2.3 CONFIGURING SSR NOTEBOOK BASIC INPUT/OUTPUT SYSTEM (BIOS)	2-2
2.3.1 Mitac 7020 BIOS Settings	2-3
2.3.2 Mitac 7521T BIOS Settings	2-7
2.4 RELOAD SOFTWARE	2-9
2.5 CREATE AND MAINTAIN USER ACCOUNTS	2-10
2.6 CONFIGURE NETWORK PARAMETERS	2-15
2.7 CONFIGURE THE WIRED/BUILT-IN NETWORK INTERFACE CARD (NIC)	2-17

Section/Paragraph		Page
2.7.1	Remove NIC from SSR Notebook	2-19
2.7.2	Disable Built-In NIC	2-19
2.8	CONFIGURE THE WIRELESS NETWORK INTERFACE CARD (NIC)	2-20
2.9	CONFIGURE AIR FORTRESS REMOTE CLIENT	2-26
2.9.1	Configure the Parameters for the Air Fortress Remote Client	2-26
2.9.2	Turn the Air Fortress Remote Client On or Off	2-30
Section II	CAISI Component Configuration	2-31
2.10	MANUAL CONFIGURATION OF THE ROUTER	2-31
2.10.1	Physical Connection Procedures	2-31
2.10.2	Configure the Router	2-32
2.10.3	Verify Router Operational Status	2-40
2.10.4	Disconnection Procedures	2-42
2.11	MANUAL CONFIGURATION OF THE CAISI BRIDGE MODULE (CBM)	2-43
2.11.1	Physical Connection Procedures	2-47
2.11.2	Configuration of the CBM Wireless Bridge	2-48
2.11.2.1	Minimum Configuration of a Preset CBM Wireless Bridge	2-48
2.11.2.2	Configuration of the CBM Wireless Bridge from Scratch	2-56
2.11.3	Verify Operational Status of the CBM Wireless Bridge	2-63
2.11.4	Disable Remote Access to the CBM Wireless Bridge	2-64
2.11.5	Disconnect CBM Wireless Bridge from the Notebook Computer	2-64
2.11.6	Configure CBM Inline Encryptor	2-65
2.11.6.1	Configure the CBM Inline Encryptor from Scratch Using the Console Port	2-65
2.11.6.2	Configure the CBM Inline Encryptor from Scratch Using the Ethernet Port	2-72
2.11.7	CBM Power Cable Disconnection Procedures	2-74
2.12	MANUAL CONFIGURATION OF THE CAISI CLIENT MODULE (CCM)	2-75
2.12.1	Physical Connection Procedures	2-77
2.12.2	Configuration of the CCM Multi-Client Radio Adapter	2-78
2.12.2.1	Minimum Configuration of a Preset CCM Multi-Client Radio Adapter	2-78
2.12.2.2	Configuration of a CCM Multi-Client Radio Adapter from Scratch	2-81

		Page
Section/Paragraph		
2.12.3	Verify Operational Status of CCM Multi-Client Radio Adapter	2-88
2.12.4	Disable Remote Access to the CCM Multi-Client Radio Adapter	2-89
2.12.5	Disconnect CCM Multi-Client Radio Adapter from Notebook	2-90
2.12.6	Configure CCM Encryptor	2-90
2.12.7	CCM Power Cable Disconnection Procedures	2-90
2.13	MANUAL CONFIGURATION OF THE LEGACY SUPPORT ADAPTER (LSA)	2-91
2.13.1	Physical Connection Procedures	2-91
2.13.2	Configuration of the LSA	2-92
2.13.3	Verify Operational Status of LSA	2-105
2.13.4	LSA Disconnection Procedures	2-108
Chapter 3	CAISI ADMINISTRATION SOFTWARE APPLICATION (CAISI ADMIN)	3-1
Section I	Description of CAISI Admin	3-1
3.1	INTRODUCTION	3-1
3.2	CAISI ADMIN NAVIGATION	3-1
3.2.1	CAISI Admin Commands	3-2
3.2.2	CAISI Admin Toolbar	3-4
3.2.3	Device List	3-5
3.2.4	Device Information Fields	3-6
3.2.5	View Types	3-7
3.3	DEVICES	3-8
3.3.1	Device Properties	3-9
3.3.1.1	General Properties	3-10
3.3.1.2	Network Properties	3-11
3.3.1.3	Details Properties	3-12
3.3.1.4	Advanced Properties	3-12
3.4	DEVICE TEMPLATES	3-16
3.4.1	Device Attributes vs. Template Properties	3-16
3.4.2	Creating A Template	3-17
3.4.3	Modifying Template Properties and Device Attributes	3-19
3.4.4	Modifying General Properties	3-20

Section/Paragraph		Page
3.4.5	Modifying Network Properties	3-20
3.4.6	Modifying Device Specific Properties	3-21
3.4.7	Modifying Attribute Properties	3-22
3.4.8	Deleting a Template	3-24
3.4.9	Creating A Device	3-24
3.4.9.1	Add Device Method	3-25
3.4.9.2	Device Wizard Method	3-26
3.4.10	Modifying Device Properties	3-31
3.4.10.1	General Properties	3-32
3.4.10.2	Network Properties	3-34
3.4.10.3	Details Properties	3-36
3.4.10.4	Advanced Properties	3-37
3.4.10.5	Deleting a Device	3-38
Section II	Configuring Components using CAISI ADMIN	3-39
3.5	UTILIZING CAISI ADMIN TO CONFIGURE THE ROUTER BEFSR41/81 (Firmware 2.40.2)	3-39
3.5.1	Perform Router Connection Procedures	3-39
3.5.2	Apply Power to the SSR Notebook	3-40
3.5.3	Reset the Router to Factory Settings	3-40
3.5.4	Configure the Router	3-40
3.5.5	Verify Router Operational Status	3-52
3.5.6	Perform Disconnection Procedures	3-54
3.6	UTILIZING CAISI ADMIN TO CONFIGURE THE CBM	3-55
3.6.1	Physical Connection Procedures	3-59
3.6.2	Configure the CBM Wireless Bridge (Firmware 12.01T)	3-60
3.6.3	Verify CBM Wireless Bridge Operational Status	3-71
3.6.4	Disconnect CBM Wireless Bridge from the Notebook Computer	3-72
3.6.5	Configure the CBM Inline Encryptor (Firmware 1178W)	3-73
3.6.6	Verify Inline Encryptor Operational Status	3-83
3.6.7	CBM Power Cable Disconnection Procedures	3-84
3.7	UTILIZING CAISI ADMIN TO CONFIGURE THE CCM	3-85
3.7.1	Physical Connection Procedure	3-87

Section/Paragraph		Page
3.7.2	Configure the CCM Multi-Client Radio Adapter (Firmware 8.65)	3-88
3.7.3	Verify CCM Multi-Client Radio Adapter Operational Status	3-98
3.7.4	Disconnect CCM Multi-Client Radio Adapter from the Notebook Computer	3-99
3.7.5	Configure the CCM Inline Encryptor (Firmware 1178W)	3-99
3.7.6	CCM Power Cable Disconnection Procedures	3-99
Section III	CAISI ADMIN Management & Administration	3-100
3.8	CAISI ADMIN MANAGEMENT	3-100
3.8.1	Audit Logging	3-100
3.8.1.1	Purpose	3-100
3.8.1.2	Viewing Details in the Audit Log	3-101
3.8.1.3	Deleting the Audit Log	3-101
3.8.2	Configuration File	3-102
3.8.2.1	Saving the Configuration File	3-102
3.8.2.2	Backup and Restore	3-103
3.8.2.3	Configuration Backup	3-103
3.8.2.4	Configuration Restore	3-105
3.8.3	Printing	3-107
3.8.3.1	Print Setup	3-107
3.8.3.2	Physical Printing	3-108
3.8.3.3	Print Preview	3-110
Chapter 4	ADVANCED TROUBLESHOOTING	4-1
4.1	GENERAL TROUBLESHOOTING PROCEDURES	4-1
4.1.1	General Network Operation Rules	4-11
4.2	TROUBLESHOOTING THE SSR ACCESSORY KIT COMPONENTS	4-15
4.2.1	Troubleshooting the SSR Notebook	4-15
4.2.1.1	Troubleshooting the SSR Notebook Software	4-15
4.2.1.2	Troubleshooting the SSR Notebook Utilities	4-16
4.2.1.3	Troubleshooting the SSR Notebook Wired NIC or Built-In NIC	4-18
4.2.1.4	Troubleshooting the SSR Notebook Wireless NIC	4-20

Section/Paragraph		Page
4.2.2	Troubleshooting the Router	4-23
4.2.2.1	Troubleshooting Router Light Emitting Diodes (LEDs)	4-23
4.2.2.2	Troubleshooting the Router Configuration	4-24
4.2.3	Troubleshooting the 10BaseT Transceiver	4-27
4.3	TROUBLESHOOTING THE CBM	4-28
4.3.1	CBM General Troubleshooting Procedures	4-28
4.3.2	Troubleshooting CBM Hubs	4-31
4.3.3	Troubleshooting CBM Encryptor and Wireless Bridge	4-32
4.3.4	Troubleshooting CBM Antenna System	4-37
4.3.5	Troubleshooting CBM DSL Bridge	4-41
4.3.6	Troubleshooting CBM UPS	4-42
4.4	TROUBLESHOOTING THE CCM	4-43
4.4.1	CCM General Troubleshooting Procedures	4-43
4.4.2	Troubleshooting the CCM Hub	4-45
4.4.3	Troubleshooting CCM Encryptor and Multi-client Radio Adapter	4-46
4.4.4	Troubleshooting CCM Antenna System	4-49
4.5	TROUBLESHOOTING THE LSA	4-53
APPENDIX A	CAISI MANUAL TOOLS AND SYSTEM UTILITIES	A-1
APPENDIX B	GLOSSARY/ACRONYM LIST	B-1
APPENDIX C	QUICK CONFIGURATION GUIDE	C-1
APPENDIX D	INDEX	Index-1

LIST OF FIGURES

FIGURE NUMBER	NAME	PAGE
1-1	CBM Front View	1-7
1-2	CBM Back View	1-7
1-3	CCM Front View	1-8
1-4	CCM Back View	1-8
1-5	LSA	1-9
1-6	SSR Accessory Kit	1-9
2-1	Wired NIC and Wireless NIC	2-1
2-2	SSR Notebook	2-1
2-3	7020 BIOS Main Menu	2-3
2-4	7020 BIOS Date & Time Menu	2-3
2-5	7020 BIOS Main Menu	2-4
2-6	7020 BIOS Boot Sequence Menu	2-4
2-7	7020 BIOS Advanced Menu	2-4
2-8	7020 BIOS COM Port Menu	2-5
2-9	7020 BIOS Advanced Menu	2-5
2-10	7020 BIOS LPT Extended Mode Menu	2-5
2-11	7020 BIOS Power Menu	2-6
2-12	7020 BIOS Customize Menu	2-6
2-13	7521T BIOS Main Menu	2-7
2-14	7521T BIOS Advanced Menu	2-7
2-15	7521T BIOS I/O Device Configuration Menu	2-8
2-16	7521T BIOS Power Menu	2-8
2-17	7521T BIOS Boot Menu	2-8
2-18	SSR Notebook My Computer Screen	2-12
2-19	SSR Notebook Control Panel Screen	2-12
2-20	SSR Notebook Users and Password Screen	2-12
2-21	SSR Notebook Add New User Screen	2-13
2-22	SSR Notebook Add New User Password Screen	2-13
2-23	SSR Notebook Level of Access for New User Screen	2-13
2-24	SSR Notebook Users and Passwords Advanced Screen	2-14
2-25	SSR Notebook Local Users and Groups	2-14

FIGURE NUMBER	NAME	PAGE
2-26	SSR Notebook New User Properties Screen	2-15
2-27	SSR Notebook Network Parameters Screen	2-15
2-28	SSR Notebook System Properties Screen	2-16
2-29	SSR Notebook Identification Changes Screen	2-16
2-30	SSR Notebook DNS Suffix and Net BIOS Computer Name	2-16
2-31	SSR Notebook Network Parameters Screen	2-17
2-32	SSR Notebook Network and Dial-up Connections Screen	2-17
2-33	SSR Notebook Wired NIC Properties Screen	2-17
2-34	SSR Notebook Wired NIC TCP/IP Properties Screen	2-18
2-35	SSR Notebook NIC Card Icon	2-19
2-36	SSR Notebook Safe to Remove Hardware Prompt	2-19
2-37	SSR Notebook Built-In Ethernet NIC Prompts	2-19
2-38	SSR Notebook Network Parameters Screen	2-20
2-39	SSR Notebook Network and Dial-up Connections Screen	2-20
2-40	SSR Notebook Wireless NIC Properties Screen	2-21
2-41	SSR Notebook TCP/IP Properties for Wireless NIC	2-21
2-42	SSR Notebook Client Encryption Manager (CEM) Screen	2-22
2-43	SSR Notebook Commands Menu	2-22
2-44	SSR Notebook Change CEM Password Screen	2-22
2-45	SSR Notebook Set WEP Key Screen	2-23
2-46	SSR Notebook Aironet Client Utility (ACU) Screen	2-24
2-47	SSR Notebook Wireless NIC System Properties Screen	2-24
2-48	SSR Notebook Wireless NIC Network Security Screen	2-24
2-49	SSR Notebook AF Client Main Screen	2-26
2-50	SSR Notebook AF Clients Utilities Screen	2-26
2-51	SSR Notebook AF Configuration Password Screen	2-27
2-52	SSR Notebook AF Client Logon Successful Prompt	2-27
2-53	SSR Notebook AF Client Change Access ID Screen	2-27
2-54	SSR Notebook AF Access ID Successfully Changed Screen	2-28
2-55	SSR Notebook AF Client Utilities Screen	2-28
2-56	SSR Notebook AF Client Utilities General Tab	2-28
2-57	SSR Notebook AF Client Configuration Authorization	2-29
2-58	SSR Notebook AF Client Password Set Screen	2-29
2-59	SSR Notebook AF Client Utilities General Tab - 1	2-30
2-60	SSR Notebook AF Client Utilities General Tab - 2	2-30

FIGURE NUMBER	NAME	PAGE
2-61	Router	2-31
2-62	Router Ethernet Cable Connection	2-32
2-63	Router Front View of LEDs	2-33
2-64	Router Enter Network Password Screen	2-33
2-65	Router Main Menu Setup Tab	2-34
2-66	Router WAN Connection Type Screen	2-34
2-67	Router Main Menu Password Tab	2-35
2-68	Router Enter Network Password Screen	2-35
2-69	Router Main Menu Status Tab	2-36
2-70	Router Main Menu DHCP Tab	2-36
2-71	Router DHCP Active IP Table	2-37
2-72	Router Main Menu Log Tab	2-37
2-73	Router Main Menu Security Tab	2-38
2-74	Router Main Menu Help Tab	2-38
2-75	Router Main Menu Advanced Tab	2-39
2-76	Router Enter Network Password Screen	2-40
2-77	Router Configured Status Tab	2-41
2-78	Router Factory Default Status Tab	2-41
2-79	Router Configured DHCP Tab	2-41
2-80	Router Factory Default DHCP Tab	2-41
2-81	CBM	2-43
2-82	CBM Power Cable Connections	2-47
2-83	Wireless Bridge Console-Summary Status Screen	2-49
2-84	Wireless Bridge Console-Setup Screen	2-50
2-85	Wireless Bridge Console-Web Server Setup Screen	2-50
2-86	Wireless Bridge Console-Non-Console Browsing Allowed	2-51
2-87	Wireless Bridge Summary Status Menu	2-52
2-88	Wireless Bridge Setup Menu	2-52
2-89	Wireless Bridge Express Setup Menu	2-53
2-90	Wireless Bridge Radio Data Encryption Screen	2-53
2-91	Wireless Bridge User Management Screen	2-54
2-92	Wireless Bridge Enter Network Password Screen	2-54
2-93	Wireless Bridge User Management Screen	2-54
2-94	Wireless Bridge Web Server Setup Screen	2-55
2-95	Wireless Bridge Summary Status Screen	2-57

FIGURE NUMBER	NAME	PAGE
2-96	Wireless Bridge Setup Screen	2-57
2-97	Wireless Bridge Express Setup Screen	2-58
2-98	Wireless Bridge User Management Screen	2-58
2-99	Wireless Bridge Enter Network Password Screen	2-58
2-100	Wireless Bridge User Management Menu Screen	2-59
2-101	Wireless Bridge User Manager Setup Screen	2-59
2-102	Wireless Bridge Enter Network Password Menu	2-59
2-103	Wireless Bridge Radio Data Encryption Screen	2-60
2-104	Wireless Bridge Radio Hardware Screen	2-60
2-105	Wireless Bridge Radio Advanced Screen	2-61
2-106	Wireless Bridge Event Notifications Setup Screen	2-62
2-107	Wireless Bridge FTP Setup Screen	2-62
2-108	Wireless Bridge Configured Express Setup Screen	2-63
2-109	Wireless Bridge Default Express Setup Screen	2-63
2-110	Wireless Bridge Web Server Setup Screen	2-64
2-111	Inline Encryptor	2-65
2-112	Encryptor Security Alert - 1	2-68
2-113	Encryptor Security Alert - 2	2-68
2-114	Encryptor Enter Network Password	2-68
2-115	Encryptor User Access Screen	2-69
2-116	Encryptor LAN Settings Screen	2-69
2-117	Encryptor Security Settings Screen	2-70
2-118	CCM	2-75
2-119	Power Cable Connections	2-77
2-120	Multi-Client Radio Adapter Main Screen	2-79
2-121	Multi-Client Radio Adapter Radio Screen - 1	2-79
2-122	Multi-Client Radio Adapter Radio Screen - 2	2-79
2-123	Multi-Client Radio Adapter Privacy Screen	2-80
2-124	Multi-Client Radio Enter Key Number Screen	2-80
2-125	Multi-Client Radio Set WEP Key Screen	2-80
2-126	Multi-Client Radio Adapter Console Screen	2-80
2-127	Multi-Client Radio Adapter Password Screen	2-81
2-128	Multi-Client Radio Adapter CAISI Toolbox	2-82
2-129	Multi-Client Radio Adapter IPSU Main Screen – 1	2-83
2-130	Multi-Client Radio Adapter IPSU Main Screen – 2	2-83

FIGURE NUMBER	NAME	PAGE
2-131	Multi-Client Radio Adapter Configuration Error Prompt	2-83
2-132	Multi-Client Radio Adapter Device Does Not Answer Prompt	2-83
2-133	Multi-Client Radio Adapter Main Screen	2-84
2-134	Multi-Client Radio Adapter Radio Screen – 1	2-85
2-135	Multi-Client Radio Adapter Radio Screen – 2	2-85
2-136	Multi-Client Radio Adapter Privacy Screen	2-86
2-137	Multi-Client Radio Adapter Enter Key Number Screen	2-86
2-138	Multi-Client Radio Adapter Set WEP Key Screen	2-86
2-139	Multi-Client Radio Adapter Privacy Screen	2-86
2-140	Multi-Client Radio Adapter Ethernet Configuration Screen	2-86
2-141	Multi-Client Radio Adapter Filter Screen	2-87
2-142	Multi-Client Radio Adapter Logs Screen	2-87
2-143	Multi-Client Radio Adapter Console Screen	2-87
2-144	Multi-Client Radio Adapter Network Map	2-88
2-145	Multi-Client Radio Adapter Enter Network Password	2-89
2-146	Multi-Client Radio Adapter Identity Screen	2-89
2-147	LSA	2-91
2-148	LSA Connections	2-91
2-149	LSA CAISI Toolbox Menu	2-93
2-150	LSA EZWebCon Main Menu	2-93
2-151	LSA Assign IP Address to Server Screen	2-93
2-152	LSA Assign IP Address Status Screen – 1	2-94
2-153	LSA Assign IP Address Status Screen – 2	2-94
2-154	LSA EZWebCon Main Menu	2-94
2-155	LSA Browse Network Screen	2-95
2-156	LSA EZWebCon Main Menu	2-95
2-157	LSA EZWebCon Reload Firmware	2-95
2-158	LSA Reload Firmware Wizard Screen	2-96
2-159	LSA EZWebCon Begin Reload	2-96
2-160	LSA File Exists Screen	2-96
2-161	LSA PUC Folder – 1	2-97
2-162	LSA PUC Folder – 2	2-97
2-163	LSA PUC Folder – 3	2-98
2-164	LSA PCU Folder – 4	2-98
2-165	LSA Session Properties Screen	2-99

FIGURE NUMBER	NAME	PAGE
2-166	LSA C:\Net Tools\Lantronix\PUC Screen	2-99
2-167	LSA WS_FTP Highlighted Files	2-100
2-168	LSA WS_FTP Copied Files	2-100
2-169	LSA Download Config	2-101
2-170	LSA Send Which Configuration Screen	2-101
2-171	LSA Download IP Address Prompt	2-101
2-172	LSA Send Command File	2-102
2-173	LSA Send Command File Complete Prompt	2-102
2-174	LSA Telnet Command	2-103
2-175	LSA Login Password Prompt	2-103
2-176	LSA Username Prompt	2-103
2-177	LSA Local_2>Prompt	2-104
2-178	LSA Password Prompt	2-104
2-179	LSA Show Server Screen	2-106
2-180	LSA Show Server Boot Screen	2-106
2-181	LSA Show Ports Screen	2-107
2-182	LSA Password Prompt	2-107
3-1	CAISI Admin Main Menu Screen	3-1
3-2	CAISI Admin – Configuration Menu	3-2
3-3	CAISI Admin – View Menu	3-3
3-4	CAISI Admin – Device Menu	3-3
3-5	CAISI Admin – Settings Menu	3-4
3-6	CAISI Admin – Help Menu	3-4
3-7	CAISI Admin – Toolbar	3-5
3-8	CAISI Admin-Selecting Multiple Devices	3-5
3-9	CAISI Admin – Device List with Device Context Menu	3-6
3-10	CAISI Admin – Network View Mode	3-7
3-11	CAISI Admin – Device View Mode	3-8
3-12	CAISI Admin – Device Properties Model	3-8
3-13	CAISI Admin – Device Properties Tabs	3-9
3-14	CAISI Admin - Aironet Device Specific Properties Dialog Box	3-13
3-15	CAISI Admin - Linksys BEFSR41/81 Device Specific Properties Dialog Box	3-14
3-16	CAISI Admin - LSA MSS-100 Device Specific Properties Dialog Box	3-15

FIGURE NUMBER	NAME	PAGE
3-17	Creating A Device From A Device Template	3-16
3-18	Device Templates – Main Menu Option	3-17
3-19	Device Templates – Dialog Box	3-18
3-20	New Device Template Dialog Box	3-18
3-21	Template Properties - Dialog Box	3-19
3-22	Template Properties – Network Tab	3-20
3-23	Template Properties – Device Specific	3-22
3-24	Template Properties – Attributes (Aironet example)	3-23
3-25	New Attribute Dialog Box	3-23
3-26	Template Deletion Confirmation Dialog Box	3-24
3-27	Device Add – Main Menu Option	3-25
3-28	New Network Device Dialog Box	3-25
3-29	Device Wizard – Add Device	3-26
3-30	Device Wizard – Main Dialog Box	3-27
3-31	Device Wizard – Network Type Dialog Box	3-27
3-32	Device Wizard – Configuration Dialog Box	3-28
3-33	Device Wizard – Password Dialog Box	3-29
3-34	Device Wizard – Further Actions Dialog Box	3-30
3-35	Device Properties – Main Menu Option	3-31
3-36	Device Wizard – General Tab	3-32
3-37	Set Password Dialog Box	3-33
3-38	Device Wizard – Network Tab	3-35
3-39	Device Wizard – Details Tab	3-36
3-40	Device Wizard – Advanced Tab	3-37
3-41	Delete Confirmation Dialog Box	3-38
3-42	Router Ethernet Cable Connection	3-39
3-43	Router Link Lights	3-40
3-44	Router Add Option Menu	3-41
3-45	Router New Network Device Menu	3-41
3-46	Router Device Properties General Tab	3-42
3-47	Router Set Password Screen	3-42
3-48	Router Device Properties Network Tab	3-43
3-49	Router Unique IP Address Confirmation	3-43
3-50	Router Device Properties Advanced Tab	3-44
3-51	Router Device List Screen-Newly Created Device	3-44

FIGURE NUMBER	NAME	PAGE
3-52	Router Device Wizard Option Menu	3-45
3-53	Router Choose A Device to Create Screen	3-45
3-54	Router New Device Wizard Screen	3-45
3-55	Router New Device Wizard General Properties	3-46
3-56	Router Unique IP Address Confirmation	3-46
3-57	Router New Device Wizard Network Settings Screen - 1	3-47
3-58	Router New Device Wizard Network Settings Screen - 2	3-47
3-59	Router New Device Wizard Linksys Advanced Settings - 1	3-48
3-60	Router New Device Wizard Linksys Advanced Settings - 2	3-48
3-61	Router New Device Wizard Device Details Screen	3-49
3-62	Router New Device Wizard Password Validation Screen	3-49
3-63	Router CAISI Admin New Device Wizard Screen	3-50
3-64	Router Device List Screen-Newly Created Device	3-50
3-65	Router CAISI Admin Device List Screen	3-50
3-66	Router Configure Device Screen	3-51
3-67	Router Enter Password Screen	3-51
3-68	Router Configure Device Screen	3-52
3-69	Router Enter Network Password Screen	3-53
3-70	Router Configured Setup Screen	3-53
3-71	Router Factory Default Setup Screen	3-53
3-72	Router Configured DHCP Screen	3-54
3-73	Router Factory Default DHCP Screen	3-54
3-74	CBM	3-55
3-75	CBM Power Cable Connections	3-59
3-76	Wireless Bridge Add Option Menu	3-60
3-77	Wireless Bridge New Network Device Screen	3-61
3-78	Wireless Bridge Device Properties General Tab	3-62
3-79	Wireless Bridge Device Properties Network Tab	3-63
3-80	Wireless Bridge Device Properties Advanced Tab	3-64
3-81	Wireless Bridge Set WEP Key Screen	3-64
3-82	Wireless Bridge New Device Wizard General Properties Screen	3-65
3-83	Wireless Bridge New Device Wizard Network Settings	3-66
3-84	Wireless Bridge New Device Aironet 350 Advanced Settings	3-67
3-85	Wireless Bridge New Device Wizard Password Validation	3-67
3-86	Wireless Bridge CAISI Admin New Device Wizard	3-68

FIGURE NUMBER	NAME	PAGE
3-87	Wireless Bridge Configure Device Screen	3-68
3-88	Wireless Bridge CAISI Administration Prompt – 1	3-69
3-89	Wireless Bridge CAISI Administration Prompt - 2	3-69
3-90	Wireless Bridge Set To Factory Default Confirmation	3-69
3-91	Wireless Bridge Set User Name Screen	3-70
3-92	Wireless Bridge Device Configured Successfully Prompt	3-70
3-93	Wireless Bridge Configure Device Screen	3-71
3-94	Wireless Bridge Save Configuration Prompt	3-71
3-95	Wireless Bridge Configured Wireless Bridge Screen	3-72
3-96	Wireless Bridge Factory Default Configuration Screen	3-72
3-97	Inline Encryptor	3-73
3-98	Inline Encryptor Add Option Menu	3-74
3-99	Inline Encryptor New Network Device Screen	3-74
3-100	Inline Encryptor Device Properties General Tab	3-75
3-101	Inline Encryptor Device Properties Network Tab	3-76
3-102	Inline Encryptor Device Properties Details Tab	3-76
3-103	Inline Encryptor Device Properties Advanced Tab	3-77
3-104	Inline Encryptor Choose a Device to Create Screen	3-78
3-105	Inline Encryptor New Device Wizard	3-78
3-106	Inline Encryptor New Device Wizard General Properties	3-79
3-107	Inline Encryptor New Device Wizard Network Settings	3-79
3-108	Inline Encryptor New Device Wizard AirFortress 1100 Advanced Settings	3-80
3-109	Inline Encryptor New Device Wizard Device Details	3-80
3-110	Inline Encryptor New Device Wizard Password Validation	3-81
3-111	Inline Encryptor Configure Device Screen	3-82
3-112	Inline Encryptor Enter Network Password Screen	3-83
3-113	CCM	3-85
3-114	CCM Power Cable Connections	3-87
3-115	Multi-Client Radio Adapter Add Option Menu	3-89
3-116	Multi-Client Radio Adapter New Network Device Screen	3-89
3-117	Multi-Client Radio Adapter Set Administrative Password Screen	3-90
3-118	Multi-Client Radio Adapter Set Access Password Screen	3-90
3-119	Multi-Client Radio Adapter Device Properties Network Tab	3-91
3-120	Multi-Client Radio Adapter Device Properties Advanced Tab	3-92

FIGURE NUMBER	NAME	PAGE
3-121	Multi-Client Radio Adapter Set WEP Key Screen	3-92
3-122	Multi-Client Radio Adapter New Device Wizard General Properties	3-93
3-123	Multi-Client Radio Adapter New Device Wizard Device Network Settings	3-94
3-124	Multi-Client Radio Adapter New Device Aironet 340 Advanced Settings	3-95
3-125	Multi-Client Radio Adapter New Device Wizard Password Validation	3-95
3-126	Multi-Client Radio Adapter CAISI Admin New Device Wizard	3-96
3-127	Multi-Client Radio Adapter Configure Device Screen	3-97
3-128	Multi-Client Radio Adapter Save Configuration Prompt	3-98
3-129	Multi-Client Radio Adapter Enter Network Password Screen	3-98
3-130	Multi-Client Radio Adapter Network Map	3-99
3-131	View Audit Log – Main Menu Option	3-101
3-132	Audit Log Dialog Box	3-101
3-133	Configuration Save Menu Option	3-102
3-134	Configuration Save Toolbar Button	3-102
3-135	Configuration Backup Menu Option	3-103
3-136	Configuration Backup Dialog Box	3-103
3-137	Browse for Folder Dialog Box	3-104
3-138	New or Replace Backup Dialog Box	3-104
3-139	Backup Complete Prompt	3-105
3-140	Configuration Restore Menu Option	3-105
3-141	Configuration Restore Dialog Box	3-106
3-142	Configuration Restore Multiple Backups Dialog Box	3-106
3-143	Configuration Restore Confirmation Prompt	3-106
3-144	Restore Complete Dialog Box	3-107
3-145	Print Setup Menu Option	3-107
3-146	Print Setup Dialog Box	3-108
3-147	Configuration Print Main Menu Option	3-108
3-148	Print Dialog Box	3-109
3-149	Printer Output Sample	3-109
3-150	Printer Preview Menu Option	3-110
3-151	Print Preview Results	3-110
4-1	Troubleshooting CBM Power Cables	4-1

FIGURE NUMBER	NAME	PAGE
4-2	Troubleshooting CCM Power Cables	4-2
4-3	Troubleshooting Antenna Cables	4-3
4-4	Troubleshooting Ethernet Cables	4-3
4-5	Troubleshooting Coaxial Cables	4-3
4-6	Troubleshooting Power Cables	4-3
4-7	Troubleshooting Antenna & Cable Connectors	4-4
4-8	Troubleshooting Omni-Directional Antenna Radiation Pattern	4-4
4-9	Troubleshooting Omni-Directional Antenna Elevation Difference	4-5
4-10	Troubleshooting Panel Antenna Radiation Pattern	4-5
4-11	Troubleshooting Wireless Bridge Root Radio Hardware Screen	4-6
4-12	Troubleshooting CCM Radio Configuration Screen	4-7
4-13	Troubleshooting Wireless Bridge Root Radio Advanced Screen	4-8
4-14	Troubleshooting Wireless Bridge Express Setup Screen	4-9
4-15	Troubleshooting Root Radio Data Encryption Screen	4-10
4-16	Troubleshooting CCM Radio Set the Keys Screen	4-10
4-17	Troubleshooting CCM Radio Set Key # Screen	4-10
4-18	Troubleshooting CCM Radio Set Key Screen	4-11
4-19	Troubleshooting Example 5-4-3 Rule	4-12
4-20	Troubleshooting Cable Standards	4-13
4-21	Troubleshooting Hub Uplink Port	4-14
4-22	Troubleshooting SSR Notebook	4-15
4-23	Troubleshooting Wired NIC	4-18
4-24	Troubleshooting Xircom Advanced Tab	4-19
4-25	Troubleshooting SSR Notebook with Rabbit Ears Antenna	4-20
4-26	Troubleshooting Change Access ID Menu	4-22
4-27	Troubleshooting Air Fortress Client Utilities Menu	4-22
4-28	Troubleshooting Router	4-23
4-29	Troubleshooting Router LEDs	4-24
4-30	CAISI Reset Tool	4-24
4-31	Troubleshooting Router Setup Tab	4-26
4-32	Troubleshooting 10BaseT Transceiver	4-27
4-33	Troubleshooting CBM	4-28
4-34	Troubleshooting Wireless Bridge Ethernet Port	4-28
4-35	Troubleshooting Wireless Bridge LEDs	4-29
4-36	Troubleshooting Encryptor LEDs	4-29

FIGURE NUMBER	NAME	PAGE
4-37	Troubleshooting DSL Bridge LEDs	4-30
4-38	Troubleshooting Hub LEDs	4-30
4-39	Troubleshooting Hub BNC Light	4-31
4-40	Troubleshooting Omni-Directional Antenna	4-37
4-41	Troubleshooting Directional Antenna	4-37
4-42	Troubleshooting MMCX to N (Female) Cable	4-38
4-43	Troubleshooting Right Angle Adapter	4-38
4-44	Troubleshooting LSM Results Known Good Antenna	4-39
4-45	Troubleshooting LSM Results Suspected Bad Antenna	4-39
4-46	Troubleshooting MMCX to RPTNC Cable	4-40
4-47	Troubleshooting 12" RF Antenna Cable	4-40
4-48	Troubleshooting DSL Bridge Speed Setting	4-41
4-49	Troubleshooting Field Wire Connection	4-41
4-50	Troubleshooting CBM UPS	4-42
4-51	Troubleshooting CCM	4-43
4-52	Troubleshooting Multi-Client Radio Adapter Ethernet Port	4-44
4-53	Troubleshooting Multi-Client Radio Adapter LEDs	4-44
4-54	Troubleshooting Hub LEDs	4-45
4-55	Troubleshooting CCM Radio Configuration Screen	4-47
4-56	Troubleshooting Erected CCM Antenna	4-50
4-57	Troubleshooting MMCX to N (Female) Cable	4-50
4-58	Troubleshooting Right Angle Adapter	4-50
4-59	Troubleshooting LSM Results Known Good Antenna	4-51
4-60	Troubleshooting LSM Results Suspected Bad Antenna	4-51
4-61	Troubleshooting CCM Lightning Arrestor and RF Antenna Cable	4-51
4-62	Troubleshooting MMCX to RPTNC Cable	4-52
4-63	Troubleshooting 12" RF Antenna Cable	4-52
4-64	Troubleshooting Physical Connection of LSA	4-53
A-1	BLAST Configuration Menu	A-1
A-2	BLAST Defaults	A-1
A-3	HyperTerm - Select Properties Menu	A-2
A-4	HyperTerm – Properties Screen	A-2
A-5	HyperTerm - Port Settings Screen	A-3
A-6	HyperTerm - Settings Tab Screen	A-3

FIGURE NUMBER	NAME	PAGE
A-7	Telnet – Main Screen	A-5
A-8	Telnet – Terminal Preferences Screen	A-5
A-9	Internet Explorer Configuration Options	A-6
A-10	Client Encryption Manager (CEM) - Login Screen	A-7
A-11	WEP Key Screen	A-8
A-12	Setting the WEP Key	A-8
A-13	Aironet Client Utility (ACU) – Main Screen	A-9
A-14	ACU – System Parameters Screen	A-9
A-15	ACU – RF Network Tab	A-10
A-16	ACU – Advanced (Infrastructure) Tab	A-10
A-17	ACU – Network Security Tab	A-11
A-18	Link Status Meter (LSM)	A-12
A-19	Sample WS-Watch Screen	A-13
A-20	WS-Watch Icons	A-13
A-21	WS-Watch - Icon Configuration Screen	A-14
A-22	TJPing – Ping Screen	A-15
A-23	TJPing - Lookup Screen	A-16
A-24	TJPing - Trace Screen	A-16
A-25	TJPing – Set Options Screen	A-17
A-26	IP Address Assistant	A-17
A-27	IP Subnet Calculator	A-17
A-28	WS_FTP - Session Profile Screen	A-18
A-29	WS_FTP - File Transfer Screen	A-18
A-30	WS_FTP – Program Options Screen	A-19
A-31	Show IP Configuration Screen	A-19

LIST OF TABLES

TABLE NUMBER	NAME	PAGE
1-1	CAISI Licensed COTS Software List	1-3
1-2	CAISI Free COTS Software List	1-3
1-3	CAISI Included COTS Software List	1-4
1-4	CAISI Nomenclature Cross Reference List	1-6
1-5	CAISI Supported Components	1-11
3-1	General Device Properties	3-10
3-2	Network Device Properties	3-11
3-3	Details Device Properties	3-12
3-4	Aironet Specific Advanced Properties	3-13
3-5	Linksys Specific Advanced Properties	3-14
3-6	LSA MSS-100 Specific Advanced Properties	3-15
3-7	Template Properties	3-19
3-8	Network Types	3-28
3-9	General Properties – Miscellaneous	3-34
3-10	Audit Logging Preferences	3-100
3-11	Print Range Options	3-109

Chapter 1

INTRODUCTION

Section I. General Information

1.1 SCOPE

The Combat Service Support (CSS) Automated Information Systems Interface (CAISI) Technical Bulletin (TB 11-5895-1691-10) serves as a software user manual (SUM) for CAISI Network Managers, System Support Representatives (SSR), CSS Automation Management Office (CSSAMO) and Signal Staff (S-6) organizations.

The TB identifies management and administrative-related software tools and utilities used for the manual and automated configuration of CAISI module components.

It also encompasses detail procedures for configuring and troubleshooting CAISI components utilizing the device native applications as well as a government developed automated software configuration tool - CAISI Administration Software Application (CAISI Admin).

NOTE: *Description of hardware, installation procedures, operation and physical connections are described in detail in the CAISI Technical Manual (TM 11-5895-1691-12).*

1.2 DOCUMENT OVERVIEW

This SUM is organized in the following manner:

CHAPTER 1

Introduction - an overview of the SUM and CAISI system to include a list of the software tools and utilities that are supplied with CAISI. Also, the introduction includes an abridged description of the CAISI modules, their components and capabilities.

CHAPTER 2

Manual Configuration - Procedures for the manual process for configuring the CAISI modules.

CHAPTER 3

CAISI Admin - Procedures for the automated process for configuring the CAISI Modules.

CHAPTER 4

Diagnostics and Troubleshooting - an overview and descriptions of software tools used in both diagnostics and troubleshooting procedures. It also describes actions that are taken in order to correct the types of problems/situations that occur during normal use of CAISI.

APPENDIX A:

Manual Tools and System Utilities - Description of all applications used to configure and troubleshoot components.

APPENDIX B:

Glossary/Abbreviations and Acronyms - Provides a definition of key terms and a listing of abbreviations and acronyms used in this document.

APPENDIX C:

Quick Configuration Guide – contains the processes and steps of CAISI Admin to configure the CAISI.

INDEX:

Contains references to section paragraphs.

1.3 SOFTWARE INVENTORY

Each CAISI module consists of multiple commercial off the shelf (COTS) network devices from various vendors, each of which is supported by it's own configuration interface. Some of the devices use a web-based interface, others use a command line, and some devices use a combination of both.

CAISI Admin, utilities and tools will be supplied pre-loaded on the SSR notebook computer and will be further addressed in this manual. In addition to a standard Windows 2000 installation, Tables 1-1, 1-2, and 1-3 list the software issued on the notebook. These include utilities and tools that are also provided pre-installed on the CAISI SSR notebook.

Table 1-1 CAISI Licensed COTS Software List

Software	Purpose
WS_Watch	Allows users to monitor the network connectivity in a graphical mode, displaying network nodes and hosts (NES, gateways, routers, CAISI hubs, TCP/IP hosts, etc.) as icons. Node icons will change color to represent loss of connectivity and allow users to troubleshoot specific lines or systems on the network.
BLAST	Allows serial connections to the CAISI, similar to the way the non-network capable STAMIS devices connect to CAISI.
TJPing	Provides a graphical user interface for standard ping functionality.
IP Addr. Asst.	Subnet calculator and analyzer.
Norton Anti-Virus	Anti-virus protection (DoD site license – free for use within DoD).

Table 1-2 CAISI Free COTS Software List

Software	Purpose
Acrobat Reader	Portable data format (*.pdf) file viewer. Free from Adobe Systems, Inc.
Microsoft Office Viewers	Viewers for Microsoft Word, Excel, PowerPoint, and Access will allow users to view, but not edit, data files from the listed Microsoft Office programs. Free from Microsoft, Inc.
WS_FTP	Graphical user interface for a standard FTP client program. Free for Government use, from Ipswitch, Inc.

Table 1-3 CAISI Included COTS Software List

Software	Purpose
Internet Explorer (Windows component)	Allows SSR users to connect to the CAISI components to remotely perform system administration tasks.
Telnet client (Windows component)	Allows SSR users to connect to the CAISI components to remotely perform system administration tasks.
Hyperterm (Windows component)	Allows SSR users to connect to the console ports of CAISI components for configuration. Component of Internet Information Server (IIS) and all versions of Windows 2000.
FTP server (Windows component)	File Transfer Protocol server, allows users to transfer files to and from the SSR notebook. Component of IIS server and all versions of Windows 2000.
TFTP server	Trivial File Transfer Protocol server, allows the SSR to load new firmware images onto the Lantronix LSA devices.
Xircom NetPort card drivers	Driver for the PCMCIA adapter.
Cisco Aironet wireless card drivers and utilities	Drivers and utilities to configure and monitor the Cisco Aironet wireless Network Interface Card (NIC) and bridges and to monitor segments of the wireless network.
Air Fortress Remote Encryption Client	Drivers and utilities to configure the Air Fortress remote client and to check encryption status and statistics.
Lantronix LSA drivers and utilities	Drivers and utilities to configure and monitor the Lantronix MSS-100 and MSS-VIA serial servers.

NOTE: *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.*

1.3.1 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:

Public domain, shareware, or other privately acquired software is prohibited from being used on CAISI.

Hardware and Software modifications will be made only as authorized by the Assistant Project Manager (APM), CAISI.

Only personnel performing official duties will be allowed access to CAISI.

CAISI will be used in accordance with (IAW) documented procedures as described in TM 11-5895-1691-12 Appendix F paragraph 2.11. Undocumented usage of CAISI must be reported to the appropriate authority whose responsibility is to properly evaluate the situation and determine if it caused any additional risk to CAISI.

1.3.2 Software Developer/Maintainers and Support Engineers

This category consists of one or more individuals employed in the Post-Deployment Software Support (PDSS), or individuals acting on behalf of APM, CAISI, during production, testing, fielding, and upgrading of CAISI. These users may access CAISI either locally or remotely. Software maintainers are responsible for repairing, modifying and enhancing the system software.

For CAISI software related problems contact the Customer Assistance Office (CAO) at Fort Lee, VA. Phone numbers, fax numbers and email address are:

DSN – 687-1051
Commercial – (804) 734-1051
Fax – (804) 734-2947 / DSN 687-2947
Email - cao@lee-dns2.army.mil

NOTE: *While this manual does discuss and describe certain device-specific parameters exposed within the application, it is not intended to replace COTS device detailed documentation. Details concerning certain specific COTS device configuration parameters and appropriate settings should also be obtained from the device vendor documentation.*

Section II Equipment Description and Data

1.4 CAISI EQUIPMENT

CAISI consists of the following modules: CAISI Bridge Module (CBM), CAISI Client Module (CCM), Legacy Support Adapter (LSA) and the System Support Representative (SSR) Accessory Kit.

A CAISI system is comprised of various combinations of CBMs, CCMs, LSAs and SSR Accessory Kits to accommodate different unit needs. Depending on the size and mission of the unit, some units 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).

Table 1-4 CAISI Nomenclature Cross Reference List

Common Name	Official Name	Part #	NSN
CAISI Bridge Module (CBM)	Processor, Communications Gateway OL-701/TYQ	A3269821	5820-01-487-4020 Z53098
CAISI Client Module (CCM)	Processor, Bridge OL-700/TYQ	A3269822	5820-01-487-4023 Z53056
Legacy Support Adapter (LSA)	Interface Unit, ADP	MSS100-01	7025-01-487-4021
SSR Accessory Kit	Electronics Equipment MK-2975/TYQ	A3269820	5999-01-487-2681 Z00057

1.4.1 CAISI Bridge Module (CBM)

At least two CBMs are fielded with each CAISI. Each provides connectivity for Standard Army Management Information Systems (STAMIS) users and serves as “relays” for other CBMs and CCMs in the network, passing data through the radios to the final (STAMIS) destination in the network.

The CBM is comprised of a Wireless Bridge, an Encryptor, a DSL Bridge, and a pair of 9-port Ethernet Hubs.

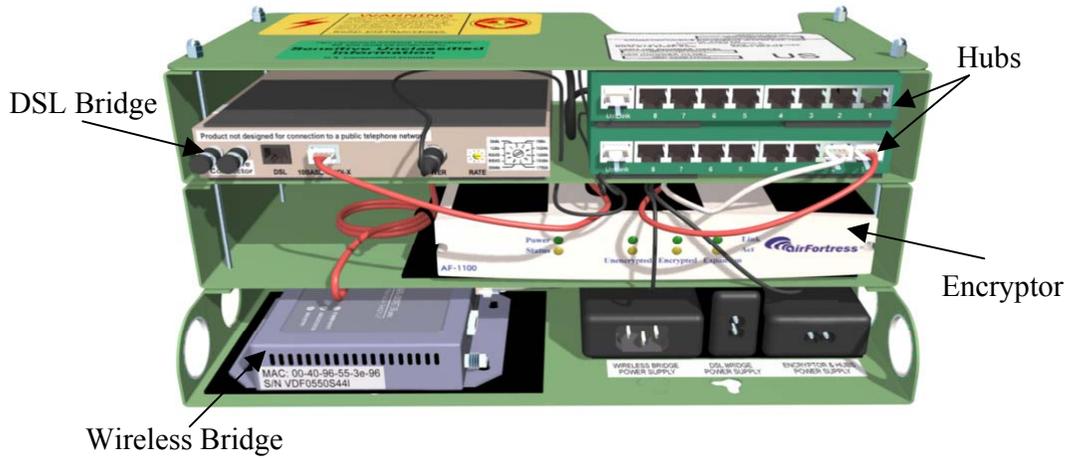


Figure 1-1 CBM Front View

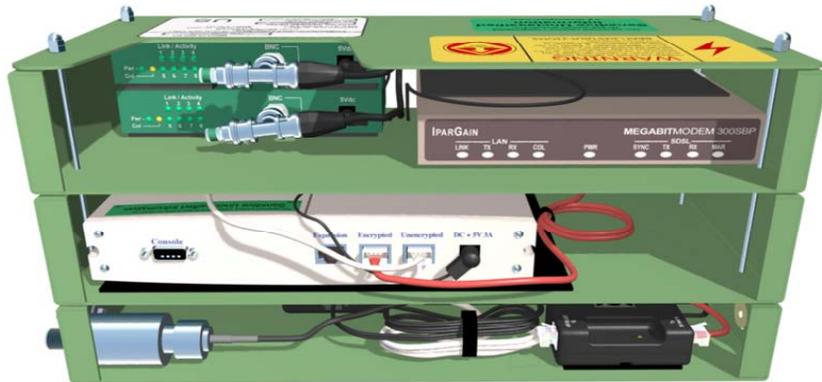


Figure 1-2 CBM Back View

1.4.2 CAISI Client Module (CCM)

The CCM acts as a client or a distant-end access point for transference of information. It does not relay information, it just accepts data. The CCM is comprised of the following: a multi-client radio adapter, inline encryptor and hub. The radio adapter is similar to the wireless bridge in the CBM, but its capabilities are much more limited. It allows you to only connect eight computers or network devices to it. Remote radios cannot connect to it. Nor can it act as a radio relay.

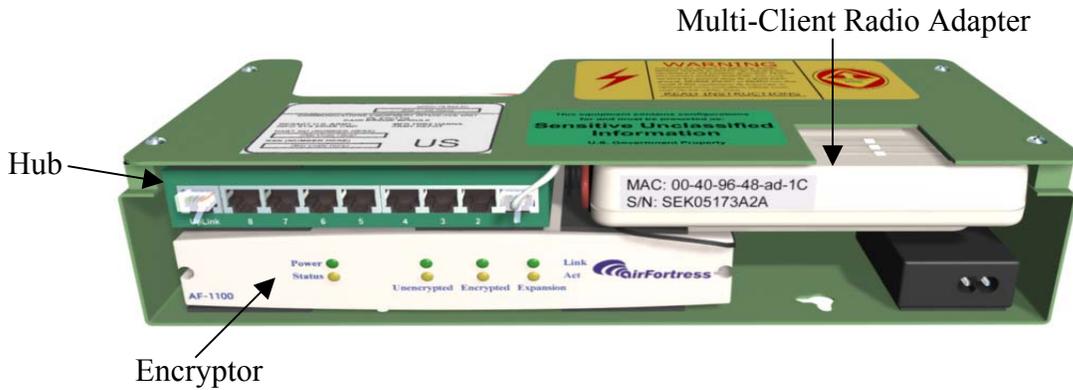


Figure 1-3 CCM Front View

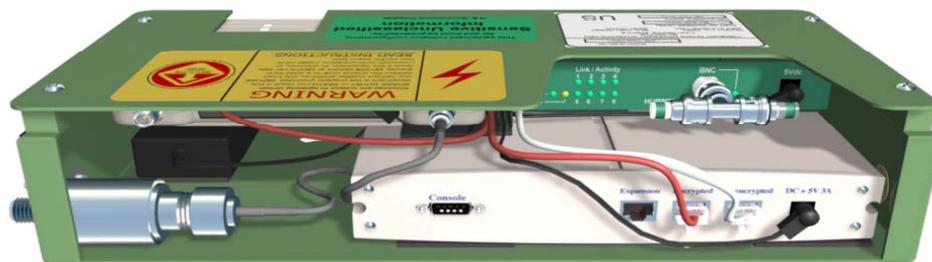


Figure 1-4 CCM Back View

1.4.3 Legacy Support Adaptor (LSA)

Some STAMIS devices are not transmission control protocol/internet protocol (TCP/IP) compliant or do not contain a Network Interface Card (NIC), therefore a LSA is needed. 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.



Figure 1-5 LSA

1.4.4 System Support Representative (SSR) Accessory Kit

The SSR Accessory Kit contains equipment primarily required for module component configuration. This equipment includes duplicate items from the CBM/CCM and unique components for use in special circumstances. It will be issued to the CSS 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
- one AB-1244B antenna mast carrying case.



Figure 1-6 SSR Accessory Kit

1.5 CAISI CONFIGURATION OVERVIEW

The SSR notebook is used for configuring, troubleshooting and monitoring CAISI components inside the CBM, CCM, and SSR Accessory Kit. This TB focuses on configuring the modules as a whole, rather than individual devices. There are two methods of configuring these modules (you can use either method):

- Manual Configuration discussed in Chapter 2.
- Automated Configuration using CAISI Admin discussed in Chapter 3.

NOTE: *The SSR notebook must be configured first manually. You may choose manual or CAISI Admin to configure the remaining components.*

Each component has unique configuration tools.

1. The Wireless Bridges are configured utilizing the SSR notebook with the CAISI Admin application or manually via tools, utilities and web pages. You must initially configure them thru the console port in order to assign an IP address before you can connect to them over the network.
2. The Multi-client radio adapters are configured via web pages only. They do not have console ports.
3. The Encryptors are configured from the console port or via secure web pages (https).
4. The notebook NIC cards (Wireless/Wired) and the encryptor software clients are both configured from utilities installed on the PC.

NOTE: *Some notebooks have a built-in NIC. In this case, the Wired NIC will not be issued.*

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 the web browser.

1.5.1 CAISI Supported Components

Device support for CAISI Admin is dependent upon the available device drivers for the application. The current release of the software includes driver support for the following hardware:

Table 1-5 CAISI Supported Components

Device Description	Firmware Version	Common Name
Cisco Aironet Wireless Bridge 340	8.65	
Cisco Aironet Client Radio Adapter 350	8.65	
Cisco Aironet Wireless Bridge 350	12.01T	
Linksys Router BEFSR41 / BEFSR81	1.40 / 2.40.2	
AirFortress™ Wireless Security Gateway (AF-1100 Inline Encryptor)	11.78W	
Lantronix MSS-100	3.6.4	

For an exact list of supported firmware versions for each device, please consult the release notes. Changes in firmware version from the supported versions above and in the release notes may result in the software being unable to configure the device. If that happens, modifications to the software and/or drivers may be required.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 2

MANUAL CONFIGURATION

Section I. Notebook Configuration

2.1 SSR NOTEBOOK

The SSR notebook is used for configuration of CAISI components and monitoring of the network. The SSR notebook is loaded with the current CAISI software baseline and is preset to the CAISI standard configuration when issued by Tobyhanna Army Depot (TYAD).

The SSR will only need to configure the notebook name, wired NIC, wireless NIC, Service Set Identification (SSID), and wired equivalent privacy (WEP) key for their unit.

The SSR notebook is issued with the software baseline that includes the operating system (Microsoft Windows 2000), utilities, drivers, CAISI Administration Software Application (CAISI Admin) software and both wired/built-in and wireless NICs.

The Wired NIC or Built-in NIC allows you to physically connect to the network for initial configuration, troubleshooting network problems and configuration of CAISI components. You may also use the wired NIC or Built-in NIC anytime wireless radio operations are limited for any reason.

NOTE: *Difference between wired NIC and built-in NIC is wired NIC is an external device issued with certain models of notebooks. Built-in NIC is actually a part of the notebook itself.*

The Wireless NIC allows you to connect to the wireless portion of the network. It may be used for monitoring and troubleshooting and for routine operations from the immediate vicinity of a CBM.



Wired NIC



Wireless NIC

Figure 2-1 Wired NIC and Wireless NIC



Figure 2-2 SSR Notebook

The current notebook model can change without notice. The notebooks could, theoretically, also require complementary metal oxide semiconductor (CMOS) updates, but as of this writing, there is neither a firmware load required nor is there procedures identified. Procedures for upgrading the firmware (CMOS) will be developed and circulated along with the required firmware, if the need arises.

2.1.1 SSR Notebook Security

You may personalize the notebook 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, that your software and personalization will be lost if you ever have to reload the system from disk.

Security concerns for the SSR notebook are in TM 11-5895-1691-12, Appendix F, paragraph 2.11. These include the topics of user identification (userids), passwords, screen savers and virus protection.

2.2 SSR NOTEBOOK SETUP

The SSR notebook must be configured to support a unit’s specific needs. The SSR will need to know how to do the following:

- | | |
|---|---------------|
| 1. Check the BIOS (Basic Input/Output System) | Paragraph 2.3 |
| 2. Reload software | Paragraph 2.4 |
| 3. Create and maintain user accounts | Paragraph 2.5 |
| 4. Configure network parameters | Paragraph 2.6 |
| 5. Configure the wired NIC/built-in NIC | Paragraph 2.7 |
| 6. Configure the wireless NIC | Paragraph 2.8 |
| 7. Configure AirFortress Remote Client | Paragraph 2.9 |

2.3 CONFIGURING SSR NOTEBOOK BASIC INPUT/OUTPUT SYSTEM (BIOS)

The BIOS settings tell the computer how to use its resources. The BIOS settings are also sometimes called the CMOS (Complementary Metal Oxide Semiconductor) setup, because the settings are saved in the CMOS.

The SSR notebook setup for BIOS settings will depend on the brand and model of computer issued to the SSR. Verify the brand and model of the SSR notebook to identify which of the following procedures need be performed.

2.3.1 Mitac 7020 BIOS Settings.

NOTE: Make sure that the battery on the notebook has been charged for 24 hours before turning it on. Charging should have been accomplished during the pre-assembly process. If you are not sure, connect power to the notebook and leave it for 24 hours before turning it on.

1. Ensure nothing is plugged into the PCMCIA (Personal Computer Memory Card International Association) slots.
2. Remove the notebook, the notebook power supply and a 2-prong power cord from the SSR Notebook Case.
3. Connect the power supply to the notebook.
4. Connect the female end of the 2-prong power cord to the power supply and plug the other end of the 2-prong power cord into an external power source.
5. Apply power to the external power source and the notebook.
6. Press the <F2> key when you see the message “Press the F2 key to enter setup.”

NOTE: The below procedures assume that the notebook is at the factory default settings. If not, click on “Exit”, click on “Get Default values” and click on the “OK” button at the confirmation screen. Wait for the system to reboot and apply step 6 above, and resume configuration procedures.

7. Set Date and Time.
 - a. Click on “Main”. The Main menu will appear, with “Date and Time” highlighted.
 - b. Click on “Date and Time” or press <Enter> with it highlighted. The “Date and Time” menu will appear.

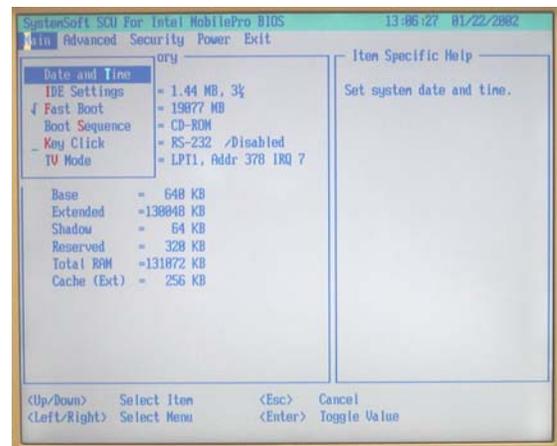


Figure 2-3 7020 BIOS Main Menu

- c. Enter the current date and time using Greenwich Mean Time (GMT).
 - d. Click on the “OK” button.

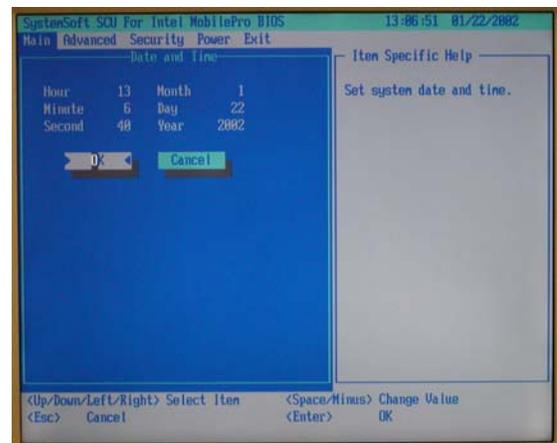


Figure 2-4 7020 Date & Time Menu

8. Set Boot Sequence.

- a. Click on “**Main**”.
- b. Click on “**Boot Sequence**” or scroll down to “Boot Sequence” and press the <Enter> key. The “Boot Sequence” menu will appear.

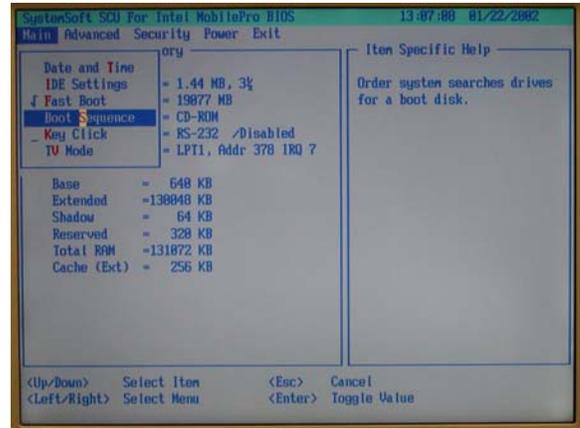


Figure 2-5 7020 BIOS Main Menu

- c. Set the “Boot Sequence” to “**CD-ROM Drive**”, “**Diskette A**” and then “**Hard Disk C**”.
- d. Click on the “**OK**” button.

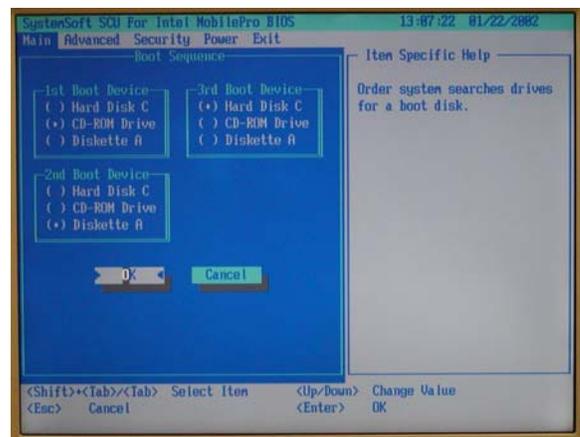


Figure 2-6 7020 BIOS Boot Sequence Menu

9. Set COM Port.

- a. Click on “**Advanced**”.
- b. Ensure “COM Port” is highlighted; press the <Enter> key.

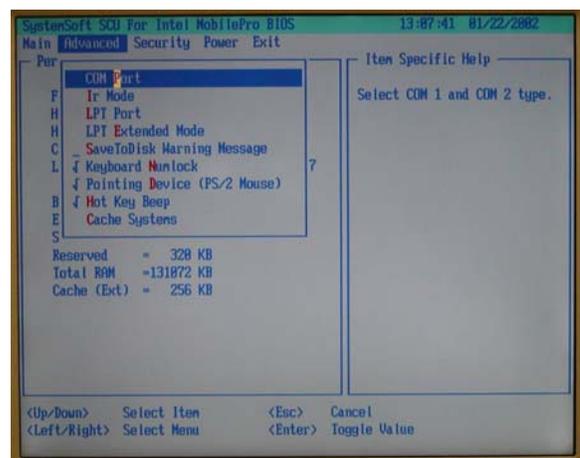


Figure 2-7 7020 BIOS Advanced Menu

- c. Set “COM1/COM2” to “**RS-232/Disabled**”, where (COM1 is enabled as an RS-232 port and COM2 is disabled).
- d. Click on the “**OK**” button.



Figure 2-8 7020 BIOS COM Port Menu

10. Set the Parallel Port.

- a. Click on “**Advanced**”.
- b. Click on “**LPT Extended Mode**” or scroll down to “LPT Extended Mode” and press the <Enter> key.

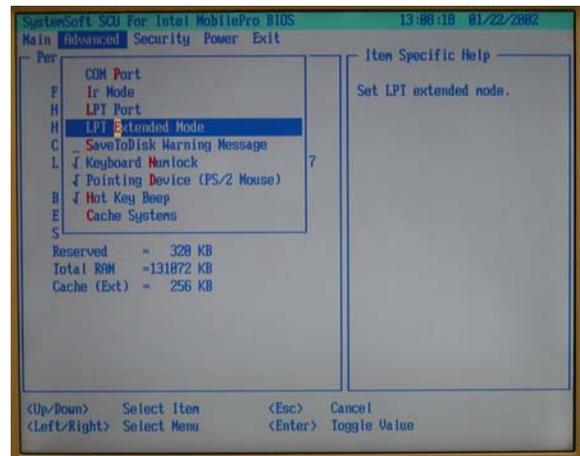


Figure 2-9 7020 BIOS Advanced Menu

- c. Set the “LPT Extended Mode” to “**ECP**”.
- d. Click on the “**OK**” button.

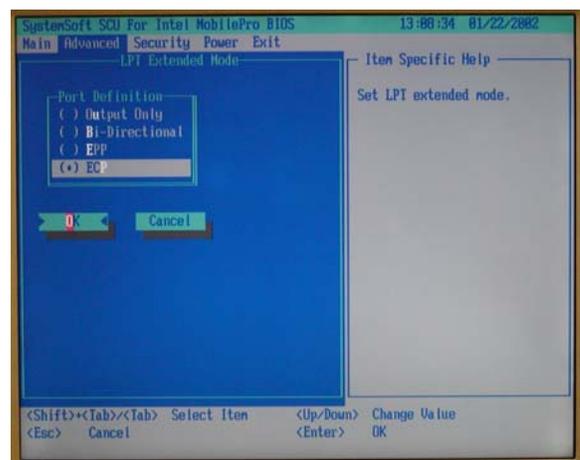


Figure 2-10 7020 BIOS LPT Extended Mode Menu

11. Set the “Customize” power options.
 - a. Click on “**Power**”.
 - b. Click on “**Customize**” or scroll down to “Customize” and press the <Enter> key.

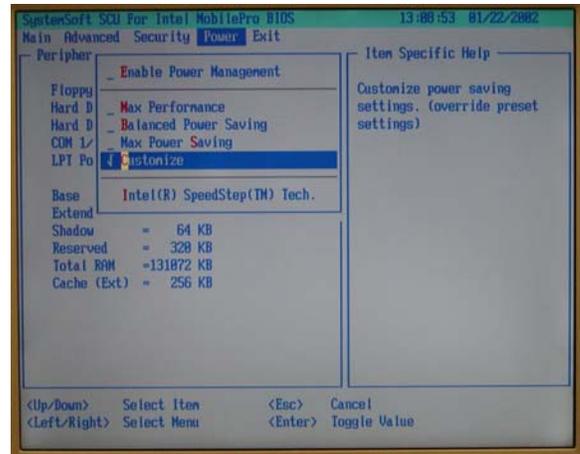


Figure 2-11 7020 BIOS Power Menu

- c. Set “Hard Disk Power Down After” to “**10 min**”.
- d. Set “Suspend Data to” to “**RAM**”.
- e. Set “Cover Close” to “**Video Off**”.
- f. Leave all other settings set to defaults.
- g. Click on the “**OK**” button.

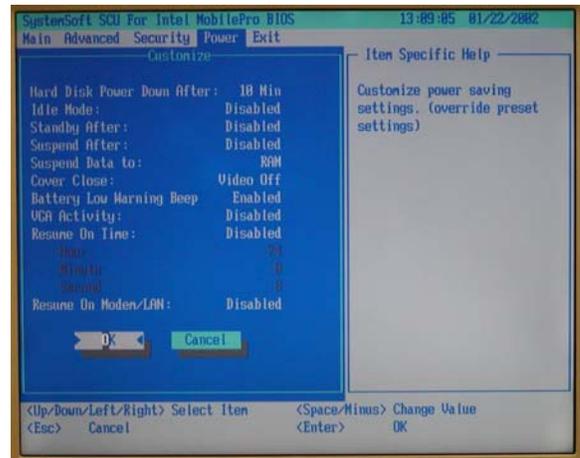


Figure 2-12 7020 BIOS Customize Menu

12. Click on “**Exit**”.
13. Ensure “**Save Changes and Exit**” is highlighted; press the <Enter> key.
14. The Notebook BIOS settings are now properly configured for operation. To reboot the notebook, click on the “**OK**” button.

2.3.2 Mitac 7521T BIOS Settings.

1. Ensure nothing is plugged into the PCMCIA (Personal Computer Memory Card International Association) slots.
2. Remove the notebook, the notebook power supply and a 2-prong power cord from the SSR Notebook Case.
3. Connect the power supply to the notebook.
4. Connect the female end of the 2-prong power cord to the power supply and plug the other end of the 2-prong power cord into an external power source.
5. Apply power to the external power source and the notebook.
6. Press the <F2> key when you see the message “Press the F2 key to enter setup.”

NOTE: The below procedures assume that the notebook is at the factory default settings. If not, you need to set it to factory default before beginning the configuration. If it is not a factory default, select “Exit” on the top menu bar by using the keyboard arrow keys. Select “Load Setup Defaults” and select “Yes” on the confirmation screen.

7. Set Date and Time.
 - a. Select “Main” from the top menu bar by using the keyboard arrow keys.
 - b. The Main menu will appear with “System Time” highlighted. If the text is not highlighted use your up ↑ and down ↓ arrow keys.
 - c. Once “System Time” is highlighted enter the current time using Greenwich Mean Time (GMT).
 - d. Press the down arrow key to select the “System Date” field and enter the current date.

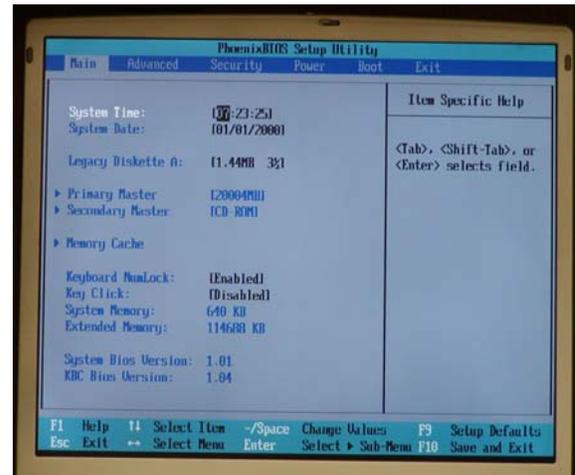


Figure 2-13 7521T BIOS Main Menu

8. Set I/O Device Configuration.
 - a. Select “Advanced” from the top menu bar by using the keyboard arrow keys.
 - b. Press the down ↓ arrow key to select “I/O Device Configuration”. Once the selection is highlighted press the <Enter> key.

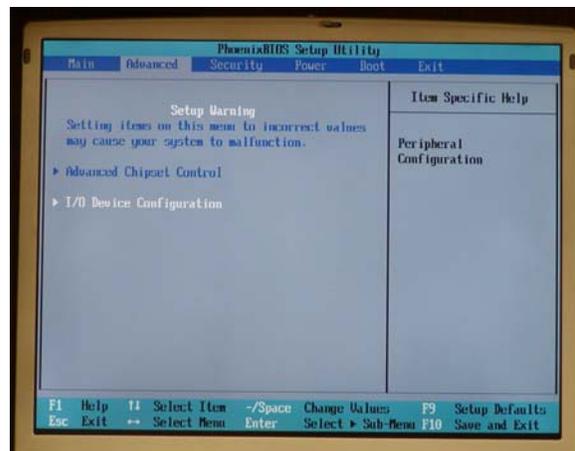


Figure 2-14 7521T BIOS Advanced Menu

- c. Arrow down to “**Parallel port: Mode:**”
- d. Press the spacebar or minus key to change the value to “**ECP**”.
- e. Press the “**ESC**” (escape) key to return to the “**Advanced**” Menu.

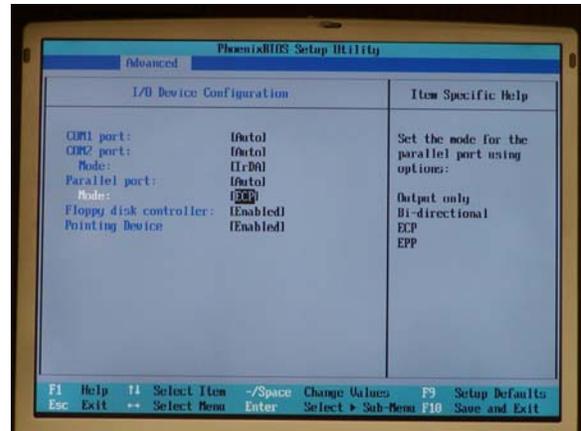


Figure 2-15 7521T BIOS I/O Device Configuration Menu

- 9. Set the Power Options.
 - a. Select “**Power**” from the top menu bar by using the keyboard arrow keys.
 - b. Arrow down to “**Hard Disk Timeout**”.
 - c. Press the spacebar or minus key to change the value to “**10 minutes**”.
 - d. Arrow down to “**Video Timeout**”.
 - e. Press the spacebar or minus key to change the value to “**10 minutes**”.

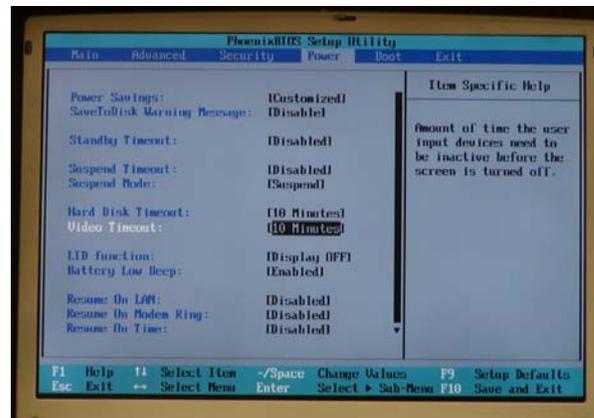


Figure 2-16 7521T BIOS Power Menu

- 10. Set the Boot Sequence.
 - a. Select “**Boot**” from the top menu bar by using the keyboard arrow keys.
 - b. Highlight the value and then use the spacebar and minus keys to arrange the values in the following sequence:
 - 1) “**CD-ROM Drive**” first.
 - 2) “**Diskette Drive**” second.
 - 3) “**Hard Drive**” third.

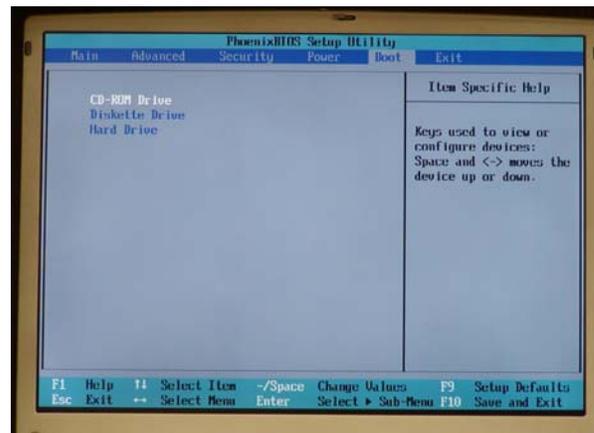


Figure 2-17 7521T BIOS Boot Menu

- 11. Select “**Exit**” from the top menu bar by using the keyboard arrow keys.
- 12. Press the “**F10**” key to exit saving changes.
- 13. When the confirmation screen appears, select “**Yes**”. If it is already highlighted, just press the <Enter> key.
- 14. The Notebook BIOS settings are now properly configured for operation. The notebook will automatically reboot.

2.4 RELOAD SOFTWARE

The notebook's software includes the operating system, utilities, drivers and application software. The SSR will be issued the notebook with the software baseline loaded. However, the SSR will need to reload the software baseline when one of the following happens:

- An un-repairable system error.
- Configuration is so scrambled that you cannot set it back.
- Loss of administrative password.

If you can still access your data, back it up before reloading. Because when you reload, you will lose everything you have done since you received it or last reloaded the baseline.

Procedures to reload software baseline:

1. Ensure notebook computer is powered on.
2. Insert installation CD #1 into the CD disk drive.
3. Shutdown notebook computer.

NOTE: *CD will not load by selecting "Run" from the start menu or by selecting the CD drive from Windows Explorer. You must shutdown the notebook computer and perform the following procedures to load the CD.*

4. Turn the notebook power on. The computer will reboot.
5. At the "Startup" menu, select "**Option 1-Load CAISI Image to Hard Drive**" and press the <Enter> key.
6. When prompted, "insert next media", remove CD #1 and replace it with CD #2.
7. Wait 15 seconds for the disk to spin up and press the <Enter> key. The load will resume.
8. When CD #2 install is complete, the installation screen will clear and a message will inform you that the load is complete.
9. Remove CD #2 and close drive.
10. Reboot the CAISI notebook. Press **Ctrl-Alt-Delete**.
11. Enter username and password, the CAISI defaults are **caisiadmin** and **BS_69dlw**.
12. A message will inform you that Windows has finished installing new device, it will prompt you to restart the computer, Click on "**Yes**".
13. Press **Ctrl-Alt-Delete**. Enter username and password, the CAISI defaults are **caisiadmin** and **BS_69dlw**.
14. A Logon Message prompt will appear, "Your password expires today. Do you want to change it now?" For classroom training, click "**No**".

2.5 CREATE AND MAINTAIN USER ACCOUNTS

The SSR is responsible for creating and maintaining user accounts on the SSR notebook. Each user whether an operator or administrator are required to have their own account on the notebook they use to discharge their duty. General accounts used by many users are prohibited. Identical usernames/passwords can be established on different SSR notebooks that users may need to work on.

NOTE: *It is a security requirement to have separate administrator accounts so the commander can trace who did what to the network. If multiple individuals share one administrator account, then this accountability cannot be enforced.*

The SSR notebook will come initially (or after a software reload) with two usable accounts. An account gives the user access to the network. The type of privilege assigned to it however, determines the type of access. The Administrator account has administrative privileges, which allows it to create and maintain other accounts. But one can grant administrator privilege to other types of accounts as well, such as “Power User”. There are two types of privileges on the SSR notebook:

1. Power User.
 - a. This account is designed to help the SSR reduce the threat of administrative password compromise and unauthorized entries.
 - b. The CAISI default username is “**caisioper**”.
 - c. The CAISI default password is “**K52+vbks**”.

2. Administrator.
 - a. This account is for the SSR to perform administrative functions only. The SSR should log out after completing tasks.
 - b. The CAISI default username is “**caisiadmin**”.
 - c. The CAISI default password is “**BS_69dlw**”.

Both of these default accounts have passwords set to expire when a user initially logons. Users logging on will be told the password is expired and given the chance to enter a new password.

1. Passwords are set to expire in 180 days. Users must change passwords IAW AR 380-19.
2. Passwords must be at least eight characters long and should contain at a minimum three of the following four character types:
 - a. uppercase letters (A .. Z)
 - b. lowercase letters (a .. z)
 - c. numbers (0 .. 9)
 - d. special characters
3. Passwords cannot contain any part of the username, for instance “caisi” or “oper”.
4. Users should select passwords that they can remember, but that are not too obvious.

5. When changing a password, you need to enter it twice. After which you should get a pop-up box telling you that the password has been changed. If you get an indication that the passwords don't match or have a problem, reenter them or select another one.
6. Once the password is successfully changed, immediately log out and log back in to ensure the system has the correct password.

NOTE: *If you cannot log back in, or if you ever lose the administrator password(s), you will need to perform software reload on the laptop from scratch. Seal the passwords in envelopes and turn them in to your security officer for safekeeping.*

To initially set your password for the default standard Power User account:

NOTE: *The password is case-sensitive but the username is not case-sensitive. Since password is case-sensitive, make sure that the <Caps Lock> and <Num Lock> are off.*

1. Log on as the default standard user.
2. Enter the username of “**caisioper**”.
3. Enter the password of “**K52+vbks**” and press the “**OK**” button.
4. A logon message will appear, “You are required to change your password at first logon”. Click on the “**OK**” button.
5. The Change Password screen will appear, enter your new password in the “New Password” field. Confirm your new password by re-entering it in the “Confirm New Password” field.
6. Press the “**OK**” button.

To initially set your password for the default Administrator account:

1. Log on as the default standard user.
2. Enter the username of “**caisiadmin**”.
3. Enter the password of “**BS_69dlw**”.
4. A logon message will appear, “Your password expires today. Do you want to change it now?”. Click on “**Yes**”.
5. The Change Password screen will appear, enter your new password in the “New Password” field. Confirm your new password by re-entering it in the “Confirm New Password” field.
6. Click on the “**OK**” button.

NOTE: *If you ever lose the administrative password, you will need to restore the baseline from the system CDs again. (See Paragraph 2.4)*

User Profile

The administrator needs to add a user profile for each actual user with their role on the SSR notebook. So an individual may have two accounts, one as a Power User and one as an Administrator.

1. To add a new user profile:
 - a. Log on as the administrative user. The CAISI default username is “**caisiadmin**”, the default password is “**BS_69dlw**”.

b. Double click on the “My Computer” icon and then double click on “Control Panel”.

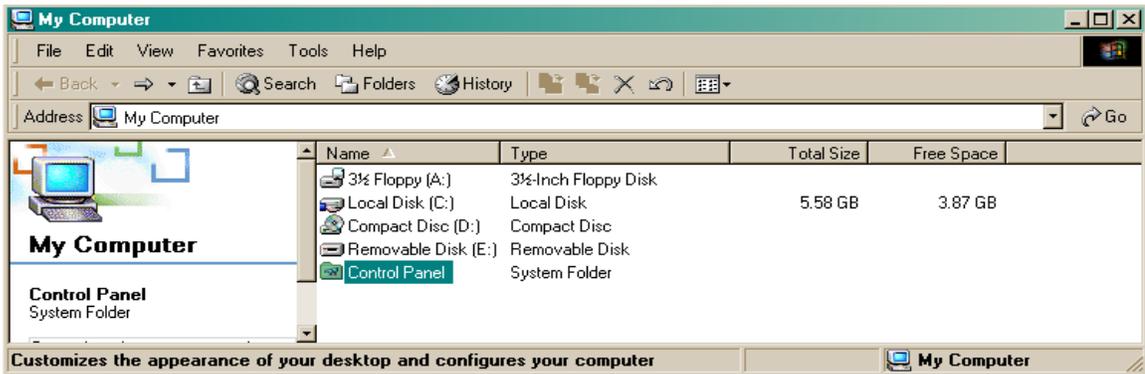


Figure 2-18 SSR Notebook My Computer Screen

c. Double click on “Users and Passwords”.

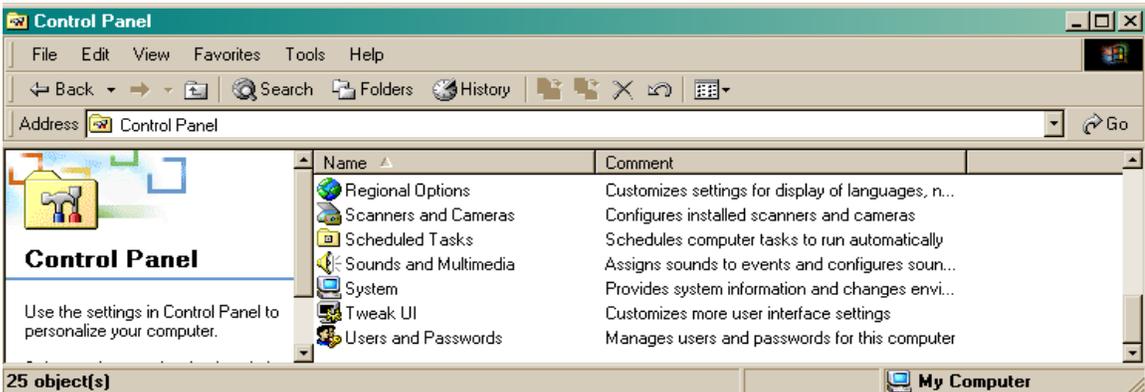


Figure 2-19 SSR Notebook Control Panel Screen

d. Click on the “Add” button.



Figure 2-20 SSR Notebook Users and Passwords Screen

- 1) Enter the user's:
 - a) User name
 - b) Full name
 - c) Description
- 2) Click on the “**Next**” button.

**Figure 2-21 SSR Notebook
Add New User Screen**

- 3) Enter the new password and re-enter to confirm.
 - a) If the person is readily available, have them enter their new password. If not, use an interim password, such as “**P@ssword!**”
 - b) Re-enter the new password in the “Confirm password” field.

**Figure 2-22 SSR Notebook
Add New User Password Screen**

- 4) Click on the “**Next**” button.
- 5) Select “**Standard User**”.
- 6) If the user requires Administrator rights:
 - a) Create a “new user” with a different user name and password.
 - b) Select “**Other**”.
 - c) Select “**Administrator**”.
- 7) Click on the “**Finish**” button.

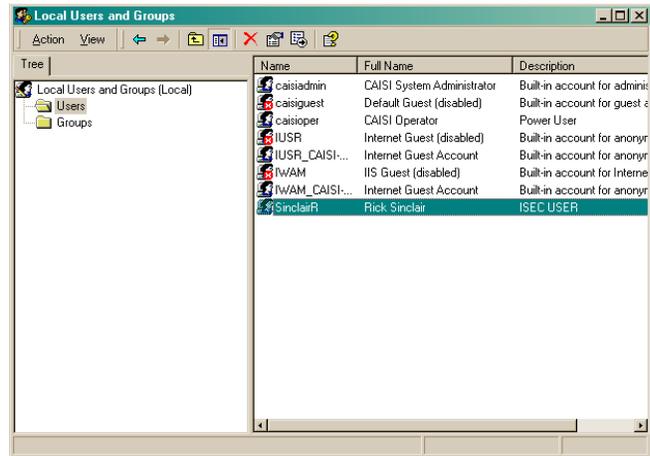
**Figure 2-23 SSR Notebook
Level of Access for New User Screen**

- 8) Click on the “Advanced” tab.
- 9) Click on the “Advanced” button.



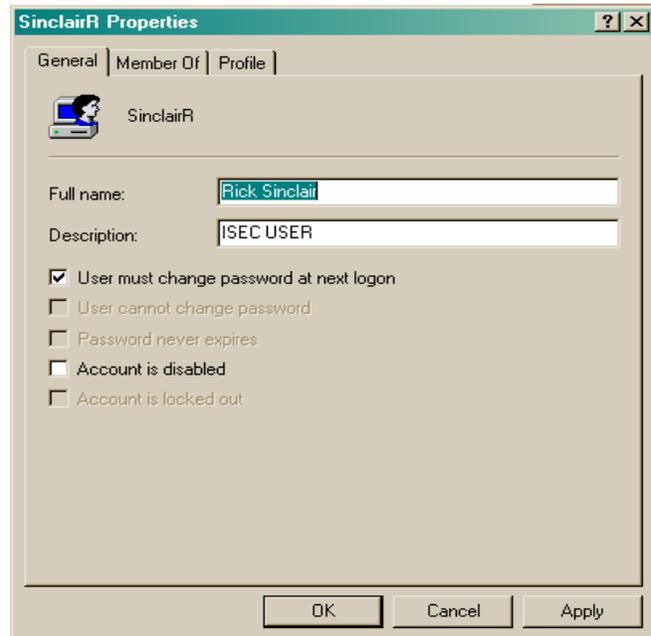
**Figure 2-24 SSR Notebook
Users and Passwords Advanced Screen**

- 10) Click on “Users”.
- 11) Right-click on the new username.



**Figure 2-25 SSR Notebook
Local Users and Groups**

- 12) Select **“Properties”**.
- 13) Check the box for **“User must change password at next logon”**.
- 14) Click on the **“Apply”** button and then click on the **“Close”** button.
- 15) Repeat this procedure for all newly created accounts when the user did not enter their own password.
- 16) Close all open windows.



**Figure 2-26 SSR Notebook
New User Properties Screen**

NOTE: Write down your passwords, seal them in an envelope, and turn it over to the security officer for safekeeping.

2.6 CONFIGURE NETWORK PARAMETERS

1. Configure Network Parameters.
 - a. Log on as the administrative user. The CAISI default username is **caisiadmin** and the password is **BS_69dlw**.
 - b. Right-click on **“My Computer”**.
 - c. Choose **“Properties”**.



**Figure 2-27 SSR Notebook
Network Parameters Screen**

- d. Click on the “**Network Identification**” tab.
- e. Click on the “**Properties**” button.

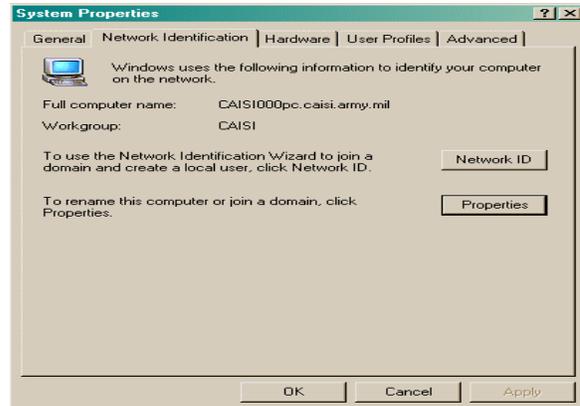


Figure 2-28 SSR Notebook System Properties Screen

- f. Change the Computer name as appropriate for your network. The CAISI default is **caisi000pc**.
- g. Change the Workgroup as appropriate for your network. The CAISI default is **caisi**.
- h. Click on the “**More**” button.

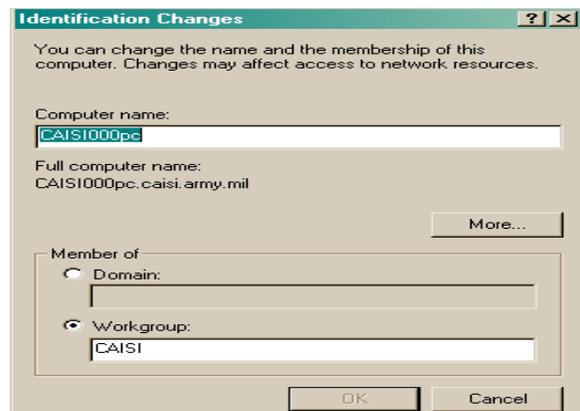


Figure 2-29 SSR Notebook Identification Changes Screen

- i. Enter your primary fully qualified DNS domain name. An example of a fully qualified DNS domain name is **caisi.army.mil**.
- j. Click on “**OK**” on the “DNS suffix” pop-up screen.
- k. Click on “**OK**” on the “Identification Changes” pop-up screen.
- l. A network identification prompt will appear, click on “**OK**” to reboot the computer.

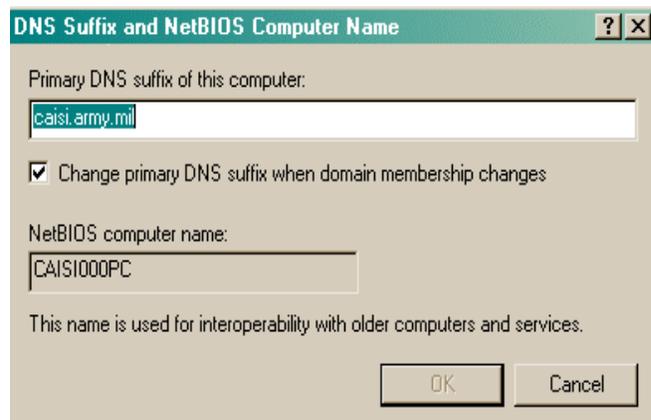


Figure 2-30 SSR Notebook DNS Suffix and Net BIOS Computer Name

- m. Click on “**OK**” on the System Properties Screen.
- n. A system settings change screen will appear, at the “Do you want to restart your computer now” prompt, Click “**Yes**”. Notebook will reboot.

2.7 CONFIGURE THE WIRED/BUILT-IN NETWORK INTERFACE CARD (NIC)

1. Ensure only the Wired NIC is inserted in the PCMCIA slot. (If Wired NIC is not issued, use built-in NIC. Screens are the same).
2. Power on the SSR notebook.
3. Log back on as the administrative user. The CAISI default username is **caisiadmin** and the password is **BS_69dlw**.
4. Right-click on “My Network Places”.
5. Choose “Properties”.
6. Right-click on the “CardBus II 10_100” or “Built-in Ethernet” network card icon.
7. Choose “Properties”.



Figure 2-31 SSR Notebook Network Parameters Screen

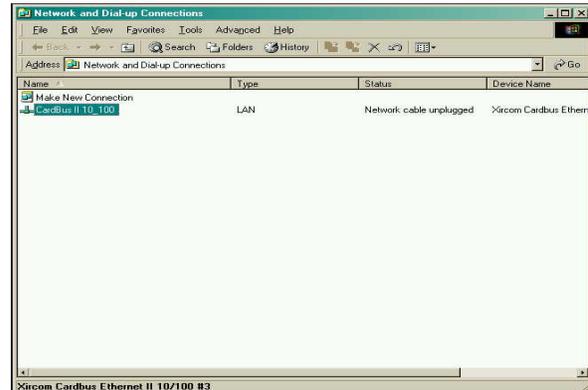


Figure 2-32 SSR Notebook Network and Dial-up Connections Screen

8. Select “Internet Protocol (TCP/IP)”.
9. Click on the “Properties” button.

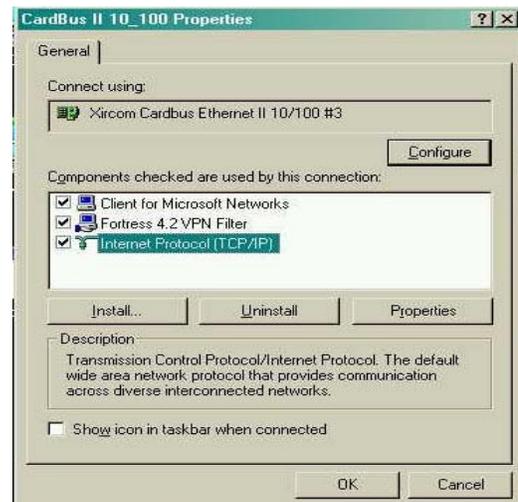


Figure 2-33 SSR Notebook Wired NIC Properties Screen

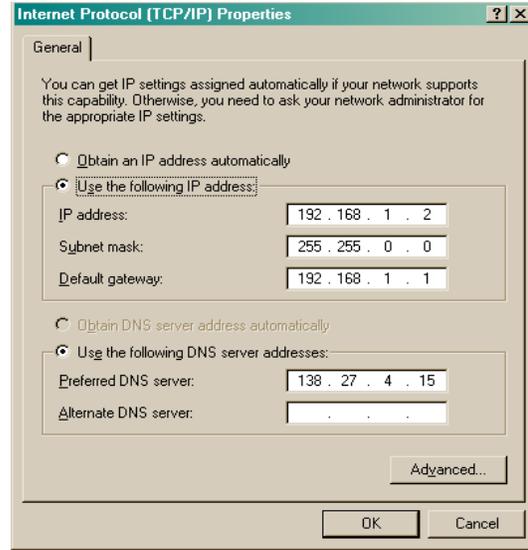
10. Select “**Use the following IP address**” and then enter:

- a. IP address:
CAISI default 192.168.1.2
- b. Subnet mask:
CAISI default 255.255.0.0
- c. Default Gateway:
CAISI default 192.168.1.1

11. Select “**Use the following DNS server addresses**” and then enter:

- a. Preferred DNS server:
CAISI default 138.27.4.15
- b. Alternate DNS server

12. Click on the “**OK**” button



**Figure 2-34 SSR Notebook
Wired NIC TCP/IP Properties Screen**

NOTE: *If you left the default private IP address, a pop-up box will inform you that the address is the same as the wireless NIC. It asks if you want to enter a different IP.*

13. You need to:

- a. Click on the “**No**” button when it asks you if you want a different IP address.
- b. Click on the “**OK**” button on the Properties screen.
- c. Exit out of the “Network and Dial-up Connections” window.

14. Configuration of the network parameters for the wired NIC/Built-in NIC is complete.

15. Reboot the notebook computer.

NOTE: *Refer to Paragraph 2.7.1 for procedures to remove the wired NIC from the notebook computer.*

NOTE: *You must have encryption turned off any time you use the wired NIC. If you are having trouble communicating, refer to Paragraph 2.9.1 for procedures on how to turn the Air Fortress Remote Client off.*

2.7.1 Remove NIC from SSR Notebook.

1. The icons shown to the right appear on the menu tray at the bottom of the notebook screen.
2. Click on the NIC icon.
3. Click on “**Stop Xircom CreditCard Ethernet Adapter 10/100**”.



**Figure 2-35 SSR Notebook
NIC Card Icon**

NOTE: *If the wireless NIC is installed in the computer instead of the wired NIC, you will get the following prompt: “Cisco Systems 340 Series Wireless LAN Adapter”.*

4. At the “Safe to Remove Hardware” message prompt, click on the “**OK**” button.
5. Click the “**Close**” button.
6. Remove the NIC from the PCMCIA slot.
7. Reboot the SSR notebook computer.



**Figure 2-36 SSR Notebook
Safe To Remove Hardware Prompt**

2.7.2 Disable Built-In NIC.

At some point you may have to refresh the settings of the Built-In NIC. You can reboot the notebook or disable – enable the built-in NIC.

1. Right-click on “**My Network Places**”.
2. Choose “**Properties**”.
3. Highlight “**Built-In Ethernet**”. Right-click.
4. Choose “**Disable**”. Message will appear that states built-in NIC is disabled.
5. Highlight “**Built-In Ethernet**”. Right-click.
6. Choose “**Enable**”. Message will appear that states built-in NIC is enabled.

NOTE: *In the lower right hand corner, the LAN connection icon is displayed. When the Built-in NIC is first connected, the message on the left appears. If you disconnect the Ethernet cable, the message on the right appears*



Figure 2-37 SSR Notebook Built-In Ethernet NIC Prompts

2.8 CONFIGURE THE WIRELESS NETWORK INTERFACE CARD (NIC)

In order to use the wireless NIC, you must configure TCP/IP and load the wireless NIC utilities.

Additionally, you must load and configure the AirFortress remote client software. Without the remote encryptor software you cannot communicate, because remote access is disabled on the radios and the encryptors are protecting the rest of the network.

1. Ensure only the wireless NIC is inserted in the PCMCIA slot. Attach rabbit ears antenna to velcro patch on upper left hand corner of notebook cover.
2. Reboot the computer.
3. Log back on as the administrative user. The CAISI default username is **caisiadmin** and the password is **BS_69dlw**.
4. Right-click on “**My Network Places**”.
5. Choose “**Properties**”.



Figure 2-38 SSR Notebook Network Parameters Screen

6. Right-click on the “**Cisco**” network card icon.
7. Choose “**Properties**”.

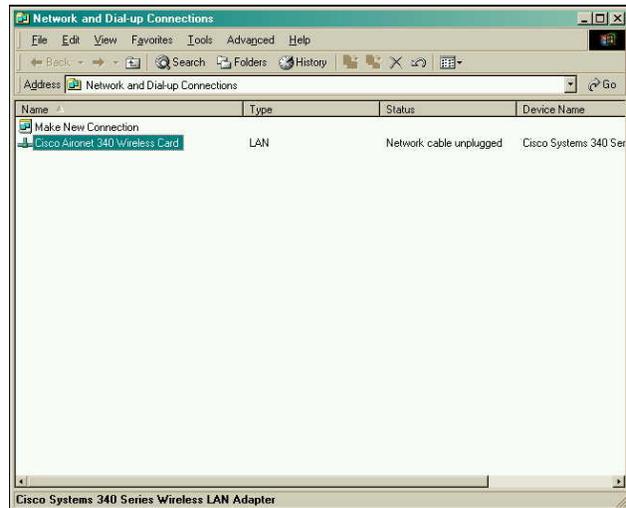
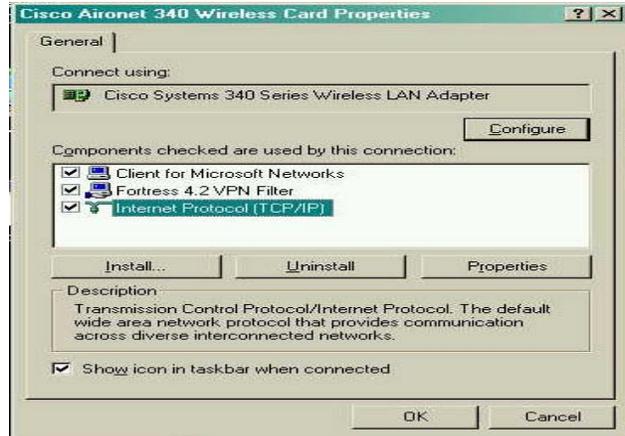


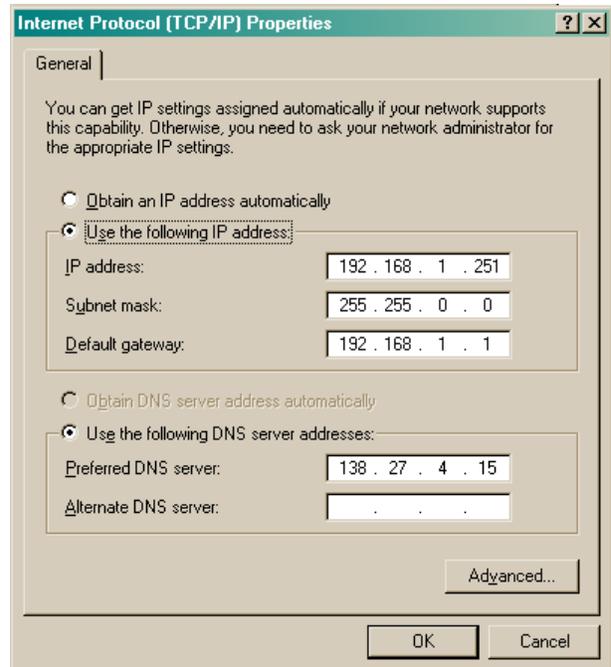
Figure 2-39 SSR Notebook Network and Dial-up Connections Screen

8. Select “**Internet Protocol (TCP/IP)**”.
9. Click on the “**Properties**” button.



**Figure 2-40 SSR Notebook
Wireless NIC Properties Screen**

10. Select “**Use the following IP address**” and then enter:
 - a. IP address:
CAISI default 192.168.1.251
 - b. Subnet mask:
CAISI default 255.255.0.0
 - c. Default Gateway:
CAISI default 192.168.1.1
11. Select “**Use the following DNS server addresses**” and then enter:
 - a. Preferred DNS server
CAISI default 138.27.4.15
 - b. Alternate DNS server
12. Click on the “**OK**” button.



**Figure 2-41 SSR Notebook
TCP/IP Properties for Wireless NIC**

NOTE: If you left the default private IP address, a pop-up box will inform you that the address is the same as the wired NIC. It asks if you want to enter a different IP.

13. You need to:
 - a. Click on the “**No**” button.
 - b. Click on the “**OK**” button on the Properties screen.
14. At the bottom of the notebook screen, click on the ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear.

15. Select the “**Aironet Client Encryption Manager**” (CEM) utility to set the Wired Equivalent Privacy (WEP) key for the wireless NIC.

- a. Enter the default password, **Cisco**.
- b. Click on the “**OK**” button.

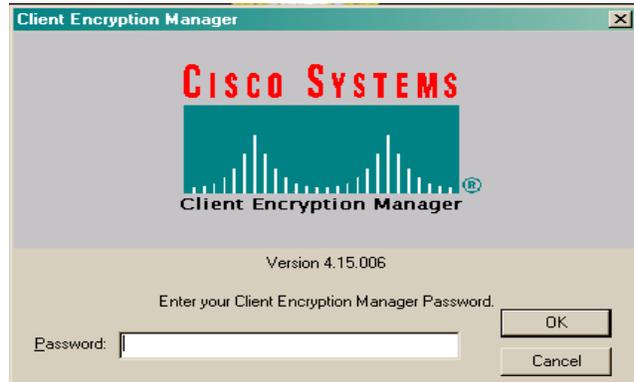


Figure 2-42 SSR Notebook Client Encryption Manager (CEM) Screen

- c. Select “**Commands**”.
- d. Select “**Change Password**”.

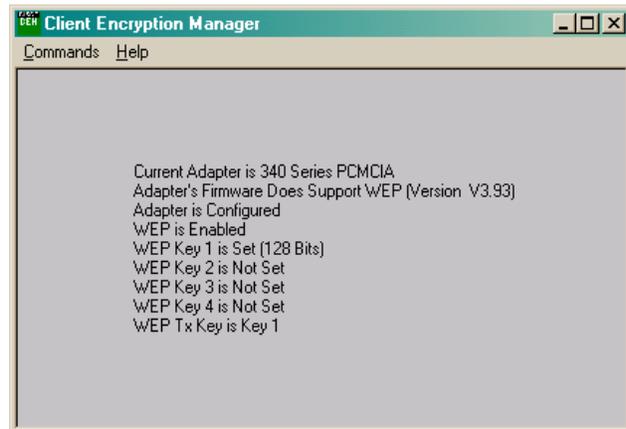


Figure 2-43 SSR Notebook Commands Menu

- e. Enter your old password in the “Existing Password” field.
- f. Enter your new password in the “New Password” and “confirm New Password” fields.
- g. Click on the “**OK**” button.
- h. Make sure to write it down, seal it in an envelope and give it to your security officer.

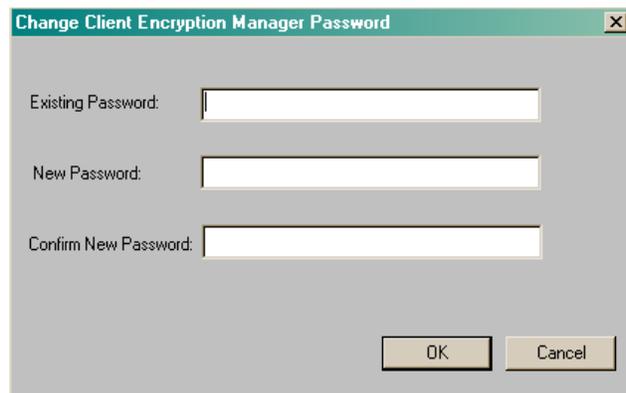
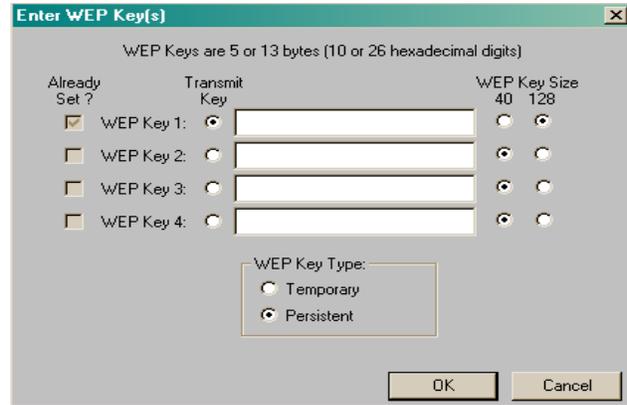


Figure 2-44 SSR Notebook Change CEM Password Screen

NOTE: *If you change the password for the CEM utility and forget it, there is no way to recover it. You need to uninstall the program and reinstall it by reloading the CAISI Software baseline. Reinstalling on top of the existing program does not reset the password – you must completely uninstall it to eliminate the old password.*

- i. Select “**Commands**”.
- j. Select “**Enter WEP key**”.
- k. In the “WEP Key 1” field, enter the new 26-character WEP key provided by the CSS S6.
The CAISI default is
0123456789abcdef0123456789
- l. Click on the “**OK**” button.



**Figure 2-45 SSR Notebook
Set WEP Key Screen**

NOTE: *The CAISI default WEP key is to be used only for classroom training. It is the SSR’s responsibility to change this field before the CAISI is deployed and to ensure a 128-bit key and not a 40-bit key is used.*

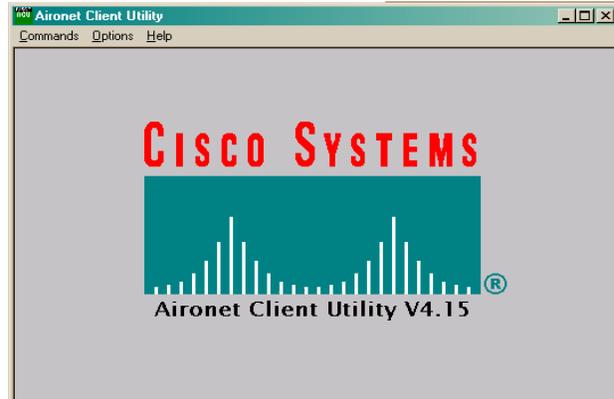
SECURITY CONSIDERATIONS

- Once a card is keyed, there is no quick and easy way to zeroize it. The only way to do so is to set a new key on top of the old one.
- Once cards are keyed, they must be protected as SBU information.
- You must use the same WEP key code that is in the wireless bridges. If you have forgotten it, check with your security officer. If the password is lost you can enter a new one without knowing the old one, however you would have to change them all, not just this one.
- If the key code is lost or compromised or if a keyed device is lost: you must change the key codes in all the wireless bridges, Ethernet adapters, and NICs in the battle area. They must match each other in order to communicate and they must be protected from possible intrusion or monitoring by hostile forces.

16. Close the CEM tool.
17. At the bottom of the notebook screen, click on the ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear.

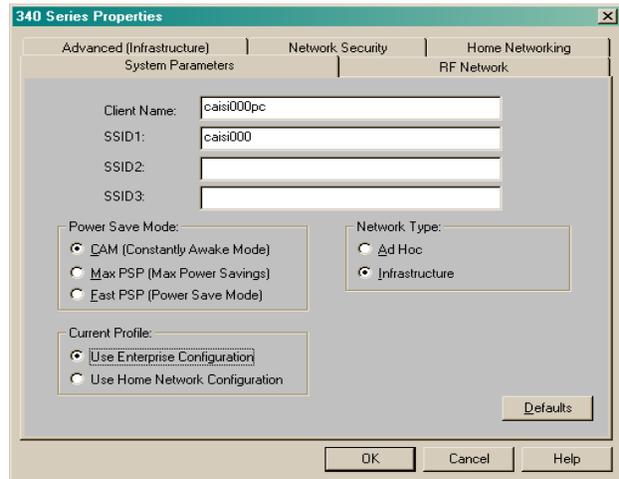
18. Select the “**Aironet Client Utility**” (ACU) utility to assign the wireless NIC a hostname and Service Set ID (SSID).

- a. Select “**Commands**”.
- b. Select “**Edit properties**”.



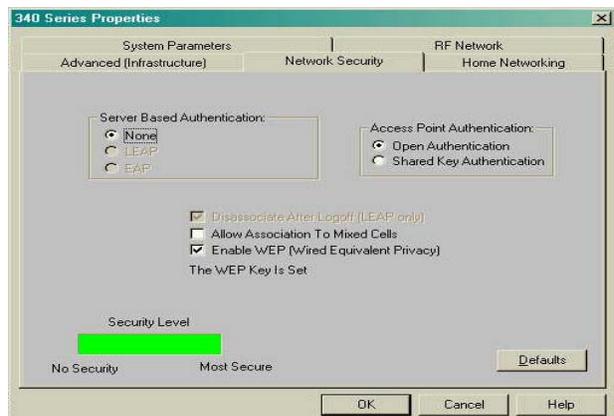
**Figure 2-46 SSR Notebook
Aironet Client Utility (ACU) Screen**

- c. Enter your assigned host name in the “Client Name” field.
The CAISI default is caisi000pc.
- d. Enter your assigned SSID in the “SSID1” field.
The CAISI default is caisi000.
- e. Click on “**Network Security**”.



**Figure 2-47 SSR Notebook
Wireless NIC System Properties Screen**

- f. Ensure WEP is enabled.
- g. Ensure level of security (Access Port Authentication) is set to “**Open Authentication**”.
- h. Click on the “**OK**” button.



**Figure 2-48 SSR Notebook
Wireless NIC Network Security Screen**

19. Close the ACU tool.

20. Configuration of the network parameters for the wireless NIC is complete. Reboot the notebook computer.

NOTE: *Refer to Paragraph 2.7.1 for procedures to remove the wireless NIC from the Notebook computer. The procedures are the same as those for the wired NIC.*

NOTE: *You must have encryption turned (**on**) any time you use the wireless NIC to access the CAISI LAN. Refer to Paragraph 2.9.1 for procedures on how to verify the Air Fortress Remote Client (encryption) is on.*

2.9 CONFIGURE AIR FORTRESS REMOTE CLIENT

The Air Fortress Remote Client software works exactly like the hardware encryptor, except that it operates on the client computer, in this case the SSR notebook. It encrypts and decrypts the network traffic as it passes in and out of the notebook. It sits between the computer and the NIC – in the same way that the inline encryptor sits between the hub and the radio.

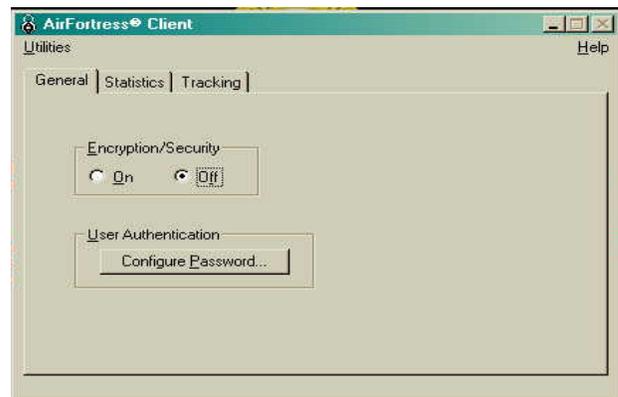
The AirFortress (AF) Client includes drivers and utilities to configure the Air Fortress remote client and to check encryption status and statistics.

2.9.1 Configure the Parameters for the Air Fortress Remote Client

1. Look in the system tray for the small padlock icon.

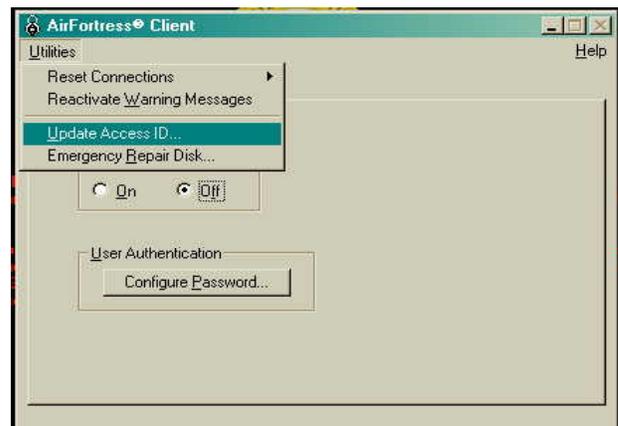
NOTE: When you are in secure mode, the icon will be a locked padlock.  When you are non-secure, it will be unlocked. 

2. Double-click on the padlock icon and the Air Fortress Client screen will appear.



**Figure 2-49 SSR Notebook
AF Client Main Screen**

3. Click on the “Utilities” menu and select “Update Access ID”.



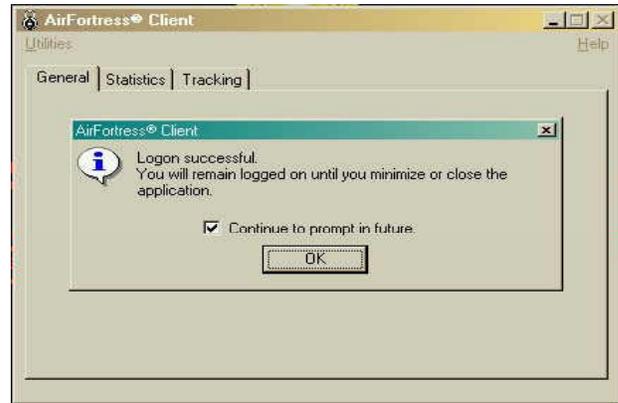
**Figure 2-50 SSR Notebook
AF Client Utilities Screen**

4. A dialog box will appear asking for your administrator’s password.
 - a. Enter the CAISI default password “**fortress**” or the password you previously entered as prescribed by your DOIM, S6 or CSSAMO.
 - b. Click on the “**OK**” button.



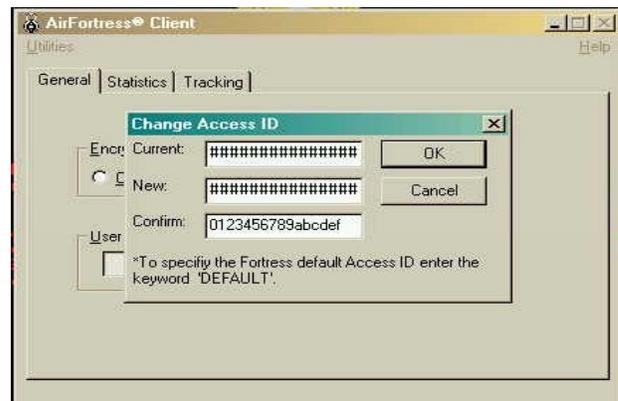
**Figure 2-51 SSR Notebook
AF Configuration Password Screen**

- c. At the AirFortress Client “Logon successful” prompt, click on the “**OK**” button.



**Figure 2-52 SSR Notebook
AF Client Logon Successful Prompt**

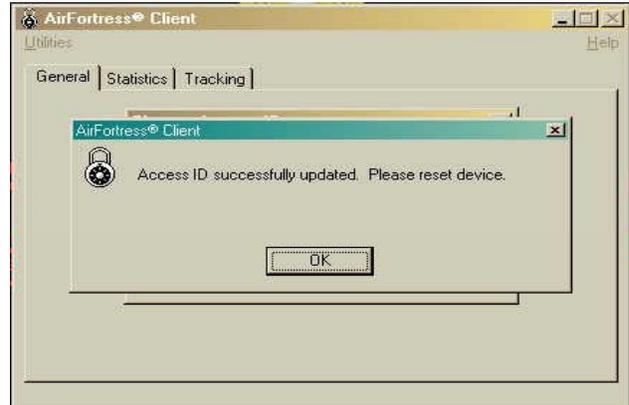
- d. The “Change Access ID” menu will appear.
 - e. Enter one of the following in the “Current” field:
 - 1) If the encryptor is new from the factory, enter the word **default**.
 - 2) If the encryptor is from Tobyhanna, enter the CAISI default **0123456789abcdef**.
 - 3) Enter your network’s pre-shared Access ID as prescribed by your DOIM, S6 or CSSAMO in both the “New” and “Confirm” fields.
 - 4) Click on the “**OK**” button.



**Figure 2-53 SSR Notebook
AF Client Change Access ID Screen**

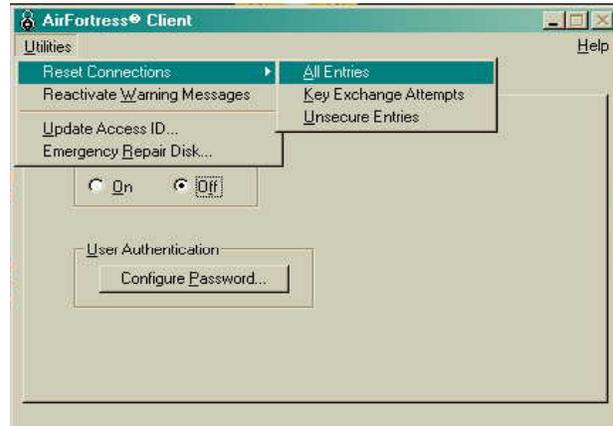
NOTE: The Access ID must be 16 hexadecimal digits and must match the one you entered in the inline encryptors.

- f. You will get a message saying that the AccessID was set and instructing you to please reset the device. Click on the “OK” button.



**Figure 2-54 SSR Notebook
AF Access ID Successfully Changed Screen**

- 5. Click on the “Utilities” menu and select “Reset Connections” then “All Entries”.



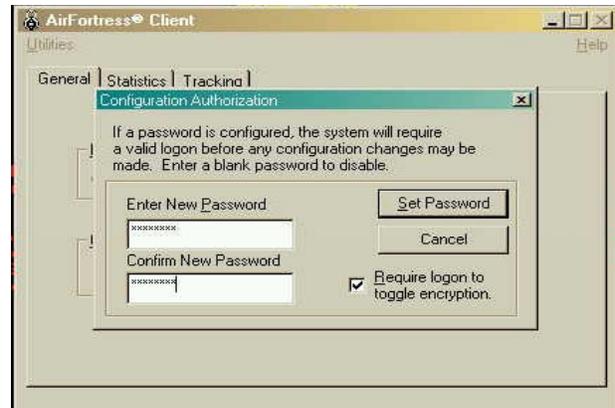
**Figure 2-55 SSR Notebook
AF Client Utilities Screen**

- 6. To change the administrator’s password, click on the “Configure Password” button.



**Figure 2-56 SSR Notebook
AF Client Utilities General Tab**

- a. Enter and confirm the new password.
- b. Click on the “Set Password” button.



**Figure 2-57 SSR Notebook
AF Client Configuration Authorization**

- c. At the “Password successfully set” prompt, click on the “OK” button.
- d. Close the AirFortress Client utility by clicking the minimize icon at the top of the menu.



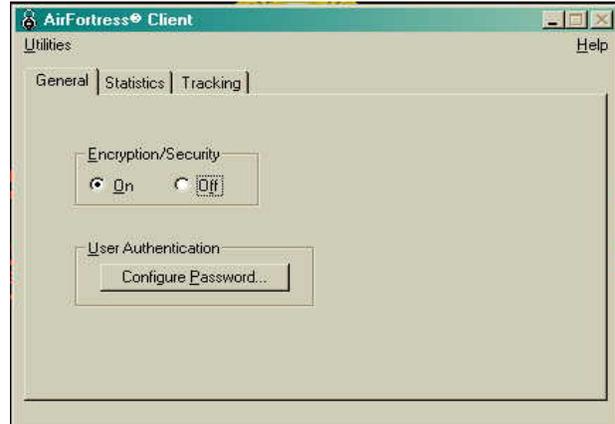
**Figure 2-58 SSR Notebook
AF Client Password Set Screen**

NOTE: *If you lose the password, reinstalling the client is not enough to reset it – you will need to reload the notebook from CD. Seal the password in an envelope and turn it into your security officer for safekeeping.*

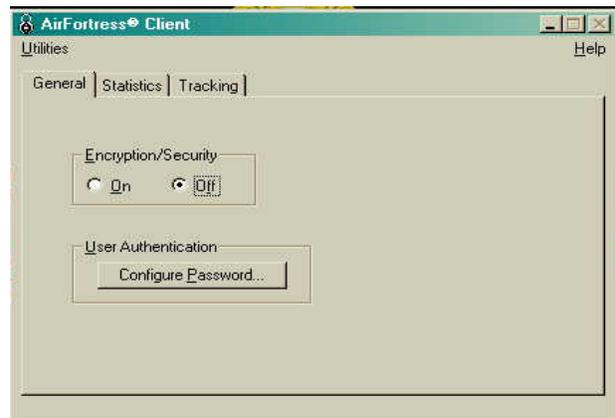
2.9.2 Turn the Air Fortress Remote Client On or Off

1. Look in the system tray for the small padlock icon.

2. Double-click on the icon and the Air Fortress Client screen will appear.
3. On the “**General**” tab:
 - a. Select encryption “**On**” if you are going to use your wireless NIC to get onto the Sensitive But Unclassified (SBU) CAISI network.
 - b. Select encryption “**Off**” if you are going to troubleshoot the wireless network or if you are going to use the wired NIC or built-in NIC instead of the wireless NIC.
4. Close the AirFortress Client utility by clicking the minimize icon at the top of the menu.



**Figure 2-59 SSR Notebook
AF Client Utilities General Tab -1**



**Figure 2-60 SSR Notebook
AF Client Utilities General Tab - 2**

Section II. CAISI Component Configuration

2.10 MANUAL CONFIGURATION OF THE ROUTER

The CAISI 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”. For more information on when to utilize a router, refer to TM 11-5895-1691-12, Paragraph I.3.9.

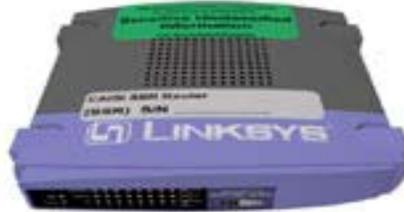


Figure 2-61 Router

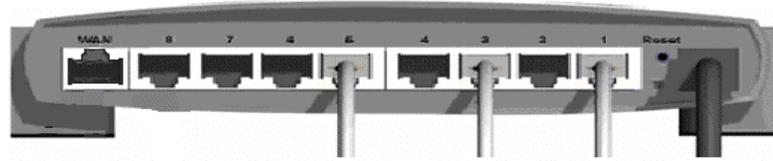
Two versions of Linksys router are in the CAISI system. (Version 2 is used as a basis for procedures and screenshots).

Version 1 has an uplink switch for port 8. Port 8 can be used for crossover “X” or straight-through “=” connections. Power supply consists of a power adapter and a 3-prong power cord.

Version 2 has an automatic sensor for crossover or straight-through connections, therefore all 8 ports can be used for connection. Power supply consists of a wall-style power adapter.

2.10.1 Physical Connection Procedures.

1. Remove the router and power supply from the SSR Transit case
2. Connect the female end of the power supply to the port labeled “Power” on the back of the router.
3. Plug the male end of the power supply into an external power source.
4. If the router is receiving power, the “Power” LED on front of the device will be lit green.
5. Remove a white straight-through Ethernet cable from your SSR Notebook case.
6. Connect one end of the white straight-through Ethernet cable to the Wired NIC/Built-in NIC on your SSR notebook and the other end into an available port on the router (ports 1-7 for version 1 or ports 1-8 for version 2).



**Figure 2-62 Router
Ethernet Cable Connection**

7. Apply power to the SSR notebook.

2.10.2 Configure the Router.

1. Logon to the notebook computer.
 - a. Press “**Ctrl-Alt-Delete**” keys.
 - b. When prompted enter the username and password, the CAISI defaults are **caisiadmin** and **BS_69dlw**
 - c. A Logon Message prompt will appear, “Your password expires today. Do you want to change it now?” For classroom training, click on the “**No**” button.

Unlike most other communications devices, the router does not have a serial “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).

2. Open Internet Explorer.
 - a. To open Internet Explorer on the notebook desktop, double click on the Explorer Icon.
 - b. Enter the router’s private address in your browser address bar.
 - c. If you do not know the IP address or password, you can reset the router to factory defaults.
 - 1) To reset the router to factory defaults, obtain a reset tool from the SSR Notebook case or SSR Transit case.

Version 1

- a. Insert the tip of the reset tool into the reset buttonhole on the back of the router and hold for 15 seconds.
- b. During this process the “**Diag**” light will light up, the “**Link**” light will light up momentarily, then both lights will go off, and the router will now be reset.
- c. If the green “**Link**” light does not flash, try again.

Version 2

- a. Insert the tip of the reset tool into the reset buttonhole on the back of the router and observe the following:

- b. The "**Diag**" light will light up red, all of the LEDs on the "100" level will blink twice, then all of the LEDs on the "Full/Col" level will blink twice, then all of the LEDs on the "Link/Act" level will blink twice. The "Diag" LED will then go out. The router will now be reset.
- c. If the "**Diag**" light does not go out, try again.



Figure 2-63 Router Front View of LEDs

- d. If the router has been previously configured, or if it has been reset to "factory defaults", enter **http://192.168.1.1** into the browser's address window.

NOTE: *Configure your notebook as a DHCP client, or assign it an address on the 192.168.1 subnet (for instance, the CAISI notebook is set to the static address 192.168.1.2).*

- 3. The "**Enter Network Password**" screen will appear.
 - a. You may leave the "User Name" field blank.
 - b. Enter one of the following passwords in the "Password" field: "**admin**" (factory default) "**system**" (CAISI default), or the password you previously assigned the device as prescribed by your DOIM, S6 or CSSAMO.



Figure 2-64 Router Enter Network Password Screen

- c. Click on the "**OK**" button.

Security Warning

Do not check the "Save this password in your password list" option box. If you do, then anyone using your machine gets free access to the router. You should never check this option on any pop up password screen in any application.

When you first login, the main configuration screen will appear. This is your basic set up screen. Fill out the screen as follows:

4. Main Menu Setup Tab

- a. Enter the Host Name provided by the CSSAMO, S6 or DOIM and press the “**Tab**” key.
The CAISI default is **caisirouter**
- b. Enter the domain name provided by the CSSAMO, S6 or DOIM and press the “**Tab**” key. The CAISI default is **caisi.army.mil**
- c. Leave the LAN IP address set to the CAISI default **192.168.1.1**
- d. Leave the LAN Subnet Mask set to the CAISI default **255.255.255.0**
Your private subnet will be **192.168.1.0**
- e. Leave the WAN IP address set to “**Obtain an IP Address Automatically**” if you’re behind a DHCP server.

or

- f. Set the WAN properties if there is no DHCP server as directed by your DOIM, S6 or CSSAMO. Click the down arrow in the WAN Connection Type dialog box, select “**StaticIP**”. Enter the following information:
 - 1) IP Address.
 - 2) Subnet Mask.
 - 3) Default gateway.
 - 4) Enter one or more DNS server addresses. At least one is required.
- g. Leave all other settings as is.
- h. Click on the “**Apply**” button.
- i. Click “**Continue**” on the “Settings are successful” screen.

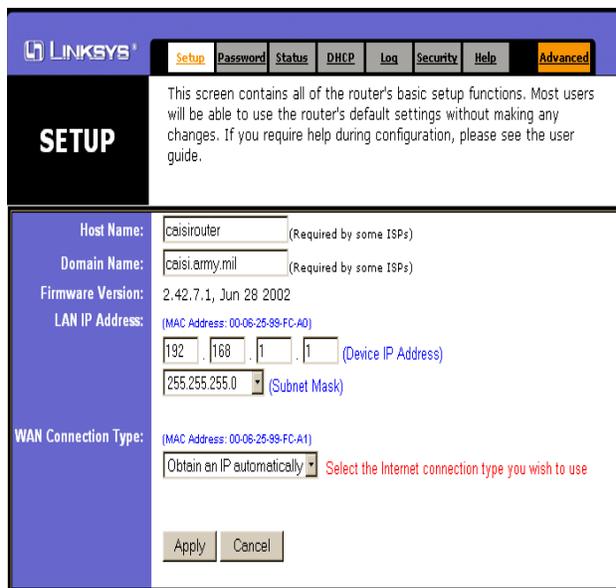


Figure 2-65 Router Main Menu Setup Tab

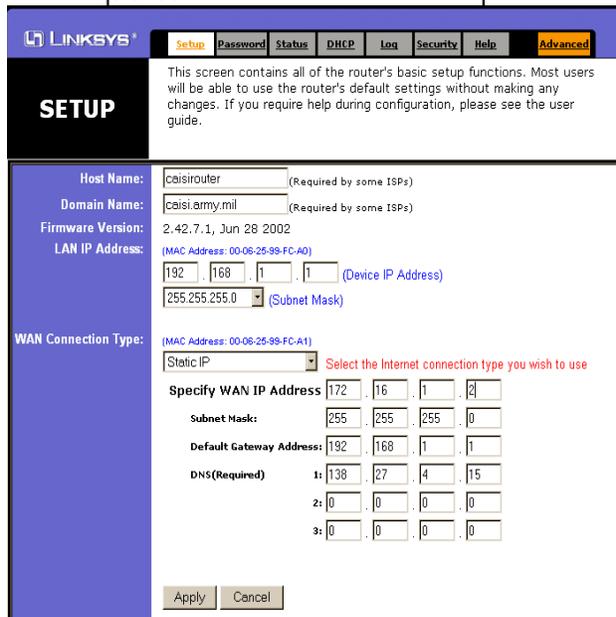
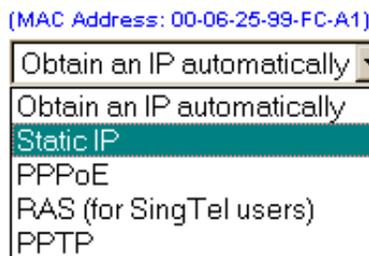


Figure 2-66 Router WAN Connection Type Screen

5. Main Menu Password tab:
 - a. Click on the “**Password**” tab at the top of the screen.
 - b. Enter your new password. The CAISI default is “**system**”.
 - c. Re-enter your new password to confirm.
 - d. Delete the “**Public**” and “**Private**” entries from the SNMP community boxes to disable SNMP and prevent intruders from viewing or changing your configuration with SNMP tools.
 - e. Set “UPnP Services” to “**Disable**”.
 - f. Leave “Restore Factory Defaults” to “**No**”.
 - g. Click on the “**Apply**” button.
 - h. Click on “**Continue**” on the “Settings are successful” screen.

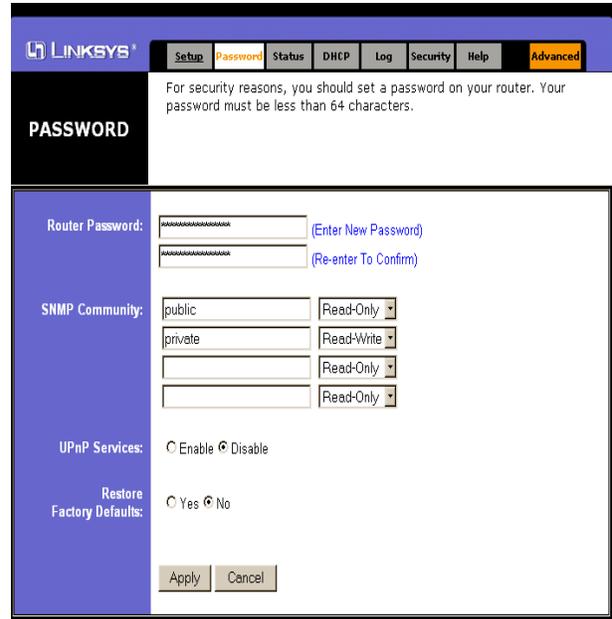


Figure 2-67 Router Main Menu Password Tab

6. The “**Enter Network Password**” screen will appear.
 - a. You may leave the “User Name” field blank.
 - b. Enter one of the following passwords in the “Password” field: “**system**” (CAISI default), or the password you previously assigned the device as prescribed by your DOIM, S6 or CSSAMO.
 - c. Click on the “**OK**” button.



Figure 2-68 Router Enter Network Password Screen

Security Warning

When you set the passwords you must write them down, seal them in an envelope, and turn them in to the security officer. This is extremely important. If you set and lose a password, you will have to reset to default settings and reconfigure via the 10BaseT port from the private side. The default password is “**Admin**” and the IP is **192.168.1.1** on the private side.

7. Main Menu Status tab.

- a. Click on the “**Status**” tab at the top of the screen.
- b. This screen is a read-only information screen, which shows your basic setup.
- c. If your basic set up screen was set up to get an address automatically, this screen will show the address issued to you by the DHCP server.
- d. It is normal to show an IP address of “0.0.0.0” at this time, because you are configuring the router off line and cannot yet get an address.
- e. After the router has been connected to the network, the address will fill in, along with the subnet mask, gateway and remaining DNS servers.

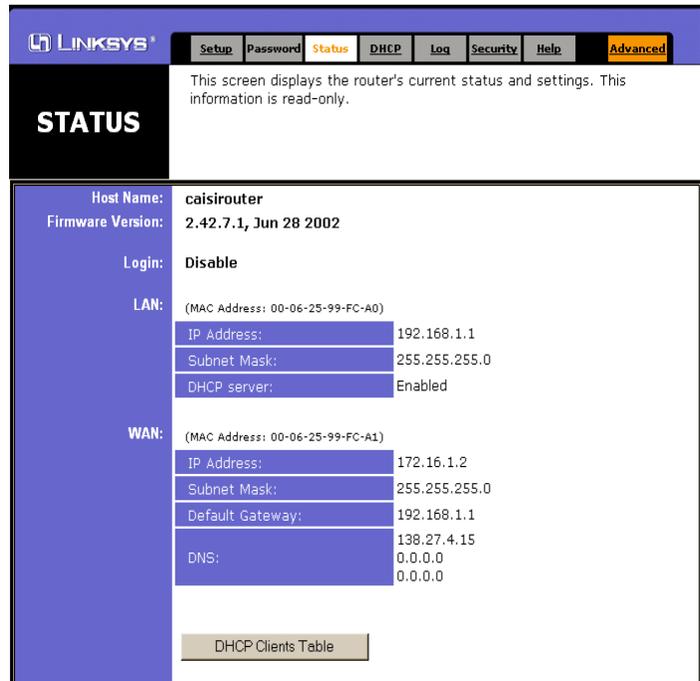


Figure 2-69 Router Main Menu Status Tab

8. Main Menu DHCP tab:

- a. Click on the “**DHCP**” tab at the top of the screen.
- b. Leave DHCP server set to “**Enable**”.
- c. Change the default values to:
 - 1) Set the “Starting IP Address” to “**100**”.

“**192.168.1.100**” reserves the first fifty addresses for assignment to STAMIS clients that require static IP addresses.

 - 2) Set Number of DHCP Users to “**150**”.
- d. Click on the “**Apply**” button.
- e. Click on “**Continue**” on the “Settings are successful” screen.

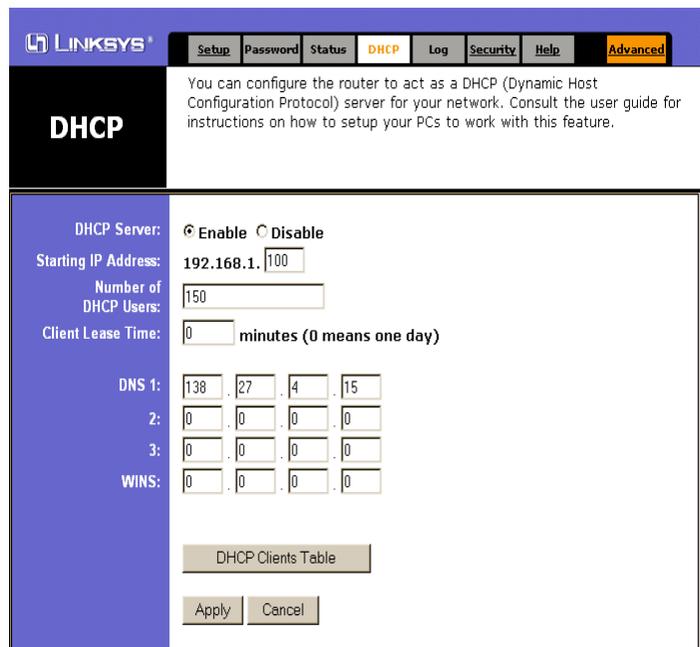


Figure 2-70 Router Main Menu DHCP Tab

- f. To see who is a currently active DHCP client, click on the “**DHCP Clients Table**” button.

A screen similar to the following will appear:

At this time it will show your notebook if you drew an address from the router. If your notebook has a static IP address, this table will be blank.

DHCP Active IP Table		
DHCP Server IP Address:		192.168.1.1
Client Hostname	IP Address	MAC Address
WilliamsDL	192.168.1.100	00-40-96-29-21-FD

Figure 2-71 Router DHCP Active IP Table

Configuration of the router is now complete. If you are not going to view the remaining tabs you may close the web browser.

The remaining tabs are not normally used with the standard CAISI configuration; however a brief explanation of their functionality is discussed below.

- 9. Click on the “**Log**” tab to display the log screen.
 - a. If you want to see who is connecting to whom, “**Enable**” the Access Log. Then check it, periodically.
 - b. If you don’t need this information, leave Access Log set to “**Disable**”.

NOTE: The log can be sent to a specific IP address.



Figure 2-72 Router Main Menu Log Tab

- Click on the “Security” tab.

This screen is intended to configure your router to use programs that are not part of the standard CAISI tool kit.

These tools are not required because the reach-back networks to which CAISI connects (the installation LAN or NIPRNET) have similar firewall tools already in operation to screen traffic.

Do not make any changes to this screen.

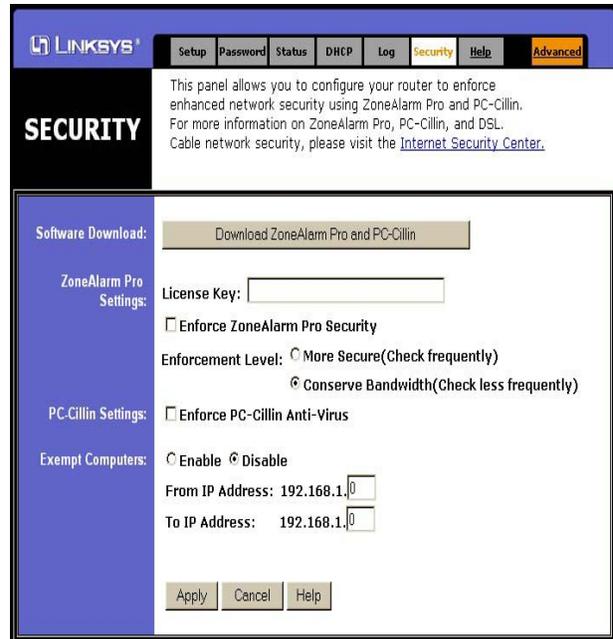


Figure 2-73 Router Main Menu Security Tab

- Click on the “Help” tab.

The items listed in the blue area on the left side – each pop up a help file in a new window.

The items listed in the white area on the right side are links to web sites.



Figure 2-74 Router Main Menu Help Tab

- Click on the “Advanced” tab. Figure 2-75.

NOTE: The advanced screen opens on the “Filters” tab.

You will not normally need to set any filters, but you can if you need to. Any IP addresses, ports or MAC addresses you enter in this screen are denied the ability to pass through the router.

By using the Filters screen, you can configure the router to block specific internal users from accessing the NIPRNET and Internet.

You can set up different filters for different users based on their IP addresses or their network Port number.

To block users by MAC address, click on the “**Edit MAC Filter Setting**” button.

Near the bottom of the Filters screen are several settings, you may want to change.

SPI (Stateful Packet Inspection). This feature checks the state of an incoming packet to verify that the destination IP address matches the source IP of the original request. This helps keep intruders from spoofing active connections to computers behind the router. Default is Disable.

Block Wan Request. This feature prevents the router from answering pings from the public side. It also hides the network ports. These two actions effectively hide the router from intruders. Default is Enable.

Multicast Pass Through. This feature allows multicast packets to pass through the router. Multicast is used to make packets available to everyone on the network, rather than addressing them to specific addresses. Multicast is frequently used for services such as broadcasts of CNN or other streaming video. If you do not need multicasts, you may disable this function. Default is Enable.

IPSec Pass Through and PPTP Pass Through. These features enable clients on the private to establish secure connections to servers on the public side. Default is Enable.

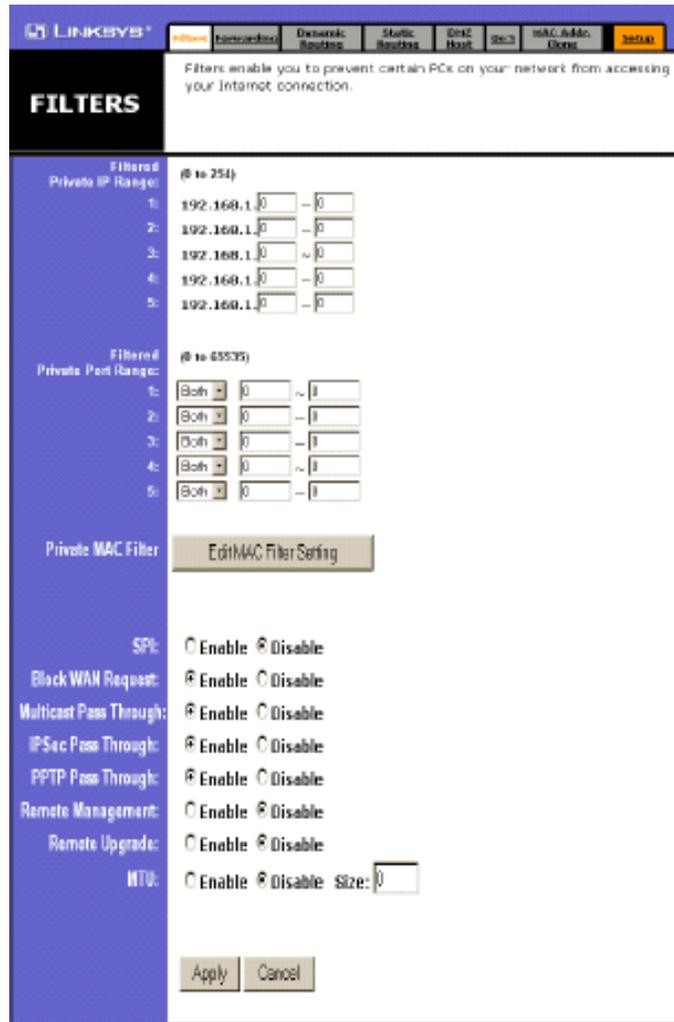


Figure 2-75 Router Main Menu Advanced Tab

Remote Management and Remote Upgrade. This prevents intruders from logging onto your router through the public WAN port. You will only be able to connect to, configure, and monitor the router from one of the private LAN ports. Default is Disable.

MTU (Maximum Transmission Unit), unless the DOIM, S6 or CSSAMO has asked you to enable it and given you an MTU value. The MTU parameter is only used if the network to which the CAISI is connected has a small packet size limitation. This is not normally the case. Default is Disable and Size = 0.

2.10.3 Verify Router Operational Status

1. Open Internet Explorer on the notebook desktop.
2. In the address toolbar at the top of Explorer, enter the IP address you gave the router during configuration. In this case, enter the IP – “**192.168.1.1**”.
3. Click on “**GO**” on the Explorer toolbar or click on “**Enter**” on the notebook keyboard.
4. The “**Enter Network Password,**” screen will appear.
 - a. You will be prompted for a user name and password.
 - b. You may leave the “User Name” field blank.
 - c. Enter the password you assigned the device as prescribed by your DOIM, S6 or CSSAMO in the “Password” field. The CAISI default is “**system**”.
 - d. Click on the “**OK**” button.



Figure 2-76 Router Enter Network Password Screen

- e. To confirm that the router is configured, select the “Status” tab.
 - 1) If you successfully configured the router, you should now see the CAISI default Host name, **caisirouter** and Domain name **caisi.army.mil**
 - 2) At factory defaults, the Host name and Domain name fields were empty and the “WAN Connection Type” was set to “Obtain an IP automatically”.

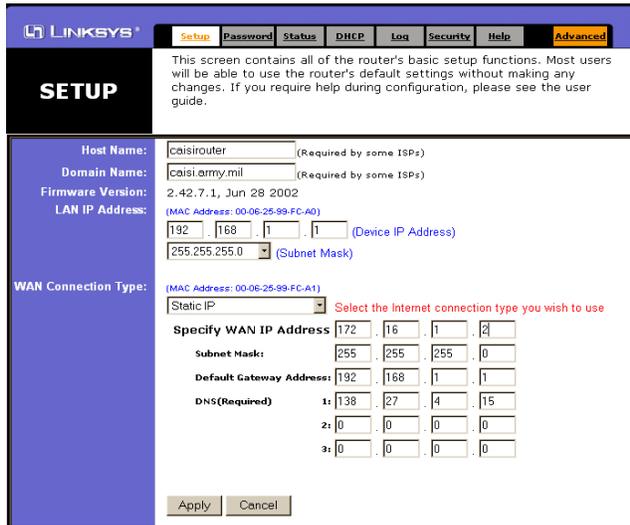


Figure 2-77 Router Configured Status Tab

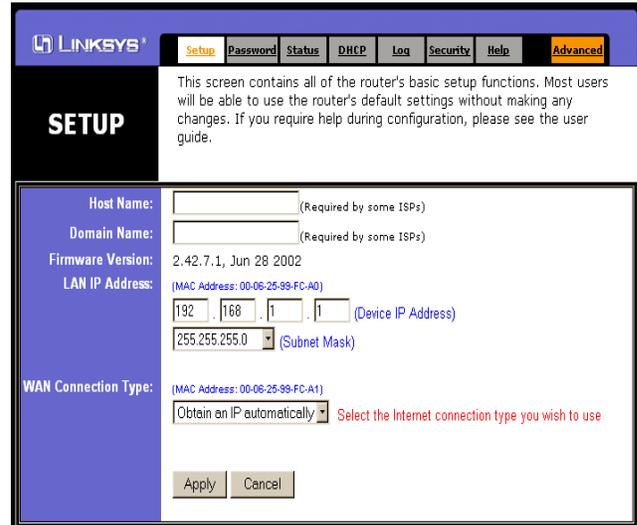


Figure 2-78 Router Factory Default Status Tab

- f. You can also verify configuration by selecting the “DHCP” tab.
 - 1) If you successfully configured the router, the number of DHCP users should be set to **150**.
 - 2) At factory defaults, the number of DHCP users is 50.

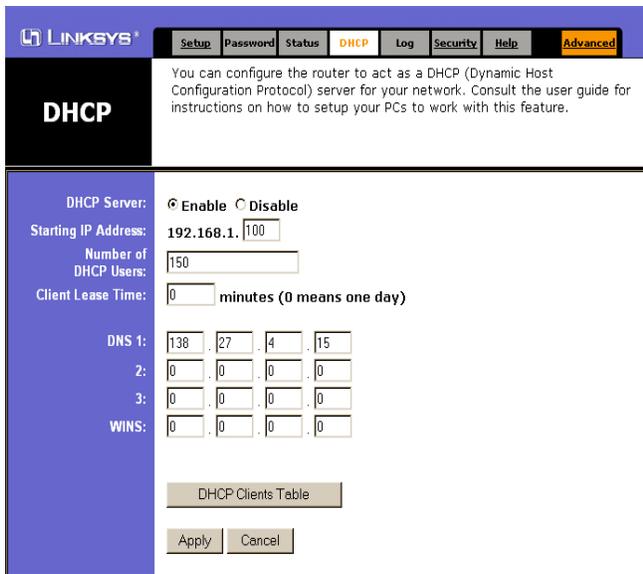


Figure 2-79 Router Configured DHCP Tab

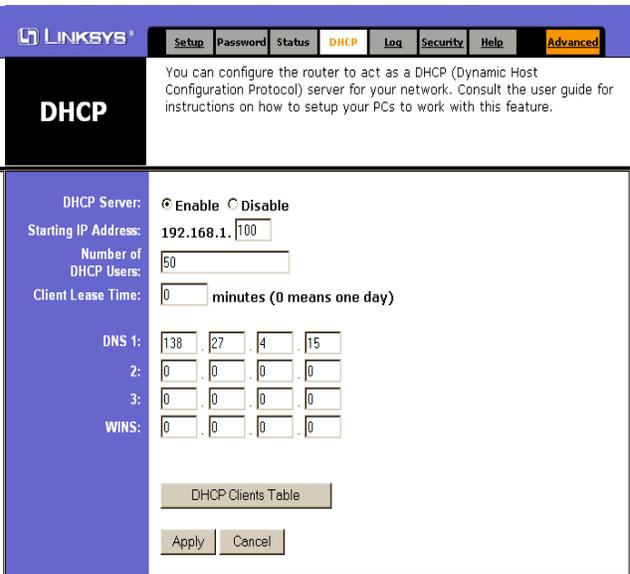


Figure 2-80 Router Factory Default DHCP Tab

- g. Close the web browser.

2.10.4 Disconnection Procedures

1. Disconnect the power supply from the external power source.
2. Disconnect the other end of the power supply from the port labeled “Power” on the back of the router.
3. Disconnect the white straight-through Ethernet cable from the Wired NIC/Built-in NIC on your SSR notebook and the router.

2.11 MANUAL CONFIGURATION OF THE CAISI BRIDGE MODULE (CBM)

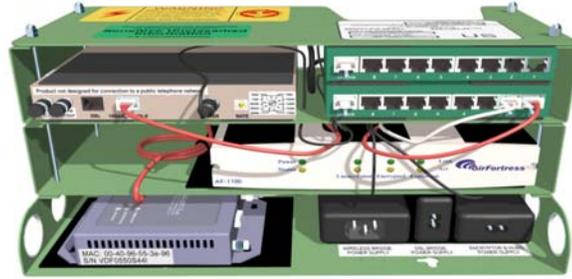


Figure 2-81 CBM

The CBM includes three components that require configuration before it can be put into operation. They are:

1. Wireless Bridge Paragraph 2.11.1
2. Inline Encryptor Paragraph 2.11.6
3. DSL (No software configuration required)
 For physical connection procedures refer to TM 11-5895-1691-12 Paragraph 2.19.1

The following WARNINGS and CAUTIONS apply to the entire lesson.

WARNINGS

- Severe injury or death can occur if this equipment, its antennas, or connected communications cables come near electric 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. This may cause severe injury or death. **Never operate a wireless device without an antenna. It can damage the radio.**

**Five Safety Steps to Follow
If Someone Is the Victim of Electrical Shock
WARNINGS**

- Do not try to pull or grab the individual.
- If possible, turn off the electrical power.
- If you cannot turn off the electrical power, push, pull or lift the person to safety using a dry wooden pole, a dry rope or some other insulating material.
- Send for help as soon as possible.
- After the injured person is free of contact with the source of electrical shock, move the person a short distance away and immediately start first aid, if necessary.

**UPS BATTERY SAFETY
WARNINGS**

- Batteries can present a risk of electrical shock and burn from high short-circuit current.
- Observe proper precautions.
- Do not open the UPS or the batteries.

**UPS INSTALLATION SAFETY
CAUTIONS**

- 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
CAUTIONS**

- 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.

CAUTIONS

- Never connect cables when the power is on.
- Never pull directly on cables.
- Always connect and disconnect using the plugs at the ends 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 that plugs match their connectors before installing.
- Make sure the UPS power is OFF before inserting its plug into an external power source.

CAUTION

The CAISI Bridge Module (CBM) transit case weighs 46 pounds. Use safe lift and carry procedures when handling the transit case. This is a two-person lift and carry.

SECURITY CONSIDERATIONS

- The radios are in the unprotected zone and you cannot communicate with them from the protected zone.
- 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. Nor are the DSL links encrypted because they are a part of the protected distribution system (PDS).
- Due to security vulnerabilities you should not remotely configure the radios. To configure a radio you should connect to the console port.
- There is no reset button or “zeroize” switch to reset or remove the configuration, encryption key, or passwords. The wireless bridges 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.

2.11.1 Physical Connection Procedures

NOTE: *Ensure an antenna is connected to the CBM IAW procedures outlined TM 11-5895-1691-12 Paragraph 2.18 before performing the following procedures.*

1. Connect CBM power cables.
 - a. Remove the UPS, a 3-prong and a 2-prong power cable 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 cable 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.**



Figure 2-82 CBM Power Cable Connections

2. Connect CBM wireless bridge to notebook wired NIC/built-in NIC.
 - a. Disconnect the red crossover cable from the port labeled “Encrypted” on the back of the encryptor.
 - b. Remove the RJ-45 straight-through adapter and a straight-through Ethernet 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 NIC.
 - e. You are now connected from your NIC to the “Network” port on the power injector.

NOTE: *If the wireless bridge is not installed in a CBM, refer to TM 11-5895-1691-12, Paragraph 2.32.1.1 for physical connection procedures.*

2.11.2 Configuration of the CBM Wireless Bridge

The wireless bridges issued to the SSR from TYAD will be preset to the CAISI standard configuration. This includes the bridges in the SSR Accessory Kits as well as the bridges installed in the CBMs. **At a minimum, the SSR needs to change the SSID, WEP key, and passwords.** Additionally, the SSR needs to ensure that one of the CBM bridges in each CAISI is set to the root bridge mode.

If the wireless bridge password has been lost, the bridge will need to be reset to factory defaults and configured from scratch. For procedures on configuring the wireless bridge from scratch refer to Paragraph 2.11.2.2.

2.11.2.1 Minimum Configuration of a Preset CBM Wireless Bridge

NOTE: *A standard CAISI SSR notebook, configured as follows is required for wireless bridge set up. It 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. Wired NIC or Built-in NIC must be used.*

1. Connect a straight-through nine-pin serial cable (blue) from your terminal's serial port to the serial port on the bridge. Your "terminal" will normally be the CAISI notebook, but can be any computer running Blast or Hyperterm.
2. Apply power to the SSR Notebook.
3. Enter your username and password. The CAISI defaults are "**caisiadmin**" and "**BS_69dlw**".
4. A Logon Message prompt will appear, "Your password expires today. Do you want to change it now?" For classroom training, click on the "**No**" button.
5. At the bottom of the SSR notebook screen, click on ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear. Click on "**Hyperterm COM1 (9,600)**".
6. Apply power to the bridge by pressing the "**I**" (ON) side of the UPS rocker switch in. Watch the lights.
7. Watch the terminal screen. When the "**Please enter your username**" message appears on the console "Summary Status" screen, enter the CAISI default username "**root**" and press the <**Enter**> key.
8. At the password prompt enter the CAISI default password "**system**" and press the <**Enter**> key. If you have previously configured the bridge, enter your root password instead.

The Home screen, also known as the Summary Status screen will appear, as shown in Figure 2-83.

```

BR350-41c715  [Cisco 350 Series Bridge 12.01T]  Uptime: 00:00:22
-----
Associations
[Clnts: 0] of 0  [Rptrs: 0] of 0  [Brdgs: 0] of 1  [APs]: 0
-----
Events
  Time      Severity      Description
00:00:12 (Warning): Lost Authentication with Parent
00:00:12 (Warning): Lost Authentication with Parent
00:00:04 (Warning): Lost Authentication with Parent
00:00:04 (Warning): Lost Authentication with Parent
00:00:04 (Warning): Lost Authentication with Parent
-----
Network Ports                                     ====[Diagnostics]===
  Device      Status      Mb/s      IP Addr.   MAC Addr.
[Ethernet]    Up          100.0     192.168.1.4  00409641c715
[Bridge Radio] No Link     11.0      192.168.1.4  00409641c715
-----
Home - [Network] - [Associations] - [Setup] - [Logs] - [Help] (Auto Apply On) ^R, =,
<ENTER>, or [Link Text]:

```

Figure 2-83 Wireless Bridge Console - Summary Status Screen

Explanation of Figure 2-83

The bridge name, firmware version, and uptime are shown at the top of the screen. The association status is on the next line. Because this is a non-root radio and no root is present, there are no associations. The events in the following area are warnings that association has been lost. Actually, no association has yet been established; but this is where it would show if there were a root present.

Below the events are the statuses of the two interfaces (Ethernet and Radio) including the connection speed, IP address and MAC address for each. The screen above shows that the Ethernet interface is up because the SSR notebook is connected, ready to continue the configuration in the browser.

If the bridge is new from TYAD, web browsing is still enabled and you can switch to the browser at this point. If the bridge has been deployed in your unit, you previously changed the SSID, WEP key, and passwords and disabled remote access. So you need to re-enable remote access before switching to the browser.

- From the Home screen, enter an “S” to jump to the setup screen, shown on Figure 2-84. This screen is essentially the main menu. This screen does not require setup it serves as a gateway to the configuration screens.

```

BR350-41c715      Setup      Uptime: 00:20:12
====[Express Setup]====
                Associations
[Defaults Associations]  [Address Filters]      [Advanced]
[Spanning Tree]        [Port Assignments]

                Event Log
[Defaults Event]       [Event Handling]        [Notifications]

                Services
[Console/Telnet] [Boot Server]  [Routing]      [Name Server]
[Time Server]   [FTP]          [Web Server]   [SNMP]

                [Cisco Services]          [Security]

                Network Ports      ==== [Diagnostics] ====
[Id Ethernet]  [Hw Ethernet]  [Fltr Ethernet]  [Adv Ethernet]
[Id Bridge Radio] [Hw Bridge Radio] [Fltr Bridge Radio] [Adv Bridge Radio]
-----
[Home] - [Network] - [Associations] - Setup - [Logs] - [Help]
[END]
(Auto Apply On) :Back, ^R, =, <ENTER>, or [Link Text]:

```

Figure 2-84 Wireless Bridge Console - Setup Screen

10. From the Setup screen, enter a “W” to jump to the Web Server Setup screen, shown on Figure 2-85.

```

BR350-41c715      Web Server Setup      Uptime: 00:20:12

[Allow Non-Console Browsing?][_]
HTTP [Port          ][80  ]

Default [HelpRoot
URL][http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/air/ap3x
x]

[Extra Web Page File ][          ] [LoadNow]
Default [WebRoot URL ][mfs0:/StdUI/          ]

[Apply] [OK] [Cancel] [Restore Defaults]
-----
[Home] - [Network] - [Associations] - [Setup] - [Logs] - [Help]
[END]
(Auto Apply On) :Back, ^R, =, <ENTER>, or [Link Text]:

```

Figure 2-85 Wireless Bridge Console - Web Server Setup Screen

11. If there is not an “X” between the square brackets after [Allow Non-Console Browsing?], type the command “AL” and the prompt at the bottom of the screen will fill in the rest of the command: **(Auto Apply On) :Back, ^R, =, <ENTER>, or [Link Text]: Allow Non-Console Browsing?** Press the <Enter> key to complete the command. An “X” will now appear after [Allow Non-Console Browsing?], as shown on Figure 2-86.

```
BR350-41c715      Web Server Setup      Uptime: 00:33:14
[Allow Non-Console Browsing?][X]
HTTP [Port          ][80          ]
Default [HelpRoot
URL][http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/air/ap3x
x]
[Extra Web Page File ][          ] [LoadNow]
Default [WebRoot URL ][mfs0:/StdUI/          ]
[Apply] [OK] [Cancel] [Restore Defaults]
-----
[Home] - [Network] - [Associations] - [Setup] - [Logs] - [Help]
[END]
(Auto Apply On) :Back, ^R, =, <ENTER>, or [Link Text]:
```

Figure 2-86 Wireless Bridge Console – Non-Console Browsing Allowed

12. Type the command “AP” and press the <Enter> key to apply it.

NOTE: *Before Proceeding –From this point forward, all configurations can be done in a web browser instead of the console, if you prefer. The screens are identical. If you choose to continue configuration through the console you need not allow non-console browsing. If you remain in the console, visualize the console screen as a web page.*

Like a web-based product, the texts between square brackets are links. For instance, if this were a web screen and you clicked on [Setup] you would jump to the setup screen.

As you type a command at the colon prompt at the bottom of the screen, the console interface will automatically fill in the remainder of the value as soon as it recognizes the link that you are trying to access and will load the next screen as if it was a jump button.

If it is a data entry button, press enter as soon as it completes the command for you. You will then get a prompt asking you for input, or telling you the appropriate values and asking you for input.

When you input a value, it is not immediately saved or acted upon. Enter “ap” and the “apply” command will fill in. Press <Enter> to apply your change.

At any colon prompt, you can press “=” (the equals sign key) to jump directly to the “Home” screen. This is sometimes necessary because there is no “back” button.

Continue configuration of the wireless bridge in a web browser.

13. Open Internet Explorer on the notebook desktop.
 - a. In the address toolbar at the top of Explorer, enter the IP address assigned to the wireless bridge. In this case enter the CAISI default IP - **192.168.1.3** (CBM root) or **192.168.1.4** (non-root).
 - b. Click on **“GO”** on the Explorer toolbar or click on **“Enter”** on the notebook keyboard.
 - c. The **“Enter Network Password,”** screen will appear.
 - 1) You will be prompted for a user name and password.
 - 2) Enter **“root”** in the **“User Name”** field.
 - 3) Enter the CAISI default is password, **“system”** in the **“Password”** field.
 - 4) Click on **“OK”**.
14. Click on the **“Setup”** button near the top of the screen, or the **“[Setup]”** hyperlink near the bottom of the screen.

The Setup Menu will appear.

BR350-51e694 Summary Status				
Cisco 350 Series Bridge 12.01T				
Home	Map	Network	Associations	Setup Logs Help
Uptime: 01:59:30				
Current Associations				
Clients: 0 of 0	Repeaters: 0 of 0	Bridges: 0 of 1	APs: 0	
Recent Events				
Time	Severity	Description		
00:52:26	Warning	Lost Authentication with Parent		
00:52:26	Warning	Lost Authentication with Parent		
00:52:23	Warning	Lost Authentication with Parent		
00:52:23	Warning	Lost Authentication with Parent		
00:37:25	Warning	Lost Authentication with Parent		
Network Ports				
Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	Up	100.0	192.168.1.4	00409651e694
Bridge Radio	No Link	11.0	192.168.1.4	00409651e694

Figure 2-87 Wireless Bridge Summary Status Menu

As mentioned earlier, the Setup screen is really the Main Menu. From here you jump to the actual configuration setup screens, as required. As a reminder: **at a minimum you need to change the SSID, WEP key, and passwords; when you are done, it is recommended remote access to the bridges be disabled as a security precaution.**

15. Click on the **“Express Setup”** hyperlink near the top of the screen.

BR350-51e694 Setup				
Cisco 350 Series Bridge 12.01T				
Home	Map	Network	Associations	Setup Logs Help
Uptime: 00:10:57				
Express Setup				
Associations				
Display Defaults	Spanning Tree	Port Assignments	Advanced	
Address Filters	Protocol Filters	VLAN	Service Sets	
Event Log				
Display Defaults	Event Handling	Notifications		
Services				
Console/Telnet	Boot Server	Routing	Name Server	
Time Server	FTP	Web Server	SNMP	
Cisco Services	Security	Accounting	Proxy Mobile IP	
Network Ports				
Ethernet	Identification	Hardware	Filters	Advanced
Root Radio	Identification	Hardware	Filters	Advanced

Figure 2-88 Wireless Bridge Setup Menu

16. The “Express Setup” menu will appear.
 - a. Set the [Default IP Address] as required, for your network or as directed by your DOIM, S6 or CSSAMO. The default for a CAISI root bridge is **192.168.1.3** and non-root **192.168.1.4**
 - b. Set the [Radio Service Set ID (SSID)] as required, for your network or as directed by your DOIM, S6 or CSSAMO. The default for a CAISI bridge is “caisi000”.
 - c. Set the [Role in Radio Network] to “**Non-Root Bridge w/Clients**” unless this will be the root bridge. In that case, set it to “**Root Bridge**”.
 - d. Click on the “**Apply**” button. Click on the “**OK**” button to approve.

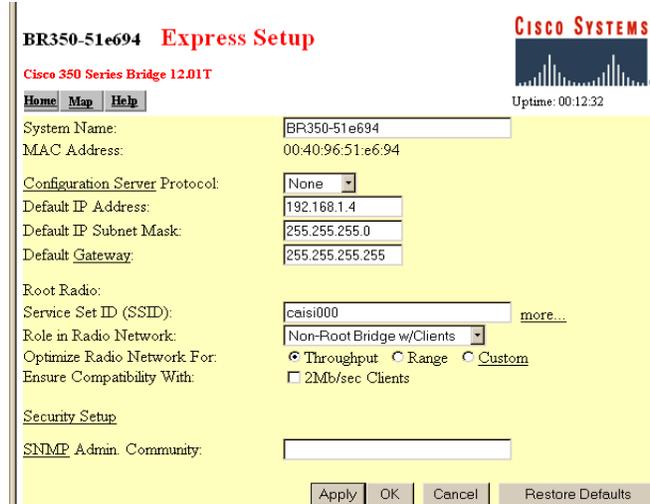


Figure 2-89 Wireless Bridge Express Setup Menu

17. Click on the “**Back**” button to return to the “Setup” screen and then jump to Services, “**Security**”.

18. Click on the “**Radio Data Encryption (WEP)**” hyperlink and the “Root Radio or Bridge Radio Data Encryption” screen will appear.

- a. “Use of Data Encryption by Stations” is already set to “**Full Encryption**”.
- b. The “Key Size” for WEP Key 1 is already set to “**128 bit**”.
- c. All you have to do is enter the new WEP key as prescribed by your DOIM, S6 or CSSAMO into the “Encryption Key” field for WEP Key 1.
- d. Click on the “**Apply**” button. Click on the “**OK**” button to approve.

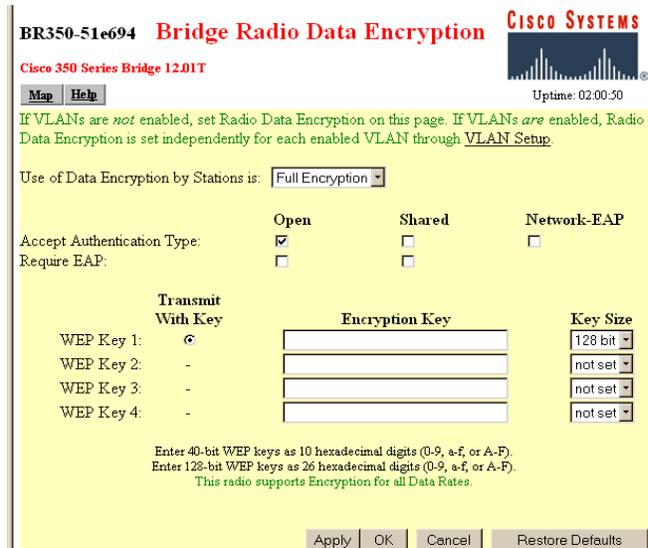


Figure 2-90 Wireless Bridge Radio Data Encryption Screen

19. Click on the **“Back”** button to return to the **“Setup”** screen and then jump to Services, **“Security”**.

- a. Choose **“User Information”** then **“Add New User”**.
- b. Create a root user:
 - 1) In the **“user name”** field type **“root”**.
 - 2) In the **“change password”** field, type your new password as prescribed by your DOIM, S6 or CSSAMO and re-enter to confirm.
 - 3) Ensure all capabilities are selected.
 - 4) Click on the **“Apply”** button.
- c. The **“Enter Network Password”** screen will appear. Enter your new password to confirm it was set successfully.

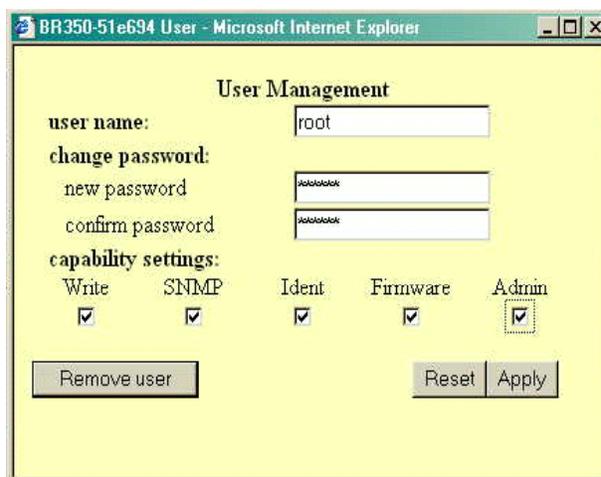


Figure 2-91 Wireless Bridge User Management Screen



Figure 2-92 Wireless Bridge Enter Network Password Screen

20. Create a monitor user.

- a. Choose **“Add New User”**.
 - 1) In the **“username”** field type **“monitor”**.
 - 2) In the **“change password”** field type your new password as prescribed by your DOIM, S6 or CSSAMO and re-enter to confirm.
 - 3) Ensure only the **“Admin”** capability is selected.
 - 4) Click on the **“Apply”** button.

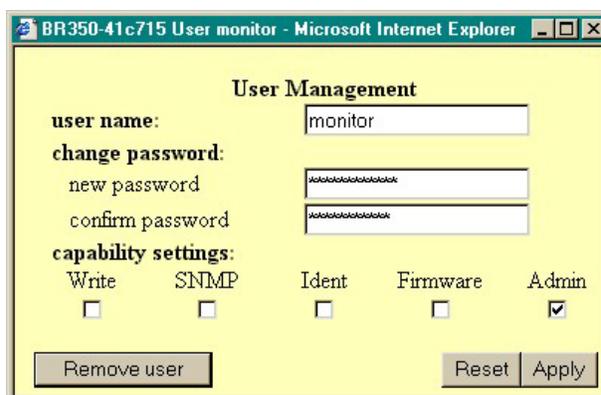


Figure 2-93 Wireless Bridge User Management Screen

NOTE: Write down the new passwords, seal them in an envelope and turn them in to your security officer for safekeeping.

Once you are confident in the configuration of the radios you may avoid wireless network vulnerabilities by disabling Non-Console Browsing.

21. Click on the “**Back**” button to return to the “Setup” screen and jump to Services, “**Web Server**”. The “Web Server Setup” screen will appear.

- a. Click on the “**no**” button next to “Allow Non-Console Browsing”.
- b. Click on the “**Apply**” button. Click on the “**OK**” button to approve.

Nothing will appear to happen. This means that it worked – you lose contact with the bridge because it no longer allows access except through the console port.

Figure 2-94 Wireless Bridge Web Server Setup Screen

Minimum configuration of a preset CBM wireless bridge is complete.

If you are going to proceed with the configuration of the CBM inline encryptor refer to Paragraph 2.11.5 for procedures to disconnect the wireless bridge from the notebook.

If you have performed all necessary configuration procedures involving the wireless bridge and are ready to power down the equipment, refer to Paragraph 2.11.7 for procedures on disconnecting the wireless bridge power cables.

2.11.2.2 Configuration of the CBM Wireless Bridge from Scratch.

If you are issued a wireless bridge direct from the factory, or if you have to reset your bridge because of lost passwords or for any other reason, follow the below procedures to configure the device from scratch.

NOTE: *A standard CAISI SSR notebook, configured as follows is required for wireless bridge set up. It 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. Wired NIC or Built-in NIC must be used.*

1. Connect the blue straight-through nine-pin serial cable from your terminal's serial port to the serial port on the bridge. Your "terminal" will normally be the SSR notebook, but can be any computer running Blast or Hyperterm.
2. Apply power to the SSR notebook.
3. Enter your username and password. The CAISI defaults are "**caisiadmin**" and "**BS_69dlw**".
4. A Logon Message prompt will appear, "Your password expires today. Do you want to change it now?" For classroom training, click on the "**No**" button.
5. At the bottom of the SSR notebook screen, click on ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear. Click on "**Hyperterm COM1 (9,600)**".

NOTE: *You must initially configure the wireless bridges from the console to assign an IP address before you can connect to them over the network.*

6. Apply power to the bridge by pressing the "**I**" (ON) side of the UPS rocker switch in. Watch the lights.
7. Watch the terminal screen. When the, "**Please enter your username**" message appears on the console "Summary Status" screen, press the <**Enter**> key. If you get the "Express Setup" screen, the bridge is at factory defaults and you can skip the next step. Otherwise proceed as follows:
 - a. Immediately enter the command "**:resetall**" (a colon and the words "reset" and "all" – all run together with no spaces between) then press the <**Enter**> key.

THIS PROCEDURE MUST BE COMPLETED WITHIN TWO MINUTES OF APPLYING POWER TO THE BRIDGE.

- b. Type "**yes**" at the "Are you sure?" prompt.
- c. If you get a message telling you that the "**:resetall**" command timed out, cycle power and try again.
 - 1) To cycle power, unplug the Ethernet cable between the power injector and the bridge, wait five seconds, then plug it back in.

- 2) Sometimes a bridge takes so long to boot (because of DHCP timeouts) that there is very little time left for you to sneak the “:resetall” command in before the two-minute time limit.
- 3) Keep trying until the command processes successfully.
- d. Wait for the bridge to reboot. It should come to the “Express Setup” screen when it returns.
8. Set the IP Address, as required for your network or as directed by your DOIM, S6 or CSSAMO as follows. Type “Add” and press the <Enter> key.
9. At the “Enter Address” prompt, enter the address provided by your DOIM, S6 or CSSAMO or enter “192.168.1.4” (for non-root), set to “192.168.1.3” (for root), the default IP for the CAISI Bridge. Press the <Enter> key.
10. Turn DHCP off as follows. Type “pr” and press the <Enter> key. Type “n” then press the <Enter> key.
11. Apply changes as follows. Type “ap” and then press the <Enter> key.

NOTE: From this point forward, all configurations can be done in a web browser instead of the console if you prefer. The screens are identical.

12. Close Hyperterm window.
13. Open your web browser; enter the IP address you assigned to the radio or enter the CAISI default “192.168.1.4” (for non-root), and “192.168.1.3” (for root).
14. Navigate to the “Express Setup” screen.
 - a. From the “Summary Status” menu, select “Setup” then “Express Setup”.

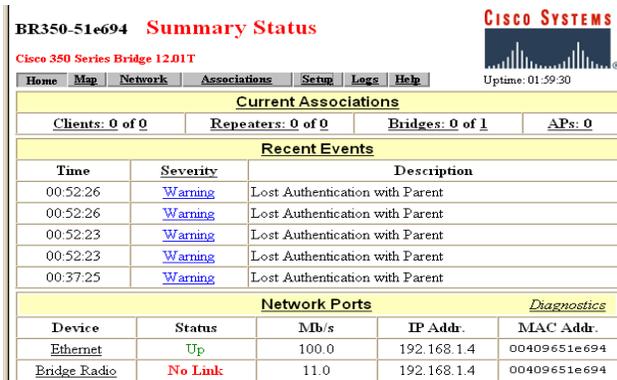


Figure 2-95 Wireless Bridge Summary Status Screen

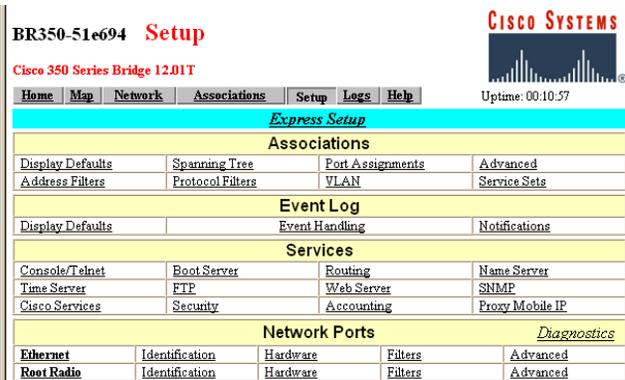


Figure 2-96 Wireless Bridge Setup Screen

- b. The “Express Setup” screen will appear.
- 1) Set the IP [Subnet Mask], as required for your network or as directed by your DOIM, S6 or CSSAMO. The CAISI default is “255.255.255.0”.
 - 2) Set the Default [Gateway], as required for your network or as directed by your DOIM, S6 or CSSAMO. The factory default is “255.255.255.255”.

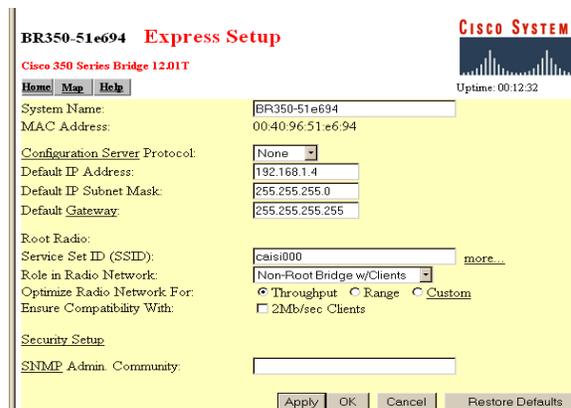


Figure 2-97 Wireless Bridge Express Setup Screen

- 3) Set the [Radio Service Set ID (SSID)] as required, for your network or as directed by your DOIM, S6 or CSSAMO. The CAISI default is “caisi000”.

NOTE: The CAISI default SSID is for hardware testing and classroom training only. The SSR must change the SSID before deploying the radio.

- 4) Set the [Role in Radio Network] to “Non-Root Bridge w/Clients” unless this will be the root bridge. In that case, set it to “Root Bridge”.

- 5) Apply changes; click on the “OK” button to approve.

15. Click on the “Back” button to return to the “Setup” screen and then jump to Services, “Security”.

16. Choose “User Information” then “Add New User”.

17. Create a root user:

- a. In the “user name” field, type “root”.
- b. In the “change password” field type your new password as prescribed by your DOIM, S6 or CSSAMO and re-enter to confirm. The default root password is “system”.
- c. For this user select all capabilities (select all the check boxes).
- d. Click on the “Apply” button.
- e. If the “Enter Network Password” screen appears, enter your new password to confirm it was set successfully.



Figure 2-98 Wireless Bridge User Management Screen



Figure 2-99 Wireless Bridge Enter Network Password Screen

18. Create a monitor user. Choose “**Add New User**”.
19. In the “username” field, type “**monitor**”.
 - a. In the “change password” field type your new password as prescribed by your DOIM, S6 or CSSAMO and re-enter to confirm. The default root password is “**access**”.
 - b. For this user only select the “**Admin**” capability.
 - c. Click on the “**Apply**” button

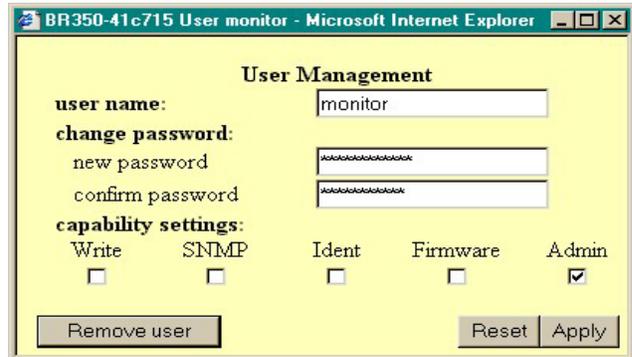


Figure 2-100 Wireless Bridge User Management Menu Screen

NOTE: *The default passwords are for hardware testing and classroom training only. The SSR must change the passwords before deploying the radio. Write down your new passwords, seal them in an envelope and turn them in to your security officer for safekeeping.*

20. Click on the “**Back**” button to return to the “Security Setup” screen, and then jump to “**User Manager**”.
 - a. Set “User Manager” to “**Enabled**”.
 - b. Set “Allow Read-Only Browsing without Login?” to “**no**”.
 - c. Leave “Protect Legal Credit Page” set to “**no**”.
 - d. **Apply** changes; click on the “**OK**” button to approve.
 - e. The “Enter Network Password” screen will appear.
 - 1) Enter “**root**” in the “User Name” field.
 - 2) Enter your new password in the “Password” field. The CAISI default is “**system**”.
 - 3) Click on the “**OK**” button.
 - f. The “User Manager” screen will return.

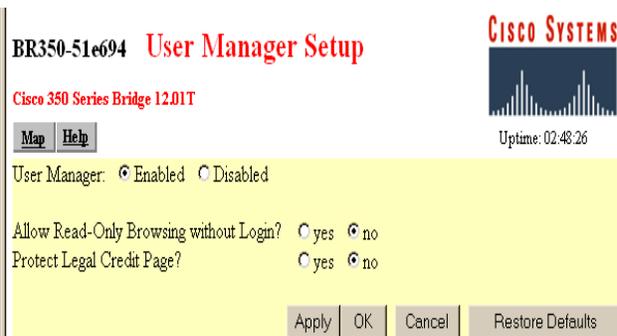


Figure 2-101 Wireless Bridge User Manager Setup Screen



Figure 2-102 Wireless Bridge Enter Network Password Menu

NOTE: You must have defined the users before you can enable the user manager. Otherwise you would lock yourself out of the radio, since there would be no authorized root user.

21. Click on the **“Back”** button to return to the **“Security Setup”** screen then choose **“Radio Data Encryption (WEP)”**.
 - a. Set the **“Key Size”** for key 1 to **“128 bit”**.
 - b. Set the **“Encryption Key”** to a new key as prescribed by your DOIM, S6 or CSSAMO. The CAISI default WEP key is **“0123456789abcdef0123456789”**.
 - c. Click on the **“Apply”** button. Click on the **“OK”** button to approve.

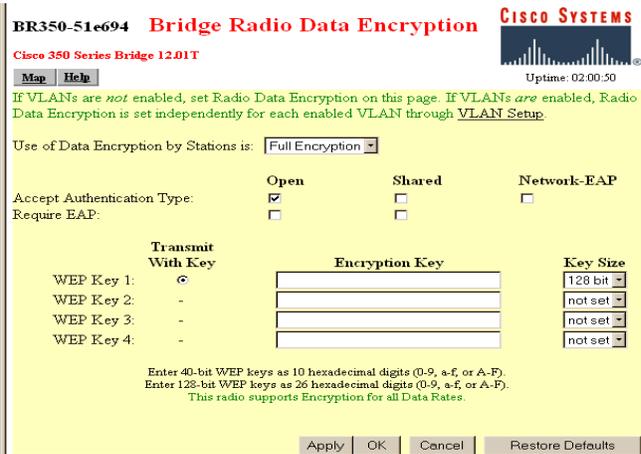


Figure 2-103 Wireless Bridge Radio Data Encryption Screen

NOTE: You must set the key size before you set the encryption key, but if you attempt to apply just the key size it does not take. The CAISI default WEP key is for hardware testing and classroom training only. The SSR must change the WEP key before deploying the radio.

- d. Set **“Use of Data Encryption by Stations”** to **“Full Encryption.”** Leave all other settings at their defaults. **“Accept Authentication type”** is set **“open”** by default. All the others are unset.
- e. Click on the **“Apply”** button. Click on the **“OK”** button to approve.

NOTE: You must set and apply the WEP key size and WEP key before you can turn encryption on. **“Full encryption”** will not be an option until you apply the key.

22. Click on the **“Back”** button to return to the **“Setup”** screen and jump to Network Ports, Root Radio/Bridge Radio **“Hardware”**.
 - a. Set **“Allow Broadcast SSID to Associate”** to **“no”**.
 - b. Set **“World Mode”** to **“yes”**.
 - c. Set **“Frag Threshold”** to **“1024”**.
 - d. Set **“RTS Threshold”** to **“1024”**.
 - e. Set **“Search for less-congested Radio Channel”** to **“yes”**.

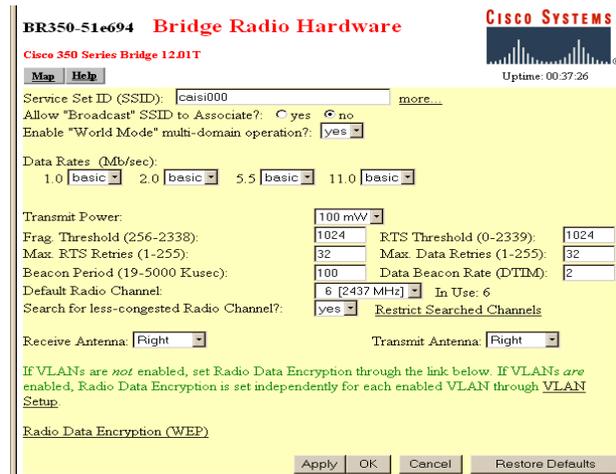


Figure 2-104 Wireless Bridge Radio Hardware Screen

- f. Set both the “Receive Antenna” and “Transmit Antenna” values to “**Right**”.
- g. Click on the “**Apply**” button. Click on the “**OK**” button to approve.
23. Click the “**Back**” button to return to the “Setup” screen and then jump to Services, “**Name Server**”.
- a. Set “**Domain Name System (DNS)**” to “**Disabled**”.
- b. Apply changes. Click on the “**OK**” button to approve.
24. Click the “**Back**” button to return to the “Setup” screen and then jump to Network Ports, Ethernet “**Hardware**”.
- a. Set “**Loss of Backbone Connectivity Action**” to “**NoAction**”.
- b. Apply changes. Click on the “**OK**” button to approve.
25. Click on the “**Back**” button to return to the “Setup” screen and jump to Network Ports, Root Radio/Bridge Radio “**Advanced**”.
- a. Set “Disallow Infrastructure Stations on any other SSID” to “**yes**”.
- b. Set “Require use of Radio Firmware 5.02L” to “**yes**”.
- c. Make sure that “Ethernet Encapsulation Transform” is set to “**RFC1042**”.
- d. Set “Bridge Spacing (km)” to “**6**”.
- e. Scroll down and set “Radio Preamble” to “**long**”.
- f. Click on the “**Apply**” button. Click on the “**OK**” button to approve.

The screenshot shows the 'Bridge Radio Advanced' configuration page for a Cisco BR350 Series Bridge 12.01T. The page is titled 'BR350-51e694 Bridge Radio Advanced' and includes a 'Cisco Syst' logo and 'Uptime: 00:52:36'. The configuration is organized into several sections:

- General Settings:** Requested Status (Up), Current Status (Up), Packet Forwarding (Enabled), Forwarding State (Blocking), Default Multicast Address Filter (Allowed), Maximum Multicast Packets/Second (0).
- Radio Cell Role:** Radio Cell Role (Repeater/Non-PoP), SSID for use by Infrastructure Stations (such as Repeaters) (0).
- Advanced Settings:** Disallow Infrastructure Stations on any other SSID (yes), Use Aironet Extensions (yes), Classify Workgroup Bridges as Network Infrastructure (yes), Require use of Radio Firmware 5.02L (yes), Ethernet Encapsulation Transform (RFC1042), Bridge Spacing (km) (6).
- Quality of Service Setup:** Enhanced MIC verification for WEP (None), Temporal Key Integrity Protocol (None), Broadcast WEP Key rotation interval (sec) (0 (Off)).
- Advanced Primary SSID Setup:** Preferred Access Point 1, 2, 3, and 4 (all set to 00:00:00:00:00:00).
- Radio Modulation:** Radio Modulation (Standard), Radio Preamble (Long).

Buttons for 'Apply', 'OK', 'Cancel', and 'Restore Default' are visible at the bottom right of the configuration area.

**Figure 2-105 Wireless Bridge
Radio Advanced Screen**

26. Click on the **“Back”** button to return to the **“Setup”** screen and jump to Event Log, **“Notifications”**.
 - a. At **“Should Notify-Disposition Events generate SNMP Traps?”** click on **“No”**.
 - b. At **“Should Notify-Disposition Events generate Syslog Messages?”** click on **“No”**.
 - c. Leave all other settings at defaults.
 - d. Click on the **“Apply”** button. Click on the **“OK”** button to approve.

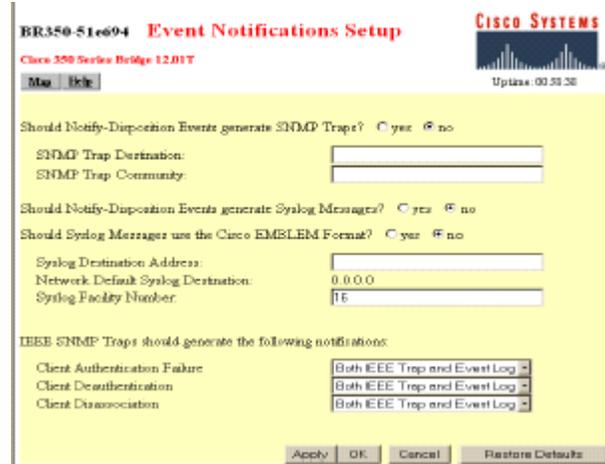


Figure 2-106 Wireless Bridge Event Notifications Setup Screen

27. Click on the **“Back”** button to return to the **“Setup”** screen and jump to Services, **“FTP”**.
 - a. Set the protocol to **“FTP”**.
 - b. Set Default File Server to **“192.168.1.2”** or the address of your SSR notebook.
 - c. Set the FTP directory to **“C:\net tools\aironet\firmware”**.
 - d. Set the user name to **“caisiadmin”**.
 - e. Set the password to your password or to the default. The default is **“BS_69dlw”**.
 - f. Click on the **“Apply”** button. Click on the **“OK”** button to approve.



Figure 2-107 Wireless Bridge FTP Setup Screen

28. At this time, the CAISI default configuration is complete. Click the **(x)** at the top right of the screen to close the web browser.

2.11.3 Verify Operational Status of the CBM Wireless Bridge

1. Open Internet Explorer on the notebook desktop.
2. In the address toolbar at the top of Explorer, enter the IP address with which you gave the wireless bridge during configuration. In this case enter the IP - **192.168.1.3** (CBM root) or **192.168.1.4** (non-root).
3. Click on “**GO**” on the Explorer toolbar or click on “**Enter**” on the notebook keyboard.
4. If the “**Enter Network Password**” screen appears:
 - a. Enter the user name and password you previously assigned the device. The CAISI default user name is “**root**” and the default password is “**system**”.
 - b. Click on the “**OK**” button.
5. To confirm that the wireless bridge is configured navigate to the “**Express Setup**” screen.
 - a. If you successfully configured the wireless bridge, you should see the SSID you assigned it or the CAISI default SSID, **caisi000**.
 - b. At factory defaults, the SSID is tsunami.

BR350-51e694 Express Setup

Cisco 350 Series Bridge 12.01T

Home Map Help

Uptime: 00:12:32

System Name: BR350-51e694

MAC Address: 00:40:96:51:e6:94

Configuration Server Protocol: None

Default IP Address: 192.168.1.4

Default IP Subnet Mask: 255.255.255.0

Default Gateway: 255.255.255.255

Root Radio:

Service Set ID (SSID): caisi000 more...

Role in Radio Network: Non-Root Bridge w/Clients

Optimize Radio Network For: Throughput Range Custom

Ensure Compatibility With: 2Mb/sec Clients

Security Setup

SNMP Admin. Community:

Apply OK Cancel Restore Defaults

Figure 2-108 Wireless Bridge Configured Express Setup Screen

BR350-51e694 Express Setup

Cisco 350 Series Bridge 12.01T

Home Map Help

Uptime: 00:12:32

System Name: BR350-51e694

MAC Address: 00:40:96:51:e6:94

Configuration Server Protocol: None

Default IP Address: 192.168.1.4

Default IP Subnet Mask: 255.255.255.0

Default Gateway: 255.255.255.255

Root Radio:

Service Set ID (SSID): tsunami more...

Role in Radio Network: Root Bridge

Optimize Radio Network For: Throughput Range Custom

Ensure Compatibility With: 2Mb/sec Clients

Security Setup

SNMP Admin. Community:

Apply OK Cancel Restore Defaults

Figure 2-109 Wireless Bridge Default Express Setup Screen

2.11.4 Disable Remote Access to the CBM Wireless Bridge

Once you are confident in the configuration of the radios you may avoid wireless network vulnerabilities by disabling Non-Console Browsing.

1. Disable remote access to the bridge.
 - a. Click **“Back”** to return to the **“Setup”** screen and jump to Services, **“Web Server”**.
 - b. Click on the **“no”** button next to **“Allow Non-Console Browsing?”**
 - c. Click on the **“Apply”** button. Click on the **“OK”** button to approve.



Figure 2-110 Wireless Bridge Web Server Setup Screen

Nothing will appear to happen. This is normal – you lose contact with the bridge because it no longer allows access except through the console port.

2.11.5 Disconnect CBM Wireless Bridge from the Notebook Computer.

1. Disconnect the standard serial cable from the serial port on the CBM wireless bridge and the serial port on the notebook.
2. Disconnect the white straight-through cable from the Wired NIC/Built-in NIC and the RJ-45 straight-through adapter.
3. Disconnect the red crossover cable from the RJ-45 straight-through adapter.
4. Re-attach the red crossover Ethernet cable to the **“external”** or **“encrypted”** port on the back of the encryptor.

If you have performed all necessary configuration procedures involving the wireless bridge and are ready to power down the equipment, refer to Paragraph 2.11.7 for procedures on disconnecting the wireless bridge power cables.

2.11.6 Configure CBM Inline Encryptor

The encryptors issued to the SSR from Tobyhanna Army Depot will be preset to the CAISI standard configuration. This includes the encryptors in the SSR Accessory Kits as well as the encryptors installed in the CBMs/CCMs. **At a minimum, the SSR needs to change the Access ID and passwords.**



Figure 2-111 Inline Encryptor

SECURITY CONSIDERATIONS

- You must periodically change the Access IDs.
- Due to security vulnerabilities you should not remotely configure the encryptor.

2.11.6.1 Configure the CBM Inline Encryptor from Scratch Using the Console Port

NOTE: *A standard CAISI SSR notebook, configured as follows is required for inline encryptor set up. It 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. The wired NIC or built-in NIC must be used.*

1. Ensure the encryptor is receiving power. Refer to physical connection procedures in paragraph 2.11.1.

NOTE: *If the encryptor is not installed in a CBM, refer to TM 11-5895-1691-12, Paragraph 2.32.1.1 for physical connection procedures.*

2. Connect your notebook to the serial port of the encryptor with the beige nine-pin female to nine-pin female null model (crossover) serial cable from the SSR Accessory Kit.
3. Ensure the notebook is receiving power.
4. Enter your user name and password. The CAISI defaults are **caisiadmin** and **BS_69dlw**.
5. If the following Logon Message appears, “Your password expires today. Do you want to change it now?” Click on the “**No**” button. Once you are issued the notebook you can change this password as prescribed by your DOIM, S6 or CSSAMO.

NOTE: *If the encryptor needs to be reset back to factory defaults, skip to step # 10.*

6. At the bottom of the SSR notebook screen, click on ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear. Select “**Hyperterm COM1 (38,400)**”.

7. When the Com1 38400 HyperTerminal screen appears, press the <Enter> key.
8. At the Air Fortress login prompt, enter the administrator username and press the <Enter> key. Both the factory default and CAISI default usernames are “**sysadm**”.
9. A password prompt will appear, type in the CAISI default password: “**system**” or “**system00**” (if the firmware version on the encryptor is 1178W or later), “**sysadm**” (factory default) or the password you previously assigned the device and press the <Enter> key.

NOTE: *To check the encryptor firmware version perform procedure #19 below to logon to the encryptor via the web. Click on the “**Help**” button in the menu panel on the left side of the screen. Then click on the “**ver**” hyperlink near the bottom of the help topic list when it appears.*

10. If the password has been lost, **reset the encryptor to factory defaults**.
 - a. If Hyperterm is currently running close the session.
 - b. At the bottom of the SSR notebook screen, click on ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear. Select “**Hyperterm COM1 (38,400)**”.
 - c. When the Com1 38400 HyperTerminal screen appears, press the <Enter> key.
 - d. Cycle the encryptor power by disconnecting the single power lead from the back of the encryptor and then reconnecting it. You will hear a loud beeping sound. This is normal and will cease when the encryptor has completed the boot up process.
 - e. At the Air Fortress Log in prompt, enter **default_reset** as both the username and password. (**This procedure must be completed within 2 minutes of cycling power**).
 - f. When the Air Fortress has finished rebooting, (the loud steady beeping sound has stopped) log back in with the factory default username and password, “**sysadm**”.
 - g. Traffic at this point will stop flowing as soon as you log on.
11. Enter the **set engine crypto aes** command and press the <Enter> key.
12. Enter the **set engine accessid** command and press the <Enter> key.
 - a. You will be prompted for the new access ID. The Access ID is the pre-shared key used to initiate key negotiations amongst the encryptors.
 - b. At the “New Access ID” prompt, set the key to the new 16-digit hexadecimal number Access ID prescribed by your DOIM, S6 or CSSAMO and re-enter to confirm.

NOTE: *The Access ID is not shown in the clear so nothing will appear as you type.*

- c. For classroom training and hardware testing set the Access ID to the CAISI default, **0123456789abcdef**.

NOTE: *You may be prompted for the old key. If the encryptor is fresh from Tobyhanna, use the CAISI default. If you don't know the old key, reset the encryptor and configure it from scratch. In order to communicate, all encryptors and remote clients that will be on the same network (where the radios have the same SSID) must have the same key.*

13. Enter the **set engine rekey 2** (CAISI default) command and press the <Enter> key.
14. Enter the **passwd sysadm** command and press the <Enter> key.
 - a. Enter your new password as prescribed by your DOIM, S6 or CSSAMO and re-enter to confirm when prompted.
 - b. For classroom training set the new password to the CAISI default, “**system00**” when prompted.

NOTE: *Write down the new password, seal it in an envelope and turn it in to your security officer for safekeeping. If you lose it, you will have to reconfigure the encryptor from scratch.*

15. Set the IP address.
 - a. The factory default address for the encryptor is **192.168.254.254**.
 - 1) You may change the address to any address that does not conflict with you network.
 - 2) To do so, enter the **set device ip** command and press the <Enter> key.
 - 3) For classroom training, enter “**set device ip 192.168.254.254**”, the factory default IP address. (You can leave it set to this IP address).
16. Enter the **exit** command to log out and press the <Enter> key.

NOTE: *If you forget to logout, the https procedures in the following steps will not work.*

17. Minimize Hyperterm.

NOTE: *You can only set the encryptor browser password and perform firmware upgrades in the web browser.*

18. Connect your notebook NIC to the hub in a CBM/CCM with a white straight-through Ethernet cable.
19. Open Internet Explorer.
 - a. Use the secure web browser to connect to the encryptor, as follows:
 - b. Enter the factory default IP address “**https://192.168.254.254**” or your own previously assigned encryptor address in the browser address bar.

NOTE: *Notice that using the browser in secure mode (**https** instead of **http**) means that you must type in the entire command, not just the address.*

- c. When the Security Alert appears click on the “OK” button.



Figure 2-112 Encryptor Security Alert - 1

- d. A second Security Alert will appear click on the “Yes” button.

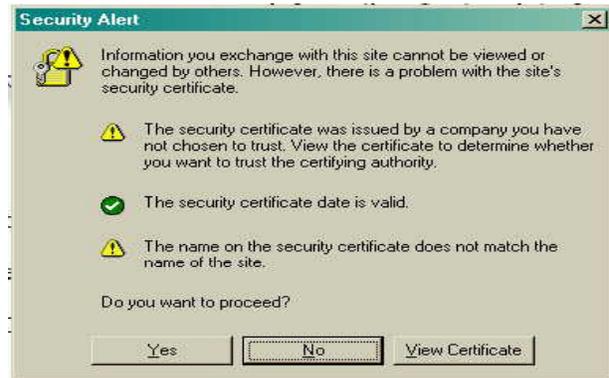


Figure 2-113 Encryptor Security Alert - 2

NOTE: To access the encryptor from the web, a different username and password than that which you used in the console is required. The default web access username is “admin” and cannot be changed. You can only change the password.

- e. The “Enter Network Password” screen will appear.
 - 1) You will be prompted for a user name and password.
 - 2) Enter “admin” (factory default) in the “User Name” field.
 - 3) Enter one of the following passwords in the “Password” field: “admin” (factory default), “system00” (CAISI default), or the password you assigned the device as prescribed by your DOIM, S6 or CSSAMO.
 - 4) Click on the “OK” button. The welcome screen will appear.

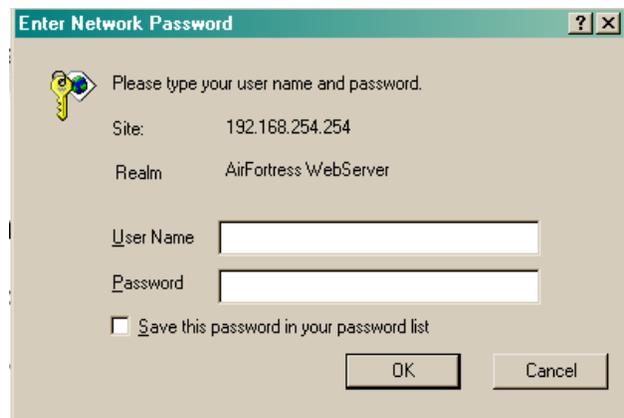


Figure 2-114 Encryptor Enter Network Password

NOTE: *If the password is lost, reset the encryptor to factory defaults and begin again at step 1). You will need to redo the console settings as well as the web settings.*

20. Click on the “**User Access**” button in the menu panel on the left side of the screen. The User Access screen will appear.
 - a. Enter the old password “**admin**” (factory default), “**system00**” (CAISI default) or your current one, as appropriate in the “**Current Password**” field.
 - b. Enter your new password in the “**New Password**” and “**Retype New Password**” fields. The CAISI default is “**system00**”.
 - c. Click on the “**OK**” button.

Figure 2-115 Encryptor User Access Screen

21. Click on “**Help**”, the “**Enter Network Password**” screen will appear.
 - a. Enter your new password to verify it has successfully been changed.
 - b. Click on the “**OK**” button.

NOTE: *Write down the new password, seal it in an envelope and turn it in to your security officer for safekeeping.*

22. Verify encryptor is configured.
 - a. To confirm the encryptor settings you configured in Hyperterm are set; click on the “**LAN SETTINGS**” button.
 - 1) The Air Fortress default IP address should appear **192.168.254.254**.
 - 2) However, if you changed the encryptor IP address you should see the IP Address you assigned the device.

Figure 2-116 Encryptor LAN Settings Screen

b. Alternatively, click the “**SECURITY SETTINGS**” button.

1) The CRYPTO ALGORITHM should be set to **AES**. (Advanced Encryption Standard)

2) Click “**OK**”.

NOTE: *You already set the RE-KEYING INTERVAL and the ACCESS ID in the Hyperterm session.*



Figure 2-117 Encryptor Security Settings Screen

23. Close web browser.

24. Maximize Hyperterm window.

- a. Log back in using the following procedures:
- b. A username prompt will appear, enter the CAISI default username, “**sysadm**” and press the <Enter> key.
- c. A password prompt will appear, type in the CAISI default password: “**system**” or “**system00**” (if the firmware version on the encryptor is 1178W or later), “**sysadm**” (factory default) or the password you previously assigned the device and press the <Enter> key.
- d. Enter the “**enable fips**” command and press the <Enter> key. You are required to operate in FIPS mode.

IMPORTANT PROCEDURAL NOTE: *After all or any actions involving “https” you should disable web access to the encryptor.*

25. Enter the “**disable ssh**” command and press the <Enter> key.

26. Enter the “**disable afweb**” command and press the <Enter> key.

27. Enter the “**exit**” command and press the <Enter> key to log out.

IMPORTANT PROCEDURAL NOTE: *As long as you are logged in to the encryptor console port, traffic will not flow through the encryptor. You must log out when you are finished with the configuration.*

Configuration of the encryptor is now complete.

28. Disconnect the nine-pin female to nine-pin female null model (crossover) serial cable from your notebook and from the serial port of the encryptor.
29. Disconnect the white straight-through Ethernet cable from the NIC in the SSR notebook and the CBM hub.

Refer to Paragraph 2.11.7 for encryptor power cable disconnection procedures.

NOTES

If you immediately try to connect to another encryptor device using the same default IP address, you will likely get a “not found” error. Your computer actually connects to the device by its MAC address. And your computer thinks that it knows the MAC address of the encryptor because you just tried to connect to the same IP address. But it’s wrong, because you just changed encryptors and the new one has the same IP address as the old one but its MAC is different.

Confusion can also arise when you change the IP address of the encryptor or any device. Your computer still thinks that the MAC is valid for the old IP address. But when it tries to contact the new IP address it gets the same MAC for it. Now it gets confused, because there are two entries in memory (the address resolution protocol (ARP) cache) with the same MAC.

If either situation occurs, it will be short lived. ARP entries are automatically deleted as they time out. Wait a few minutes and try again. If you are curious or in a hurry, open a DOS window on the laptop and enter the command “**arp -a**” to see the arp cache. To fix the problem enter the command “**arp -d 192.168.254.254**” (or whatever the old or duplicate address is) to delete the offending entry. This will clear the address from your arp cache and force your computer to rediscover the MAC address corresponding to the IP address.

2.11.6.2 Configure the CBM Inline Encryptor from Scratch Using the Ethernet Port

Normally you cannot configure the encryptor remotely. The following instructions are provided for completeness only. This is only possible if web access has not been disabled. It also does not work unless you are connected to the internal (trusted) port of the encryptor. This means that you must be at the same site as the encryptor and connected through the Ethernet port. You cannot connect via radio and configure the encryptor.

1. Connect your notebook to an available port on the CBM/CCM hub with a white straight-through Ethernet cable. Or connect directly to the encryptor “Unencrypted” port with a red crossover cable.
2. Use the secure web browser to connect to the encryptor, as follows:
3. Enter the factory default IP address “**https://192.168.254.254**” or your own previously assigned encryptor address in the browser address bar. Notice that using the browser in secure mode (**https** instead of **http**) means that you must type in the entire command, not just the address.

NOTE: *To access the encryptor from the web a different username and password from that which you used in the console is required.*

4. Enter “**admin**” (factory default) as the username and one of the following passwords: “**admin**” (the factory default password), “**system00**” (CAISI default), or your own previously assigned encryptor password. The welcome screen will appear.
5. Click on the “**SECURITY SETTINGS**” button in the menu panel on the left side of the screen. The Security Setting screen will appear.
6. At the top of the screen, choose “**AES**” as the Crypto Algorithm.
7. In the center of the screen, set the re-keying interval to a value between “**1 and 4**”. The factory default is “4”. The CAISI default is “2”.
8. At the bottom of the screen, enter a new 16-digit hexadecimal number in the “**New Access ID**” and “**Confirm New Access ID**” fields. For classroom training, enter the CAISI default Access ID “**0123456789abcdef**”, click on “**OK**”.

NOTE: *If the encryptor is set to factory default you do not need to enter an Access ID in the “Current Access ID” field. However if the encryptor is set to the CAISI default Access ID or you previously changed the ID you must enter your current ID in the “Current Access ID” field in order for your new Access ID to be accepted. If you don’t know the current Access ID, perform the reset procedures above and reconfigure the encryptor.*

NOTE: *The Access ID is the preshared key used to initiate key negotiations amongst the encryptors. The CAISI default key may only be used in classroom training. The key must be changed before the encryptor is deployed.*

NOTE: *In order to communicate, all encryptors and remote clients that will be on the same net must have the same Access ID you are required to change Access ID for SBU systems at least semiannually, or whenever a knowledgeable individual leaves the unit or the Army.*

9. Click on the **“USER ACCESS”** button in the menu panel on the left side of the screen. The User Access screen will appear. Click on the **“OK”** button.
10. Enter the old password **“admin”** (factory default), **“system00”** (CAISI default) or your current one, as appropriate in the “Old Password” field. Enter your new password in the **“New Password”** and “Retype New Password” fields. Click on the **“OK”** button.
11. “Password changed successfully. Please reboot the system by clicking under SYSTEM OPTIONS.” message will appear. Click on the **“OK”** button. You may or may not have to reboot the system. If the login menu promptly appears, you do not have to. Login in with the new password to verify it has successfully been changed.
12. Click on **“SYSTEM OPTIONS”**.
13. Click on the **“OK”** button under “REBOOT UNIT”. The encryptor will reboot. Once the “Status” LED stops blinking, the encryptor is ready for use.
14. Login menu should appear. If not, click on the **“Back”** button or press **“F5”**.
 - a. User Name: “admin” is the CAISI default.
Password: “system00” is the CAISI default that is used for training purposes.
 - b. Click **“OK”**.

NOTE: *Write down the new password, seal it in an envelope and turn it in to your security officer for safekeeping. If you lose it, you will have to reconfigure the encryptor from scratch.*

15. Optionally, you may change the IP address of the encryptor. Its factory default address is **“192.168.254.254”**. You may, of course, change it to any address that does not conflict with your network.
 - a. To do so, click on the **“LAN SETTINGS”** button in the menu panel on the left side of the screen. The LAN Settings screen will appear.
 - b. Change the IP address, subnet mask, and default gateway as prescribed by your DOIM, S6 or CSSAMO. These settings are used only for communication with the encryptor; they are not used to pass traffic.
16. Close the web browser.
17. Ensure that your notebook is connected to the serial port of the encryptor with a nine-pin female to nine-pin female null modem (crossover) serial cable from the SSR Transit case or SSR Notebook case.

18. At the bottom of the SSR notebook screen, click on ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear. Select "**Hyperterm COM1 (38,400)**".
 - a. When the Com1 38400 HyperTerminal screen appears, press the <Enter> key.
 - b. A username prompt will appear, enter the CAISI default username, "**sysadm**" and press "**Enter**".
 - c. A password prompt will appear, type in the CAISI default password: "**system**" or "**system00**" (if the firmware version on the encryptor is 1178W or later), "**sysadm**" (factory default) or the password you previously assigned the device and press the <Enter> key.
 - d. Type the "**passwd sysadm**" command press the <Enter> key.
 - 1) Enter your new password when prompted. Reenter it when prompted.

NOTE: *Write down the new password, seal it in an envelope and turn it in to your security officer for safekeeping. If you lose it, you will have to reconfigure the encryptor from scratch.*

19. Enter the "**disable ssh**" command press the <Enter> key.

IMPORTANT PROCEDURAL NOTE: *After all or any actions involving "**https**" you should disable web access to the encryptor.*

20. Enter the "**disable afweb**" command and press the <Enter> key.
21. Enter the "**exit**" command and press the <Enter> key.
22. Disconnect the white straight-through Ethernet cable from the NIC in the SSR notebook and the CBM hub.
23. Disconnect the null-modem serial cable from the encryptor and the SSR notebook.

If you have performed all necessary configuration procedures involving the inline encryptor and are ready to power down the equipment, refer to Paragraph 2.11.7 for procedures on disconnecting the encryptor power cables.

2.11.7 CBM Power Cable Disconnection Procedures

1. Turn off power to the UPS by pressing the "**O**" (OFF) side of the UPS rocker switch in.
2. Disconnect the UPS from the external power source.
3. Disconnect the wireless bridge, hub and encryptor power cords from the UPS "Battery Backup Protected Outlets".
4. Disconnect the 2-prong power cable from the hub and encryptor power supply.
5. Disconnect the 3-prong power cable from the wireless bridge power supply.

2.12 MANUAL CONFIGURATION OF THE CAISI CLIENT MODULE (CCM)



Figure 2-118 CCM

The CCM includes two components that require configuration before it can be put into operation. They are:

1. Multi-Client Radio Adapter Paragraph 2.12.1
2. Inline Encryptor Paragraph 2.12.6

The following WARNINGS and CAUTIONS apply to the entire lesson.

WARNINGS

- Severe injury or death can occur if this equipment, its antennas, or connected communications cables come near electric 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. This may cause severe injury or death. **Never operate a wireless device without an antenna. It can damage the radio.**

**Five Safety Steps to Follow
If Someone Is the Victim of Electrical Shock
WARNINGS**

- Do not try to pull or grab the individual.
- If possible, turn off the electrical power.
- If you cannot turn off the electrical power, push, pull or lift the person to safety using a dry wooden pole, a dry rope or some other insulating material.
- Send for help as soon as possible.
- After the injured person is free of contact with the source of electrical shock, move the person a short distance away and immediately start first aid, if necessary.

CAUTIONS

- Never connect cables when the power is on.
- Never pull directly on cables.
- Always connect and disconnect using the plugs at the ends 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 that plugs match their connectors before installing.

Security Considerations

- Only the “external” radio link is encrypted, not the “internal” (LAN) link (connected to the hub).
- You must periodically change the encryptor Access IDs.
- Due to security vulnerabilities you should not remotely configure the radios.
- Your network cables from the LSA to the hub in the CCM should be included in your protected distribution system. They are not encrypted – only the radio links are encrypted.

Security Considerations

- The reset button on the radio 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 a SSR reconfigures it.

2.12.1 Physical Connection Procedures

NOTE: *Ensure an antenna is connected to the CCM IAW procedures outlined TM 11-5895-1691-12 Paragraph 2.18 before performing the following procedures.*

1. Connect CCM power cables.
 - a. Remove the 2-prong power cable from the CCM carrying case.
 - b. Connect the female end of the 2-prong power cable to the power supply in the base of the chassis.
 - c. Connect the male end of the 2-prong power cable into an external power source.



Figure 2-119 Power Cable Connections

2. Connect Multi-client radio adapter to notebook wired NIC or built-in NIC.
 - a. The multi-client radio adapter does not have a console port. You can only configure it over the network.
 - b. Disconnect the red crossover cable from the “Encrypted” port on the back of the inline encryptor.
 - c. Remove the RJ-45 straight-through adapter and a white straight-through Ethernet cable from the SSR Notebook case or SSR Transit case.
 - d. Connect the end of the red crossover cable to the RJ-45 straight-through adapter.
 - e. Connect one end of the straight-through Ethernet cable to the RJ-45 straight-through adapter and the other end to the NIC on the SSR notebook.

- f. You are now connected from your NIC to the “Ethernet” port on the multi-client radio adapter.

NOTE: *If the multi-client radio adapter is not installed in a CCM, refer to TM 11-5895-1691-12, Paragraph 2.33.1.2 for physical connection procedures.*

2.12.2 Configuration of the CCM Multi-Client Radio Adapter

The Multi-client radio adapters issued to the SSR from TYAD will be preset to the CAISI standard configuration. This includes the radio adapters in the SSR Accessory Kits as well as the radio adapters installed in the CCMs. **At a minimum, the SSR needs to change the SSID, WEP key, and passwords.**

If the Multi-client radio adapter password or IP address is lost the radio adapter will need to be reset to factory defaults and configured from scratch. For procedures on configuring the radio adapter from scratch refer to Paragraph 2.12.2.2.

2.12.2.1 Minimum Configuration of a Preset CCM Multi-Client Radio Adapter

1. Apply power to the external power source. The lights on the multi-client radio adapter, encryptor and hub in the CCM should come on.
2. Apply power to the SSR notebook.
3. Enter your username and password. The CAISI defaults are “**caisiadmin**” and “**BS_69dlw**”.
4. A Logon Message prompt will appear, “Your password expires today. Do you want to change it now?” For classroom training, click on “**No**”.
5. Open Internet Explorer.
 - a. In the address toolbar at the top of Explorer, enter one of the following 192.168.200.1 (Cisco default) or 192.168.1.5 (CAISI default) or the new IP address you previously assigned the radio adapter and press the <**Enter**> key.

NOTE: *If you don't know the IP address, follow the procedures in Paragraph 2.12.2.2 to configure the radio adapter from scratch.*

- b. Click on “**Go**” on the Explorer toolbar or click the “**Enter**” key on the notebook keyboard.

- c. Click on “**Write Access**”.
- d. Click on “**Allow Config Changes**”.
- e. Select “**Radio**” from the “**Configuration**” menu. The Radio screen will appear.



Figure 2-120 Multi-Client Radio Adapter Main Screen

- 1) Enter your SSID as prescribed by your DOIM, S6 or CSSAMO in the “Service Set Identification” field. The CAISI default is “caisi000”.
- 2) Click on the “**Save**” button.
- 3) Leave all other fields at their defaults.

Item	Value
Service set identification	a string of at least 1 characters <input type="text" value="caisi000"/> <input type="button" value="Save"/>
Allowed bit rates in megabits/second	1 , 1 2 , 1 5.5 , 1 11 , 2 , 2 5.5 , 2 11 , 5.5 , 5.5 11 or 11
Basic bit rates in megabits/second	1 , 1 2 , 1 5.5 , 1 11 , 2 , 2 5.5 , 2 11 , 5.5 , 5.5 11 or 11
Enable world mode	on or off
RTS/CTS packet size threshold	a number of 2400 or less <input type="text" value="1024"/> <input type="button" value="Save"/>
Privacy configuration	
Parent node Id	our parent's network address <input type="text" value="any"/> <input type="button" value="Save"/> or any
Time to look for specified parent	off or a time in seconds <input type="text" value="off"/> <input type="button" value="Save"/>
Maximum number transmit retries	a number from 8 to 64 <input type="text" value="64"/> <input type="button" value="Save"/>
Refresh rate in 1/10 of seconds	a number from 5 to 150 <input type="text" value="100"/> <input type="button" value="Save"/>
Enable the diversity antennas	on or off
Transmit power level	1 , 5 , 15 , 30 or full
Maximum fragment size	a number from 256 to 2048 <input type="text" value="1024"/> <input type="button" value="Save"/>
Enable radio options	a password <input type="text"/> <input type="button" value="Save"/>

Figure 2-121 Multi-Client Radio Adapter Radio Screen - 1

NOTE: The SSID must match the root radio’s SSID in order to know what network to join. The CAISI default SSID is for hardware testing and classroom training only. The SSR must change the SSID before deploying the radio.

NOTE: You can make only one change at a time. If the field has a “Save” button next to it, you must use the button to save changes to that field. If you make several changes at once, only the one whose button you selected will be changed. The other changes will be lost.

- 6. Click on “**Privacy configuration**” on the radio screen and the privacy screen will appear.

Item	Value
Service set identification	a string of at least 1 characters <input type="text" value="caisi000"/> <input type="button" value="Save"/>
Allowed bit rates in megabits/second	1 , 1 2 , 1 5.5 , 1 11 , 2 , 2 5.5 , 2 11 , 5.5 , 5.5 11 or 11
Basic bit rates in megabits/second	1 , 1 2 , 1 5.5 , 1 11 , 2 , 2 5.5 , 2 11 , 5.5 , 5.5 11 or 11
Enable world mode	on or off
RTS/CTS packet size threshold	a number of 2400 or less <input type="text" value="1024"/> <input type="button" value="Save"/>
Privacy configuration	
Parent node Id	our parent's network address <input type="text" value="any"/> <input type="button" value="Save"/> or any
Time to look for specified parent	off or a time in seconds <input type="text" value="off"/> <input type="button" value="Save"/>
Maximum number transmit retries	a number from 8 to 64 <input type="text" value="64"/> <input type="button" value="Save"/>
Refresh rate in 1/10 of seconds	a number from 5 to 150 <input type="text" value="100"/> <input type="button" value="Save"/>
Enable the diversity antennas	on or off
Transmit power level	1 , 5 , 15 , 30 or full
Maximum fragment size	a number from 256 to 2048 <input type="text" value="1024"/> <input type="button" value="Save"/>
Enable radio options	a password <input type="text"/> <input type="button" value="Save"/>

Figure 2-122 Multi-Client Radio Adapter Radio Screen - 2

- a. Click on “Set the keys”.

Item	Value
Encrypt radio packets	off , on , mixed on or mixed off
Authentication mode	open or shared key
Set the keys	
Key number for transmit	a key number from 1 to 4 <input type="text" value="1"/> <input type="button" value="Save"/>

Figure 2-123 Multi-Client Radio Adapter Privacy Screen

- b. Enter “1” as the key number.
Click on the “Save” button.

Enter a key number from 1 to 4

[Abort](#)

Figure 2-124 Multi-Client Radio Adapter Enter Key Number Screen

- c. Enter your WEP key and click on “Save” you will need to repeat this procedure. The default CAISI WEP key on radios from Tobyhanna is **0123456789abcdef0123456789**

Enter a key of hex digits

[Abort](#)

Figure 2-125 Multi-Client Radio Adapter Set WEP Key Screen

- d. Leave all other fields at their defaults.

NOTE: *The CAISI default WEP key is for hardware testing and classroom training only. The SSR must change the WEP key before deploying the radio.*

- 7. Select “Console” from the Configuration menu.
- 8. Select “Set write privilege password”.

Item	Value
Set readonly privilege password	
Set write privilege password	
Display the remote operator list	
Add an operator host	a network address or an IP address <input type="text"/> <input type="button" value="Save"/>
Remove an operator host	all , a network address or an IP address <input type="text"/> <input type="button" value="Save"/>
SNMP community properties	
Terminal type	teletype , ansi or colour
Console expects complete lines	on or off

Figure 2-126 Multi-Client Radio Adapter Console Screen

- a. Enter your new password as prescribed by your DOIM, S6 or CSSAMO.
- b. Click on “**Save**” and repeat procedure.
- c. The CAISI default is “**system**”.

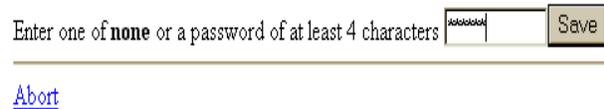


Figure 2-127 Multi-Client Radio Adapter Password Screen

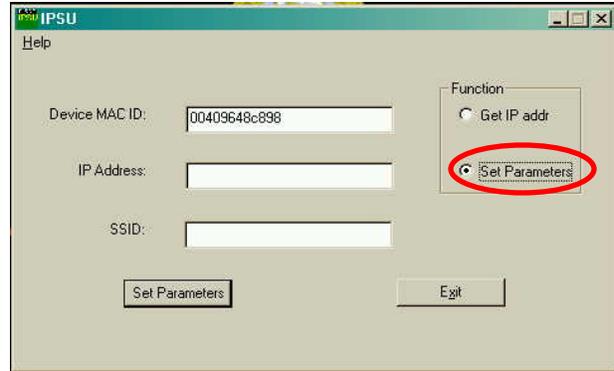
NOTE: *The CAISI default password is for hardware testing and classroom training only. The SSR must change the password before deploying the radio.*

9. At this point, the minimum configuration of the radio adapter is complete. The radio is ready for deployment. Close Internet Explorer.

2.12.2.2 Configuration of a CCM Multi-Client Radio Adapter from Scratch

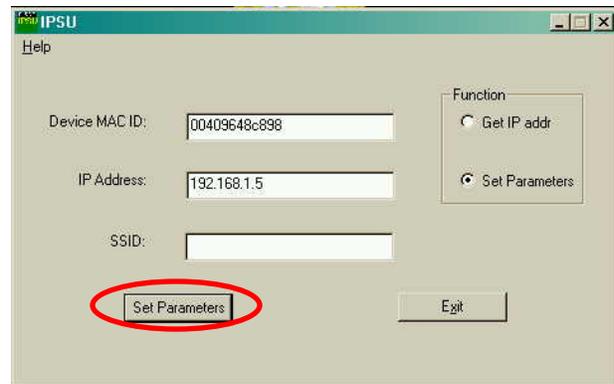
1. Apply power to the external power source. The lights on the radio, encryptor and hub in the CCM should come on.
2. Apply power to the SSR notebook.
3. Enter your username and password. The CAISI defaults are “**caisiadmin**” and “**BS_69dlw**”.
4. A Logon Message prompt will appear, “Your password expires today. Do you want to change it now?” For classroom training, click on the “**No**” button.
5. Reset the Radio to “factory defaults”. (Remove CAISI reset tool from SSR notebook case or SSR Transit case).
 - a. Use the radio adapter’s reset button to reset the radio.
 - 1) With the radio powered, insert your CAISI reset tool into the reset button (very small hole located on the back of the radio next to the power input). You will feel or hear a small click.
 - 2) Press and hold the button for approximately ten – fifteen seconds. Continue to hold the reset button until:
 - a) The “**Status**” LED (middle) on the CCM turns to red or amber.
 - b) The “**Ethernet**” LED (top) flickers briefly.
 - 3) Remove the reset tool. The CCM radio will reboot and power itself back to a ready state.

- d. Enter the MAC address of the radio into the “Device MAC ID” field. (The MAC address is on the label. Do not include the dashes).
- e. Click on “Set Parameters”.
- f. The IP Address field will change from brown to white and the “Get IP address” button will change to the “Set Parameters” button.



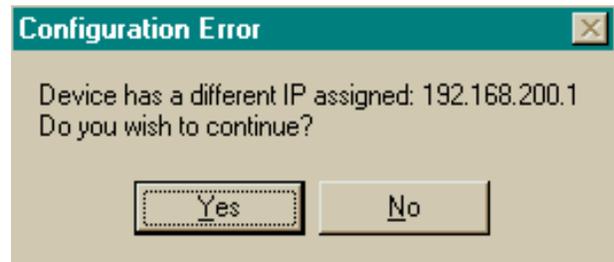
**Figure 2-129 Multi-Client Radio Adapter
IPSU Main Screen - 1**

- g. Enter the desired IP address into the “IP Address” field, and press the “Set Parameters” button at the bottom of the menu screen.
 - 1) The CAISI default address is **192.168.1.5**
 - 2) The Cisco factory default address is **192.168.200.1**



**Figure 2-130 Multi-Client Radio Adapter
IPSU Main Screen - 2**

- h. If the device already has some other address, such as if the device was previously configured or if a DHCP server assigned one, you will see that address instead, *but the change will fail*. No error will be displayed; the address will just not change.



**Figure 2-131 Multi-Client Radio Adapter
Configuration Error Prompt**

- i. If you get a “Device does not answer” message, press and hold the Reset button on the radio for about 10 seconds, then try again by starting back at the IPSU utility.



**Figure 2-132 Multi-Client Radio Adapter
Device Does Not Answer Prompt**

NOTE: DHCP can not be used to set the IP address because the multi-client radio adapters will be in the Untrusted zone and will not be able to communicate with the DHCP server.

7. Click on the “Exit” button.
8. Cycle power on the multi-client radio adapter. This will clear the ARP tables in memory.

You must use the Ethernet port to communicate from your notebook to the Multi-client radio adapter.

9. Open Internet Explorer.
 - a. In the address toolbar at the top of Explorer, enter one of the following 192.168.200.1 (Cisco default) or 192.168.1.5 (CAISI default) or the new IP address you previously assigned the radio adapter and press the <Enter> key.
 - b. Click on “Go” on the Explorer toolbar or click on “Enter” on the notebook keyboard.
 - c. Click on “Allow Config Changes”.
 - d. Select “Radio” from the “Configuration” menu. The radio screen will appear.

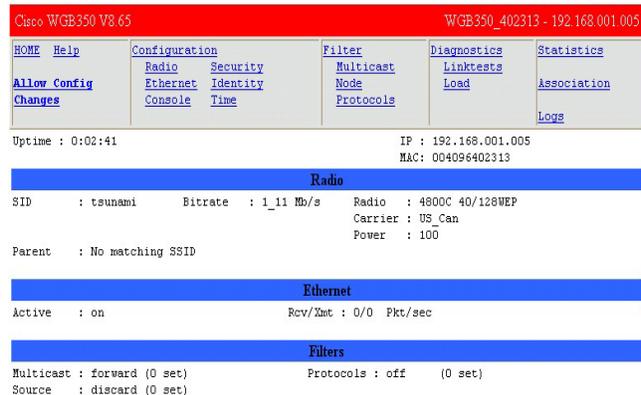


Figure 2-133 Multi-Client Radio Adapter Main Screen

NOTE: The selected value of the field is in bold letters. Figure 2-134.

If there is a “Save” button next to the field, you must use the button to save the changes to that field.

- 1) Enter your SSID as prescribed by your DOIM, S6 or CSSAMO in the “Service Set Identification” field. The CAISI default is “**caisi000**”.
- 2) Click on the “Save” button.
- 3) Set “Enable World Mode” to “**on**” by clicking on the selection.
- 4) Change the “RTS/CTS packet size threshold” from the default 2048 to **1024**. Click on the “Save” button.
- 5) While still on this screen, scroll down and click on “**off**” next to “Enable the diversity antennas.”
- 6) Leave the “transmit power level” set to **full**, unless directed to reduce it for overseas areas.

- 7) Change the “Maximum fragment size” from 2048 to **1024**. Click on the “Save” button.
- 8) Leave all the other fields at their defaults.

Item	Value
Service set identification	a string of at least 1 characters <input type="text" value="caisi000"/> Save
Allowed bit rates in megabits/second	1 , 1 2 , 1 5.5 , 1 11 , 2 , 2 5.5 , 2 11 , 5.5 , 5.5 11 or 11
Basic bit rates in megabits/second	1 , 1 2 , 1 5.5 , 1 11 , 2 , 2 5.5 , 2 11 , 5.5 , 5.5 11 or 11
Enable world mode	on or off
RTS/CTS packet size threshold	a number of 2400 or less <input type="text" value="1024"/> Save
Privacy configuration	
Parent node Id	our parent's network address <input type="text" value="any"/> Save or any
Time to look for specified parent	off or a time in seconds <input type="text" value="off"/> Save
Maximum number transmit retries	a number from 8 to 64 <input type="text" value="64"/> Save
Refresh rate in 1/10 of seconds	a number from 5 to 150 <input type="text" value="100"/> Save
Enable the diversity antennas	on or off
Transmit power level	1 , 5 , 15 , 30 or full
Maximum fragment size	a number from 256 to 2048 <input type="text" value="1024"/> Save
Enable radio options	a password <input type="text"/> Save

Figure 2-134 Multi-Client Radio Adapter Radio Screen - 1

NOTE: The SSID must match the root radio’s SSID in order to know what network to join. The CAISI default SSID is for hardware testing and classroom training only. The SSR must change the SSID before deploying the radio.

NOTE: You can make only one change at a time. If the field has a “Save” button next to it, you must use the button to save changes to that field. If you make several changes at once, only the one whose button you selected will be changed. The other changes will be lost.

10. Click on “**Privacy configuration**” on the radio screen and the privacy screen will appear.

Item	Value
Service set identification	a string of at least 1 characters <input type="text" value="caisi000"/> Save
Allowed bit rates in megabits/second	1 , 1 2 , 1 5.5 , 1 11 , 2 , 2 5.5 , 2 11 , 5.5 , 5.5 11 or 11
Basic bit rates in megabits/second	1 , 1 2 , 1 5.5 , 1 11 , 2 , 2 5.5 , 2 11 , 5.5 , 5.5 11 or 11
Enable world mode	on or off
RTS/CTS packet size threshold	a number of 2400 or less <input type="text" value="1024"/> Save
Privacy configuration	
Parent node Id	our parent's network address <input type="text" value="any"/> Save or any
Time to look for specified parent	off or a time in seconds <input type="text" value="off"/> Save
Maximum number transmit retries	a number from 8 to 64 <input type="text" value="64"/> Save
Refresh rate in 1/10 of seconds	a number from 5 to 150 <input type="text" value="100"/> Save
Enable the diversity antennas	on or off
Transmit power level	1 , 5 , 15 , 30 or full
Maximum fragment size	a number from 256 to 2048 <input type="text" value="1024"/> Save
Enable radio options	a password <input type="text"/> Save

Figure 2-135 Multi-Client Radio Adapter Radio Screen - 2

- a. Click on “Set the keys”.

Item	Value
Encrypt radio packets	off , on , mixed on or mixed off
Authentication mode	open or shared key
Set the keys	
Key number for transmit	a key number from 1 to 4 <input type="text"/> Save

Figure 2-136 Multi-Client Radio Adapter Privacy Screen

- b. Enter “1” as the key number. Click on the “Save” button.

Enter a key number from 1 to 4 Save

[Abort](#)

Figure 2-137 Multi-Client Radio Adapter Enter Key Number Screen

- c. Enter your WEP key and click on “Save” you will need to repeat this procedure. The default CAISI WEP key is **0123456789abcdef0123456789**

Enter a key of hex digits Save

[Abort](#)

Figure 2-138 Multi-Client Radio Adapter Set WEP Key Screen

- d. Once your key is set, set “Encrypt Radio Packets” to “on”.
- e. Leave the “Authentication mode” set to “open”.

Item	Value
Encrypt radio packets	off , on , mixed on or mixed off
Authentication mode	open or shared key
Set the keys	
Key number for transmit	a key number from 1 to 4 <input type="text"/> Save

Figure 2-139 Multi-Client Radio Adapter Privacy Screen

NOTE: The CAISI default WEP key is for hardware testing and classroom training only. The SSR must change the WEP key before deploying the radio.

- 11. Select “Ethernet” from the “Configuration” menu.
 - a. The Ethernet configuration screen will appear.
 - b. Reduce the “Wired LAN node stale out time” from the default 700 to **300** and click on “Save”.
 - c. Turn “Do not stale out client nodes” **off**. The default is “on”.
 - d. If the DOIM, S6 or CSSAMO has specified an MTU size for your network, enter it in the “Maximum frame size” field.

Item	Value
Connection active	on or off
Maximum frame size	a size from 1518 to 4096 <input type="text" value="1518"/> Save
Add client address	a network address <input type="text"/> Save or current
Remove client address	all or a network address <input type="text"/> Save
Display the client addresses	
Wired LAN node stale out time	a time in seconds from 5 to 1000 <input type="text" value="300"/> Save
Do not stale out client nodes	on or off

Figure 2-140 Multi-Client Radio Adapter Ethernet Configuration Screen

12. Select “**Filter**” from the top menu.
 - a. Under “Packet direction by filters,” Click on “**Both**”.

Item	Value
Packet direction affected by filters	both or to radio

Figure 2-141 Multi-Client Radio Adapter Filter Screen

13. Select “**Logs**” from the “Statistics” menu.
 - a. Go to “A community name of at least 1 character,” located mid way down the screen under the “Value” column.
 - 1) Delete “**Public**”.
 - 2) Enter a space (null) by tapping on the keyboard spacebar.
 - 3) Click on the “**Save**” button.
 - b. Scroll down to “**Enable Reception of Syslog Messages**” then click on “**Off**”.
 - c. Leave all the other fields at their defaults.

Item	Value
Log and alarm history	
Clear the history buffer	
Type of logs to print	all , error/severe or severe
Type of logs to save	all , error/severe or severe
Type of logs to light status led	all , error/severe , severe or off
Set alarms on statistics	
Log network roaming	off
Log backbone node changes	on or off
IP destination for SNMP traps	none, an IP address or a name <input type="text" value="none"/> <input type="button" value="Save"/>
Community for SNMP traps	a community name of at least 1 characters <input type="text"/> <input type="button" value="Save"/>
Type of logs to cause a trap	all , error/severe , severe or off
Enable authentication failure trap	on or off
Unix syslogd address	host IP address or a name <input type="text" value="000.000.000.000"/> <input type="button" value="Save"/>
Type of logs to send to syslog	all , error/severe , severe or off
Syslog facility number to send	a number from 16 to 23 <input type="text" value="16"/> <input type="button" value="Save"/>
Enable reception of syslog messages	on or off

Figure 2-142 Multi-Client Radio Adapter Logs Screen

14. Select “**Console**” from the Configuration menu.
 - a. Select “**Set write privilege password**” and enter your new password as prescribed by your DOIM, S6 or CSSAMO twice.
 - b. The CAISI default is “**system**”.
 - c. Click on the “**Save**” button and repeat procedure.

Item	Value
Set readonly privilege password	
Set write privilege password	
Display the remote operator list	
Add an operator host	a network address or an IP address <input type="text"/> <input type="button" value="Save"/>
Remove an operator host	all , a network address or an IP address <input type="text"/> <input type="button" value="Save"/>
SNMP community properties	
Terminal type	teletype , ansi or colour
Console expects complete lines	on or off

Figure 2-143 Multi-Client Radio Adapter Console Screen

NOTE: *The CAISI default password is for hardware testing and classroom training only. SSRs must change the password before deploying the radio.*

15. At this point, the radio adapter is fully configured and ready to use.
16. Close Internet Explorer.

2.12.3 Verify Operational Status of CCM Multi-Client Radio Adapter.

1. Open Internet Explorer.
2. In the address toolbar at the top of Explorer, enter the IP address with which you gave the radio adapter during configuration. During classroom training, use the CAISI default IP – **http://192.168.1.5**.
3. Click on “**GO**” on the Explorer toolbar or click on “**Enter**” on the notebook keyboard.
4. Click on the “**Statistics**” menu.
5. Select “**all**” next to “Show Network Map”.
 - a. Locate the multi-client radio adapter you just configured by finding its MAC address in the list of devices on the network.
 - b. Once you’ve located the multi-client radio adapter, verify the IP address is the one you assigned the device.
6. Click on “**Done**”.
7. Close Internet Explorer.

Device	Node Id	IP Address	Ver	Name
WGB340	00409648c898	192.168.001.005	8.58	Name ICMP message received: 192.168.001.002 destination port unreachable
Enode	0010a49f8c53	192.168.001.002		

Figure 2-144 Multi-Client Radio Adapter Network Map

2.12.4 Disable Remote Access to the CCM Multi-Client Radio Adapter

Once you are confident in the configuration of the radios you may avoid wireless network vulnerabilities by disabling remote access to the multi-client radio adapter.

1. To disable remote access perform the following procedures:

- a. Select “**Write Access**” from the top menu.
- b. The “**Enter Network Password**” screen will appear.



Figure 2-145 Multi-Client Radio Adapter Enter Network Password

- 1) Enter “**ccm000**” in the “**User Name**” field. (You can leave this field blank.)
- 2) Enter the password you assigned the device as prescribed by your DOIM, S6 or CSSAMO in the “**Password**” field. The CAISI default is “**system**”.
- 3) Click on the “**OK**” button.

- c. Select “**Allow Config Changes**” from the top menu.
- d. Select “**Identity**” from the “**Configuration**” menu. Make sure that “**Use BOOTP/DHCP on startup**” is **off**.
- e. Enter **0.0.0.255** in the “**Internet address**” field and click on the “**Save**” button.
- f. Nothing will appear to happen, because you will lose contact with the multi-client radio adapter. Without a valid address, no one can talk to it. Not even intruders, even if they have managed to penetrate your WEP key.
- g. Close Internet Explorer.

Item	Value
Use BOOTP/DHCP on startup	off, bootp, only or on
System name	a string WGB340_48c898 Save
DHCP class id	a string WGB340 Save
Internet address	an IP address 0 0 0 255 Save
Internet subnet mask	subnet mask IP address 255.255.255.000 Save
Internet default gateway	an IP address 000.000.000.000 Save
IP routing table configuration	
DNS server 1	an IP address 000.000.000.000 Save
DNS server 2	an IP address 000.000.000.000 Save
Domain name	a string Save
System location	a string Save
System contact name	a string Save

Figure 2-146 Multi-Client Radio Adapter Identity Screen

NOTE: Set the address to **0.0.0.255**. Do not set it to **0.0.0.0** because this would automatically re-enable DHCP.

NOTE: Once the radio’s IP address is removed, you will no longer have access to the radio. If you need to access the radio you will have to reset it to factory defaults.

2.12.5 Disconnect CCM Multi-Client Radio Adapter from Notebook

1. Disconnect the white straight-through Ethernet cable from the NIC in your SSR notebook and the RJ-45 straight-through adapter.
2. Disconnect the red crossover cable from the RJ-45 straight-through adapter and the “Ethernet” port on the back of the multi-client radio adapter.
3. Re-attach the short red crossover cable you initially removed from the “Encrypted” port on the back of inline encryptor.

If you have performed all necessary configuration procedures involving the Multi-client radio adapter and are ready to power down the equipment, refer to Paragraph 2.12.7 for procedures on disconnecting the Multi-client radio adapter power cables.

2.12.6 Configure CCM Encryptor

The AirFortress inline encryptor installed in the CCM is a duplicate of the device in the CBM. For CCM inline encryptor configuration procedures refer to Paragraph 2.11.6.

2.12.7 CCM Power Cable Disconnection Procedures

1. Disconnect the male end of the 2-prong power cable from the external power source.
2. Disconnect the female end of the 2-prong power cable from the power supply in the base of the chassis.

2.13 MANUAL CONFIGURATION OF THE LEGACY SUPPORT ADAPTER (LSA)

The purpose of the LSA is to provide network connectivity for the Legacy STAMIS systems that were designed to communicate via the serial port. The LSA provides a virtual circuit from one host computer's serial port to another over the 10Base-T network. The adapter will plug into the STAMIS host's serial port. From there, it will connect to the nearest CCM or CBM with CAT-5 network cable.



Figure 2-147 LSA

2.13.1 Physical Connection Procedures

1. Connect LSA power cables.
 - a. Remove the LSA, the LSA power adapter and a 3-prong power cable from the STAMIS transit box.
 - b. Connect the power supply to LSA.
 - c. Plug the female end of the 3-prong power cable into the power supply and the other end into an external power source.

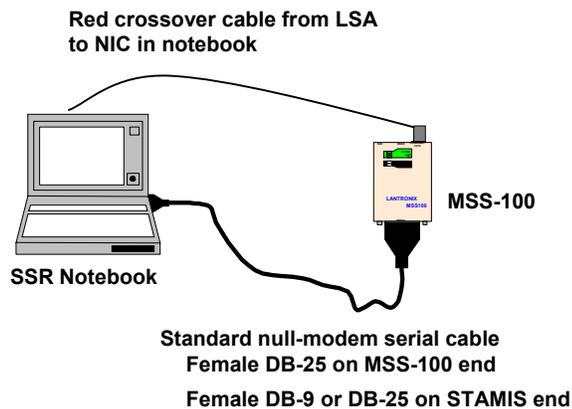


Figure 2-148 LSA Connections

2. Connect LSA to Notebook Wired NIC/Built-in NIC.
 - a. Connect one end of a null modem cable to the serial port located on the SSR Notebook.
 - b. Connect the other end of the nul modem cable to the LSA (MSS-100) serial port.
 - c. Connect a red crossover Ethernet cable from the NIC in the notebook to the 10/100 network port on the LSA.

2.13.2 Configuration of the LSA

The Legacy Support Adapters issued to the SSR from Tobyhanna Army Depot will be preset to the CAISI standard configuration. **At a minimum, the SSR needs to change the SSID, WEP key, and passwords.**

NOTE: *A standard CAISI SSR notebook, configured as follows is required for wireless bridge set up. It 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. The wired NIC or built-in NIC must be used.*

There are four main procedures required to set up the LSA:

- Set the IP address and load new firmware.
- Configure the device.
- Load the CAISI-VEE program files.
- Enable passwords and start the CAISI-VEE program.

Before beginning set up of the LSA you need to reset the device to factory defaults.

1. Restore the LSA to factory default parameters: **(Reset the LSA)**
 - a. Complete initial connections.
 - b. Remove power to the LSA.
 - c. Push the reset button on the rear of the LSA (use the reset tool from the SSR Notebook case or SSR Transit case) and **keep the button pressed in.**
 - d. Apply power to LSA **while also holding in the reset button.**
 - e. Hold it until the serial lights stop blinking (about 5-10 seconds) then release.
 - f. All configuration parameters are set back to the factory default parameters.

2. Set IP Address and Load Firmware.

Assign an IP address or use EZWebCon to verify the IP address.

- a. To assign an IP address automatically by DHCP.
 - 1) Connect to the Linksys router or other DHCP server.
 - 2) Once connected, an IP address will be assigned to the LSA.
 - 3) The LSA by default is DHCP enabled.

NOTE: *If loading firmware, do not use the DHCP method. Assign the IP address manually.*

b. Set IP address manually using EZWebCon.

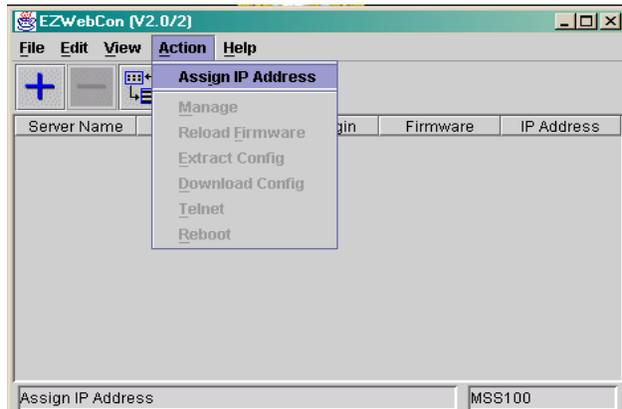
- 1) At the bottom of the SSR notebook screen, click on ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear.
- 2) Click on the "EZWebCon" menu selection. The EZWebCon menu will appear.



**Figure 2-149 LSA
CAISI Toolbox Menu**

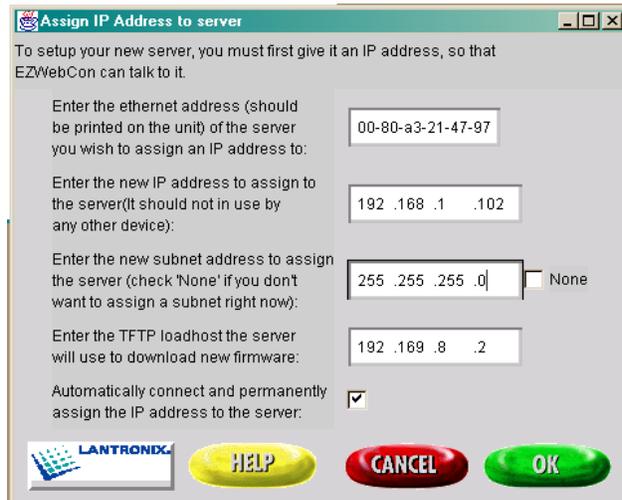
- 3) Select "Action" from the menu bar.
- 4) Click on "Assign IP Address".

NOTE: Click on *View* to change to List View.



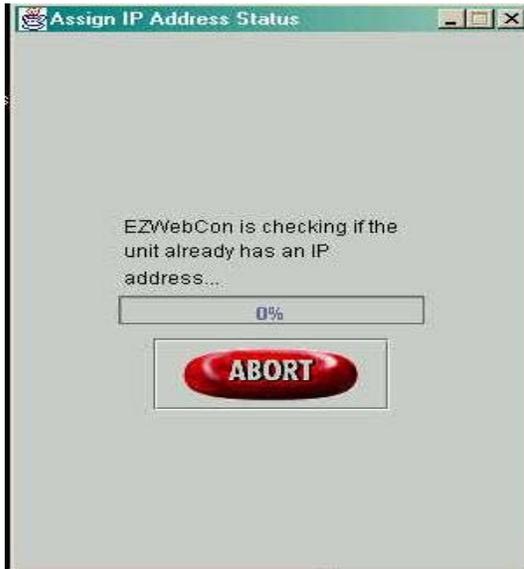
**Figure 2-150 LSA
EZWebCon Main Menu**

- 5) Enter the MAC address (Ethernet address written on the back of LSA).
- 6) Enter the new IP address.
- 7) Uncheck the "none" box to the right of the Subnet Mask field.
- 8) Change the Subnet Mask as prescribed by your DOIM or S6. For classroom purposes leave the Subnet Mask set to the CAISI default, 255.255.255.0



**Figure 2-151 LSA
Assign IP Address to Server Screen**

- 9) Enter the CAISI notebook’s IP as the TFTP loadhost server so you may copy the CAISI-VEE files later on.
- 10) Leave the box next to, “**Automatically connect and permanently assign the IP address to the server**” checked.
- 11) Click on the “**OK**” button. A pop up screen will display the changes.



**Figure 2-152 LSA
Assign IP Address Status Screen - 1**

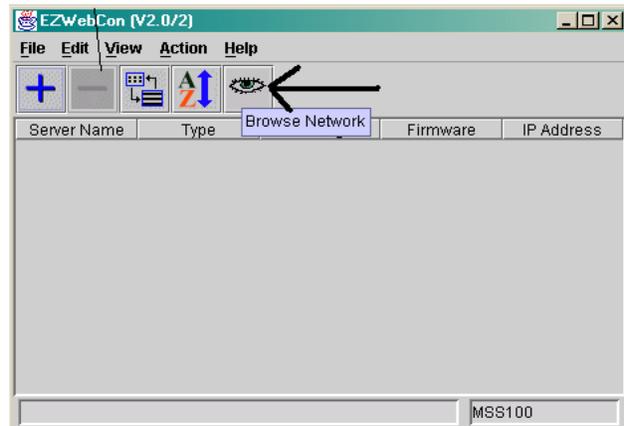


**Figure 2-153 LSA
Assign IP Address Status Screen - 2**

- 12) Cycle power.

NOTE: *The procedure to assign an IP address may take several minutes. The progress bar will appear to stall at certain intervals.*

3. Verify IP using EZWebCon. Use EZWebCon to locate the LSA(s) through the network connection.
 - a. Click on the Browse button (the Eye) on the Main Menu.



**Figure 2-154 LSA
EZWebCon Main Menu**

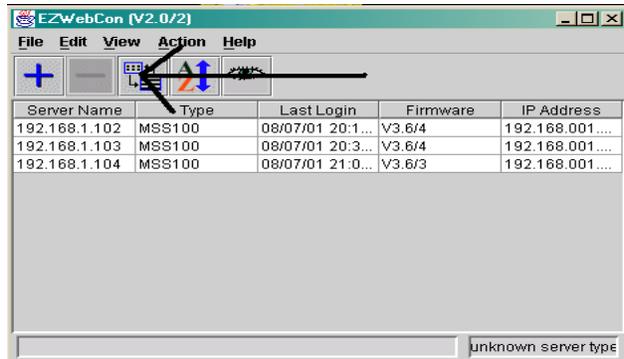
- b. A dialogue box will appear listing the IP address of the LSA(s) in this segment of the network.
- c. Click on “**Select All**”.
- d. Click on “**OK**”.



**Figure 2-155 LSA
Browse Network Screen**

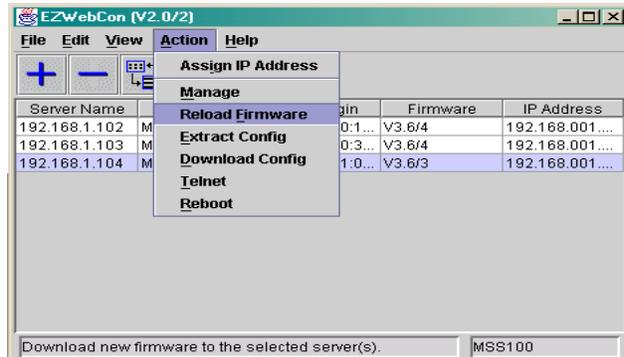
NOTE: *You don't have to wait for EZWebCon to finish its scanning routing. If you know there are only three LSA in your network, once all the devices appear in the table, you can interrupt the process by clicking the “Select All” and “OK,” otherwise the process may take up to 4 minutes to finish scanning the network.*

- 4. Check and Load Firmware using EZWebCon.
 - a. Click on “**Toggle View**” to show LSA parameters.
 - b. If icons are displayed instead of List View, click on Toggle button again.
 - c. The firmware version is listed in the Firmware column.



**Figure 2-156 LSA
EZWebCon Main Menu**

- 5. Load firmware: Check if the firmware is current. If not:
 - a. Highlight the LSA(s) that needs updating.
 - b. Click on “**Action**”.
 - c. Click on “**Reload Firmware**”.



**Figure 2-157 LSA
EZWebCon Reload Firmware**

NOTE: *The hourglass symbol will not appear, but the process will have started. It may take up to a minute for it to load.*

Once process is complete the Reload Firmware Wizard will appear.

6. ReLoad firmware: Wizard Steps:

- a. Click on “**Browse local**”. The “**Firmware**” directory should appear.
- b. If the firmware directory does not automatically appear in the menu field navigate to C:\NetTools\Lantronix\firmware.”
- c. Click on “**MSS100.sys**”.
- d. Click on “**Open**” to select the firmware file.
- e. Click on “**Next**”.
- f. Select the server(s) (LSA) that need the new firmware.

NOTE: *The field(s) you select will not be highlighted, but will be outlined.*

- g. Click on “**Begin Reload**”.

- h. Click on “**YES**”.

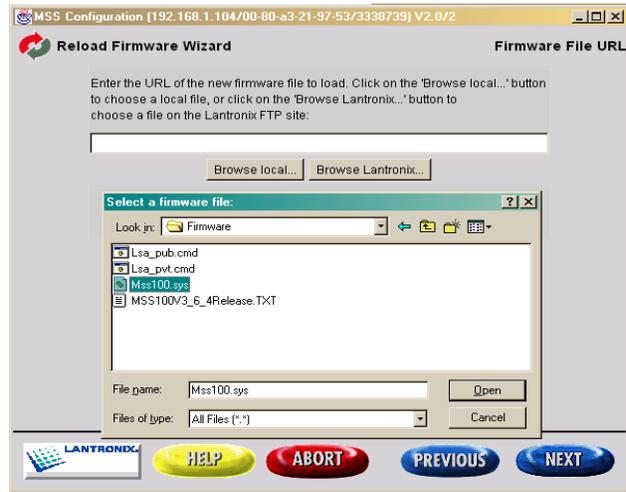


Figure 2-158 LSA Reload Firmware Wizard Screen

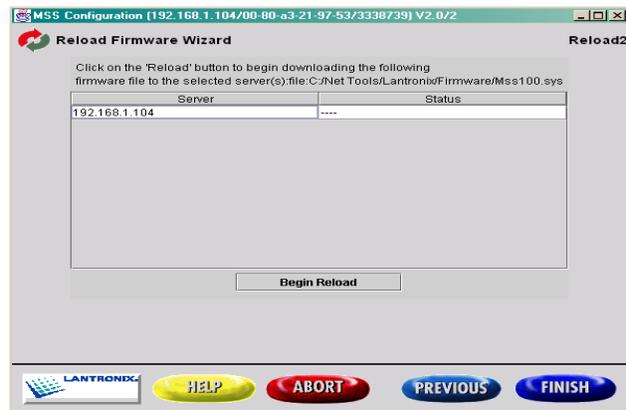


Figure 2-159 LSA EZWebCon Begin Reload

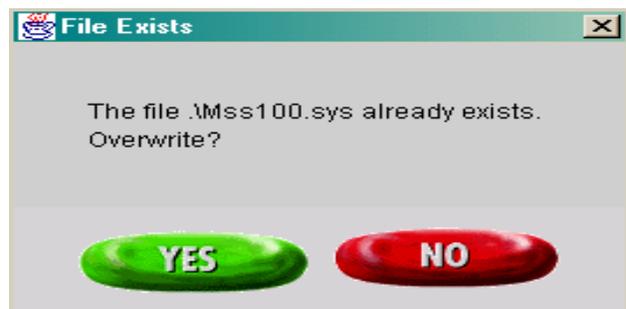


Figure 2-160 LSA File Exists Screen

NOTE: *This procedure takes a few minutes. If the process has begun the buttons on the menu will appear slightly grayed. Once the process is complete the main EZWebCon screen will appear.*

7. To verify that the firmware is updated you may refresh the screen.
 - a. There are two refresh options. These options will allow you to view the most current information.
 - 1) Hold the <Ctrl> button while tapping on the “R” key.
 - 2) Click twice on the “Toggle View” button. 
8. Close EZWebCon and open Windows Explorer.
9. Configure the LSA.

The user serviceable files need to be updated. There are nine (9) CAISI-VEE files. Only two of these files require user service. They are the “HOSTS” file and “CAISIVEE.CFG” file.

LSA “HOSTS” file – is like a local DNS database. It is used if there is no real DNS or DNS is temporarily down. User must enter the IP and the Host names for all STAMIS systems that need to be contacted.

LSA “CAISIVEE.CFG” file –controls how the LSA responds. It is used to set the DNS database search priority and specifies the domains to search when performing DNS resolution.

a. **Update “HOSTS” file for your STAMIS server names and addresses:**

- 1) Open Windows Explorer.
- 2) Navigate to the “C:\Net Tools\Lantronix\PUC” folder.

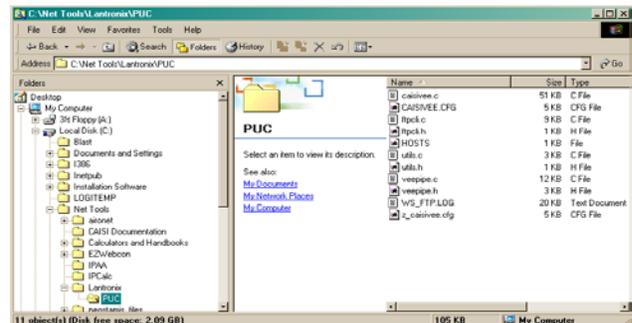


Figure 2-161 LSA PUC Folder - 1

- 3) Right-click on the “HOSTS” file.
- 4) Select “Send To”.
- 5) Select and click on “Notepad”.

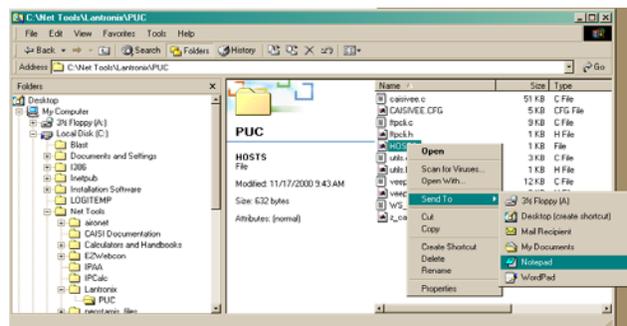
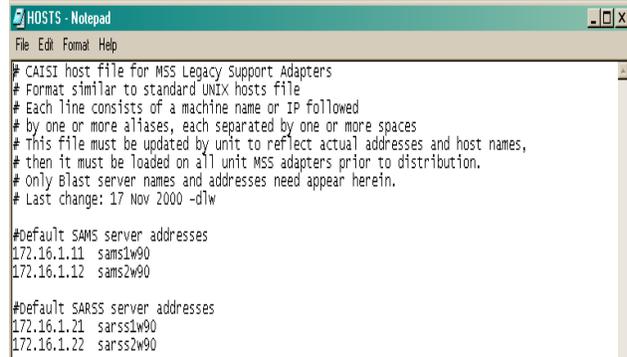


Figure 2-162 LSA PUC Folder - 2

- 6) Overwrite your STAMIS server names in the place of the ones in the file.
- 7) Overwrite your STAMIS server addresses in the place of the ones in the file.
- 8) Save and close the file. Click on “File”. Click on “Save”.



**Figure 2-163 LSA
PUC Folder - 3**

- 9) Close the Notepad by clicking the (X) at the top right of the screen or by selecting “File” from the main menu bar and then selecting “Exit”.

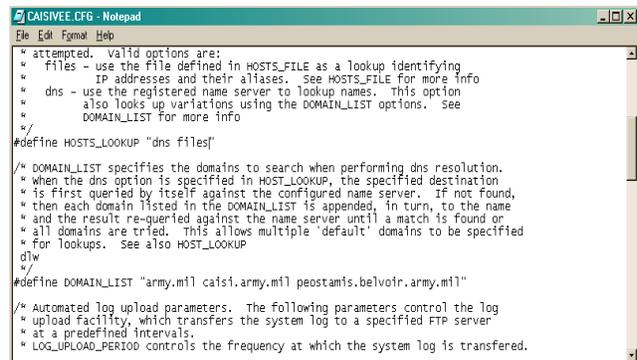
NOTE: The “#” sign is used to indicate comments. Any line that begins with # will be ignored.

b. Update “CAISIVEE.CFG” file with your Domain:

- 1) Open Windows Explorer.
- 2) Navigate to the “C:\Net Tools\Lantronix\PUC” folder.
- 3) Right-click on the “CAISIVEE.CFG” file.
- 4) Select “Send To”.
- 5) Select and click on “Notepad”.

NOTE: When performing the below procedures *be careful not to change any other text.*

- 6) To select the order of DNS resolution.
 - a) Scroll down the “CAISI VEE Configuration File” to “#define DOMAIN_LIST”
 - b) Enter your domain(s) in place of “caisi.army.mil” and any other domains that your STAMIS clients need to communicate with.
- 7) Save and close the file. Click on “File”. Click on “Save”.



**Figure 2-164 LSA
PUC Folder - 4**

NOTE: The “#” sign does not indicate comments in this file. Comments are enclosed between /* and */ and can run over more than one line.

8) Close the Notepad by clicking the (X) at the top right of the screen or by selecting “File” from the main menu bar and then selecting “Exit”.

10. Load CAISI-VEE Program Files. The files will be loaded using WS_FTP.

- a. At the bottom of the SSR notebook screen, click on ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear.
- b. Click on the "WS_FTP32" menu selection.
- c. In the “Host Name/Address” box enter the IP address of the LSA.
- d. User ID is “root”.
- e. Password is “system”.
- f. Click “OK” button.

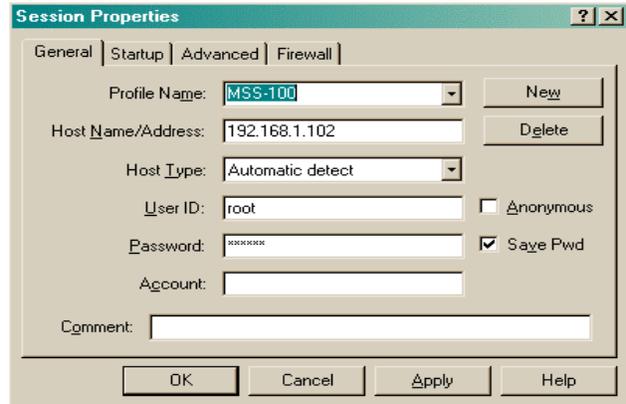


Figure 2-165 LSA Session Properties Screen

The left box in Figure 2-166, pictured below shows the “C:\Net Tools\Lantronix\PUC” folder in the CAISI notebook. The right box shows the “/flash” folder in the MSS-100.

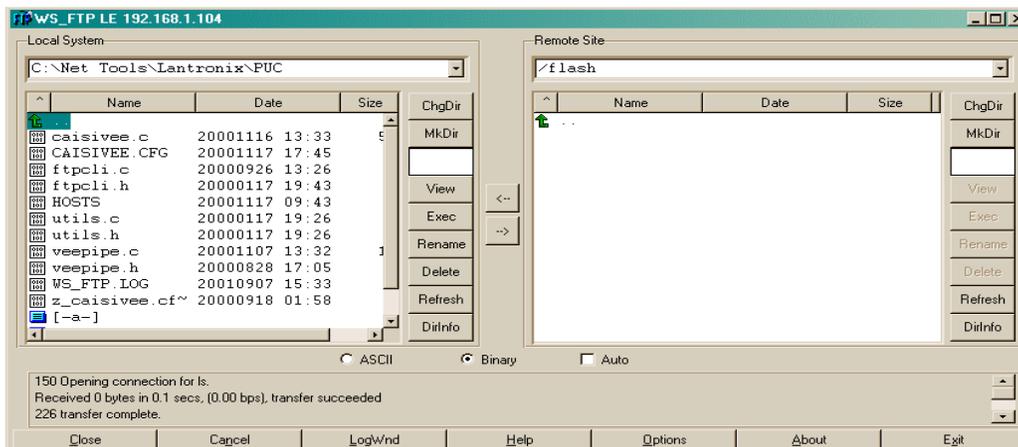
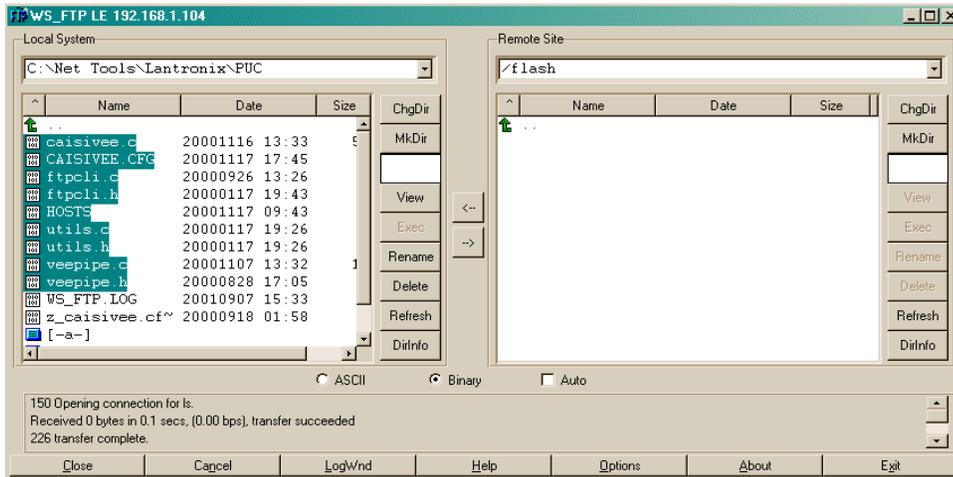


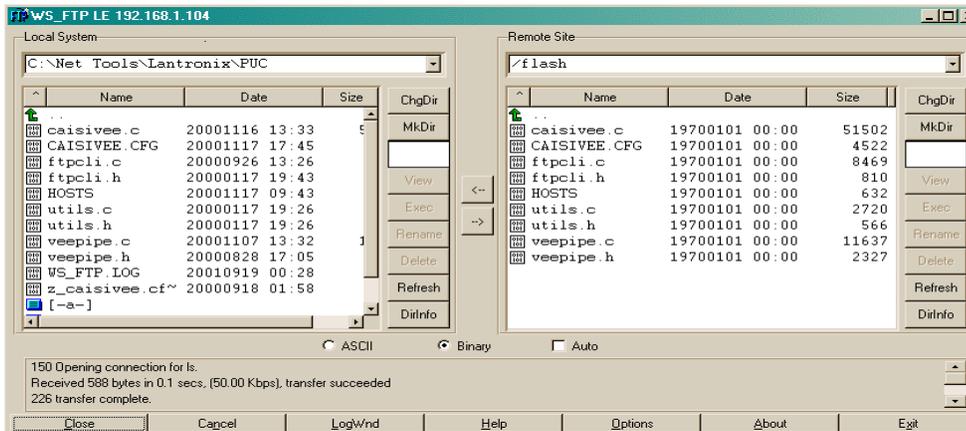
Figure 2-166 LSA C:\Net Tools\Lantronix\PUC Screen

- g. Highlight ONLY the first nine files shown to the left.
- h. Click on the first file.
- i. Hold the Shift key down while clicking on the last file.
- j. Click on the right arrow “→”.



**Figure 2-167 LSA
WS_FTP Highlighted Files**

- k. Once the files are copied, you will see the nine CAISI-VEE files in both windows.



**Figure 2-168 LSA
WS_FTP Copied Files**

- l. To exit out of WS_FTPLE, click the “Exit” button.
11. Download commands.
- a. At the bottom of the SSR notebook screen, click on ">>>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear.
 - b. Click on the "EZWebCon" menu selection.
 - c. Click on the LSA to be configured.

- d. Click on “Action”.
- e. Click on “Download Config”.

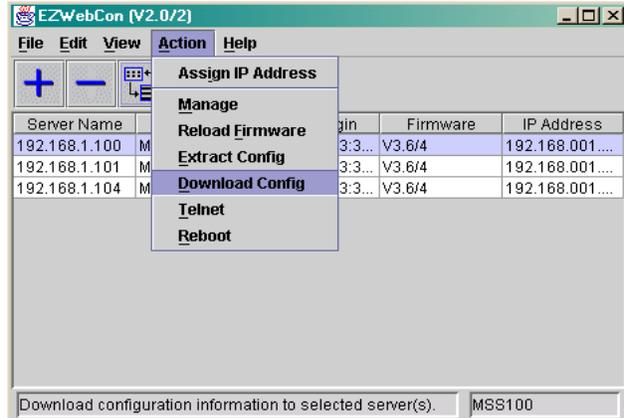


Figure 2-169 LSA Download Config

NOTE: The menu item in the drop down menu will be highlighted but the hourglass icon will not appear.

- f. When the process is completed the “Send Which Configuration” screen will appear.
- g. Click on “Lsa_pvt.cmd”.
- h. Click on the “Open” button.

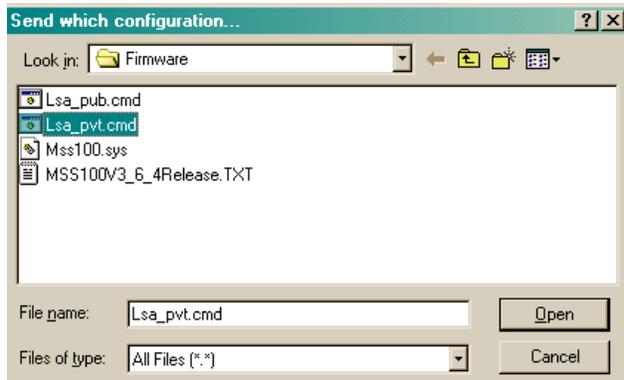


Figure 2-170 LSA Send Which Configuration Screen

- i. Click on the “NO” button. (This will skip all the optional installation settings).

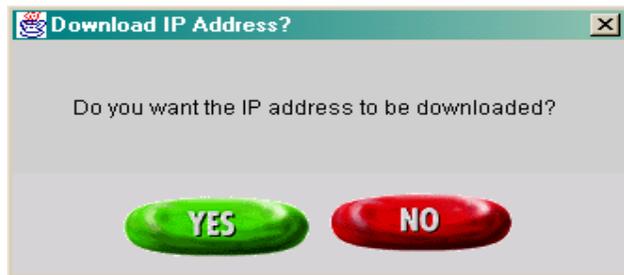


Figure 2-171 LSA Download IP Address Prompt

- j. As the commands are being sent to the LSA, you will see a progress bar.



Figure 2-172 LSA Send Command File

- k. Once the process is complete, click on "OK".

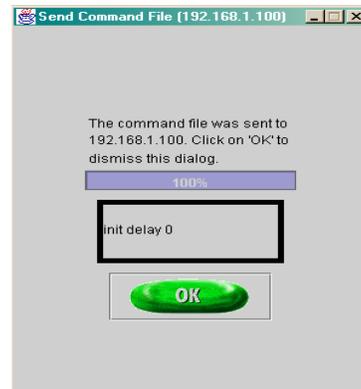


Figure 2-173 LSA Send Command File Complete Prompt

- l. Close EZWebCon by clicking the (X) at the top right of the screen or by selecting "File" from the main menu bar and then selecting "Exit".

12. Configure Unit Network Properties

The parameters that must be set in the LSA are IP, Subnet mask, Gateway, Domain Name and DNS. There are two ways to obtain these parameters.

They are by a DHCP server or manually.

- a. Set Properties by a DHCP Server.
 - 1) Make sure DHCP is set on the LSA (Default).
 - 2) Set by the command "**change DHCP enable**".
 - 3) Attach an Ethernet cable to your LSA. Make sure the LSA is behind the DHCP Server.
 - 4) Unplug the LSA if necessary to obtain new parameters.

b. Set Properties Manually.

1) Telnet to the LSA that needs to be configured.

- a) Select the Command Prompt icon from the toolbar at the bottom of the screen.



- b) Enter the command: “
- telnet xxx.xxx.xxx.xxx**
- ” where the xxx’s is the IP address of the LSA. Example: telnet 192.168.1.150

- c) Press the <Enter> key.

```

Command Prompt
C:\>Telnet 192.168.1.150

```

**Figure 2-174 LSA
Telnet Command**

- d) Enter the default password “
- access**
- ” and press the <Enter> key.

```

Command Prompt - Telnet 192.168.1.150
Lantronix MSS100 Version 03.6/4(000712)
Type HELP at the 'Local 2>' prompt for assistance.
Login password>

```

**Figure 2-175 LSA
Login Password Prompt**

- e) Enter your initials for the Username and press the <Enter> key.

```

Command Prompt - Telnet 192.168.1.150
Lantronix MSS100 Version 03.6/4(000712)
Type HELP at the 'Local_2>' prompt for assistance.
Login password>

Username> rls
Local_2> _

```

**Figure 2-176 LSA
Username Prompt**

- f) At the “Local_2>” prompt, type “set priv” and press the <Enter> key.

```

Command Prompt - Telnet 192.168.1.150
Lantronix MSS100 Version 03.6/4000712>
Type HELP at the 'local 2>' prompt for assistance.
Login password>

Username> rls
Local_2> set Priv
Password> _
    
```

**Figure 2-177 LSA
Local_2> Prompt**

- g) Enter the password “system” at the Password> prompt and press the <Enter> key.

```

Command Prompt - Telnet 192.168.1.150
Lantronix MSS100 Version 03.6/4000712>
Type HELP at the 'local 2>' prompt for assistance.
Login password>

Username> rls
Local_2> set Priv
Password> system
Local_2>> _
    
```

**Figure 2-178 LSA
Password Prompt**

You can tell whether or not you are connected to the LSA via its serial port or via its 10Base-T port by the command prompt you see at the console.

- “Local_1>” prompt - you are connected to the LSA via its serial port.
- “Local_1>>” prompt - you are a privileged user connected to the LSA via its serial port.
- “Local_2>” prompt - you are connected to the LSA via its 10Base-T port.
- “Local_2>>” prompt - you are a privileged user connected to the LSA via its 10Base-T port.

- h) The “>>” prompt indicates a privileged user. Enter the following commands. (xxx's are to be replaced with the appropriate IP address as prescribed by your DOIM, S6 or CSSAMO).

- change ipaddress xxx.xxx.xxx.xxx
- change subnet mask xxx.xxx.xxx.xxx
- change gateway xxx.xxx.xxx.xxx
- change domain caisi.army.mil
- change nameserver xxx.xxx.xxx.xxx
- init delay 0 (**This command restarts the LSA**).

NOTE: *This process may take a few minutes. Watch the lights on the LSA as the server reboots. The LSA has successfully rebooted when the “OK” light is slowly blinking steady.*

13. Enable Passwords. (Change the configuration passwords).
 - a. If you are not already in a Telnet session, telnet to the LSA.
 - b. Type the command, “**telnet xxx.xxx.xxx.xxx**”, where the xxx’s is the IP address of the LSA. Example: telnet 192.168.1.150
 - c. Enter the default password, “**access**” and press <Enter> key.
 - d. Enter your initials as the username and press the <Enter> key.
 - e. Enter the command “**set priv**” and press <Enter> key.
 - f. Enter the password “**system**” and press <Enter> key.
 - g. Enter the command “**change loginpass abcdef**” (default is access) and press <Enter> key.
 - h. Enter the command “**change privpass 123abc**” (default is system) and press <Enter> key.
 - i. Close the Command Prompt menu by clicking the (X) at the top right of the screen.

2.13.3 Verify Operational Status of LSA.

Although you can use web pages and EZWebCon to check LSA configuration, disadvantages exist with each method:

1. The Web pages do not give you access to complete information.
2. EZWebCon can not be accessed while the CAISI-VEE program is running. You must stop the CAISI-VEE program or you will get inaccurate results.

Alternatively you can use telnet to check the configuration and make changes on-the-fly without stopping the CAISIVEE program.

1. At the bottom of the SSR notebook screen, click on the **Command Prompt**. The Command Prompt menu will appear. There are four telnet commands that you need to check the configuration.
 - a. Telnet to the LSA.
 - 1) At the login password prompt enter the login password.
 - 2) At the username prompt enter your initials.
 - 3) Type the command, “**show server**”.

- 4) The resulting screen should look like Figure 2-179. Check the firmware version, the inactivity timer, and the IP address information.

```

Telnet - 192.168.1.50
Connect Edit Terminal Help
MSS100 Version V3.6/4(000712)      Uptime:          1:48:45
Hardware Addr: 00-80-a3-21-9b-4a   Name/NodeNum:    MSS_219B4A/ 0
Ident String: MSS100

Inactive Timer (min):             2   Serial Delay (msec):      30
Password Limit:                   3   Session Limit:           4
Queue Limit:                       32  Node/Host Limits:        32

LAT Circuit Timer (msec):          80  Keepalive Timer (sec):    20
Multicast Timer (sec):             30  Retrans Limit:           10

TCP/IP Address:                   192.168.1.50  Subnet Mask:             255.255.255.0
Nameserver:                       172.16.1.10   Backup Nameserver:       138.27.4.15
TCP/IP Gateway:                   192.168.1.1   Backup Gateway:          (undefined)
Domain Name:                      CAISI.ARMY.MIL   IP Time:                 None
DHCP Server:                      None           TCP Keepalives:          Enabled
Load Address: 00-40-96-35-a9-77    Lease Time:            0:00
Prompt:                            Local_2n%P>

Characteristics:
Incoming Logins: Telnet (Passwords Required)
LAT Groups: 0

Local_2>>

```

**Figure 2-179 LSA
Show Server Screen**

- b. Type the command, “**show server boot**”.
- 1) Check the boot flags. The resulting screen should look like Figure 2-180.

```

Telnet - 192.168.1.50
Connect Edit Terminal Help
Local_2>> show server boot
MSS100 Version V3.6/4(000712)      Uptime:          2:04:50
Hardware Addr: 00-80-a3-21-9b-4a   Name/NodeNum:    MSS_219B4A/ 0
Ident String: MSS100

Prom Version:                     V1.2 (April 12, 1999)

TFTP Loadhost:                    192.168.1.2
Backup TFTP Host:                  (undefined)
NetWare Loadhost:                  (undefined)

Software File:                     (default path) MSS100.SYS
Startup File:                      (undefined)
Boot Flags:                        No Boot No RARP No DHCP
Boot Gateway:                      (undefined)

Local_2>>

```

**Figure 2-180 LSA
Show Server Boot Screen**

- c. Type the command, “**show ports**”.
- 1) The resulting screen should look like Figure 2-181. Check the Flow control and baud rate. Also the characteristics. They must include: Autobaud, Inactive Limit, Password, Telnet Pad, and IncPassword.

```

Telnet - 192.168.1.50
Connect Edit Terminal Help
Local_2>> show ports

Port 1: Username: Port_1          Physical Port 1 (Local Mode)
Char Size/Stop Bits:           8/1      Baud Rate:           9600
Flow Ctrl:                      Cts/Rts   Session Limit:       4
Parity:                          None     Modem Control:       None
Access:                          Dynamic  Break Ctrl:          Local
Local Switch:                    None    Start Character:     None
Forward:                         None    Backward:             None
Port name:                       Port_1   Terminal Type:       None
Dedicated SDK: caisivee.c

Characteristics:  Autobaud  Inactive Limit  Password  Telnet Pad
                  IncPassword

Sessions:         0      Current Session:  None
Input/Output Flow Ctrl:  N/N  DSR/DTR/CTS/RTS/CD:  Y/Y/Y/Y/Y/Y

Seconds Since Zeroed:  7540  Framing Errors:      0
Accesses Local/Rem:   1/0    Parity Errors:       0
Flow Control Violations:  0    Overrun Errors:      0
Bytes Input:          753    Bytes Output:        5415
Input Flow On/OFF:    0/0    Output Flow On/OFF:  0/0

Local_2>>

```

**Figure 2-181 LSA
Show Ports Screen**

- d. Type the command, “**ping xxx.xxx.xxx.xxx**” where the xxx’s is the IP address of the LSA. Example: ping 192.168.1.150
- 1) Use the ping command to check outgoing network connectivity. You can ping IP addresses or hostnames. The local HOSTS file is not used, however, so you can only ping names that are in the DNS server.

```

Telnet - 192.168.1.50
Connect Edit Terminal Help
Local_2>> ping 192.168.1.1
Ping 192.168.1.1 (192.168.1.1): 50 data bytes (any key to stop)
50 bytes from 192.168.1.1: icmp_seq=1. time = 0 ms
50 bytes from 192.168.1.1: icmp_seq=2. time = 40 ms
50 bytes from 192.168.1.1: icmp_seq=3. time = 0 ms
50 bytes from 192.168.1.1: icmp_seq=4. time = 0 ms
50 bytes from 192.168.1.1: icmp_seq=5. time = 0 ms
192.168.1.1: 5 attempts 5 successes 0% packet loss
Local_2>> ping 172.16.1.1
Ping 172.16.1.1 (172.16.1.1): 50 data bytes (any key to stop)
50 bytes from 172.16.1.1: icmp_seq=1. time = 100 ms
50 bytes from 172.16.1.1: icmp_seq=2. time = 40 ms
50 bytes from 172.16.1.1: icmp_seq=3. time = 40 ms
50 bytes from 172.16.1.1: icmp_seq=4. time = 40 ms
50 bytes from 172.16.1.1: icmp_seq=5. time = 0 ms
172.16.1.1: 5 attempts 5 successes 0% packet loss
Local_2>> ping www.belvoir.army.mil
Ping WWW.BELVOIR.ARMY.MIL (140.153.243.2): 50 data bytes (any key to stop)
50 bytes from 140.153.243.2: icmp_seq=1. time = 240 ms
50 bytes from 140.153.243.2: icmp_seq=2. time = 180 ms
50 bytes from 140.153.243.2: icmp_seq=3. time = 130 ms
50 bytes from 140.153.243.2: icmp_seq=4. time = 140 ms
50 bytes from 140.153.243.2: icmp_seq=5. time = 0 ms
WWW.BELVOIR.ARMY.MIL: 5 attempts 5 successes 0% packet loss
Local_2>>

```

**Figure 2-182 LSA
Password Prompt**

2. Close the Telnet session by clicking the (X) at the top right of the screen.

2.13.4 LSA Disconnection Procedures

1. Disconnect the 3-prong power cable from the power supply and the external power source.
2. Disconnect the power supply from the LSA.
3. Disconnect the red crossover cable from the NIC and the Ethernet port on the LSA.
4. Disconnect the null modem cable from the SSR notebook serial port and the LSA.

Chapter 3

CAISI ADMINISTRATION SOFTWARE APPLICATION (CAISI ADMIN)

Section I Description of CAISI Admin

3.1 INTRODUCTION

The CAISI Administration Software Application (CAISI Admin) is a proprietary application designed and created specifically for CAISI. It is modeled after and developed to operate in a Microsoft Windows NT/2000 environment. CAISI Admin employs an easy-to-use interactive Graphical User Interface (GUI) to facilitate and simplify the configuration of various CAISI COTS devices. The software application allows the System Support Representative (SSR) to configure a new device using a pre-existing template in which parameters have already been set. This eliminates the need to have intimate knowledge of all the device's parameters. Since the SSR is only required to update a few parameters to make the device operate within his/her unit, the configuration segment of deployment planning is significantly reduced.

3.2 CAISI ADMIN NAVIGATION

This section contains information on commands, CAISI Admin's toolbar, its device lists and the overall presentation of CAISI Admin.

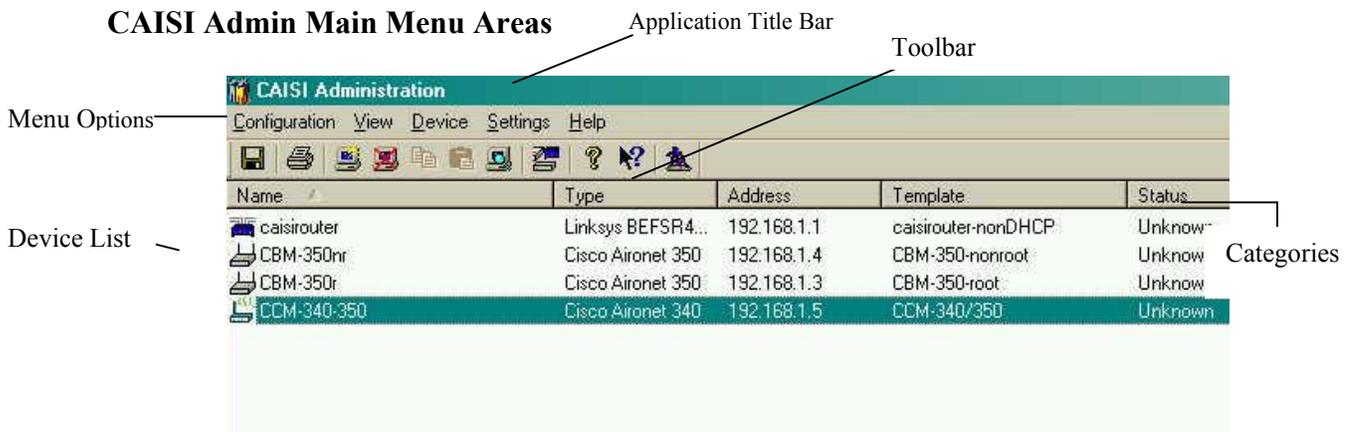


Figure 3-1 CAISI Admin Main Menu Screen

The main view window operates like any standard Windows list view. Users familiar with Windows software should quickly become familiar with the CAISI Admin window. Each area is described in the following section for clarity.

All commands that can be executed in the CAISI Admin are accessed via the main menu. Commands are organized into several groups or menus. Clicking a specific menu displays a drop down box containing individual commands. To execute a specific command, select or click the command from the drop down box. Menus can also be accessed using the 'Alt' key on the keyboard. Notice that one letter in each menu is underlined. Pressing the 'Alt' key and

subsequently clicking this letter on the keyboard opens the associated menu. To exit from keyboard menu mode, simply click the ‘Alt’ key again.

Some commands are displayed along with hot-key sequences, which are keyboard shortcuts for the command. For instance, the “Configuration” menu contains the command “Save” followed by the sequence ‘**Ctrl+S**’. This notation indicates that the “Save” command can also be executed by holding down the Control (Ctrl) key on the keyboard while pressing the letter ‘s’. Keyboard shortcuts such as described can be much quicker than moving the mouse to the menu and selecting the command from the subsequent drop down list.

Other commands are followed by an ellipsis or series of dots, such as the “Print Setup...” command on the “Configuration” menu. The ellipsis indicates that the command opens a dialog box to perform the indicated action. Finally, some menu items will appear grayed out, which indicates that particular command is not currently available. For instance, the “Delete” command under the “Device” menu is not available until a device from the device list is selected.

3.2.1 CAISI Admin Commands

Commands are separated into the following menus:

- Configuration
- View
- Device
- Setting
- Help

Configuration - Commands for saving, restoring and printing the device configuration file as well as exiting the application.

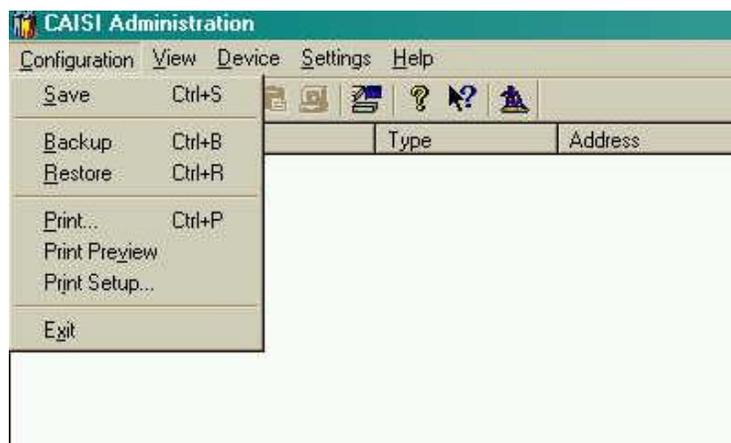


Figure 3-2 CAISI Admin-Configuration Menu

View – Commands for controlling the device list/main window view and accessing the audit log.

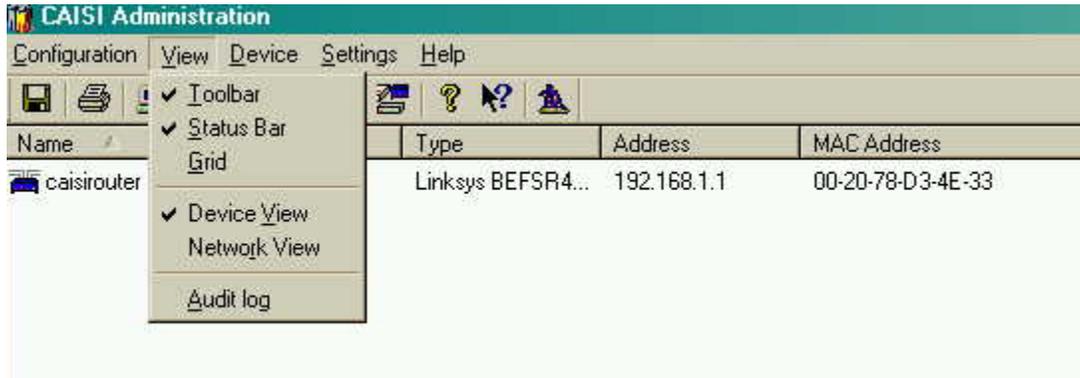


Figure 3-3 CAISI Admin-View Menu

Device – Commands for manipulating (adding, deleting, modifying) devices and the device list.



Figure 3-4 CAISI Admin-Device Menu

Settings – Commands for setting global preferences for the CAISI Admin.



Figure 3-5 CAISI Admin -Settings Menu

Help – Commands for accessing Application help and information. Online help is not available in this release.

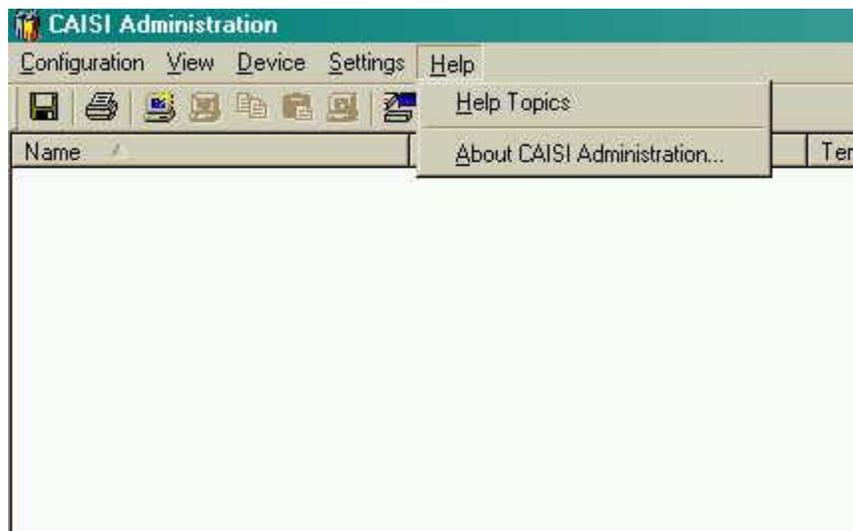


Figure 3-6 CAISI Admin-Help Menu

3.2.2 CAISI Admin Toolbar

The toolbar provides shortcuts for commonly used menu commands. When the mouse cursor is moved over a specific tool, a border appears around that tool and a “tooltip” appears. A tool tip is a small yellow popup screen that provides a brief description of the tool.

Tooltips can be used to quickly determine what a specific tool does. Tools that are grayed out (appear only in shades of gray) are not available at the moment. For instance, the device delete

tool is not available until a device from the device list is selected. However, tools that are grayed out will still display a tooltip if the mouse cursor is positioned over the tool for a brief time.

The toolbar and its available commands are show in the figure below.

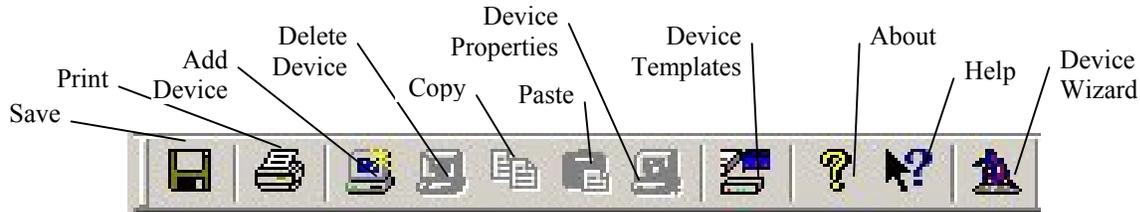


Figure 3-7 CAISI Admin-Toolbar

3.2.3 Device List

Devices are displayed within the white region of the main window below the main menu, toolbar and column headers. Devices are displayed one entry per row, with the left most field indicating the name of the device. Other columns show additional information for the device depending upon view settings (see “View Types” below). Icons to the far left of each device indicate the basic device type or driver. Devices are initially displayed in alphabetic order of device name. For long device lists, a vertical scroll bar will appear to the far right of the view window. Additionally, you may also see a horizontal scroll bar at the bottom of the window depending on the additional field columns.

A device can be selected by clicking anywhere on the row for that device description. When a device is selected, the background for the device changes to dark blue with white text. Multiple devices can be selected using the Shift and Control (Ctrl) keys on the keyboard as follows:

1. Select (left click on) the first device in the range.
2. Press and hold either Shift key on the keyboard.
3. Select (left click on) the last device in the range.
4. Release the Shift key. The first and last devices and all devices in between should be selected.

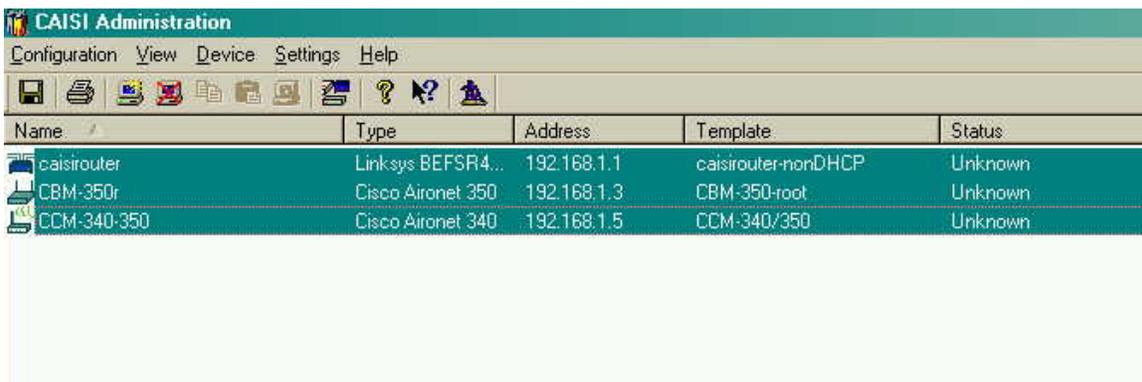


Figure 3-8 CAISI Admin-Selecting Multiple Devices

Selecting Multiple Devices Listed Separately

1. Select (left click on) the first device.
2. Press and hold either Control (Ctrl) key on the keyboard.
3. Select (left click on) additional devices. Each device selected will be added to the device selection.
4. To remove a device from the selection, click on it again.
5. When done, release the Control (Ctrl) key.

Right clicking on a device in the list brings up a context-sensitive menu that shows the options available for that device (Figure 3-9). This provides a convenient way to access commands for a specific device. Some commands on the context-sensitive menu can be executed with multiple selections, such as “Delete”. Other commands can only be executed with a single device selection, such as “Properties”, and will be grayed out if multiple devices are selected.

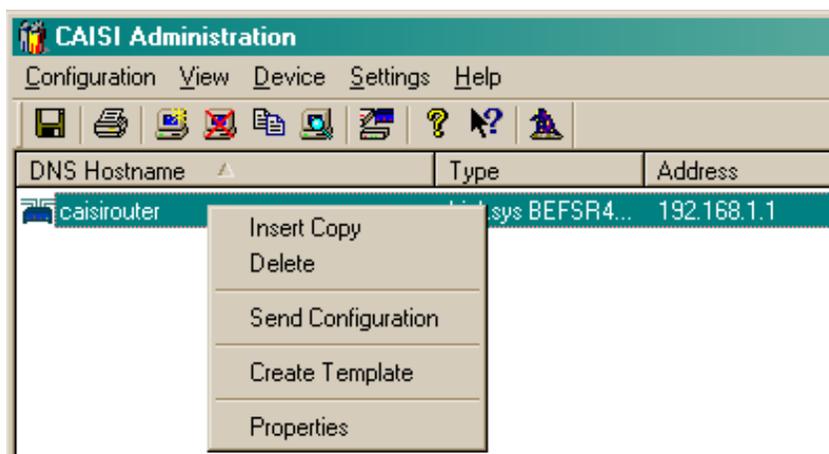


Figure 3-9 CAISI Admin-Device List with Device Context Menu

Two new commands that will help in creating devices are the “Insert Copy” and “Create Template” commands.

“Insert Copy” command allows you to make a copy of an existing device. Two devices may be identical to each except for one or two fields, ex: IP address and DNS hostname.

“Create Template” command allows you to make the current device a template.

3.2.4 Device Information Fields

Immediately below the toolbar is a list of column headers that identify each column in the list view. Besides identifying the columns, the headers provide other useful functions. Clicking on any header sorts the devices in the list according to that column field. Clicking on the same header again, toggles the sort order from ascending to descending, which reverses the sort order. Continuing to click the same header toggles the sort order back and forth.

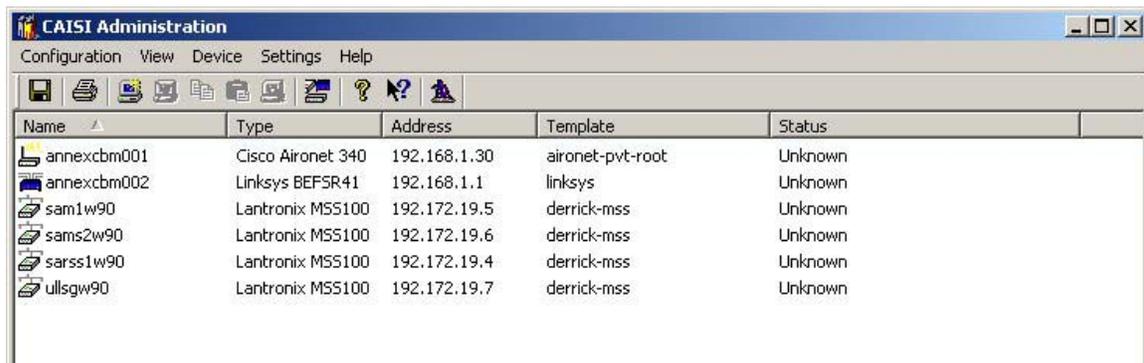
The current sort column and order is depicted with a small triangle just to the right of the column name. When the arrow is pointing up, the field is sorted in ascending order, which means alphabetically from A-Z or numerically from 0-9. When the arrow is pointing down, the sort order is descending which reverses these orders. Initially the list is sorted by name in ascending (A-Z) order, which means a gray triangle appears to the right of the header “Name” in the first column pointing up.

The header columns can also be dragged to the left or right to change the size/width of a given field. If the mouse cursor is placed over a border between two column headers, the cursor changes to a left/right arrow icon. At this point, clicking and holding the left mouse button and moving the mouse to the left or right will move that border, effectively changing the width of the field immediately to the left of the border. Note that the column border can be moved all the way to the far left up to the previous column, which has the effect of hiding the field being resized.

3.2.5 View Types

The CAISI Admin provides an option on the “View” menu to control which columns are displayed in the device list. The default mode is ‘Network View’ and displays the following fields:

- Name – name of the device
- Type – identifies basic device type or driver
- Address – network address of the device
- Template – pre-configured device template used to create device
- Status – operational status of device (future implementation)



Name	Type	Address	Template	Status
annexcbm001	Cisco Aironet 340	192.168.1.30	aironet-pvt-root	Unknown
annexcbm002	Linksys BEFSR41	192.168.1.1	linksys	Unknown
sam1w90	Lantronix MSS100	192.172.19.5	derrick-mss	Unknown
sams2w90	Lantronix MSS100	192.172.19.6	derrick-mss	Unknown
sarss1w90	Lantronix MSS100	192.172.19.4	derrick-mss	Unknown
ullsgw90	Lantronix MSS100	192.172.19.7	derrick-mss	Unknown

Figure 3-10 CAISI Admin-Network View Mode

The network view mode is intended for ascertaining a device’s operational status. In the current release, the status field is not updated and does not accurately reflect the device’s status.

NOTE: *This feature is planned to be included in a future release of the CAISI Administration software.*

An alternative display is the ‘Device View’ mode, which displays the following information:

- Name – name of the device
- Type – identifies basic device type or driver
- Address – network address of the device
- MAC Address – unique Media Access Control (MAC) device address
- Location – optional notes concerning device’s location
- Notes – optional miscellaneous device comments

This mode is useful for viewing details for devices such as the MAC address and location.

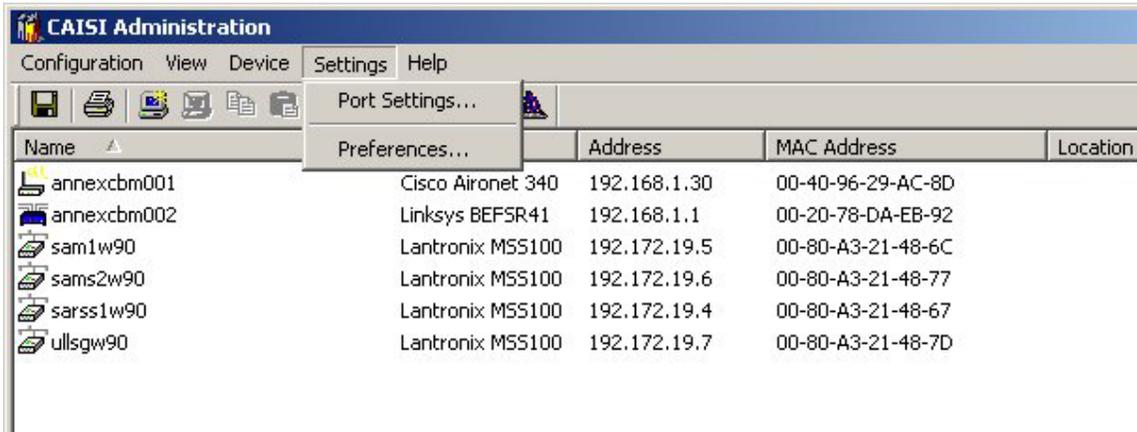


Figure 3-11 CAISI Admin-Device View Mode

3.3 DEVICES

Conceptually, a device represented in the CAISI Admin consists of a device type and a list of device properties. The device type identifies the driver used to communicate to the device when the configuration is sent. The properties list stores all other information about the device, including its network configuration, identification and all device-specific parameters.

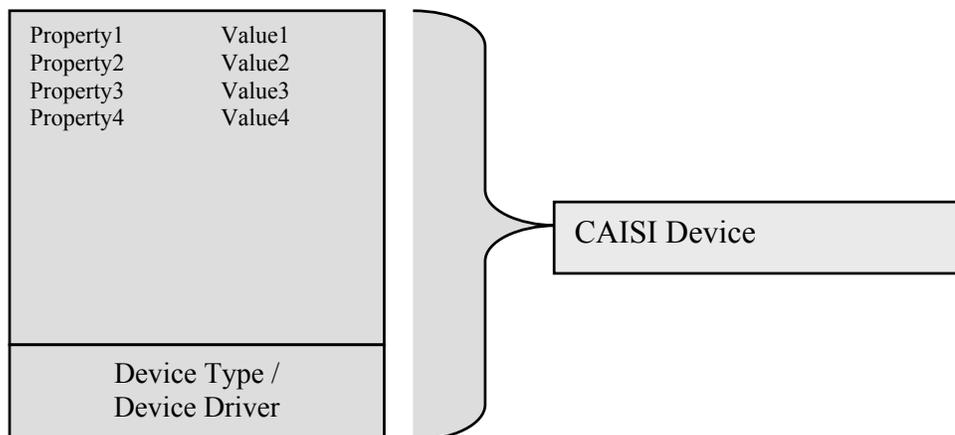


Figure 3-12 CAISI Admin-Device Properties Model

When the configuration for a given CAISI device is sent to that physical device, the CAISI Admin uses the driver to establish communication with the device, and then formats each property into a parameter command that is then issued to the device.

The device properties dialogs within the application provide convenient interfaces for changing common device properties, such as network address and gateway. Additional properties for a given device exist which are not exposed in the dialogs. These ‘hidden’ properties are sent to the physical unit in the same manner as the exposed properties.

The “Device Templates” dialogs allow these ‘hidden’ properties to be modified, added or removed as necessary.

3.3.1 Device Properties

There are four tabs on the Device Properties Screen:

- General Properties – are required for each device. Contains the administrative and access passwords.
- Network Properties - are required for each device. Contains the Internet Protocol (IP) address information.
- Details Properties – are optional.
- Advanced Properties – special configuration properties for each device.

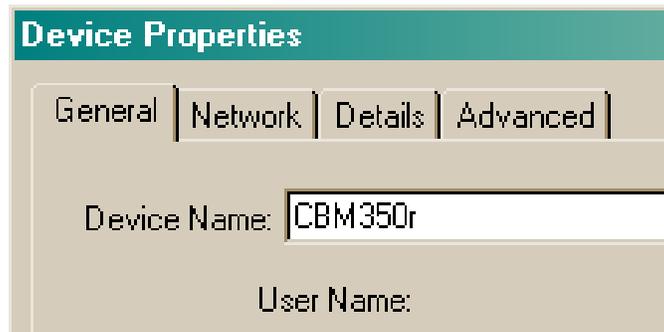


Figure 3-13 CAISI Admin-Device Properties Tabs

3.3.1.1 General Properties

General properties are required for each device and are used to define and setup the administrative and access passwords for the device. Additionally, the general device properties contain device template, status, and property modification and usage information that is not directly modifiable by the user.

Table 3-1 General Device Properties

Property	Description
Device Name (Host Name)	The Name used to identify the device both within the CAISI Admin and the name on the network in which the device physically belongs. The device name is restricted to 14 characters in length. (No spaces and no special characters)
Administrative Password	The Administrative password is used to gain privileged access to the device in order to administer the device.
Access Password	The Access password is the password needed by users to gain access to the device. This password does not allow administrative privileges.
Static Properties	(These properties are not editable and are not used by the physical device in any way)
Device	The Device identifies the type of device.
Template	The Template identifies the device template from which the device was created.
Status	The Status indicates the current status of the device (future implementation).
Created	The Created indicates when the device was first created in the CAISI Admin.
Modified	The Modified indicates the last time the device properties were modified.
Last Updated	The Last Updated indicates when the device properties were last sent to the device.

3.3.1.2 Network Properties

Network properties are required for each device and are used to define how each device gets its Internet Protocol (IP) Address and how it appears across a Local Area Network (LAN) or diverse Wide Area Network (WAN). For example, some devices may need to appear outside a firewall and therefore require a public IP Address whereas others may need to maintain a private IP address for use behind a firewall.

Table 3-2 Network Device Properties

Property	Description
DNS Hostname	Same as the device name. Automatically filled in.
Obtain network settings automatically (DHCP): IP address automatically assigned by a DHCP server. or Use the following settings: Give the device a specific address	
IP Address	The Internet Protocol (IP) address is a 32-bit number made up of four numbers or octets ranging from 0-255 with each being separated by periods. This is a required setting.
Subnet Mask	The subnet mask is a number that when combined with the IP address, identifies what network the device is to be on. The subnet mask is a 32-bit number made up of four numbers ranging from 0-255 separated by periods. This is a required setting.
Gateway	The gateway is the IP address of a local router on the same LAN as the device that is used to route IP traffic to destinations beyond the LAN. The gateway acts as a connection between separate IP networks allowing them to communicate with each other.
Domain	The Domain is part of the Domain Name Server (DNS) system naming structure and is the domain name by which a domain is known to the network. The domain name consists of a sequence of labels separated by periods. The device will be associated with the domain that is entered. CAISI default is "Warning.US.Government". For security issues, the default is used to let anyone who gets into the site know that it is a government site. Due to the fact that majority of the devices used will be behind the encryptor, domain name will make no difference.
First DNS	The First (DNS) is the IP address of the primary DNS server that is used in mapping IP addresses to the names assigned to network devices used by the device that cannot be resolved through the local name (hosts) table. This is not a required setting.
Second DNS	The Second DNS is the IP address of the secondary DNS server. This is not a required setting.
Third DNS	The Third DNS is the IP address of the tertiary DNS server. This is not a required setting.

3.3.1.3 Details Properties

Details properties are optional for all devices. The device details properties allows the user to store additional information associated with the device configuration for reference. These properties are not actually sent to the device but are stored information.

Table 3-3 Details Device Properties

Property	Description
Location	An optional 255-character text field that can be used to describe where the device is physically located.
Notes	An optional 255-character text field that can be used to house any additional information or important instructions that pertain to the particular device.

3.3.1.4 Advanced Properties

Many devices require some special configuration properties in order to take full advantage of all the capabilities of that device. Since these properties can vary drastically between devices, a special device specific property page is added to the standard General, Network, and Details properties that are common to all devices. This special property page is where additional configuration information can be entered for the device.

In the following sections are descriptions of the special configuration properties for each of the devices currently supported by the CAISI Administration application. In these sections, a table will be presented that outlines each of the device specific properties available for configuration as well as a screen shot of the actual device specific properties dialog.

Examples of Advanced Properties of Components are as follows:

CISCO Aironet 340 / 350 Wireless Bridge Properties

The “Advanced” dialog for the Aironet 340 and 350 devices allow the user to configure the most common parameters necessary for establishing a wireless link to another unit.

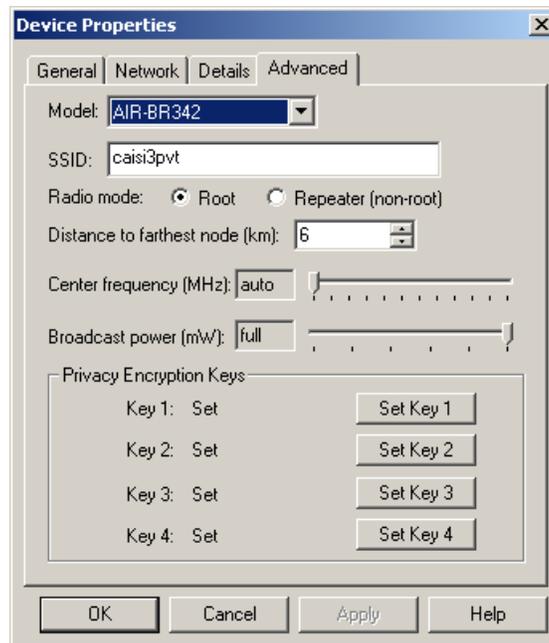


Figure 3-14 CAISI Admin-Aironet Device Specific Properties Dialog Box

The following table details the Aironet device specific properties available for configuration in the CAISI Admin:

Table 3-4 Aironet Specific Advanced Properties

Property	Description
Model (only for workgroup)	Identifies the specific Aironet 340 / 350 model (bridge or workgroup), which controls certain radio settings that differ between the models.
SSID	Service Set Identifier. Acts as a passcode between wireless units. All wireless units that will participate in the wireless network must have matching SSID's.
Radio Mode	Determines the role of the unit in a wireless hierarchy
Root	Master unit in wireless hierarchy. Controls all wireless routing. Only one unit can be root within a hierarchy. (This property grayed out for workgroup bridge.)
Repeater (Non-Root)	Slave unit in wireless hierarchy. Receives routing information from separate root unit. (This property grayed out for workgroup bridge.)
Distance to farthest node (Km)	Distance in kilometers to farthest wireless unit. Used to adjust for propagation delays. (This property grayed out for workgroup bridge.)
Center frequency (MHz)	Center frequency of transmissions. Actual transmission frequencies will vary slightly above and below this value. (This property grayed out for workgroup bridge.)
Broadcast Power (mW)	Transmission power. Adjustable to handle country-specific broadcast limits and terrain requirements.
Privacy Encryption Keys	Keys used for encryption of wireless traffic per IEEE 802.11.
Key 1	Encryption key 1
Key 2	Encryption key 2
Key 3	Encryption key 3
Key 4	Encryption key 4

Linksys BEFSR41 / BEFSR81 Properties

Since the Linksys BEFSRX1 series units act as firewalls, additional network configuration parameters are necessary to properly define the firewall behavior. Specifically, parameters are required for the additional private network segment, DHCP serving and port forwarding. The following table details the Linksys device specific properties available for configuration in the CAISI Admin:

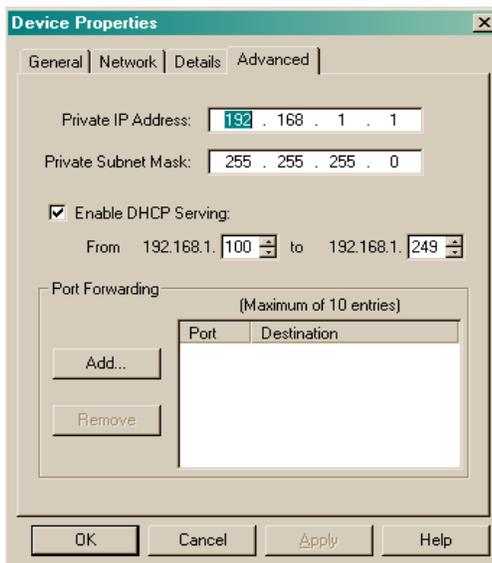


Figure 3-15 CAISI Admin-Linksys BEFSR41/81 Device Specific Properties Dialog Box

Table 3-5 Linksys Specific Advanced Properties

Property	Description
Private IP Address	The network address of the firewall unit on the private (protected) network segment.
Private Subnet Mask	The subnet mask associated with the private IP address above.
Enable DHCP Serving	Controls whether the DHCP server is enabled.
From IP	Starting address for pool of IP's leased to DHCP clients.
To IP	Ending address for pool of IP's leased to DHCP clients.
Port Forwarding	Provides redirection of network packets to machines behind the firewall on a per-port basis.
Port	Destination port of incoming network packet.
Destination	IP address of machine in private network to which to redirect packets.
Add	Dialog for adding new port redirection assignment.
Remove	Removes selected assignment from redirection list.

LSA MSS-100 VEE Properties

The LSA MSS-100 micro terminal server is used to provide Virtual End-To-End (VEE) compatibility with clients that cannot operate over an Ethernet interface. VEE compatibility is accomplished via a software emulation program running on the MSS100. The VEE dialog tab controls specific behavior of the emulation software.

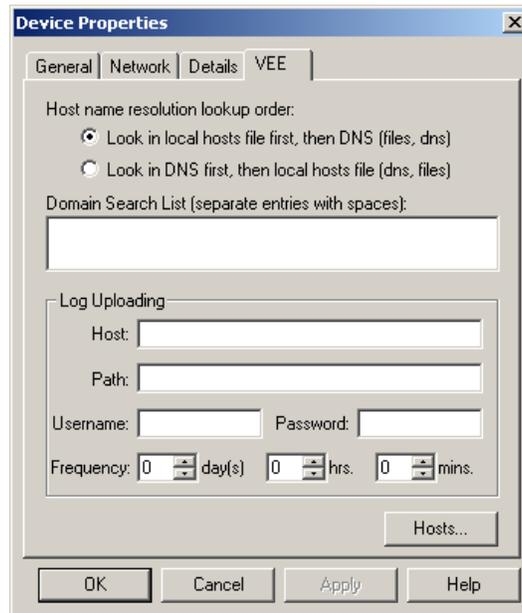


Figure 3-16 CAISI Admin-LSA MSS-100 Device Specific Dialog Box

The following table details the LSA MSS-100 device specific properties available for configuration in the CAISI Administration application:

Table 3-6 LSA MSS-100 Specific Advanced Properties

Property	Description
Look in local hosts first...	Controls order of name resolution lookups. Names are first resolved by looking in hosts text file on MSS100. If not found, name is resolved via the configured DNS servers.
Look in DNS first...	Controls order of name resolution lookups. Names are first resolved via the configured DNS servers. If DNS lookup fails, name is resolved using hosts text file.
Domain Search List	Space separated list of domain suffixes to try when resolving names.
Log Uploading	Allows VEE activity logs to be uploaded via FTP to central server.
Host	Name or IP address of server to receive log file (destination).
Path	File path on destination server to store log file. The supplied account must have write permission in the directory.
Username	Username of account for FTP authentication.
Password	Password of account for FTP authentication.
Frequency	Controls how frequently logs are uploaded to server.
Days	Number of days between log upload attempts.
Hours	Number of hours between log upload attempts.
Minutes	Number of minutes between log upload attempts.
Hosts	Dialog for modifying host aliases list in local hosts file.

3.4 DEVICE TEMPLATES

The network devices within the CAISI system contain many parameters that must be configured for proper operation. If all operational parameters had to be manually specified every time a device was added into the CAISI Admin, managing devices would become laborious. The CAISI Admin software application alleviates cumbersome device property setting through the use of device templates of which the main templates the user will need are supplied pre-created within the CAISI Admin Application.

Device templates allow the CAISI system administrator to pre-define devices with certain parameters. The templates mimic the CAISI device in that they contain the exact same property dialogs for configuring the device parameters. However, templates are not associated with a physical device and thus do not appear in the main device list. When a device is created in CAISI, a template is selected as the starting point for the device. The newly created device inherits all the pre-defined properties that were entered into the various text blocks, checklists and drop-down menu selections that the user has entered when creating the template. This allows the user to quickly create devices without having to re-enter common parameters manually every time.

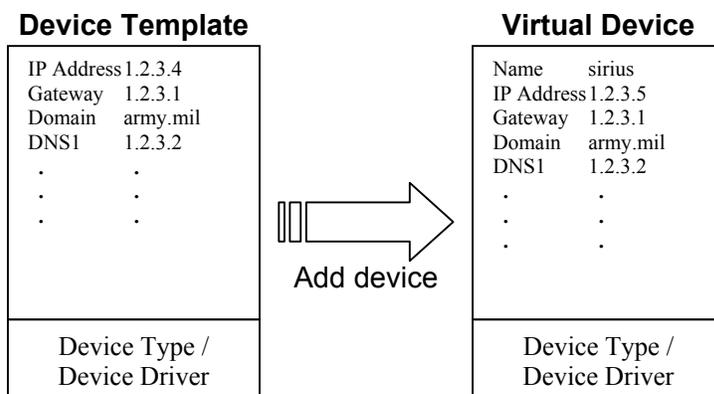


Figure 3-17 Creating a Device From a Device Template

Since network devices must have certain unique identification information (name, IP address) CAISI Admin prompts the user to supply the name and IP address for the new device. You will also be prompted for a password. All other device properties, however, are copied from the template. Any of the inherited template properties can be modified in the device by using the “Device Properties” dialog, so that the user can override any particular device value if necessary.

3.4.1 Device Attributes vs. Template Properties

The sum total of a CAISI device definition consists of its device driver and properties. Many of the more common device properties are exposed in the device property dialogs. However, many other parameters for a device are not exposed but are crucial to the proper operation of the device. These ‘hidden’ parameters, or device attributes, rarely require modification by the user.

The ‘hidden’ attributes within CAISI Admin cannot be accessed or modified within an existing device to prevent accidental modification of sensitive configuration parameters. However, all

attributes can be directly manipulated within device templates using the “Attributes” tab in the template properties dialog.

The “Attributes” tab displays attributes created using the standard dialogs as well as attributes that are static and not modifiable through any dialog. The attributes list box displays a comprehensive list of configuration parameters for a device template and is intended to allow advanced configuration of CAISI devices. Using the attributes list box, templates can be established for specific device behavior by manually modifying or adding any additional static device-specific parameters. When new devices are created from this template, they will inherit all of the advanced parameters along with the standard parameters assigned by the device property dialogs.

NOTE: *The “Attributes” tab allows greater control over the device configuration and should be used with caution. Only users that are intimately familiar with a given device should attempt modifications directly to the attribute list. If there is ever a reason why a user would need to access and/or change these attributes manually then refer to Chapter 2 of this manual, “CAISI Manual Procedures Overview, Configuration And Tools” for detailed instruction in the use of tools, configuration utilities and setup steps using manual software procedures.*

3.4.2 Creating a Template

To create a new template:

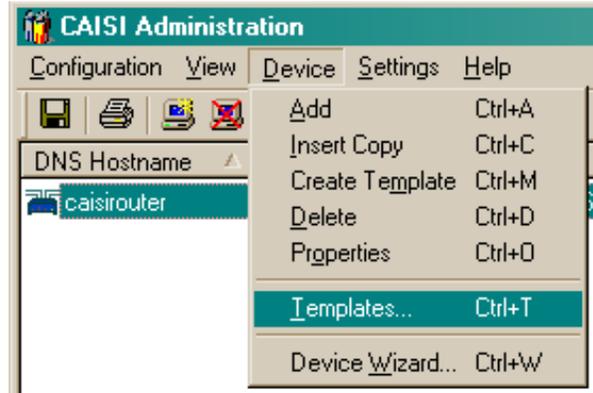


Figure 3-18 Device Templates-Main Menu Option

1. Click on the “**Device**” main menu option.
2. Click on the “**Templates**” sub-menu option. The “Device Templates” dialog box will then be displayed. (The “Device Templates” dialog box displays a list of all device templates currently defined in the CAISI Admin system).

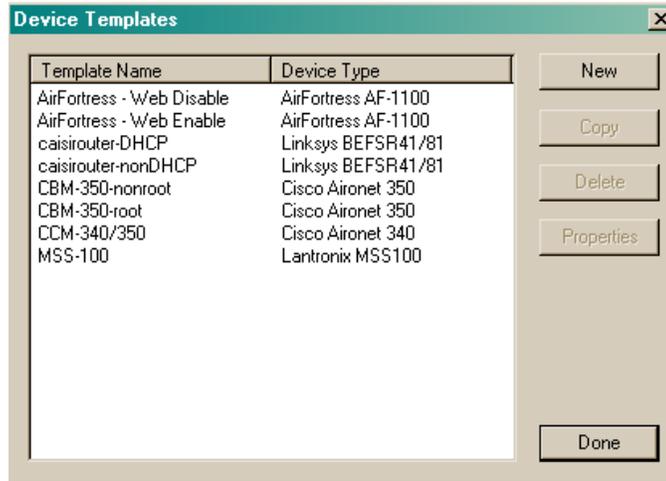


Figure 3-19 Device Templates-Dialog Box

- Click on the button labeled “**New**”. The “New Device Template” dialog will then be displayed.

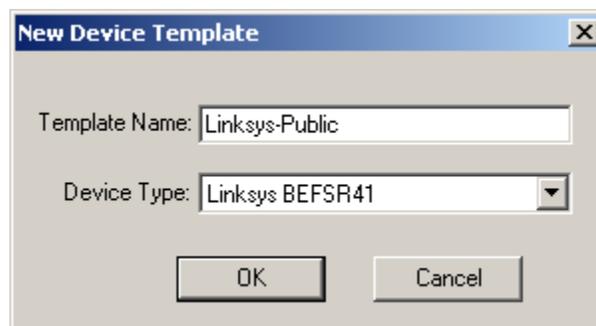


Figure 3-20 New Device Template Dialog Box

- Type in a name to be used for the new template in the “**Template Name**” edit box. This name can be any length and may contain any combination of characters. Try to input a name that will be descriptive. Make sure the component name is included in the template name dialog box.
- Click on the arrow in the “**Device Type**” drop-list to reveal all of the available CAISI Admin devices.
- Click on the appropriate device to select it. This will be the device type that the template is based on. The template will then conform to the same attributes and properties as the device.
- Click on the “**OK**” button. The new template will then be added to the list of existing templates.

NOTE: *The configuration MUST be saved either before exiting the application or when the application prompts to save the configuration or changes will not be saved to the permanent configuration file.*

3.4.3 Modifying Template Properties and Device Attributes

The differences between attributes and properties determine what is editable by a user and what is not. Most device attributes will not need to be modified once they have been correctly setup in the template. Since detailing all of the possible attributes and properties for each device is beyond the scope of this section, this section will only describe how to view and modify template attributes and properties.

There are four tabs associated with template properties. The following table helps to detail each of the four template property tabs:

Table 3-7 Template Properties

Property Tab	Description
General	General template properties are used to define the template name and provide descriptive text used to help describe the template and its use. Additionally, the general template properties contain static information regarding the device type the template is based on, when it was created, when it was last modified, and last usage information.
Network	Network template properties are used to define the baseline IP Addresses, subnet masks, domain names, and DNS entries for the template. When a device is created from the template, it will initially inherit these settings.
(Device Specific)	These template properties are specific to the type of device the template is based on. Please refer to Section 3.3.1.4 for more details on individual device properties.
Attributes	These template properties are additional attributes that can be set for the device selected.

To modify template properties:

1. Click on the “**Device**” main menu option (Figure 3-18).
2. Click on the “**Templates**” sub-menu option. The “Device Templates” dialog will then be displayed (Figure 3-19).
3. Click on the name of the template to modify. (Highlight it).
4. Click on the button labeled “**Properties**”.

The “Template Properties” dialog box will then be displayed.

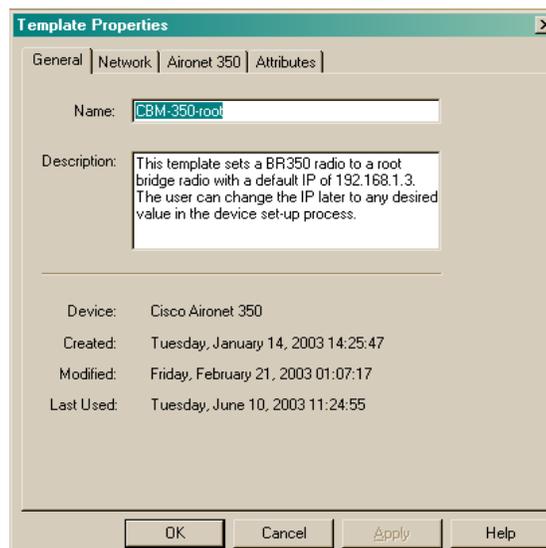


Figure 3-21 Template Properties - Dialog Box

3.4.4 Modifying General Properties

1. Select the tab labeled “**General**” from the “Template Properties” dialog box.
2. Edit the name and/or description properties as necessary. The template name may be any length and should be something descriptive. The template description should be used to add any additional text that can aide in better describing the template and how it is used.
3. Click on “**Apply**” and/or “**OK**” button to update the template configuration.
4. Click on the “**OK**” button to exit the “Device Templates” dialog box.

3.4.5 Modifying Network Properties

Select the tab labeled “**Network**” from the “Template Properties” dialog box.

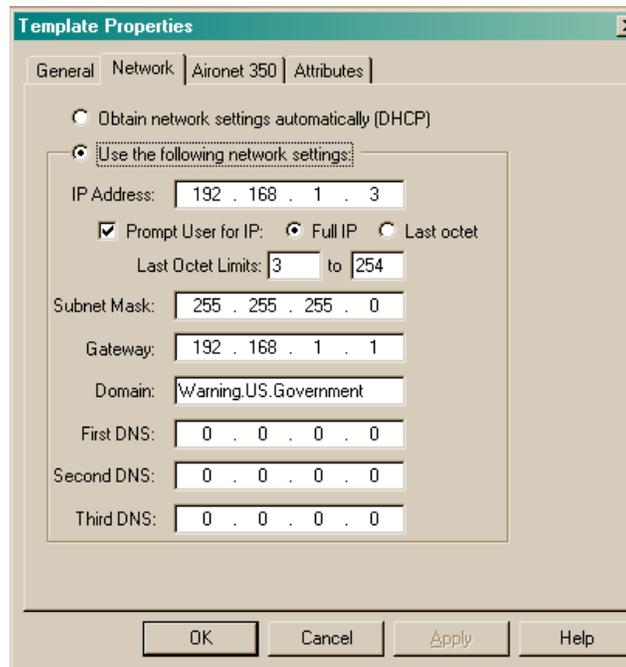


Figure 3-22 Template Properties – Network Tab

Edit one or more of the individual networking properties.

There are two different methods used to setup a device’s networking properties:

- Obtain network settings automatically (DHCP) – Selecting this radio button specifies that the device is to acquire its Internet Protocol (IP) address from a Dynamic Host Configuration Protocol (DHCP) server. Enabling this property requires no manual configuration; however a valid DHCP server must exist.
- Use the following network settings – Selecting this radio button allows custom configuration of each of the network properties.

Special attention is required if manual input of the IP address has been selected (DHCP is unselected). The IP address specified in the template should be that of the primary LAN server. These addresses typically end in “.0” although that is not a requirement.

After the IP address has been entered, check the “Prompt User for IP” checkbox and click on the “Full IP” to enable setting the full IP address during device creation.

NOTE: *The template can be setup to control how IP address values are entered during device creation. The entire IP address or only the last octet of the IP address in the template can be restricted to prevent unwanted changes during device creation. In fact, the last octet can be restricted to allow for only a certain range of values.*

To prevent all but the last octet of the IP address from being modified during device creation, check the “Prompt User for IP” check box and then click the “Last Octet” radio button. Unless otherwise specified in the “Last Octet Limits” range values, the default range values for the last octet are 1-254.

To prevent the full IP address from being modified during device creation, uncheck the “Prompt User for IP” check box.

For a description of the remaining fields, please refer to Paragraph 3.3.1.2 Network Properties.

1. Click on “**Apply**” and/or “**OK**” button to update the template configuration. The changes will be sent to the device the next time the device is configured.
2. Click on the “**OK**” button to exit the “Device Templates” dialog box (Figure 3-22).

NOTE: *The configuration MUST be saved either before exiting the application or when the application prompts to save the configuration, or changes will not be saved to the permanent configuration file.*

3.4.6 Modifying Device Specific Properties

1. Click on the tab to the right of the one labeled “**Network**”. The label of the tab will vary depending on the device type for which the template was created.
2. Edit the device specific properties. The following figure shows the device specific properties for an Aironet Root Bridge template.

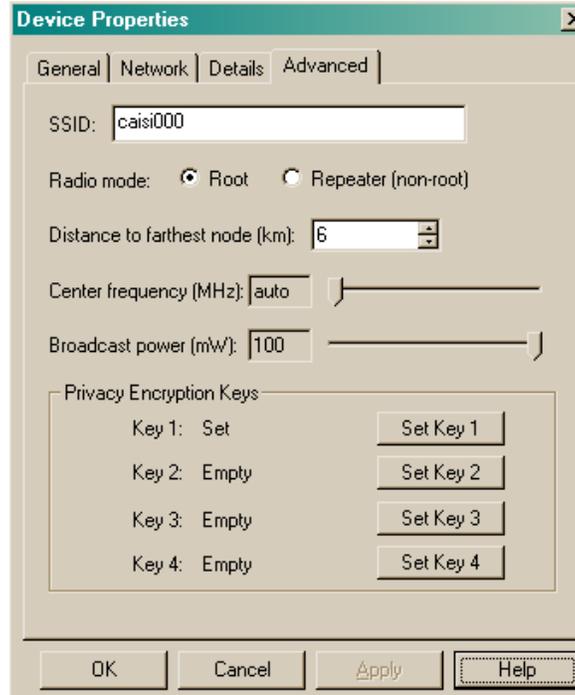


Figure 3-23 Template Properties – Device Specific

3. Click on “**Apply**” and/or “**OK**” button to update the template configuration. The changes will be sent to the device the next time the device is configured.
4. Click on the “**OK**” button to exit the “Device Templates” dialog box.

NOTE: *The configuration MUST be saved either before exiting the application or when the application prompts to save the configuration or changes will not be saved to the permanent configuration file.*

3.4.7 Modifying Attribute Properties

1. Click on the tab labeled “**Attributes**”. An attribute properties dialog will be displayed. Since each device will have different attributes, the content of the attribute dialog will vary. The following figure depicts what a typical attribute properties dialog might look like for the CISCO Aironet device.

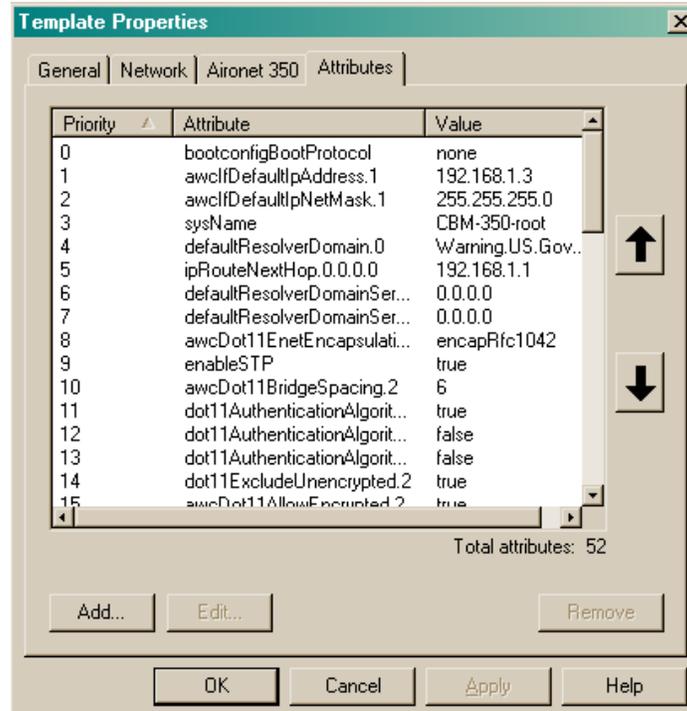


Figure 3-24 Template Properties – Attributes (Aironet example)

2. Click on the attribute to be modified.

Note that there may be one or more attributes that have an asterisk () to the left of the name. The asterisk means that that particular attribute is a priority attribute and will be sent first during device configuration. This prioritization may be necessary in some cases since changing one attribute may directly impact the setting of other attributes.*

To toggle an attribute to and/or from a priority state, simply select the attribute to change and click the “**Priority**” button.

3. Click on the button labeled “**Edit**”. The “New Attribute” dialog will be displayed and allow editing of the attribute name or value.

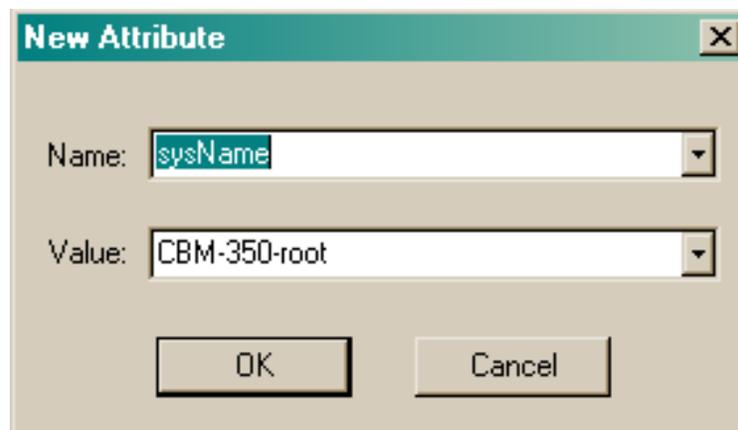


Figure 3-25 New Attribute Dialog Box

4. Make the appropriate changes to either the attribute name or the attribute's value. You will need to consult the proper device configuration documentation for valid name-pair attributes.
5. Click on “**OK**” to update the attribute list.
6. Click on “**Apply**” and/or “**OK**” in the template properties attribute dialog to update the template configuration. The changes will be sent to the device the next time the device is configured.

NOTE: *The configuration MUST be saved either before exiting the application or when the application prompts to save the configuration or changes will not be saved to the permanent configuration file.*

3.4.8 Deleting a Template

It may be necessary to delete one or more defined templates from the CAISI Admin system. Deleting a template does not have an affect on any devices that were created from the template.

To delete an existing template:

1. Click on the “**Device**” of the main menu.
2. Click on the “**Templates**” sub-menu option. The “Device Templates” dialog will then be displayed.
3. Click on the name of the template to be deleted.
4. Click on the button labeled “**Delete**”. A confirmation prompt will then be displayed.

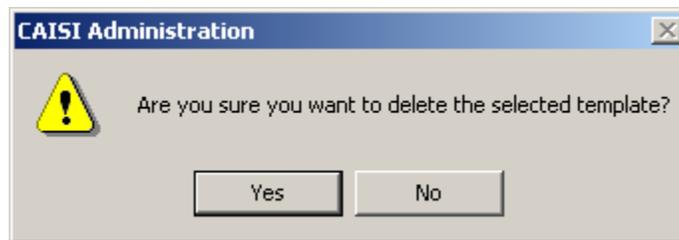


Figure 3-26 Template Deletion Confirmation Dialog Box

5. Click on the button labeled “**Yes**” to complete the deletion of the selected template, which will remove it from the list of available templates.

NOTE: *The configuration MUST be saved either before exiting the application or when the application prompts to save the configuration or changes will not be saved to the permanent configuration file.*

3.4.9 Creating a Device

There are two method used for creating a device:

- Manually, using the Add Device Method
- Automatically, using the Device Wizard

For first time users, it is recommended that device creation be done using the built-in device wizard. This is because the wizard steps through each portion of the creation process thereby acting as a tour guide during device creation.

3.4.9.1 Add Device Method

To create a device through the CAISI Admin main menu:

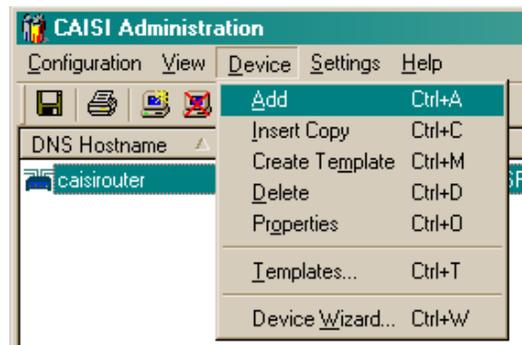


Figure 3-27 Device Add-Main Menu Option

1. Click on “**Device**” in the main menu.
2. Click on the “**Add**” sub-menu option. The “New Network Device” dialog will then be displayed.

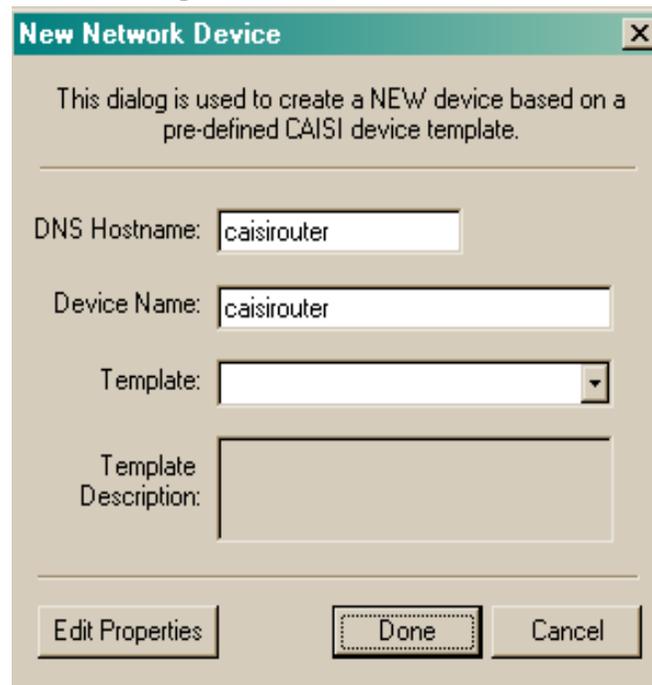


Figure 3-28 New Network Device Dialog Box

3. Click on the “**DNS Hostname**” edit box and enter a host name for the device. The name can only contain alphanumeric characters and dashes and must be no longer than 14 characters. This is the name provided by your DOIM, S6 or CSSAMO.

4. Create a **“Device Name:”** if you want it to be different from the **“DNS Hostname”**.
5. Click on the down arrow in the **“Templates”** drop-list to select a template from the list of CAISI Admin defined templates. The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited. This means that the IP address will automatically change. The application will attempt to figure out the next available IP address in that range and populate the **“IP Address”** field with that address.

NOTE: Depending on how the original template was setup, all, some, or none of the IP address field may be editable during device creation.

NOTE: At this point, you have two options. You can finish creating the device by just clicking on the **“Done”** button or click on **“Edit Properties”** to further modify the properties of the device you are creating. Refer to Section 3.4.10 if you click on **“Edit Properties”**.

6. Click on the **“Done”** button to create the device.

NOTE: The configuration **MUST** be saved either before exiting the application or when the application prompts to save the configuration or changes will not be saved to the permanent configuration file.

3.4.9.2 Device Wizard Method

To create a device using the CAISI Admin device wizard:

1. Click on **“Device”** in the main menu.

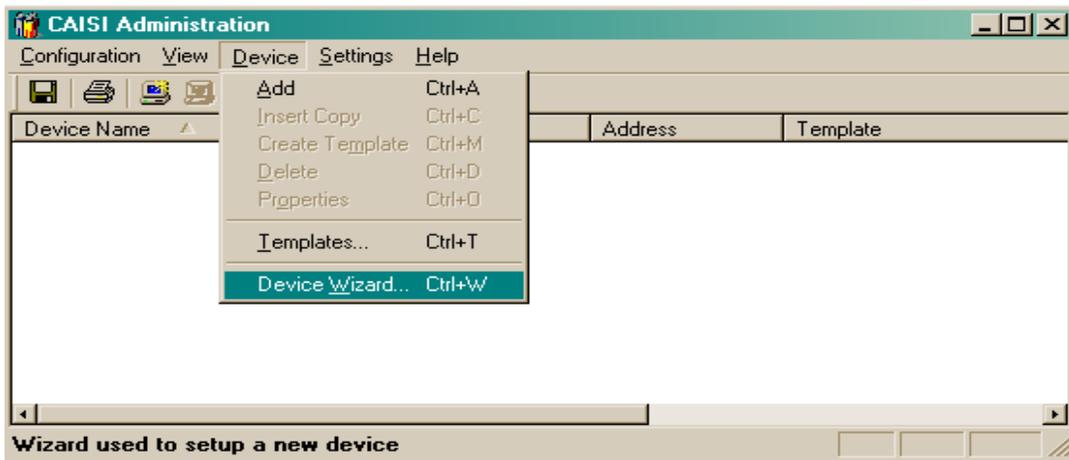


Figure 3-29 Device Wizard- Add Device

2. Click on the **“Device Wizard”** sub-menu option. The main screen for the device wizard will then be displayed.



Figure 3-30 Device Wizard-Main Dialog Box

3. Click on the radio button next to the device you want to create. As you click on the individual radio buttons, the image to the left will display the device type selected.
4. Click on the button labeled “**Next >**” to continue. The next dialog presented requires the user to select the type of network to which the device will be attached.

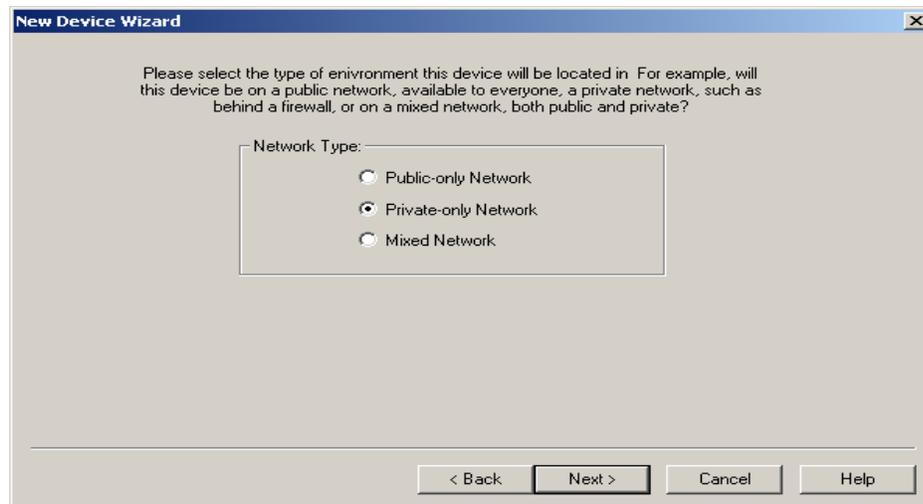


Figure 3-31 Device Wizard – Network Type Dialog Box

The Network Types are explained in Table 3-8.

Table 3-8 Network Types

Property Tab	Description
Public-only	Public indicates that the device will be configured as part of a public network on the outside of any LAN firewalls.
Private-only	Private indicates that the device will be configured as part of a private network, probably behind a firewall on a LAN. Private IP addresses for the CAISI Admin system are in the following ranges: 10.0.0.1 - 10.255.255.254 172.16.0.1 - 172.31.255.254 192.168.0.1 - 192.168.255.254
Mixed	Mixed indicates that the device can be configured as either public or private. NOTE: Templates that have the network IP set to DHCP mode will only show up under this option.

- Click on the radio button next to the network type that the device is to participate in and then click on the button labeled “Next >”. A general configuration dialog will then be displayed.

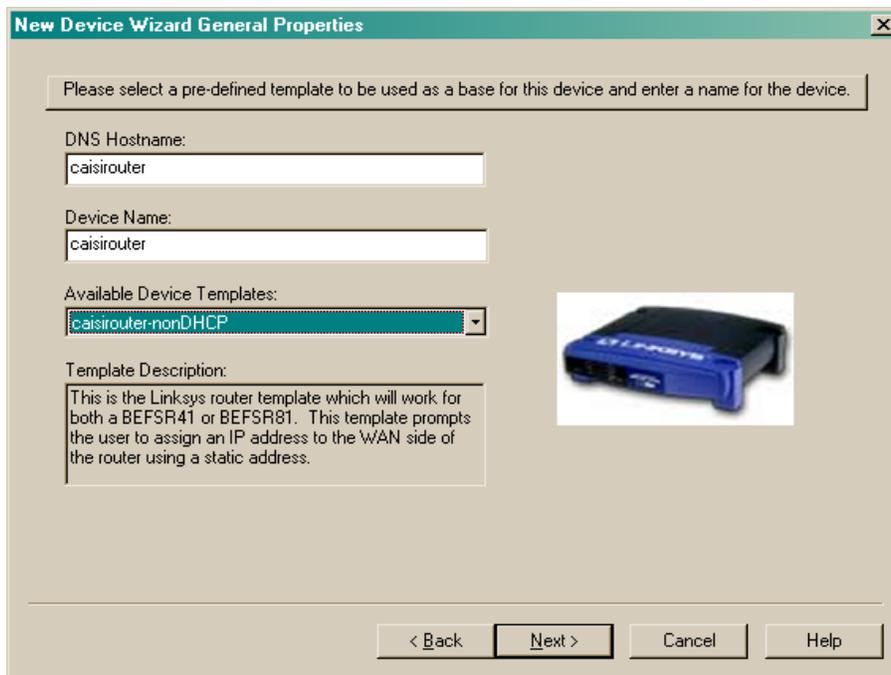


Figure 3-32 Device Wizard-Configuration Dialog Box

- Enter a DNS Hostname to be used for the new device. This name will be sent to the device and is used to identify the device on the network. The name must be no more than 14 characters in length and contain alphanumeric characters (A-Z, a-z, 0-9) and dashes.
- Click on the arrow in the “**Available Device Templates**” drop-list to reveal all of the available CAISI Admin templates for the network type that was selected.

8. Click on a template to select it. The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited. This means that the “IP Address” and “Subnet Mask” fields will automatically change. The application will attempt to figure out the next available IP address in that range and populate the “IP Address” field with that address.

NOTE: *As can be seen in Figure 3-32, the template selected has been setup to only allow the user to edit the first three fields. The Template Description field is grayed out, which means that it is read-only.*

9. Click on “Next>”. The “New Device Wizard Network Settings” screen will appear.

NOTE: *Depending on how the original template was setup, all, some, or none of the IP address field may be editable during device creation.*

10. Make any necessary changes to the network settings and click on “Next >”. The “New Device Wizard Device Advanced Settings” screen will then be displayed.

Depending on what device you are adding, the advanced settings screen will be different for each device. Refer to the specific device procedures later in this TB. Click on “Next>”.

11. The “New Device Wizard Device Details” screen will appear. “Notes” and “Location” fields are both optional, mainly for documentation purposes. Click on “Next>”.
12. The “New Device Wizard Password Validation” screen will appear. Some devices will require two passwords – administrative password and an access password, other devices will only need the administrative password. The passwords are defined as:

Figure 3-33 Device Wizard-Password Dialog Box

- Administrative Password – Also known as the privileged password. It allows privileged operations that would otherwise be denied.

- Access Password – This password is used to allow access to the device. A typical example would be to view device configuration.
13. Enter an Administrative password to be used for the device. There may be some strong password enforcements placed on the password depending on the type of device being created and/or the CAISI Admin password preferences that have been enabled.
 14. Confirm the password entered in the first administrative password edit box by re-typing it into the “Confirm Administrative (Write) Password” box.
 15. Enter an Access password to be used for the device. There may be some strong password enforcements placed on the password depending on the type of device being created and/or the CAISI Admin password preferences that have been enabled.
 16. Confirm the password entered in the first access password edit box by re-typing it into the “Confirm Access (Read) Password” box.

NOTE: Write down all device passwords and store them in a secure location where they will not be compromised. If passwords are lost or forgotten after a device has been configured, the device will be UNUSABLE and will have to be reset. The application DOES NOT save passwords.

17. Click on the button labeled “**Finish**” to complete the device creation process. At this point, a dialog is presented with several options:



Figure 3-34 Device Wizard-Further Actions Dialog Box

- **Send configuration to device** – This option will begin the process of sending the configuration to the device. This will require physically connecting the device to a LAN or serial port.
- **View device properties** – This option will reveal all the properties for the device just created. Any further modifications to the properties can be done here before the configuration is sent to the device.
- **Done. No further action** – This option causes no further action to take place. The application will return to the main screen.

NOTE: Click the appropriate option. Depending on the option selected, the application will present different actions. If the “Send configuration to device” option is selected, refer to the appropriate section for the device being configured. If the “View device properties” option is selected, please refer to Paragraph 3.4.10 for viewing and modifying devices.

3.4.10 Modifying Device Properties

Once a device exists in the CAISI Admin, its properties can be modified at any time for any reason. The next few sections describe how to modify the various properties for a device. There are two important points to remember when modifying device properties:

- Modifications to device properties are not sent to the device immediately.
- Modifications to device properties are not permanent until the CAISI Admin configuration has been saved. This means that the configuration must be saved prior to exiting the application or all changes will be lost.

To modify the properties of a device:

1. Select the appropriate device from the list of devices.
2. Click on “**Device**” in the main menu. **OR** 2. Right-click on device
3. Click on “**Properties**” sub-menu option.

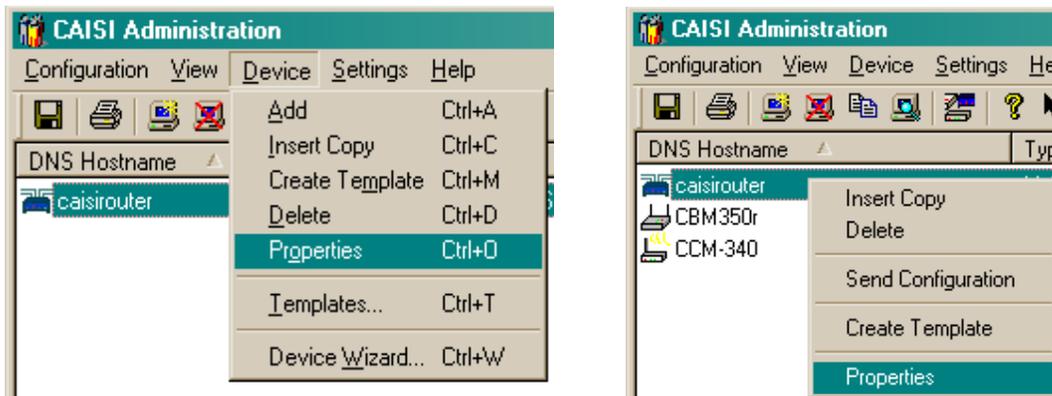


Figure 3-35 Device Properties-Main Menu Option

3.4.10.1 General Properties

The general properties for a device were previously outlined.

To modify the general properties for a device:

1. Click on the tab labeled “**General**”. The general device properties dialog will then be displayed.

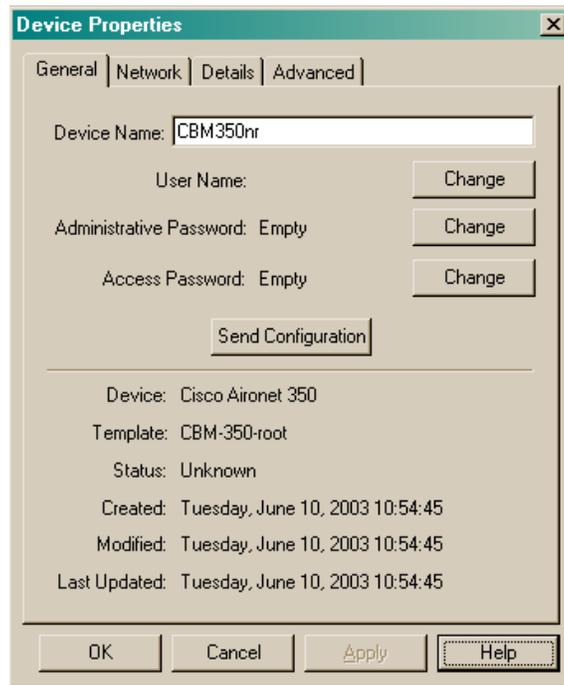


Figure 3-36 Device Wizard-General Tab

2. In the “Device Name” edit box, enter a valid name for the device. The name must be no longer than 14 characters and must contain only alphanumeric (A-Z, a-z, 0-9) characters and dashes.
3. As can be seen in Figure 3-36, there can be two passwords associated with each device.
 - Administrative Password – Also known as the privileged password. It allows privileged operations that would otherwise be denied.
 - Access Password – This password is used to allow access to the device. A typical example would be to view device configuration.
4. To change either the administrative password or the access password: Click on the “**Change**” button next to the password to be changed. A dialog similar to the following will be displayed.

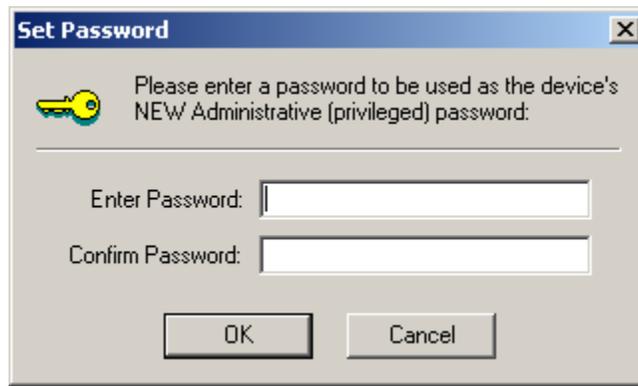


Figure 3-37 Set Password Dialog Box

5. Enter the new password to be used for the device.
6. Confirm the password entered in the first edit box by re-typing it into the second box.
7. Click on the “**OK**” button. At this point, the text next to the password changed in the device general properties dialog will change to “Changed”.

After clicking the “OK” button, the CAISI Admin has been told there is a new password to be sent to the device during the next configuration. During the actual device configuration, the application will first prompt for the old password before sending the new password. If the application is terminated before the configuration is sent to the device, all new password changes are lost. In contrast, if a device is being configured for the first time from factory defaults, and no new passwords were supplied, the CAISI Admin application will require the user to provide a new administrative and/or access password during device configuration.

It is important at this point to know that the CAISI Admin does not save each device’s active administrative and access password. Upon application termination, all current device passwords stored in the active CAISI Admin configuration are not written to disk. Therefore, the next time the application is launched; the password property fields for each device will be empty. The application will store and track password history if this preference has been enabled.

NOTE: *Since the application does not save active device passwords, it is important for the CAISI Admin administrator to write down the current passwords for each device and store these in a secure location for later reference. Without the proper passwords, the application will be unable to access the devices.*

8. Click on the “**Apply**” and/or “**OK**” button when done to temporarily update the CAISI Admin configuration.

The other, non-editable items are outlined in the following table.

Table 3-9 General Properties - Miscellaneous

Property	Description
Buttons	
Change buttons	The two change buttons are used to change/set either the administrative and/or privileged password(s). For security reasons, the actual password is not displayed. If the text to the right of the password caption indicates, “Changed”, that means that the password will be sent to the device and used as the new password. If the text indicates, “Set”, that means the password was sent to the device and is now part of the permanent device configuration.
Send Configuration button	This button is used to present the “Configure Device” dialog that is responsible for sending the device configuration (properties) to the device.
Static Properties	(These properties are not editable and are not used by the physical device in any way)
Device	The Device static text property identifies the type of device.
Template	The Template static text that identifies the device template from which the device was created.
Status	The Status static text property indicates the current status of the device (future implementation).
Created	The Created static text property indicates when the device was first created in the CAISI Admin system.
Modified	The Modified static text property indicates the last time the device properties were modified.
Last Used	The Last Used static text property indicates when the device properties were last sent to the device.

3.4.10.2 Network Properties

A device’s network properties affect how it appears across a Local Area Network (LAN) or diverse Wide Area network (WAN). In Paragraph 3.3.1.2, there is an explanation of the individual network properties that must be configured in order for a device to function correctly on any given network. Through the course of time, it may become necessary to change the behavior and identification of a networked device.

To modify the network properties for a device:

1. Click on the tab labeled “**Network**”. The network device properties dialog will then be displayed.

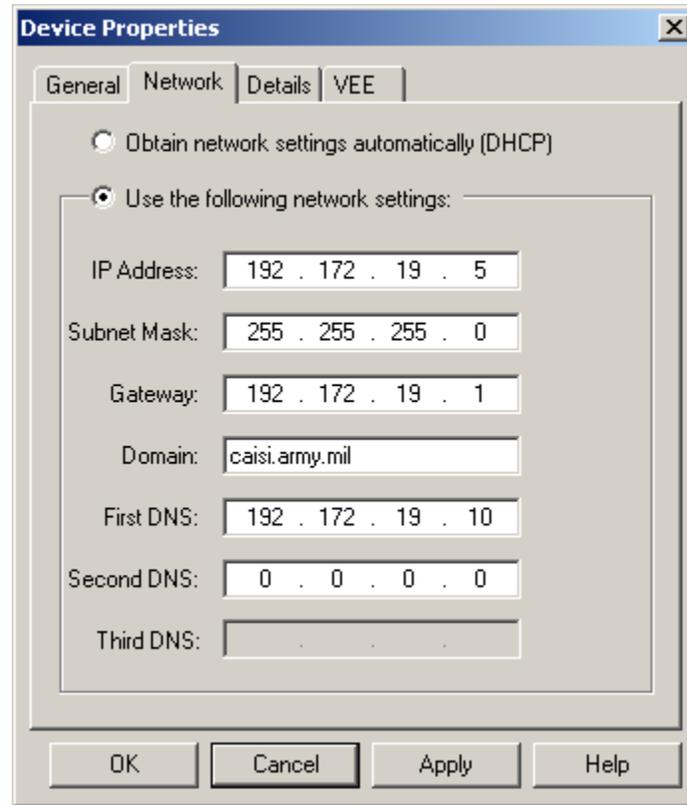


Figure 3-38 Device Wizard-Network Tab

There are two different methods used to setup a device's networking properties:

- Obtain network settings automatically (DHCP) – Selecting this radio button specifies that the device is to acquire its Internet Protocol (IP) address from a Dynamic Host Configuration Protocol (DHCP) server. Enabling this property requires no manual configuration; however a valid DHCP server must exist.
 - Use the following network settings – Selecting this radio button allows custom configuration of each of the network properties.
2. To change any of the networking properties, simply click on the property to change, make the change.
 3. Click the “**Apply**” and/or “**OK**” button. Changes made to the configuration will not be sent to the device until the application is instructed to do so.

NOTE: *The configuration MUST be saved either before exiting the application or when the application prompts to save the configuration or changes will not be saved to the permanent configuration file.*

3.4.10.3 Details Properties

As stated in Paragraph 3.4.1, the details properties are optional for all devices since these properties are never sent to the actual device.

To change the details properties for a device:

1. Click on the tab labeled “**Details**”. The device details properties dialog will then be displayed.

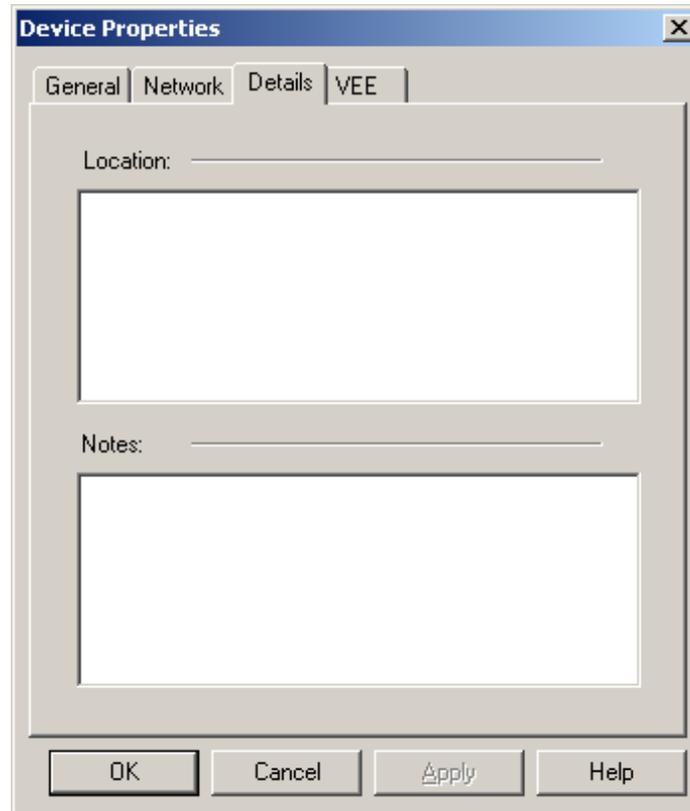


Figure 3-39 Device Wizard-Details Tab

2. Enter any text information into the location and/or notes text boxes. This information is not sent to the device during device configuration. This information is generally used as a reference to detail some important points about the device.
3. Click on the “**Apply**” and/or “**OK**” button when done to temporarily update the CAISI Admin configuration.

NOTE: *The configuration MUST be saved either before exiting the application or when the application prompts to save the configuration or changes will not be saved to the permanent configuration file.*

3.4.10.4 Advanced Properties

Paragraph 3.3.1.4 explains that each device has to have its own set of custom or advanced properties that need to be configured. These processes are done to bring out the full capabilities of the device. Paragraph 3.3.1.4 also listed a table of advanced properties for each device currently supported by the CAISI Admin application.

Since no two devices share the same properties, it is difficult to detail all of the steps required to modify these properties for each and every device. This section will not go into detail on modification of advanced properties for each device.

To modify the advanced properties for a device:

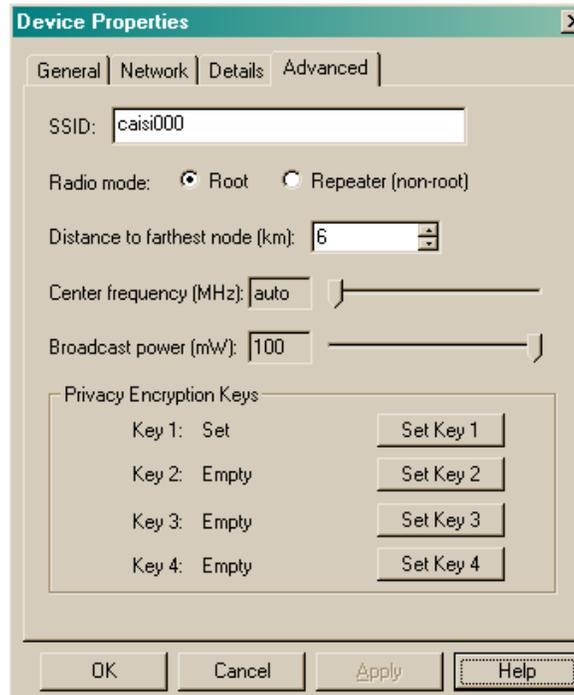


Figure 3-40 Device Wizard-Advanced Tab

1. Click on the tab located to the right of the tab labeled “**Details**”. The label of the tab will generally be “**Advanced**” but may vary between devices. Figure 3-40 depicts the device specific properties for an Aironet client device.
2. Click on the appropriate dialog controls to make any necessary changes.
3. Click on the “**Apply**” and/or “**OK**” button when done to temporarily update the CAISI Admin configuration.

NOTE: *The configuration MUST be saved either before exiting the application or when the application prompts to save the configuration or changes will not be saved to the permanent configuration file.*

3.4.10.5 Deleting a Device

It may be necessary to sometimes delete one or more devices from the CAISI Admin system.

To delete an existing device:

1. In the main view, click on the device to be deleted. To select more than one device, hold down the Ctrl key while clicking on devices.
2. Click on “**Device**” in the main menu.
3. Click on the “**Delete**” sub-menu option. A confirmation prompt will then be displayed.

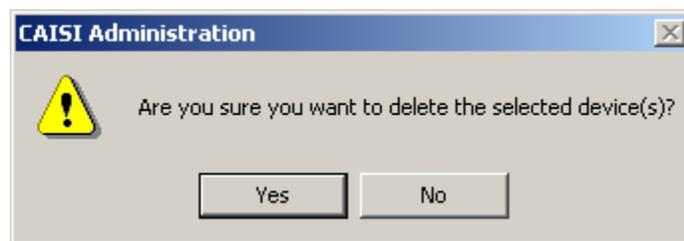


Figure 3-41 Delete Confirmation Dialog Box

4. Click on the button labeled “**Yes**” to complete the deletion of the selected device, which will remove it from the list of available devices.

NOTE: *The configuration MUST be saved either before exiting the application or when the application prompts to save the configuration or changes will not be saved to the permanent configuration file.*

Section II Configuring Components Using CAISI ADMIN

The use of the CAISI Admin tool simplifies the configuration process of CAISI components. CAISI Admin provides the SSR with two configuration options.

1. The “**Add**” option is a simplified process using a Graphic User Interface (GUI) tool.
2. The “**Device Wizard**” option is a guided process that allows the user to pick and choose the results they desire.

3.5 UTILIZING CAISI ADMIN TO CONFIGURE THE ROUTER (FIRMWARE 2.40.2)

NOTE: A standard CAISI SSR notebook, configured as follows is required for router set up. It 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. Wired or built-in NIC must be used.

Two versions of Linksys router are in the CAISI system. (Version 2 is used as a basis for procedures and screenshots).

Version 1 has an uplink switch for port 8. Port 8 can be used for crossover “X” or straight-through “=” connections. Power supply consists of a power adapter and a 3-prong power cord.

Version 2 has an automatic senser for crossover or straight-through connections, therefore all 8 ports can be used for connection. Power supply consists of a wall-style power adapter.

3.5.1 Perform Router Connection Procedures

1. Remove the router and power supply from the SSR Transit case.
2. Connect the female end of the power supply to the port labeled “**Power**” on the back of the router.
3. Plug the male end of the power supply into an external power source.
4. If the router is receiving power, the “**Power**” LED on the front of the device will be lit green.
5. Remove a white straight-through Ethernet cable from your SSR Transit case or SSR Notebook case.
6. Connect one end of the white straight-through Ethernet cable to the wired/built-in NIC on your SSR notebook and the other end into an available port on the router (ports 1-7 on version 1 router and ports 1-8 on version 2 router).

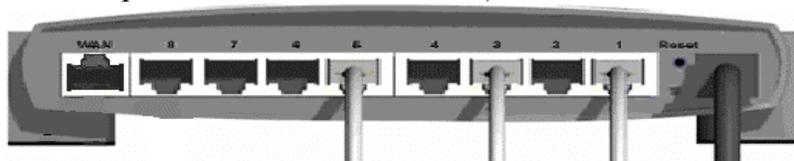


Figure 3-42 Router Ethernet Cable Connection

3.5.2 Apply Power to the SSR Notebook

1. Logon to the notebook computer.
 - a. Press “**Ctrl-Alt-Delete**”.
 - b. When prompted enter the username and password, the CAISI defaults are **caisiadmin** and **BS_69dlw**.
 - c. A Logon Message prompt will appear, “Your password expires today. Do you want to change it now?” For classroom training, click on the “**No**” button.

3.5.3 Reset the Router to Factory Settings

1. Remove a reset tool from the SSR Transit case or SSR Notebook case.

Version 1

- a. Insert the tip of the reset tool into the reset buttonhole on the back of the router and hold for 15 seconds.
- b. During this process the “**Diag**” light will light up, the “**Link**” light will light up momentarily, then both lights will go off, and the router will now be reset.
- c. If the green “**Link**” light does not flash, try again.

Version 2

- a. Insert the tip of the reset tool into the reset buttonhole on the back of the router and observe the following:
- b. The “**Diag**” light will light up red, all of the LEDs on the “100” level will blink twice, then all of the LEDs on the “Full/Col” level will blink twice, then all of the LEDs on the “Link/Act” level will blink twice. The “Diag” LED will then go out. The router will now be reset.
- c. If the “**Diag**” light does not go out, try again



Figure 3-43 Router Link Lights

3.5.4 Configure the Router

1. At the bottom of the notebook screen, click on the “>>” to the right of the “**CAISI Toolbox**” button. The CAISI Toolbox menu will appear.
2. Click on the “**CAISI Admin**” menu selection.
3. **Set-up the Router device.** There are 2 methods, 1) By selecting the “**Add**” option or 2) Use of the “**Device Wizard**” option from the “**Device**” drop-down menu. You may choose either method.

a. **“Add” Option Method**

- 1) Select **“Device”** from the CAISI Admin menu and then select **“Add”** from the **“Device”** drop-down menu.

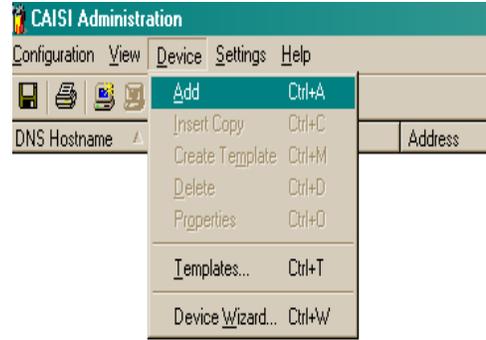


Figure 3-44 Router Add Option Menu

- 2) Set **“DNS Hostname:”** (Where **“DNS Hostname:”** = the host name of the router) to the name provided by your DOIM, S6 or CSSAMO. The CAISI default is **caisirouter**.
- 3) Create a **“Device Name:”** if you want it to be different from the **“DNS Hostname.”**
- 4) From the **“Template”** drop-down menu select **caisirouter-DHCP** or **caisirouter-nonDHCP**, as prescribed by your DOIM, S6 or CSSAMO. These settings apply to the WAN side of the router.

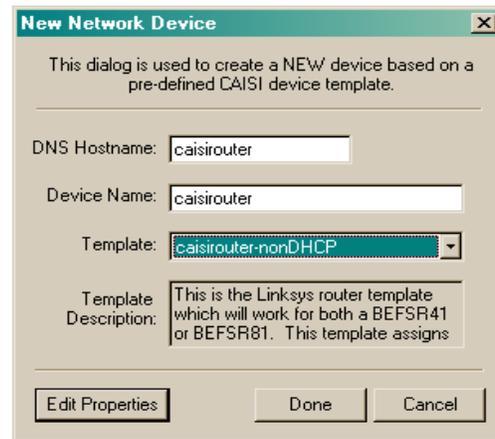


Figure 3-45 Router New Network Device Menu

NOTE: *The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited.*

- 5) For classroom training, set **“Template”** to **caisirouter-nonDHCP** from the drop down menu.

- 6) Click on the “**Edit Properties**” button. The “**Device Properties**” screen will appear with the “**General**” tab selected.
 - a) Set the “**Administrative Password**” to the password provided by your DOIM, S6 or CSSAMO.
 - b) Click on the “**Change**” button. The Set Password screen will appear.

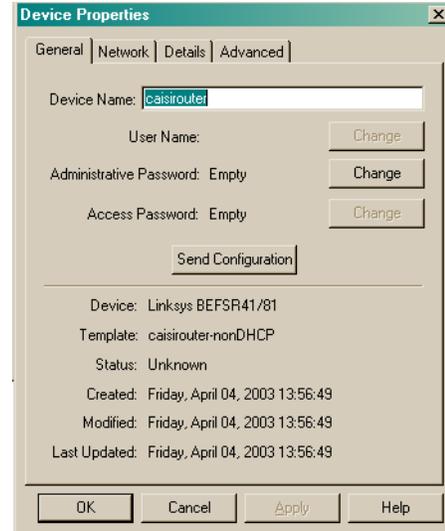


Figure 3-46 Router Device Properties General Tab

- c) Enter your new password in the “**Enter Password**” dialog box.
 - d) For classroom training set the password, to the CAISI default “**system**”.

NOTE: *As you enter the password, asterisks will appear. The password is not shown in the clear. You must change the password before you deploy the router.*

- e) Press on the <Tab> key and confirm the new password by entering the password in the “**Confirm Password**” dialog box.
 - f) Click on the “**OK**” button.

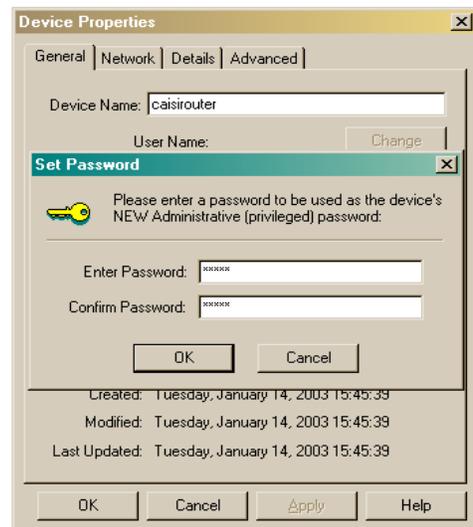


Figure 3-47 Router Set Password Screen

NOTE: *Until you actually send the configuration to the router, the administrative password field may indicate “empty” even though you entered it earlier. If you have previously sent this configuration to the router, it will indicate a status of “set”. However, the application does not store user names or passwords. They are cached during the current session, but are lost as soon as you exit from the application. An asterisk to the left of the field name indicates that the password is cached. If there is no asterisk, you must reenter the password.*

- g) If you have made changes to values on the “**General**” tab click on the “**Apply**” button.

- 7) Click on the “**Network**” tab.
 - a) If you selected **caisirouter-nonDHCP** perform the following procedure, otherwise you may skip to (7.b).
 - (1) Click on the “**Validate**” button.
 - (a) If the IP Address is unique, click on the “**OK**” button when prompted.
 - (b) If the IP Address is not unique, a list box will pop up to show you the other device configurations that use that address. Click on the “**OK**” button to dismiss the list box. If necessary, enter a new IP Address.

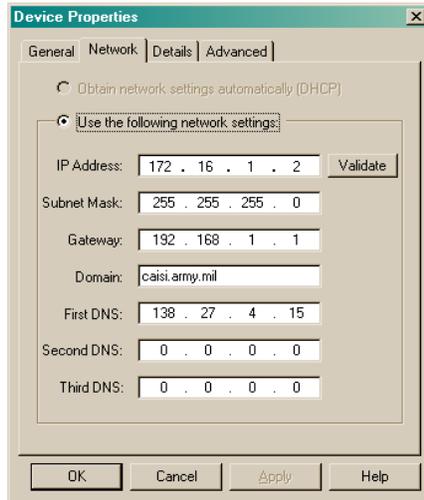


Figure 3-48 Router Device Properties Network Tab

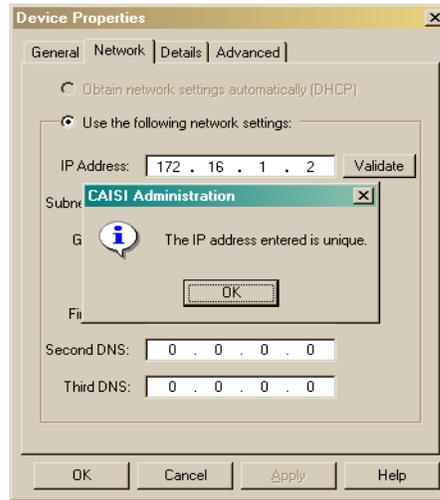


Figure 3-49 Router Unique IP Address Confirmation

- (2) Validate or change the following settings in the "Use the following Network Settings" as assigned by your DOIM or S6.
 - (a) IP Address: **(172.16.1.2 CAISI Default)**
 - (b) Subnet Mask: **(255.255.255.0 CAISI Default)**
 - (c) Gateway: **(192.168.1.1 CAISI Default)**
 - (d) Domain: **(caisi.army.mil CAISI Default)**
 - (e) First DNS: **(138.27.4.15 CAISI Default)**
 - (f) Second DNS and Third DNS: **(0.0.0.0 CAISI Default)**
 - (3) If you have made changes within this tab, click on the “**Apply**” button and proceed to Step 8.
- b) Verify that the “**Obtain network settings automatically (DHCP)**” box is selected.
- 8) Click on the “**Details**” tab.
 - a) “**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience.
 - b) If you make changes to values on the “**Details**” tab click on the “**Apply**” button.

- 9) Click on the “**Advanced**” tab.
 - a) Validate or change the following settings as assigned by your DOIM, S6 or CSSAMO.
 - (1) Private IP Address: (**192.168.1.1** CAISI Default)
 - (2) Private Subnet Mask: (**255.255.255.0** CAISI Default)
 - (3) Enable DHCP Serving: (**box is checked** CAISI Default)
 - (4) From: (**192.168.1.100** CAISI Default)
 - (5) To: (**192.168.1.249** CAISI Default)
 - (6) Port Forwarding: (**no values assigned** CAISI Default)
 - b) If you have made changes within this tab, click on the “**Apply**” button.

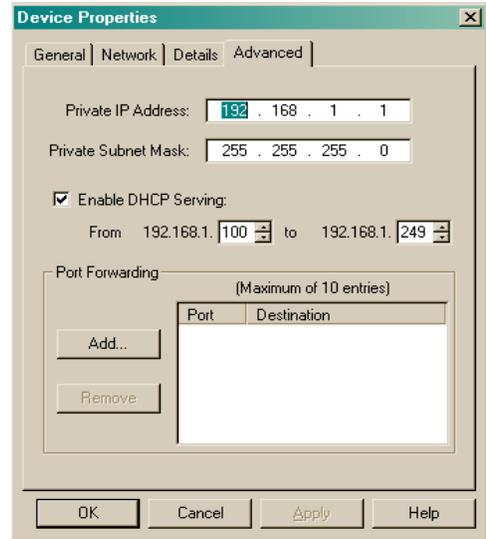


Figure 3-50 Router Device Properties Advanced Tab

- 10) Click on the “**OK**” button. The main CAISI Admin screen will appear where you should see the new device-with the name you assigned it. The CAISI default is “**caisirouter**”.

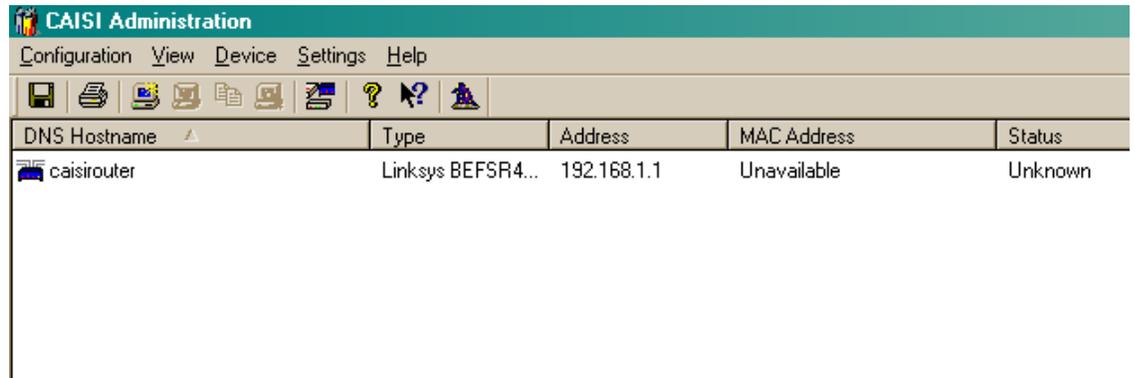


Figure 3-51 Router Device List Screen – Newly Created Device

- 11) Proceed to procedure 4. **Send the configuration to the router on page 3-50.**

b. **“Device Wizard” Method**

- 1) Select **“Device”** from the CAISI Admin menu and then select **“Device Wizard”** from the **“Device”** drop-down menu.

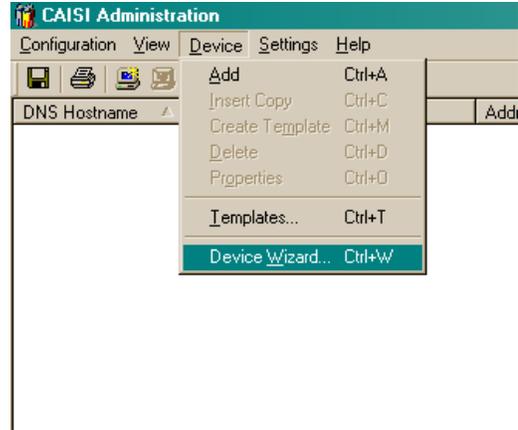


Figure 3-52 Router Device Wizard Option Menu

- 2) Set the **“Device Type”** button to **Linksys BEFSR41/81**.
- 3) Click on the **“Next>”** button.



Figure 3-53 Router Choose a Device to Create Screen

- 4) Set the **“Network Type”** to **Mixed Network**.
- 5) Click on the **“Next>”** button.

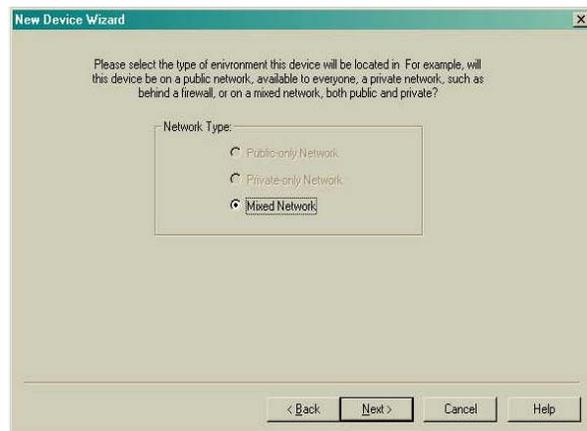


Figure 3-54 Router New Device Wizard Screen

- 6) Set “**DNS Hostname:**” (Where “DNS Hostname:” = the host name of the router) to the name provided by your DOIM, S6 or CSSAMO. The CAISI default is **caisirouter**.
- 7) Create a “**Device Name:**” if you want it to be different from the “DNS Hostname.”
- 8) From the “**Template**” drop-down menu, select **caisirouter-DHCP** or **caisirouter-nonDHCP**, as prescribed by your DOIM, S6 or CSSAMO. These settings apply to the WAN side of the router.

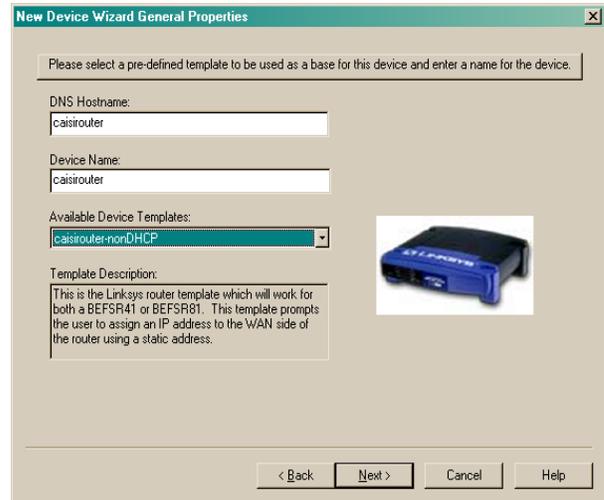


Figure 3-55 Router New Device Wizard General Properties

- 9) For classroom training, set “**Template**” to **caisirouter-nonDHCP** from the drop down menu.
- 10) Click on the “**Next>**” button.

NOTE: *The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited.*

- 11) The “**New Device Wizard Network Settings**” screen will appear.
 - a) If you selected **caisirouter-nonDHCP**, perform the following procedure, otherwise you may skip to step (11.b).
 - (1) Click on the “**Validate**” button.
 - (a) If the IP Address is unique, click the on the “**OK**” button when prompted.
 - (b) If the IP Address is not unique, a list box will pop up to show you the other device configurations that use that address. Click on the “**OK**” button to dismiss the list box. If necessary, enter a new IP Address.

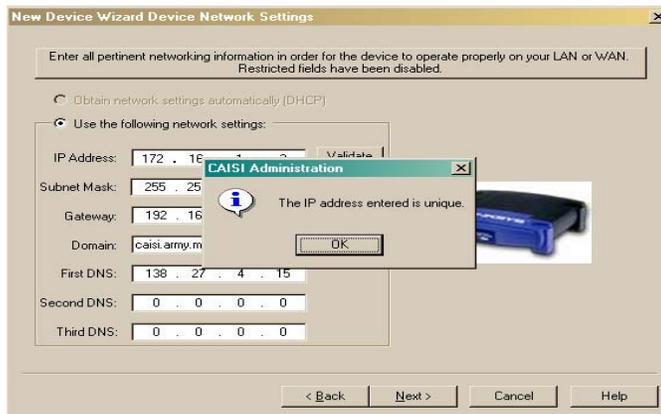
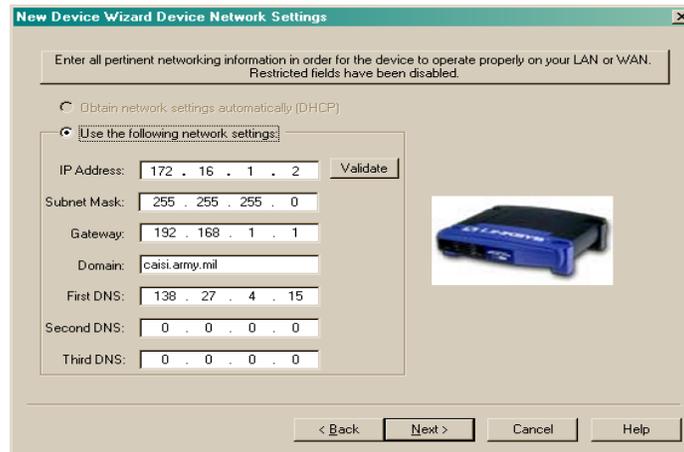


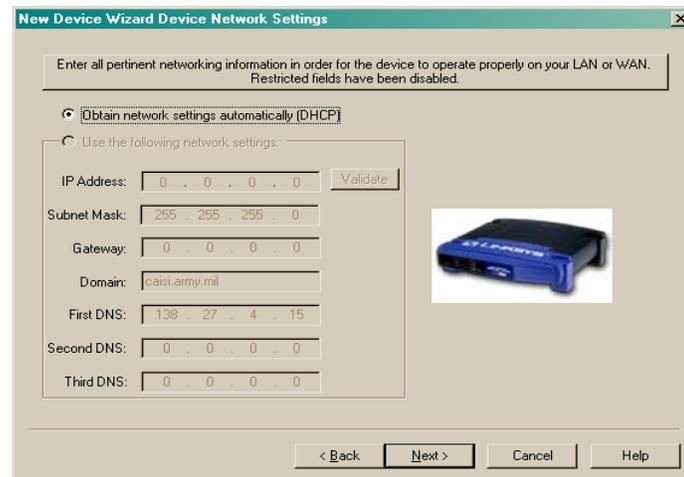
Figure 3-56 Router Unique IP Address Confirmation

- (2) Validate or change the following settings in the “**Use the following Network Settings**” as assigned by your DOIM, S6 or CSSAMO.
 - (a) IP Address: (172.16.1.2 CAISI Default)
 - (b) Subnet Mask: (255.255.255.0 CAISI Default)
 - (c) Gateway: (192.168.1.1 CAISI Default)
 - (d) Domain: (caisi.army.mil CAISI Default)
 - (e) First DNS: (138.27.4.15 CAISI Default)
 - (f) Second DNS and Third DNS: (0.0.0.0 CAISI Default)
- (3) Click on the “**Next>**” button and proceed to Step 12.



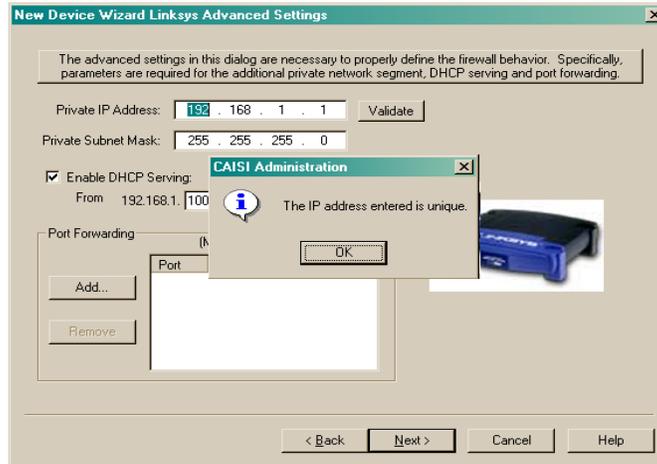
**Figure 3-57 Router
New Device Wizard Network Settings Screen -1**

- b) Verify that the “**Obtain network settings automatically (DHCP)**” box is selected and click on the “**Next>**” button.



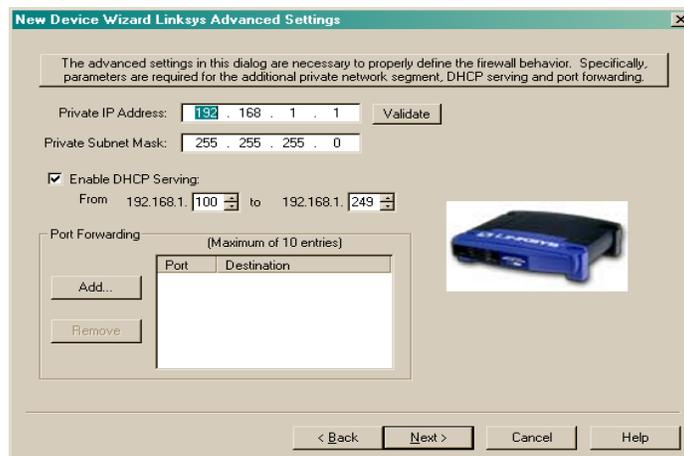
**Figure 3-58 Router
New Device Wizard Network Settings Screen - 2**

- 12) The “**New Device Wizard Linksys Advanced Settings**” screen will appear.
- Click on the “**Validate**” button.
 - If the IP Address is unique, click on the “**OK**” button when prompted.
 - If the IP Address is not unique a list box will pop up to show you the other device configurations that use that address. Click on the “**OK**” button to dismiss the list box. If necessary, enter a new IP Address, subnet mask, or both.



**Figure 3-59 Router
New Device Wizard Linksys Advanced Settings - 1**

- Validate or change the following settings as assigned by your DOIM, S6 or CSSAMO.
 - Private IP Address: (**192.168.1.1** CAISI Default)
 - Private Subnet Mask: (**255.255.255.0** CAISI Default)
 - Enable DHCP Serving: (**box is checked** CAISI Default)
 - From: (**192.168.1.100** CAISI Default)
 - To: (**192.168.1.249** CAISI Default)
 - Port Forwarding: (**no values assigned** CAISI Default)
- Click on the “**Next>**” button.



**Figure 3-60 Router
New Device Wizard Linksys Advanced Settings - 2**

- 13) The “**New Device Wizard Device Details**” screen will appear.
- “**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience.
 - Click on the “**Next>**” button.

**Figure 3-61 Router
New Device Wizard Device Details Screen**

- 14) The “**New Device Wizard Password Validation**” screen will appear.
- Set the “**Administrative Password**” to the password provided by your DOIM, S6 or CSSAMO.
 - Enter the password in the “**Administrative (Write) Password:**” box.
 - For classroom training, set the password to the CAISI default “**system**”.

NOTE: *As you enter the password, asterisks will appear. The password is not shown in the clear. You must change the password before you deploy the router.*

- Press on the “**Tab**” key and confirm the new password by entering the password in the “**Confirm Administrative (Write) Password:**” box.
- Click on the “**Finish**” button.

**Figure 3-62 Router
New Device Wizard Password Validation Screen**

15) The “CAISI Admin New Device Wizard” screen will appear. Select “**Done. No further action**” in the “Next step” box.

16) Click on the “**OK**” button.



Figure 3-63 Router CAISI Admin New Device Wizard Screen

17) The main CAISI Admin screen will appear where you should see the new device- with the name you assigned it. The CAISI default is “caisirouter”.

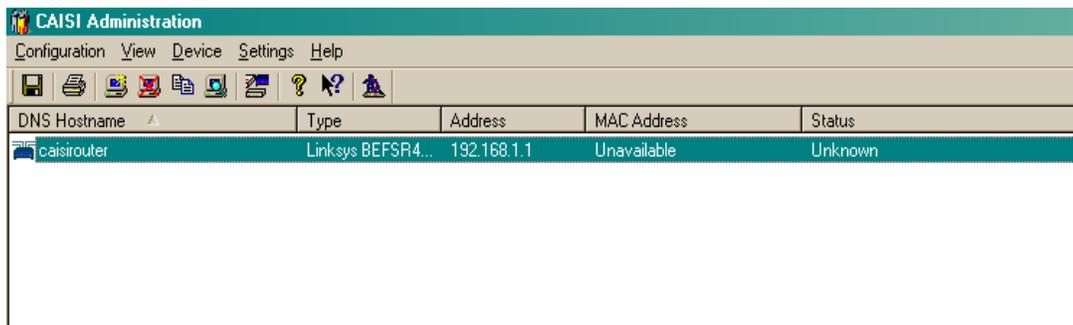


Figure 3-64 Router Device List Screen – Newly Created Device

18) Proceed to procedure 4. **Send the configuration to the router.**

4. Send the configuration to the router

a. Highlight the newly created device. The CAISI default is **caisirouter**.

b. Select “**Device**” from the CAISI Admin toolbar and then select “**Properties**” from the from the “**Device**” drop-down menu.

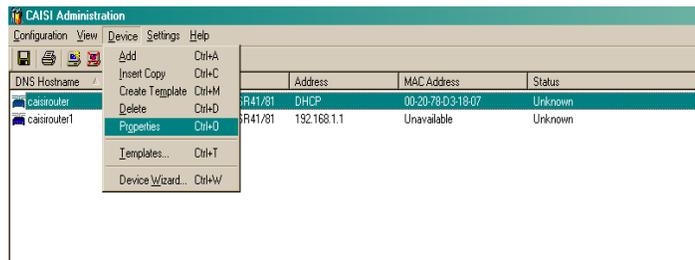


Figure 3-65 Router CAISI Admin Device List Screen

c. Click on the “**Send Configuration**” button.

- d. Select the “**Configure using IP Address:**” button and set the IP Address to the address you assigned the router. The CAISI default is **192.168.1.1**
- e. Click on the “**Start**” button on the “**Configure Device**” screen.

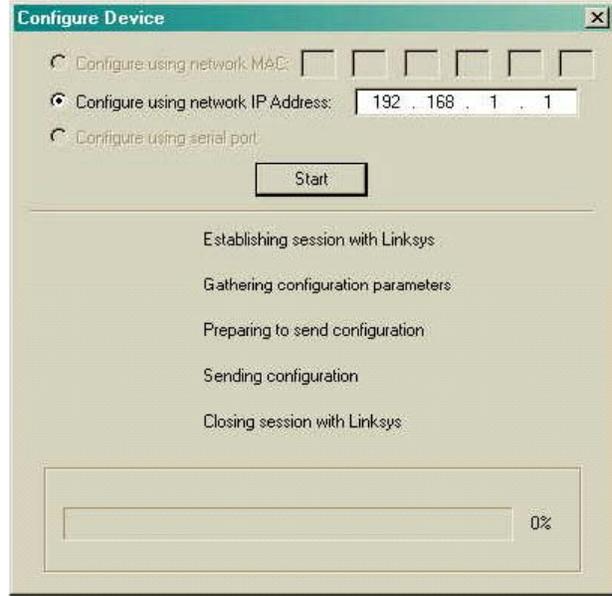


Figure 3-66 Router Configure Device Screen

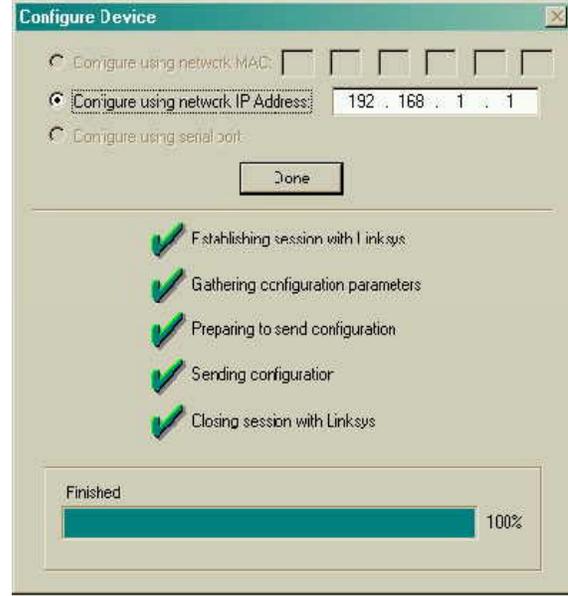
- f. If the “**Enter Password**” screen appears, enter the password you assigned to the router. The CAISI default is “**system**”. Click on the “**OK**” button.



Figure 3-67 Router Enter Password Screen

- g. Click on the “**OK**” button when the “**The device has been configured successfully**” message appears.

- h. Click on the “**Done**” button on the “**Configure Device**” screen.



**Figure 3-68 Router
Configure Device Screen**

- i. Click on the “**OK**” button on the “**Device Properties**” screen.
- j. The Router is now configured. Close CAISI Admin by clicking the (X) at the top right of the screen or by selecting “**Configuration**” from the main menu bar and then selecting “**Exit**”.
- k. At the CAISI Administration prompt, “**Do you want to save changes to the configuration before exiting the application?**” Click on the “**Yes**” button.

3.5.5 Verify Router Operational Status

1. Open Internet Explorer on the notebook desktop.
2. In the address toolbar at the top of Explorer, enter the IP address with which you gave the router during configuration. In this case enter the IP - **192.168.1.1**
3. Click on “**GO**” on the Explorer toolbar or click on “**Enter**” on the notebook keyboard.

- a. The “Enter Network Password” screen will appear.
 - 1) You will be prompted for a user name and password.
 - 2) You may leave the “User Name” field blank.
 - 3) Enter one of the following passwords in the “Password” field: “system” (CAISI default), or the password you previously assigned the device as prescribed by your DOIM, S6 or CSSAMO.
 - 4) Click on the “OK” button.

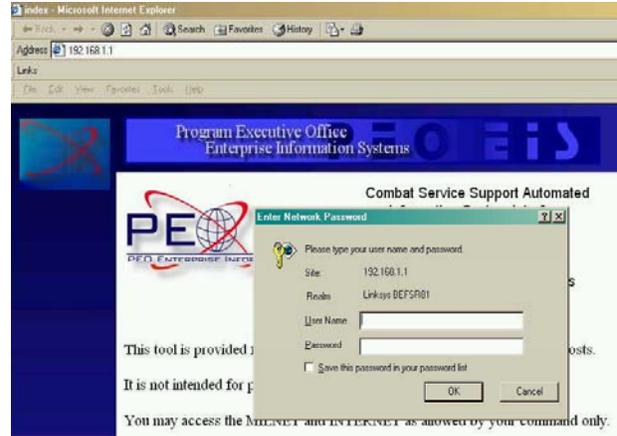


Figure 3-69 Router Enter Network Password Screen

- b. To confirm that the router is configured select the “Setup” tab.
 - 1) If you successfully configured the router you should now see the CAISI default Host name, **caisirouter** and Domain name **caisi.army.mil**
 - 2) At factory defaults, the “Host name” and “Domain name” fields were empty.

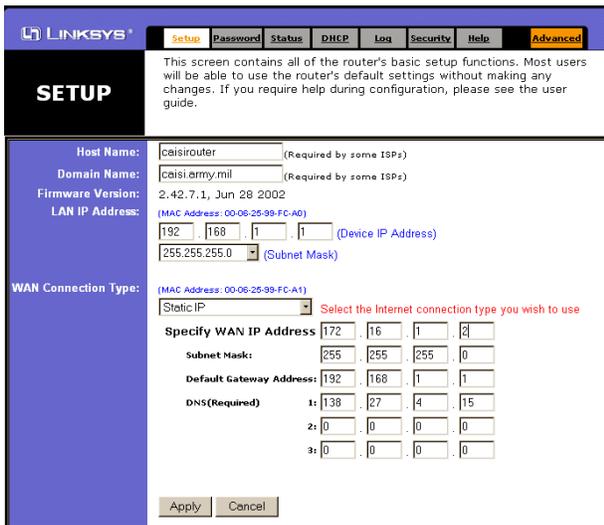


Figure 3-70 Router Configured Setup Screen

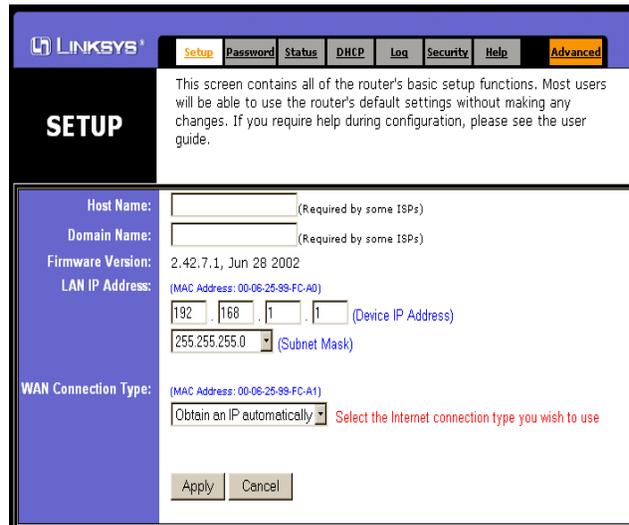


Figure 3-71 Router Factory Default Setup Screen

- 3) You can also verify configuration by selecting the “**DHCP**” tab.
 - a) If you successfully configured the router the number of DHCP users should be set to **150**.
 - b) At factory defaults, the number of DHCP users is 50.

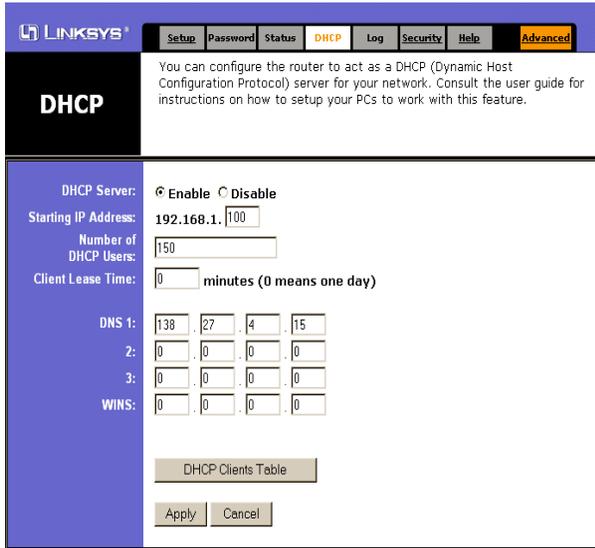


Figure 3-72 Router Configured DHCP Screen

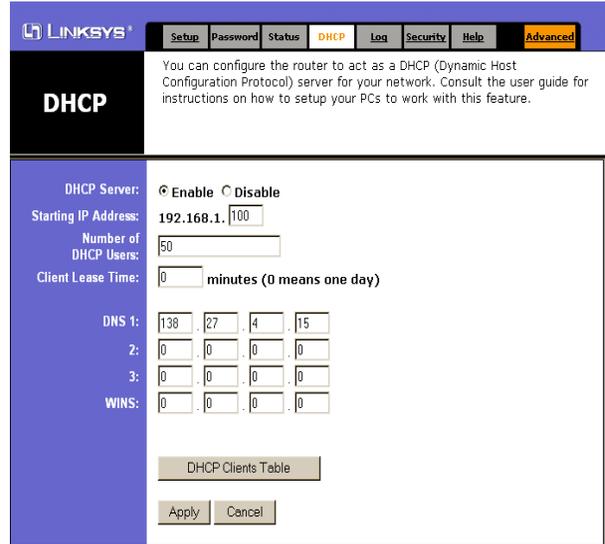


Figure 3-73 Router Factory Default DHCP Screen

3.5.6 Perform Disconnection Procedures

1. Disconnect the power supply from the external power source.
2. Disconnect the other end of the power supply from the port labeled “**Power**” on the back of the router.
3. Disconnect the white straight-through Ethernet cable from the NIC on your SSR notebook and the router.

3.6 UTILIZING CAISI ADMIN TO CONFIGURE THE CBM

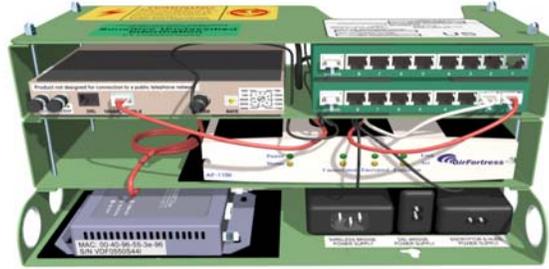


Figure 3-74 CBM

The CBM includes three components that require configuration before it can be put into operation. They are:

1. Wireless Bridge Paragraph 3.6.2
2. Inline Encryptor Paragraph 3.6.5
3. DSL (No software configuration required)

For physical connection procedures refer to TM 11-5895-1691-12 Paragraph 2.19.1

The following WARNINGS and CAUTIONS apply to the entire lesson.

WARNINGS

- Severe injury or death can occur if this equipment, its antennas, or connected communications cables come near electric 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. This may cause severe injury or death. Never operate a wireless device without an antenna. It can damage the radio.

**Five Safety Steps to Follow
If Someone Is the Victim of Electrical Shock
WARNINGS**

- Do not try to pull or grab the individual.
- If possible, turn off the electrical power.
- If you cannot turn off the electrical power, push, pull or lift the person to safety using a dry wooden pole, a dry rope or some other insulating material.
- Send for help as soon as possible.
- After the injured person is free of contact with the source of electrical shock, move the person a short distance away and immediately start first aid, if necessary.

**UPS BATTERY SAFETY
WARNINGS**

- Batteries can present a risk of electrical shock and burn from high short-circuit current.
- Observe proper precautions.
- Do not open the UPS or the batteries.

**UPS INSTALLATION SAFETY
CAUTIONS**

- 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
CAUTIONS**

- 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.

CAUTIONS

- Never connect cables when the power is on.
- Never pull directly on cables.
- Always connect and disconnect using the plugs at the ends 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 that plugs match their connectors before installing.
- Make sure the UPS power is OFF before inserting its plug into an external power source.

CAUTION

The CAISI Bridge Module (CBM) transit case weighs 46 pounds. Use safe lift and carry procedures when handling the transit case. This is a two-person lift and carry.

SECURITY CONSIDERATIONS

- The radios are in the unprotected zone and you cannot communicate with them from the protected zone.
- 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. Nor are the DSL links encrypted because they are a part of the protected distribution system (PDS).
- Due to security vulnerabilities you should not remotely configure the radios. To configure a radio you should connect to the console port.
- There is no reset button or “zeroize” switch to reset or remove the configuration, encryption key, or passwords. The wireless bridges 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.

3.6.1 Physical Connection Procedures

NOTE: *Ensure an antenna is connected to the CBM IAW procedures outlined TM 11-5895-1691-12 Paragraph 2.18 before performing the following procedures.*

1. Connect CBM power cables.
 - a. Remove the 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 cable 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.
 - g. Apply power to the bridge by pressing the “I” (ON) side of the UPS rocker switch in and watch the lights.



Figure 3-75 CBM Power Cable Connections

2. Connect CBM wireless bridge to notebook wired/built-in NIC.
 - a. Disconnect the red crossover cable from the port labeled “Encrypted” on the back of the encryptor.
 - b. Remove the RJ-45 straight-through adapter and a straight-through cable from your SSR Accessory Kit 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 NIC.
 - e. You are now connected from your NIC to the “Network” port on the power injector.

NOTE: *If the wireless bridge is not installed in a CBM, refer to TM 11-5895-1691-12, Paragraph 2.32.1.1 for physical connection procedures.*

3.6.2 Configure the CBM Wireless Bridge (Firmware 12.01T)

NOTE: A standard CAISI SSR notebook, configured as follows is required for wireless bridge set up. It 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. Wired or Built-in NIC must be used.

1. Connect a straight-through nine-pin serial cable (blue) from your terminal’s serial port to the serial port on the bridge. Your “terminal” will normally be the CAISI notebook, but can be any computer running Blast or Hyperterm.
2. Apply power to the SSR notebook.
 - a. Enter your username and password. The CAISI defaults are “**caisiadmin**” and “**BS_69dlw**”.
 - b. A Logon Message prompt will appear, “Your password expires today. Do you want to change it now?” For classroom training, click on the “**No**” button.
 - c. At the bottom of the SSR notebook screen, click on ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear. Click on “**CAISI Admin**”.
3. Set-up the Wireless Bridge device. There are 2 methods, 1) By selecting the “**Add**” option or 2) Use of the “**Device Wizard**” option from the “Device” drop-down menu. You may choose either method.

a. **“Add” Option Method**

- 1) Select “**Device**” from the CAISI Admin toolbar and then select “**Add**” from the “**Device**” drop-down menu.



Figure 3-76 Wireless Bridge Add Option Menu

- 2) Set “**DNS Hostname:**” (Where “DNS hostname” = the host name of the wireless bridge) to the name provided by your DOIM, S6 or CSSAMO.

The CAISI defaults are “**CBM-350r**” for a root bridge and “**CBM-350nr**” for a non-root bridge.

- 3) Create a “**Device Name:**” if you want it to be different from the “DNS Hostname:”
- 4) From the “**Template**” drop-down menu select a template from the list of CAISI Admin defined templates.

**Figure 3-77 Wireless Bridge
New Network Device Screen**

NOTE: *The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited.*

- 5) For classroom training, set “Template” to **CBM-350-root** (root-bridge) or **CBM-350-nonroot** (non-root bridge) as prescribed by the instructor.
- 6) Click on the “**Edit Properties**” button. The “**Device Properties**” screen will appear with the “**General**” tab selected.
 - a) Verify the “**Device Name**” (the host name you assigned the wireless bridge) is correct. The CAISI defaults are “**CBM-350r**” for a root bridge and “**CBM-350nr**” for a non-root bridge.
 - b) To set the “**User Name:**”, click on the “**Change**” button.
 - (1) Enter your new User Name into the “**Enter User Name:**” dialog box.
 - (2) The CAISI default is “**root**”.

NOTE: *you must change it before you deploy the radio.*

- (3) Click on the “**OK**” button.
- c) Set the “**Administrative Password**” to the password provided by your DOIM, S6 or CSSAMO.
 - (1) Click on the “**Change**” button. The Set Password screen will appear.

(2) Enter your new password in the “**Enter Password**” dialog box.

(3) For classroom training set the password, to the CAISI default “**system**”.

NOTE: *As you enter the password, asterisks will appear. The password is not shown in the clear.*

(4) Press on the <**Tab**> key and confirm the new password by entering the password in the “**Confirm Password**” dialog box.

(5) Click on the “**OK**” button.

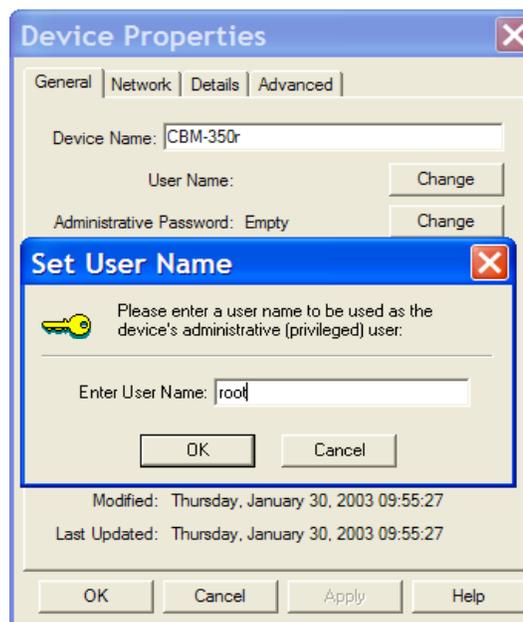


Figure 3-78 Wireless Bridge Device Properties General Tab

d) Set the “**Access Password**” to the password provided by your DOIM, S6 or CSSAMO.

(1) Click on the “**Change**” button. The Set Password screen will appear.

(2) Enter your new password in the “**Enter Password**” dialog box.

(3) For classroom training, set the password to the CAISI default “**access**”.

NOTE: *As you enter the password, asterisks will appear. The password is not shown in the clear. **You must change the password before you deploy the radio.***

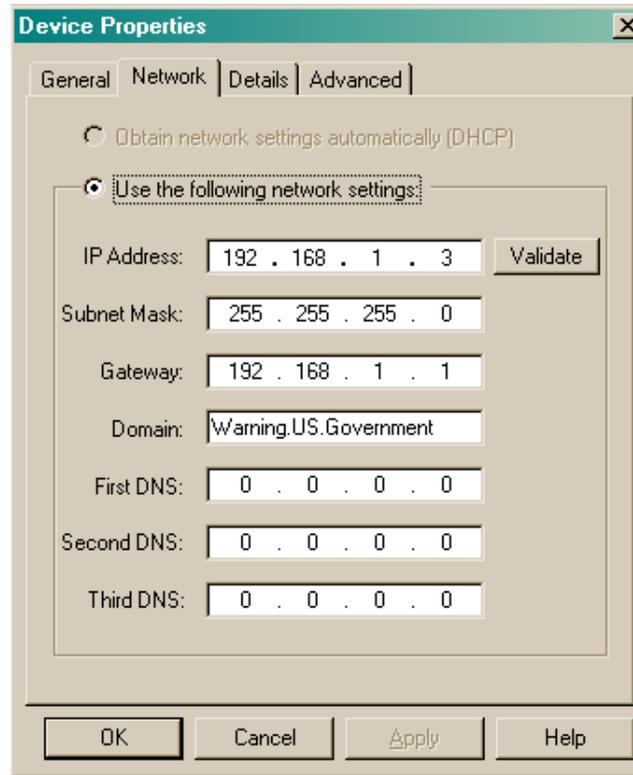
(4) Press on the <**Tab**> key and confirm the new password by entering the password in the “**Confirm Password**” dialog box.

(5) Click on the “**OK**” button.

e) If you have made changes to values on the “**General**” tab, click on the “**Apply**” button.

NOTE: *Until you actually send the configuration to the radio, the administrative password and access password fields may indicate “empty”, even though you entered it earlier. If you have previously sent this configuration to the radio, it will indicate a status of “set”. However, the application does not store user names or passwords. They are cached during the current session, but are lost as soon as you exit from the application. An asterisk to the left of the field name indicates that the password is cached. If there is no asterisk, you must reenter the password.*

- 7) Click on the “**Network**” tab.
- a) Select “**Use the following Network Settings**” and enter the following parameters as assigned by your DOIM, S6 or CSSAMO.
- (1) IP Address: (**192.168.1.3** root or **192.168.1.4** non-root CAISI Default)
 - (2) Subnet Mask: (**255.255.255.0** CAISI Default)
 - (3) Gateway: (**192.168.1.1** CAISI Default)
 - (4) Domain: (**Warning.US.Government** CAISI Default)
 - (5) First DNS: (**leave at 0.0.0.0**)
 - (6) Second DNS and Third DNS: (**leave at 0.0.0.0**)



**Figure 3-79 Wireless Bridge
Device Properties Network Tab**

NOTE: *Since there is not a DHCP server on the Untrusted Network (the radio portion of the network is on the “Encrypted” side of the encryptors and cannot see any host or server on the “Unencrypted” side), the user is advised not to select “Obtain network settings automatically (DHCP).”*

- b) Click on the “**Validate**” button.
- (1) If the IP Address is unique, click on the “**OK**” button when prompted.
 - (2) If the IP Address is not unique, a list box will pop up to show you the other device configurations that use that address. Click on the “**OK**” button to dismiss the list box. If necessary, enter a new IP Address, subnet mask, or both.
- c) If you have made changes to values on the “**Network**” tab, click on the “**Apply**” button.

- 8) Click on the “**Details**” tab.
 - a) “**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience.
 - b) If you have made changes to values on the “**Details**” tab, click on the “**Apply**” button.

- 9) Click on the “**Advanced**” tab.
 - a) Enter your unit specific SSID. The CAISI default for hardware testing and classroom training is “**caisi000**”.

NOTE: *You must change the SSID before deploying the bridge.*

- b) Set the radio mode to “**root**” if the radio is designated a “root” or click on “**non-root**” if the radio will serve as a repeater.
- c) Set “**Distance to farthest node**” to the approximate distance, in kilometers, of your longest expected radio link anywhere in the network. The CAISI default is set to **6**.
- d) Verify “**Center Frequency**” is set to “**auto**”. OCONUS countries may require a different frequency, check with your local frequency manager upon arrival.
- e) Verify “**Broadcast Power**” is set to “**100**”. OCONUS countries may require you to lower power setting, check with your local frequency manager upon arrival.
- f) Under “**Privacy Encryption Keys**”, click on the “**Set Key 1**” button.

- (1) Click on “**Long 26 digits**”,
(Do not use short key.)
- (2) Under “**Enter Key**” enter your 26 digit hexadecimal encryption key.

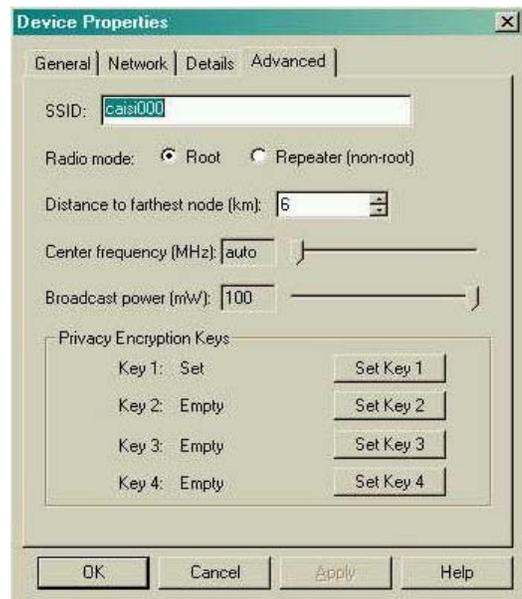


Figure 3-80 Wireless Bridge Device Properties Advanced Tab



Figure 3-81 Wireless Bridge Set WEP Key Screen

- (3) The CAISI default is **0123456789abcdef0123456789** for hardware testing and classroom training. **NOTE: You must change the key before deploying the bridge.**
- (4) Confirm the key by re-entering it into the “**Confirm Key**” field. Click on the “**OK**” button.
- g) If you have made changes within this tab, click on the “**Apply**” button and then click on the “**OK**” button.
- 10) The main CAISI Admin screen will appear where you should see the new device with the name you assigned it.
- 11) Proceed to procedure 4. **Send the configuration to the wireless bridge on page 68.**

b. **“Device Wizard” Method**

- 1) Select “**Device**” from the CAISI Admin menu and then select “**Device Wizard**” from the “**Device**” drop-down menu.
- 2) Set the “**Device Type**” button to **Cisco Aironet 350**. Click on the “**Next>**” button.
- 3) Set the “**Network Type**” to **Mixed Network**. Click on the “**Next>**” button.
- 4) Set “**DNS Hostname**” to “**CBM-350r**” for a root bridge and “**CBM-350nr**” for a non-root bridge.
- 5) Create a “**Device Name:**” if you want it to be different from the “**DNS Hostname:**”
- 6) From the “**Available Device Templates**” drop-down menu, select **CBM-350-root** or **CBM-350-nonroot**.

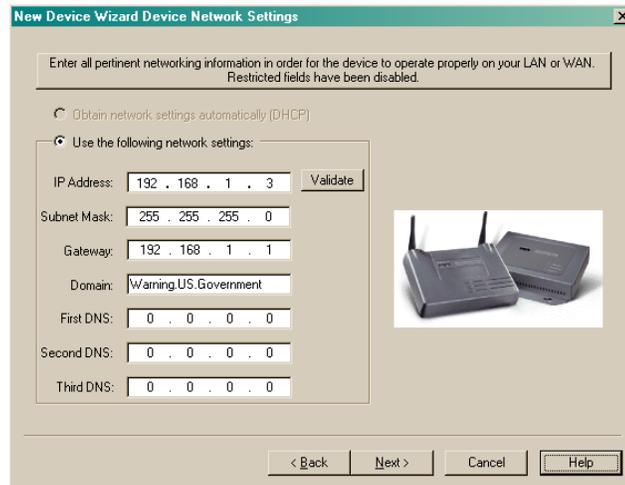
NOTE: *The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited.*

- 7) Click on the “**Next>**” button.

Figure 3-82 Wireless Bridge New Device Wizard General Properties Screen

- 8) From the “**Use the following Network Settings**”, enter the following parameters as assigned by your DOIM, S6 or CSSAMO.
 - a) IP Address: (**192.168.1.3** root or **192.168.1.4** non-root CAISI Default)
 - b) Subnet Mask: (**255.255.255.0** CAISI Default)
 - c) Gateway: (**192.168.1.1** CAISI Default)
 - d) Domain: (**Warning.US.Government** CAISI Default)
 - e) First DNS: (**leave at 0.0.0.0**)
 - f) Second DNS and Third DNS: (**leave at 0.0.0.0**)

- 9) Click on the “**Validate**” button.
 - a) If the IP Address is unique, click on the “**OK**” button when prompted.
 - b) If the IP Address is not unique, a list box will pop up to show you the other device configurations that use that address. Click on the “**OK**” button to dismiss the list box. If necessary, enter a new IP Address, subnet mask, or both.
 - c) Click on the “**Next>**” button.



**Figure 3-83 Wireless Bridge
New Device Wizard Device Network Settings**

- 10) Enter your unit specific SSID. The CAISI default for hardware testing and classroom training is “**caisi000**”. **You must change the SSID before deploying the bridge.**

- 11) Set the radio mode to “**root**” if the radio is designated a “root” or click on “**non-root**” if the radio will serve as a repeater.

- 12) Verify “**Center Frequency**” is set to “**auto**”. OCONUS countries may require a different frequency, check with your local frequency manager upon arrival.

- 13) Verify “**Broadcast Power**” is set to “**100**”. OCONUS countries may require you to lower power setting, check with your local frequency manager upon arrival.

- 14) Under “**Privacy Encryption Keys,**” click on the “**Set Key 1**” button then click on “**Long 26 digits**” (Do not use short key.)
- 15) Under “**Enter Key,**” enter your 26 digit hexadecimal encryption key. The CAISI default is **0123456789abcdef0123456789** for hardware testing and classroom training. *You must change the key before deploying the bridge.*
- 16) Confirm key by re-entering into the “**Confirm Key**” field. Click on the “**OK**” button.
- 17) If a value has been changed, click on the “**OK**” button.
- 18) Click on the “**Next>**” button.

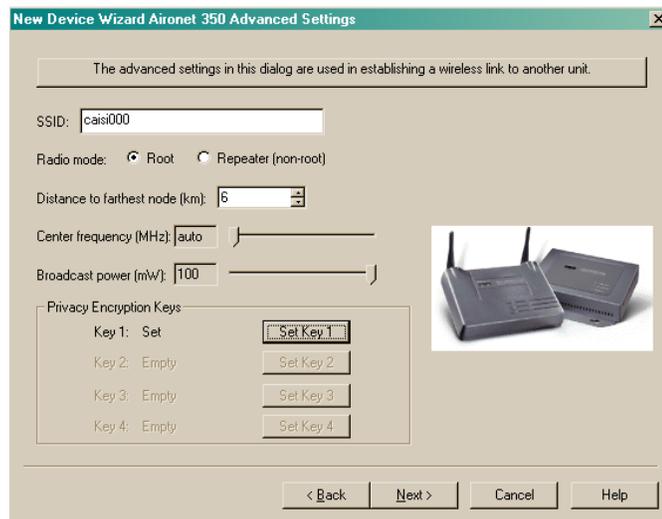


Figure 3-84 Wireless Bridge
New Device Wizard Aironet 350 Advanced Settings

- 19) The “**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience. Click on the “**Next>**” button.
- 20) Enter your new User Name into the “**User Name:**” box. (The CAISI default is “**root**”. **NOTE:** *you must change it before you deploy the radio.*
- 21) Enter your new password in the “**Administrative (Write) Password:**” box and then reenter your password into the “**Confirm Administrative (Write) Password**” box. The CAISI default is “**system**”.

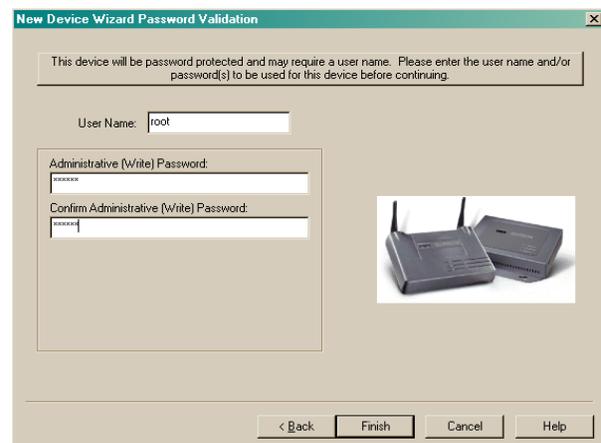


Figure 3-85 Wireless Bridge
New Device Wizard Password Validation

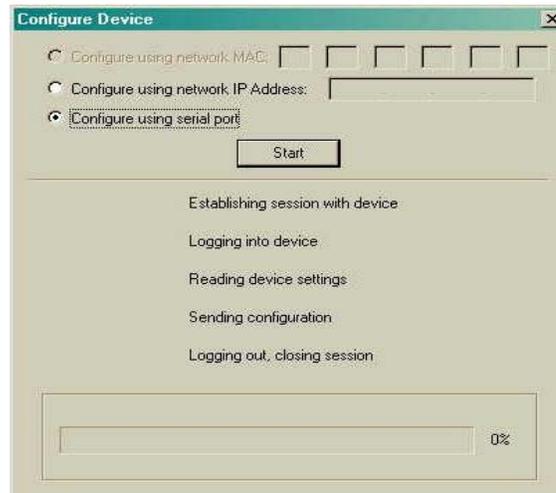
NOTE: *As you enter the password, asterisks appear. The password is not shown in the clear. **You must change the password before deploying the bridge.** You must change the password before you deploy the radio.*

- 22) Click on the “**Finish**” button.
- 23) A dialog box will appear, click on the “**Done. No further action**” button.
- 24) Click on the “**OK**” button.



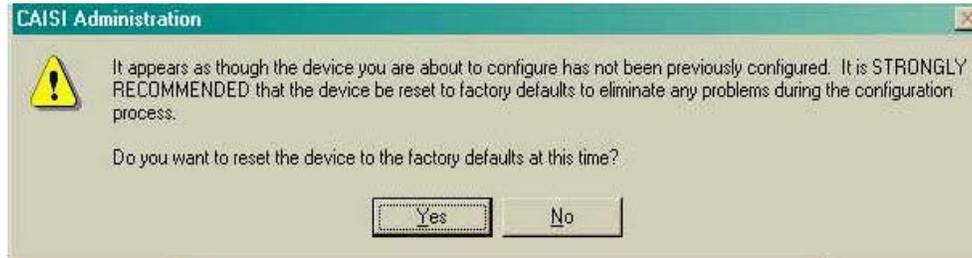
**Figure 3-86 Wireless Bridge
CAISI Admin New Device Wizard**

- 16) The main CAISI Admin screen will appear where you should see the new device with the name you assigned it. The CAISI defaults are “**CBM-350r**” for a root bridge and “**CBM-350nr**” for a non-root bridge.
- 17) Proceed to procedure 4. **Send the configuration to the wireless bridge.**
- 4. Send the configuration to the wireless bridge.
 - a. Highlight the device you just created from the main screen.
 - b. Select “**Device**” from the CAISI Admin toolbar and then select “**Properties**” from the “Device” drop-down menu.
 - c. Click on the “**Send Configuration**” button.
 - d. Select the “**Configure using serial port**” button.
 - e. Click on the “**Start**” button on the “**Configure Device**” screen.
 - f. At the “Do you want to reset the device to factory defaults at this time” prompt, click on the “**Yes**” button.



**Figure 3-87 Wireless Bridge
Configure Device Screen**

- g. At the “**Do you want to reset the device to factory defaults at this time**” prompt click on the “**Yes**” button.



**Figure 3-88 Wireless Bridge
CAISI Administration Prompt - 1**

- h. The “**Please COLD RESTART the device by power cycling the unit.**” prompt will appear.



**Figure 3-89 Wireless Bridge
CAISI Administration Prompt - 2**

- i. At this time, physically disconnect either the white Ethernet cable attached to the “**To AP/Bridge**” port on the CBM radio's power injector or the power cord into the bridge's power adapter. Wait a few seconds. Reconnect it. This will perform a Cold Restart of the CBM radio.
- j. Click on the “**OK**” button on the screen prompt immediately after performing this process.

NOTE: Do not wait for the bridge to finish rebooting before clicking the “**OK**” button.

NOTE: If you press the <CTRL> <Shift> keys, an output debug window will appear, which allows you to see the wireless bridge resetting.

- k. After the CBM radio reboots and restarts (approximately 4 1/2 minutes, refer to Paragraph 4.3.1 for light indicators), the prompt “**The Aironet 350 has been reset to factory defaults**” will appear. Click on the “**OK**” button.



**Figure 3-90 Wireless Bridge
Set to Factory Default Confirmation**

- l. If the User Name has not been entered previously, the “**Set User Name**” entry box will appear. If the box doesn't appear, then skip this step.
 - 1) Enter the assigned User Name that your DOIM, S6 or CSSAMO has assigned.
 - 2) The CAISI default is “**root**”. Click on the “**OK**” button when completed.



Figure 3-91 Wireless Bridge Set User Name Screen

The CBM radio will now start to be configured.

- m. When the Windows dialog box appears stating the “The device has been configured successfully”, click on the “**OK**” button.

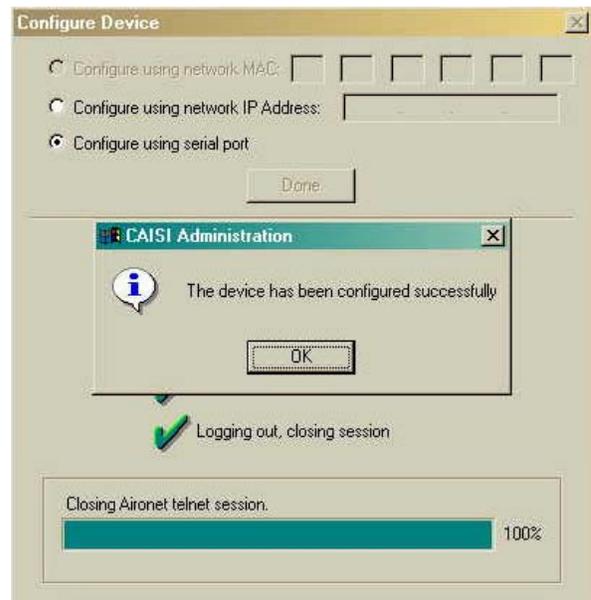
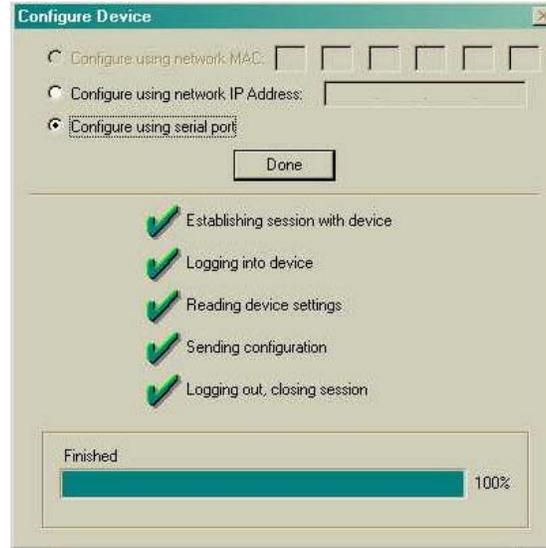


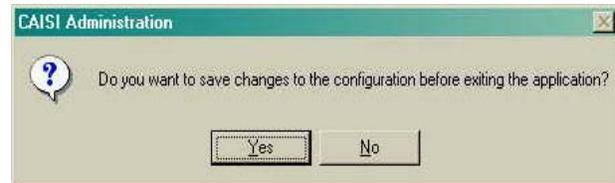
Figure 3-92 Wireless Bridge Device Configured Successfully Prompt

- n. Click on the “**Done**” button on the “**Configure Device**” screen.



**Figure 3-93 Wireless Bridge
Configure Device Screen**

- o. Click on the “**OK**” button on the “**Device Properties**” screen.
- p. Close CAISI Admin by clicking the (X) at the top right of the screen or by selecting “**Configuration**” from the main menu bar and then selecting “**Exit**”.
- q. At the CAISI Administration prompt, “Do you want to save changes to the configuration before exiting the application?” click on the “**Yes**” button.



**Figure 3-94 Wireless Bridge
Save Configuration Prompt**

3.6.3 Verify CBM Wireless Bridge Operational Status

1. The CBM root wireless bridge is now configured for operation, to verify configuration procedures perform the following:
 - a. Open Internet Explorer on the notebook.
 - 1) In the address toolbar at the top of Explorer, enter the IP address with which you gave the wireless bridge during configuration. In this case enter the IP - **192.168.1.3** (CBM root) or **192.168.1.4** (non-root).
 - 2) Click on “**GO**” on the Explorer toolbar or click on “**Enter**” on the notebook keyboard.
 - b. The “**Enter Network Password**” screen will appear.
 - 1) You will be prompted for a user name and password.
 - 2) Enter “**root**” in the “User Name” field.

- 3) Enter the password you assigned the device as prescribed by your DOIM, S6 or CSSAMO in the “Password” field. The CAISI default is “system”.
 - 4) Click on the “OK” button.
- c. To confirm that the wireless bridge is configured navigate to the “Express Setup” screen.
- 1) If you successfully configured the wireless bridge you should now see the CAISI default SSID, **caisi000**.
 - 2) At factory defaults, the SSID is tsunami.

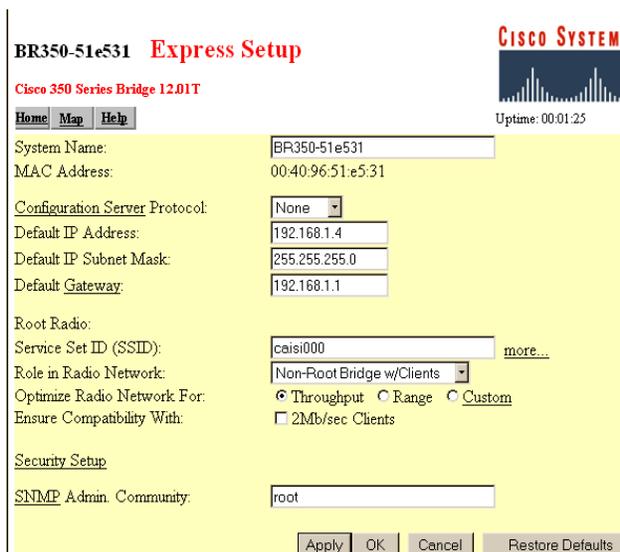


Figure 3-95 Wireless Bridge Configured Wireless Bridge Screen

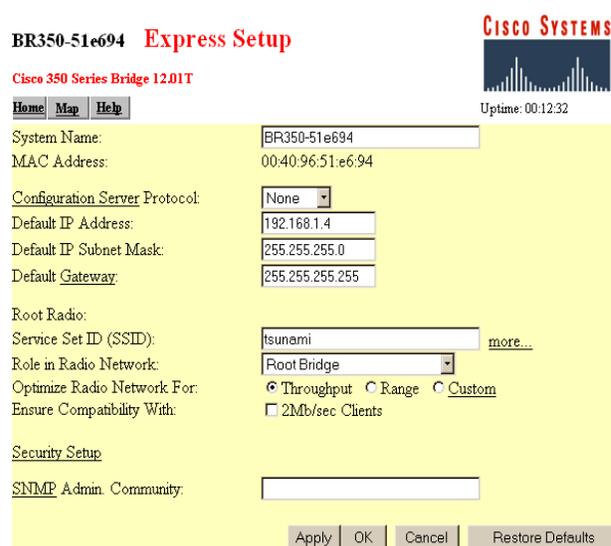


Figure 3-96 Wireless Bridge Factory Default Configuration Screen

3.6.4 Disconnect CBM Wireless Bridge from the Notebook Computer.

1. Disconnect the standard serial cable from the serial port on the CBM wireless bridge and the serial port on the laptop.
2. Disconnect the white straight-through cable from the NIC and the RJ-45 straight-through adapter.
3. Disconnect the red crossover cable from the RJ-45 straight-through adapter.
4. Re-attach the red crossover Ethernet cable to the “Encrypted” port on the back of the encryptor.

NOTE: *If you have performed all necessary configuration procedures involving the wireless bridge and are ready to power down the equipment, refer to Paragraph 3.6.6 for procedures on disconnecting the wireless bridge power cables.*

3.6.5 Configure the CBM Inline Encryptor (Firmware 1178W)

The encryptors issued to the SSR from Tobyhanna Army Depot will be preset to the CAISI standard configuration. This includes the encryptors in the SSR Accessory Kits as well as the encryptors installed in the CBMs/CCMs. **At a minimum the SSR needs to change the Access ID and passwords.**



Figure 3-97 Inline Encryptor

SECURITY CONSIDERATIONS

- You must periodically change the Access IDs.
- Due to security vulnerabilities you should not remotely configure the encryptor.

NOTE: A standard CAISI SSR notebook, configured as follows is required for inline encryptor set up. It 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. Wired or Built-In NIC must be used.

1. Ensure the encryptor is receiving power. Refer to physical connection procedures in paragraph 2.11.1.

NOTE: If the encryptor is not installed in a CBM, refer to TM 11-5895-1691-12, Paragraph 2.32.1.1 for physical connection procedures.

2. Connect your notebook to the serial port of the encryptor with the beige nine-pin female to nine-pin female null model (crossover) serial cable from the SSR Accessory Kit.
 - a. Enter your username and password. The CAISI defaults are “**caisiadmin**” and “**BS_69dlw**”.
 - b. A Logon Message prompt will appear, “Your password expires today. Do you want to change it now?” For classroom training, click on the “**No**” button.
 - c. At the bottom of the SSR notebook screen, click on “>>” to the right of the “CAISI Toolbox” button. The CAISI Toolbox menu will appear. Click on “**CAISI Admin**”.

4. Set-up the Inline encryptor device. There are 2 methods, 1) By selecting the “**Add**” option or 2) Use of the “**Device Wizard**” option from the “**Device**” drop down menu. You may choose either method.

a. **“Add” Option Method**

- 1) Select “**Device**” from the CAISI Admin toolbar and then select “**Add**” from the “**Device**” drop-down menu.



Figure 3-98 Inline Encryptor Add Option Menu

- 2) Set “**DNS Hostname:**” (Where “DNS hostname” = the host name of the wireless bridge) to the name provided by your DOIM, S6 or CSSAMO.

The CAISI default is “**CBM-AF-1100**”

- 3) Create a “**Device Name:**” if you want it to be different from the “DNS Hostname:”
- 4) From the “**Template**” drop-down menu select a template from the list of CAISI Admin defined templates.

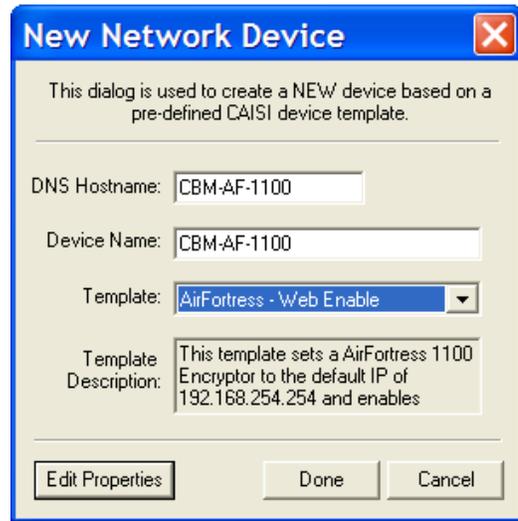


Figure 3-99 Inline Encryptor New Network Device Screen

NOTE: *The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited.*

- 5) For classroom training, set “Template” to “**AirFortress-Web Enable**”.
- 6) Click on the “**Edit Properties**” button. The “Device Properties” screen will appear with the “**General**” tab selected.
 - a) Verify the “**Device Name**” (the host name you assigned the wireless bridge) is correct. The CAISI default is “**CBM-AF-1100**”.
 - b) Set the “**Administrative Password**” to the password provided by your DOIM, S6 or CSSAMO.

(1) Click on the “**Change**” button. The “Set Password” screen will appear.

(2) Enter your new password in the “**Enter Password**” dialog box.

(3) For classroom training, set the password to the CAISI default “**system00**”.

NOTE: *As you enter the password, asterisks will appear. The password is not shown in the clear. You must change the password before you deploy the inline encryptor.*

(4) Press on the <Tab> key and confirm the new password by entering the password in the “**Confirm Password**” dialog box.

(5) Click on the “**OK**” button.

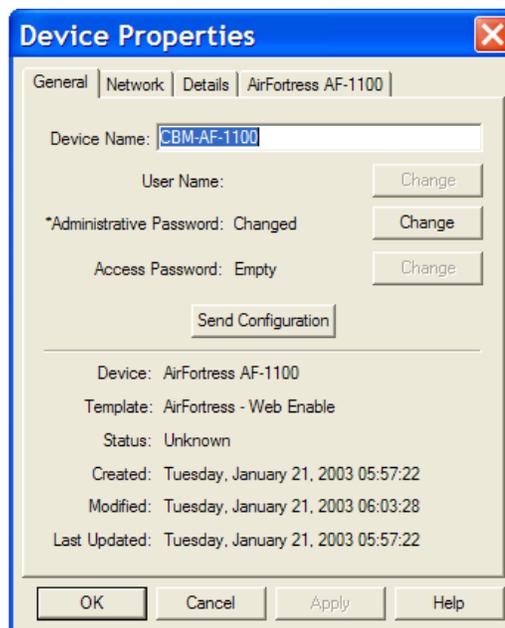


Figure 3-100 Inline Encryptor Device Properties General Tab

c) If you have made changes to values on the “**General**” tab, click on the “**Apply**” button.

NOTE: *Until you actually send the configuration to the encryptor, the administrative password and access password fields may indicate “empty” even though you entered it earlier. If you have previously sent this configuration to the encryptor, it will indicate a status of “set”. However, the application does not store user names or passwords. They are cached during the current session, but are lost as soon as you exit from the application. An asterisk to the left of the field name indicates that the password is cached. If there is no asterisk, you must reenter the password.*

7) Click on the “**Network**” tab.

a) Select “**Use the following Network Settings**” and enter the following parameters as assigned by your DOIM, CSSAMO or S6.

- (1) IP Address: (192.168.254.254 CAISI Default)
- (2) Subnet Mask: (255.255.255.0 CAISI Default)
- (3) Gateway: (192.168.254.254 CAISI Default)
- (4) Do **NOT** click on the “**Validate**” button, as there may be multiple encryptor devices with the same IP.

NOTE: *You do not have to change the CAISI Default IP address, “192.168.254.254”. All of the encryptors can have the same IP address.*

- b) If you have made changes to values on the “**Network**” tab, click on the “**Apply**” button.

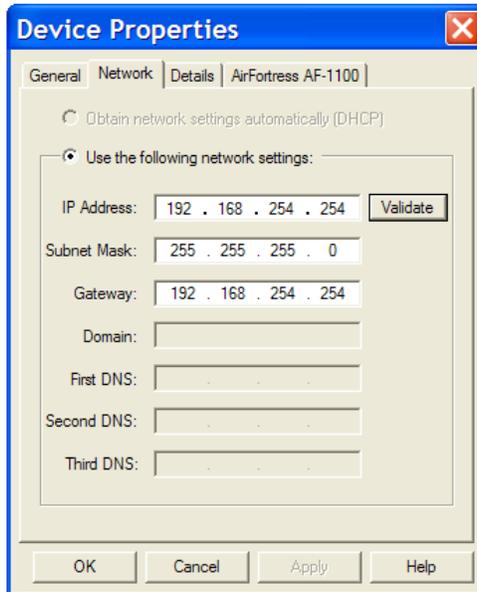


Figure 3-101 Inline Encryptor Device Properties Network Tab

- 8) Click on the “**Details**” tab.

“**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience. Click on the “**Apply**” button if any changes were made.

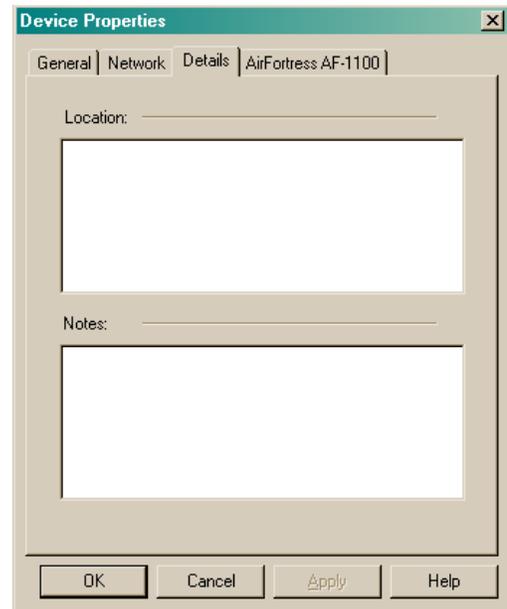


Figure 3-102 Inline Encryptor Device Properties Details Tab

9) Click on the “**AirFortress AF-1100**” tab.

a) Ensure the “**Crypto Algorithm:**” is set to **AES**.

b) Enter your unit specific “**Access ID:**” It is not case sensitive.

The CAISI default is
0123456789ABCDEF.

NOTE: *You must change the Access Id before deploying the encryptor.*

c) Change the “**Re-Keying Interval:**” to **2**. (Encryptor will verify key every 2 hours)

d) Serial Number field can be left blank.

NOTE: *A hole can be created in the “Firewall” by utilizing the “Access Point” feature. This allows the user to communicate to a device on the untrusted (radio) Network from the Trusted (STAMIS) network. This feature should only be utilized on the same CCM or CBM due to security measures. Be very careful when using this feature, as we do not encourage its use unless implemented under special circumstances.*

e) If you have made changes to values on the “**AirFortress AF-1100**” tab click on the “**Apply**” button.

f) Click on the “**OK**” button to exit the “**Device Properties**” screen.

g) The main CAISI Admin screen will appear where you should see the new device with the name you assigned it. The CAISI default is “**CBM-AF-1100**”.

h) Proceed to procedure **5. Send the configuration to the encryptor on Page 81**.

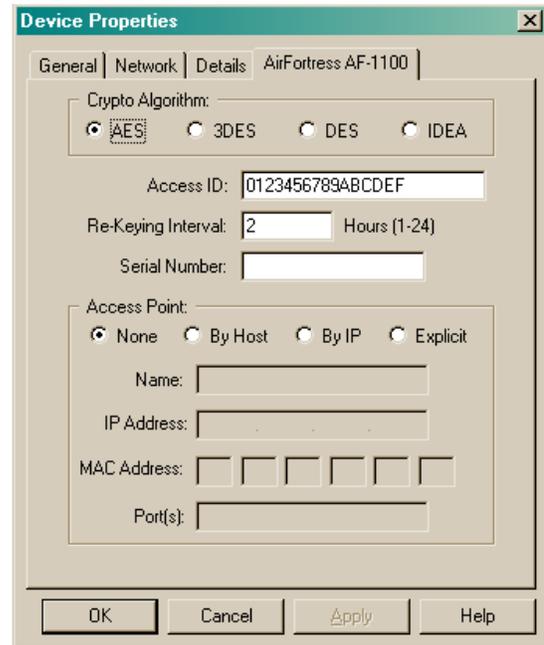


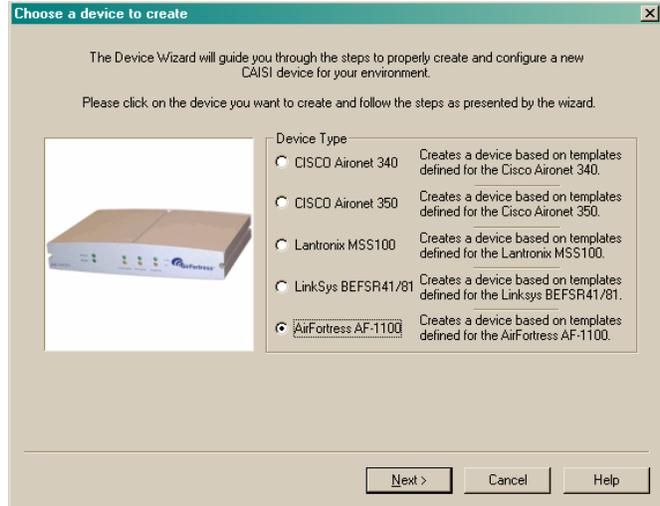
Figure 3-103 Inline Encryptor Device Properties Advanced Tab

b. **“Device Wizard” Method**

1) Select **“Device”** from the CAISI Admin menu and then select **“Device Wizard”** from the **“Device”** drop-down menu.

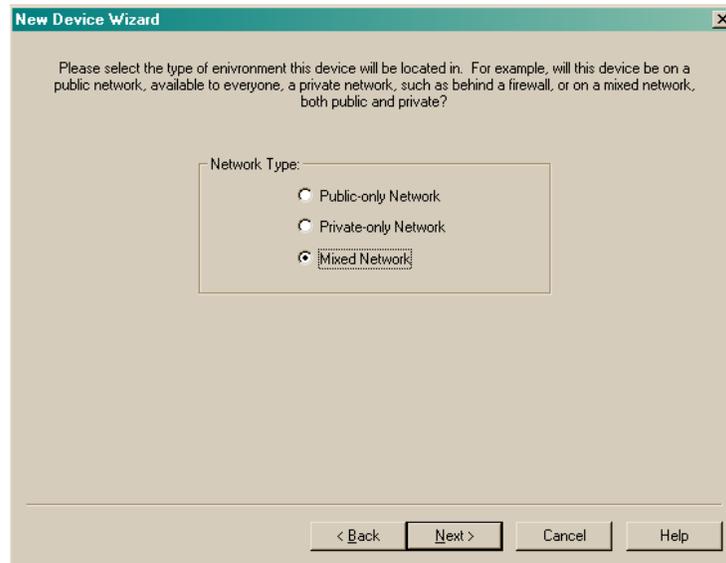
a) Set the **“Device Type”** button to **AirFortress AF-1100**.

b) Click on the **“Next>”** button.



**Figure 3-104 Inline Encryptor
Choose a Device to Create Screen**

2) Set the **“Network Type”** to **Mixed Network**. Click on the **“Next>”** button.



**Figure 3-105 Inline Encryptor
New Device Wizard**

3) Set **“DNS Hostname”** to **CBM-AF-1100**.

a) Create a **“Device Name:”** if you want it to be different from the **“DNS Hostname:”**

b) From the **“Available Device Templates”** drop-down menu, select **AirFortress – Web Enabled**.

c) Click on the **“Next>”** button.

**Figure 3-106 Inline Encryptor
New Device Wizard General Properties**

- 4) From the “**Use the following network settings:**” enter the following parameters as assigned by your DOIM or S6.
- IP Address: (**192.168.254.254** CAISI Default)
 - Subnet Mask: (**255.255.255.0** CAISI Default)
 - Gateway: (**192.168.254.254** CAISI Default)
 - Do **NOT** click on the “**Validate**” button, as there may be multiple encryptor devices with the same IP.
 - Click on the “**Next>**” button.

**Figure 3-107 Inline Encryptor
New Device Wizard Device Network Settings**

5) Make sure the “**Crypto Algorithm:**” is set to **AES**.

- a) Enter your unit specific “**Access ID:**”
The CAISI default is **0123456789ABCDEF**

NOTE: *You must change the Access ID before deploying the encryptor. It is not case-sensitive*

- b) Change the “**Re-Keying Interval:**” to **2**. (Encryptor will verify key every 2 hours)

- c) Serial Number field can be left blank.



**Figure 3-108 Inline Encryptor
New Device Wizard
AirFortress 1100 Advanced Settings**

NOTE: *A hole can be created in the “Firewall” by utilizing the “Access Point” feature. This allows the user to communicate to a device on the untrusted (radio) Network from the Trusted (STAMIS) network. This feature should only be utilized on the same CCM or CBM due to security measures. Be very careful when using this feature, as we do not encourage its use unless implemented under special circumstances.*

- d) Click the on the “**Next>**” button.

6) The “**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience.

- a) Click on the “**Next>**” button.



**Figure 3-109 Inline Encryptor
New Device Wizard Device Details**

- 7) Set the “**Administrative (Write) Password**”.
 - a) Enter your new password in the “**Administrative (Write) Password:**” box.
 - b) Reenter your password into the “**Confirm Administrative (Write) Password:**” box.
 - c) For classroom training, set the password to the CAISI default “**system00**”.

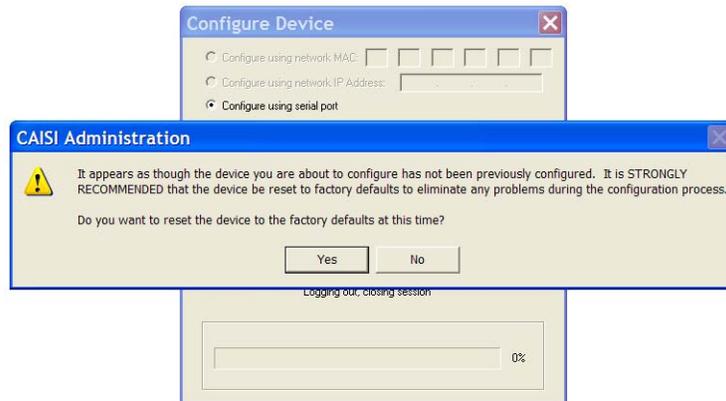


**Figure 3-110 Inline Encryptor
New Device Wizard Password Validation**

NOTE: *As you enter the password, asterisks will appear. The password is not shown in the clear. You must change the password before you deploy the inline encryptor.*

- d) Click on the “**Finish**” button.
 - e) The main CAISI Admin screen will appear where you should see the new device with the name you assigned it. The CAISI default is “**CBM-AF-1100**”.
 - f) Proceed to procedure **5. Send the configuration to the encryptor.**
5. Send the configuration to the encryptor.
 - a. Highlight the device you just created from the main screen. The CAISI default is **CBM-AF-1100**.
 - b. Select “**Device**” from the CAISI Admin toolbar and then select “**Properties**” from the “**Device**” drop-down menu.
 - c. Click on the “**Send Configuration**” button.
 - d. Select the “**Configure using serial port**” button.
 - e. Click on the “**Start**” button.

- f. At the “**Do you want to reset the device to factory defaults at this time?**” prompt, click on the “**Yes**” button.



**Figure 3-111 Inline Encryptor
Configure Device Screen**

- g. The “**Please COLD RESTART the device by power cycling the unit.**” prompt will appear.

- 1) At this time, physically disconnect either the power cable attached to back of the encryptor or on the main power supply label “**encryptor/hubs**”. Reconnect it. This will perform a Cold Restart of the encryptor.

NOTE: *Do not wait for the encryptor to finish rebooting before clicking on the “**OK**” button.*

- h. When the Windows dialog box appears stating the “**The device has been configured successfully**”, click on the “**OK**” button.
- i. Click on the “**Done**” button on the “**Configure Device**” screen.
- j. Click on the “**OK**” button to exit the “**Device Properties**” screen. The encryptor is now configured for operation.
- k. Close CAISI Admin by clicking the (X) at the top right of the screen or by selecting “**Configuration**” from the main menu bar and then selecting “**Exit**”.
- l. At the CAISI Administration prompt, “**Do you want to save changes to the configuration before exiting the application?**”, click on the “**Yes**” button.
- m. Disconnect the white straight-through Ethernet cable from the NIC in the SSR notebook and the CBM hub.

Inline Encryptor is now configured.

3.6.6 Verify Inline Encryptor Operational Status.

1. Connect your notebook NIC to the hub in a CBM or CCM with a white straight-through CAT-5 Ethernet cable.
2. Open Internet Explorer.
 - a. Use the secure web browser to connect to the encryptor, as follows:
 - b. Enter the factory default IP address “**https://192.168.254.254**” or your own previously assigned encryptor address in the browser address bar.

NOTE: Notice that using the browser in secure mode (**https** instead of **http**) means that you must type in the entire command, not just the address.

- c. When the Security Alert appears, click “**OK**”.
- d. A second Security Alert will appear, click “**Yes**”.
- e. The “**Enter Network Password**” screen will appear.
- f. You will be prompted for a user name and password.

NOTE: To access the encryptor from the web, a different username and password than that which you used in the console is required. The web access username is “*admin*” and cannot be changed. You can only change the password.

- g. Enter “**admin**” (factory default) in the “User Name” field.
- h. Enter one of the following passwords in the “Password” field: “**admin**” (factory default), “**system00**” (CAISI default), or the password you previously assigned the device as prescribed by your DOIM, S6 or CSSAMO.
- i. Click on the “**OK**” button.



**Figure 3-112 Inline Encryptor
Enter Network Password Screen**

3. Verify encryptor is configured.
 - a. To confirm the encryptor settings you configured in CAISI ADMIN are set; click the “**LAN SETTINGS**” button.
 - 1) The encryptor default IP address should appear **192.168.254.254**. However, if you changed the encryptor IP address you should see the IP Address you assigned the device.
 - b. Alternatively, click on the “**SECURITY SETTINGS**” button.
 - 1) The Crypto Algorithm should be set to **AES**.
 - 2) Close web browser.

3.6.7 CBM Power Cable Disconnection Procedures.

1. Turn off power to the UPS by pressing the “O” (OFF) side of the UPS rocker switch.
2. Disconnect the UPS from the external power source.
3. Disconnect the wireless bridge, hub and encryptor power cords from the UPS “Battery Backup Protected Outlets”.
4. Disconnect the 2-prong power cable from the hub and encryptor power supply.
5. Disconnect the 3-prong power cable from the wireless bridge power supply.

3.7 UTILIZING CAISI ADMIN TO CONFIGURE THE CCM



Figure 3-113 CCM

The CCM includes two components that require configuration before it can be put into operation. They are:

1. Multi-Client Radio Adapter Paragraph 3.7.2
2. Inline Encryptor Paragraph 3.7.5

The following WARNINGS and CAUTIONS apply to the entire lesson.

WARNINGS

- Severe injury or death can occur if this equipment, its antennas, or connected communications cables come near electric 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. This may cause severe injury or death. **Never operate a wireless device without an antenna. It can damage the radio.**

**Five Safety Steps to Follow
If Someone Is the Victim of Electrical Shock
WARNINGS**

- Do not try to pull or grab the individual.
- If possible, turn off the electrical power.
- If you cannot turn off the electrical power, push, pull or lift the person to safety using a dry wooden pole, a dry rope or some other insulating material.
- Send for help as soon as possible.
- After the injured person is free of contact with the source of electrical shock, move the person a short distance away and immediately start first aid, if necessary.

CAUTIONS

- Never connect cables when the power is on.
- Never pull directly on cables.
- Always connect and disconnect using the plugs at the ends 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 that plugs match their connectors before installing.

Security Considerations

- Only the “external” radio link is encrypted, not the “internal” (LAN) link (connected to the hub).
- You must periodically change the encryptor Access IDs.
- Due to security vulnerabilities you should not remotely configure the radios.
- Your network cables from the LSA to the hub in the CCM should be included in your protected distribution system. They are not encrypted – only the radio links are encrypted.

Security Considerations

- The reset button on the radio 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 a SSR reconfigures it.

3.7.1 Physical Connection Procedures

NOTE: Ensure an antenna is connected to the CCM IAW procedures outlined TM 11-5895-1691-12 Paragraph 2.18 before performing the following procedures.

1. Connect CCM power cables.
 - a. Remove the 2-prong power cable from the CCM carrying case.
 - b. Connect the female end of the 2-prong power cable to the power supply in the base of the chassis.
 - c. Connect the male end of the 2-prong power cable into an external power source.



Figure 3-114 CCM Power Cable Connections

2. Connect CCM Multi-client radio adapter to notebook wired NIC or built-in NIC.
 - a. The multi-client radio adapter does not have a console port. You can only configure it over the network.
 - b. Disconnect the red crossover cable from the “Encrypted” port on the back of inline encryptor.
 - c. Remove a RJ-45 straight-through adapter and a white straight-through Ethernet cable from the SSR Notebook case or SSR Transit case.
 - d. Connect the end of the red crossover cable to the RJ-45 straight-through adapter.
 - e. Connect one end of the white straight-through Ethernet cable to the RJ-45 straight-through adapter and the other end to the NIC on the SSR Notebook.

- f. You are now connected from your NIC to the “Ethernet” port on the multi-client radio adapter.

NOTE: *If the multi-client radio adapter is not installed in a CCM, refer to TM 11-5895-1691-12, Paragraph 2.33.1.1 for physical connection procedures.*

3.7.2 Configure the CCM Multi-Client Radio Adapter (Firmware 8.65)

NOTE: *A standard CAISI SSR notebook, configured as follows is required for wireless bridge set up. It 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. The wired NIC or built-in NIC must be used.*

1. Apply power to the SSR notebook.
 - a. Enter your username and password. The CAISI defaults are “**caisiadmin**” and “**BS_69dlw**”.
 - b. A Logon Message prompt will appear, “Your password expires today. Do you want to change it now?” For classroom training, click on the “**No**” button.
2. Reset the Radio to “factory defaults”.
 - a. With the radio powered, insert your CAISI reset tool into the reset button (very small hole located on the back of the radio next to the power input). You will feel or hear a small click.
 - b. Press and hold the button for approximately ten – fifteen seconds. Continue to hold the reset button until:
 - 1) The “**Status**” LED (middle) on the CCM turns to red or amber.
 - 2) The “**Ethernet**” LED (top) flickers briefly.
 - c. Remove the reset tool. The CCM radio will reboot and power itself back to a ready state. The “**Status**” LED should be lit green.
3. Open “**CAISI Admin**”.
 - a. At the bottom of the SSR notebook screen, click on “>>” to the right of the “CAISI Toolbox” button. The CAISI Toolbox menu will appear. Click on “**CAISI Admin**”
4. Set-up the Multi-Client Radio Adapter device. There are 2 methods, 1) By selecting the “**Add**” option or 2) Use of the “**Device Wizard**” option from the “Device” drop down menu. You may choose either method.

a. **“Add” Option Method**

- 1) Select **“Device”** from the CAISI Admin menu and then select **“Add”** from the **“Device”** drop-down menu.



Figure 3-115 Multi-Client Radio Adapter Add Option Menu

- 2) Set **“DNS Hostname:”** (Where **“DNS hostname”** = the host name of the wireless bridge) to the name provided by your DOIM, S6 or CSSAMO.

The CAISI default is **“CCM-340-350”**.

- 3) Create a **“Device Name:”** if you want it to be different from the **“DNS Hostname:”**
- 4) From the **“Template”** drop-down menu select a template from the list of CAISI Admin defined templates.

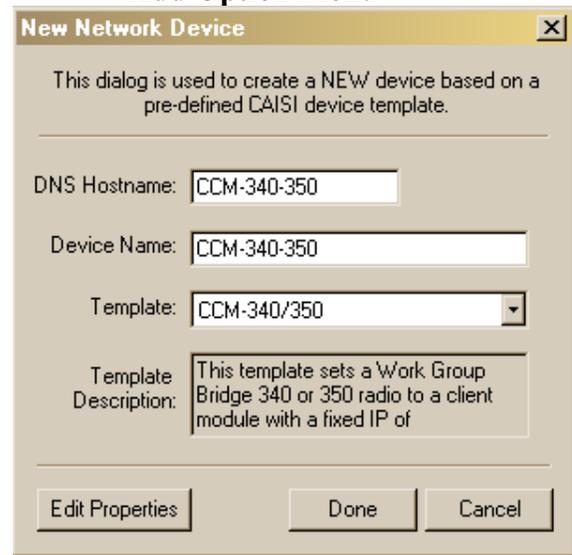


Figure 3-116 Multi-Client Radio Adapter New Network Device Screen

NOTE: *The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited.*

- 5) For classroom training, set **“Template”** to **CCM-340/350**.
- 6) Click on the **“Edit Properties”** button. The **“Device Properties”** screen will appear with the **“General”** tab selected.
 - a) Verify the **“Device Name”** (the host name you assigned the multi-client radio adapter) is correct. The CAISI default is **“CCM-340-350”**.
 - b) Set the **“Administrative Password”** to the password provided by your DOIM, S6 or CSSAMO.
 - (1) Click on the **“Change”** button. The Set Password screen will appear.

(2) Enter your new password in the “**Enter Password**” dialog box.

(3) For classroom training set the password, to the CAISI default “**system**”.

NOTE: *As you enter the password, asterisks will appear. The password is not shown in the clear. You must change the password before you deploy the radio.*

(4) Press on the <Tab> key and confirm the new password by entering the password in the “**Confirm Password**” dialog box.

(5) Click on the “**OK**” button.

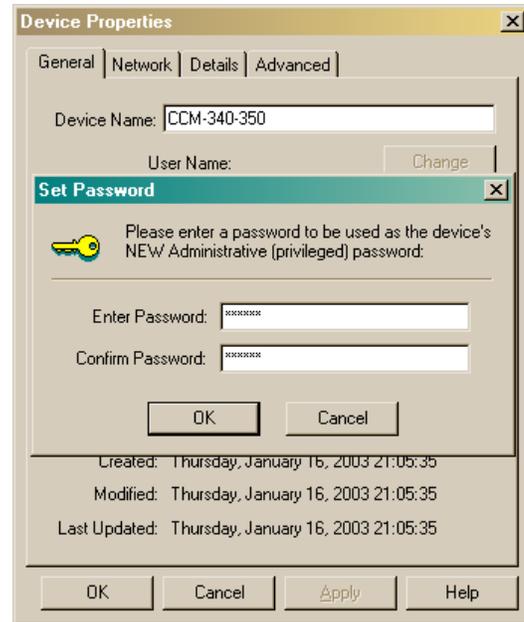


Figure 3-117 Multi-Client Radio Adapter Set Administrative Password Screen

(6) Click on the “**OK**” button on the “**Important: Do not lose device passwords**” screen.

c) Set the “**Access Password**” to the password provided by your DOIM, S6 or CSSAMO.

(1) Click on the “**Change**” button. The “**Set Password**” screen will appear.

(2) Enter your new password in the “**Enter Password**” dialog box.

(3) For classroom training, set the password to the CAISI default “**access**”.

NOTE: *As you enter the password, asterisks will appear. The password is not shown in the clear. You must change the password before you deploy the radio.*

(4) Press on the <Tab> key and confirm the new password by entering the password in the “**Confirm Password**” dialog box.

(5) Click on the “**OK**” button.

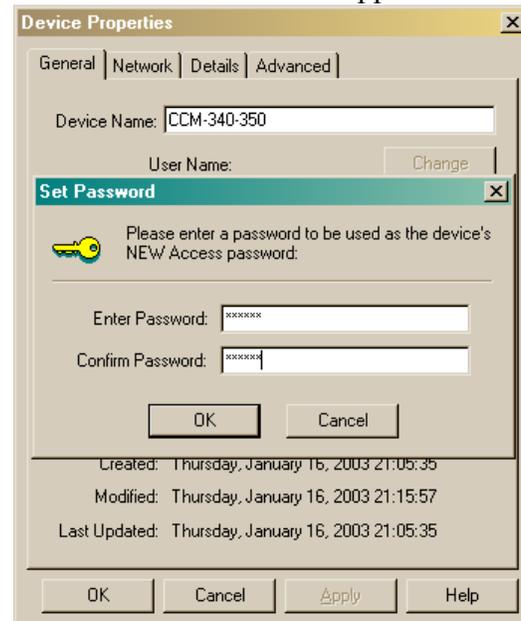


Figure 3-118 Multi-Client Radio Adapter Set Access Password Screen

- (6) Click on the “OK” button on the “**Important: Do not lose device passwords**” screen.
- d) If you have made changes to values on the “**General**” tab, click on the “**Apply**” button.

NOTE: *Until you actually send the configuration to the radio, the administrative password and access password fields may indicate “empty”, even though you entered it earlier. If you have previously sent this configuration to the radio, it will indicate a status of “set”. However, the application does not store user names or passwords. They are cached during the current session, but are lost as soon as you exit from the application. An asterisk to the left of the field name indicates that the password is cached. If there is no asterisk, you must reenter the password.*

- 7) Click on the “**Network**” tab.
- a) Select “**Use the following Network Settings**” and enter the following parameters as assigned by your DOIM, CSSAMO or S6.
- (1) IP Address: **(192.168.1.5 CAISI Default)**
 - (2) Subnet Mask: **(255.255.255.0 CAISI Default)**
 - (3) Gateway: **(192.168.1.1 CAISI Default)**
 - (4) Domain: **(Warning.US.Government CAISI Default)**
 - (5) First DNS: **(leave at 0.0.0.0)**
 - (6) Second DNS and Third DNS: **(leave at 0.0.0.0)**

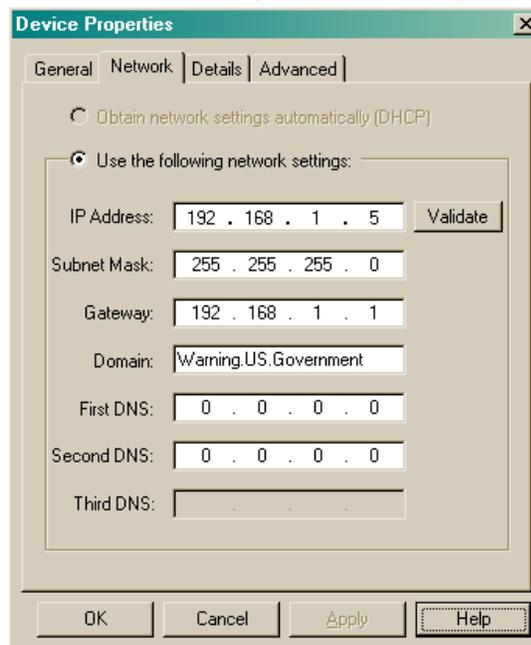


Figure 3-119 Multi-Client Radio Adapter Device Properties Network Tab

NOTE: *Since there is not a DHCP server on the Untrusted Network (the radio portion of the network is on the “Encrypted” side of the encryptors and cannot see any host or server on the “Unencrypted” side), the user is advised not to select “Obtain network settings automatically (DHCP)”.*

- b) Click on the “**Validate**” button.
 - (1) If the IP Address is unique, click on the “**OK**” button when prompted.
 - (2) If the IP Address is not unique, a list box will pop up to show you the other device configurations that use that address. Click on the “**OK**” button to dismiss the list box. If necessary, enter a new IP Address, subnet mask, or both.
 - c) If you have made changes to values on the “**Network**” tab, click on the “**Apply**” button.
- 8) Click on the “**Details**” tab.
- a) “**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience. Click on the “**Apply**” button if changes were made.
- 9) Click on the “**Advanced**” tab.
- a) Verify that the “Model:” is “**AIR-WGB340**”.
 - b) Enter your unit specific SSID. The CAISI default for hardware testing and classroom training is “**caisi000**”. *You must change the SSID before deploying the radio.*
 - c) Verify “**Broadcast Power**” is set to “**full**”. OCONUS countries may require you to lower power setting, check with your local frequency manager upon arrival.
 - d) Under “**Privacy Encryption Keys**” click on the “**Set Key 1**” button.

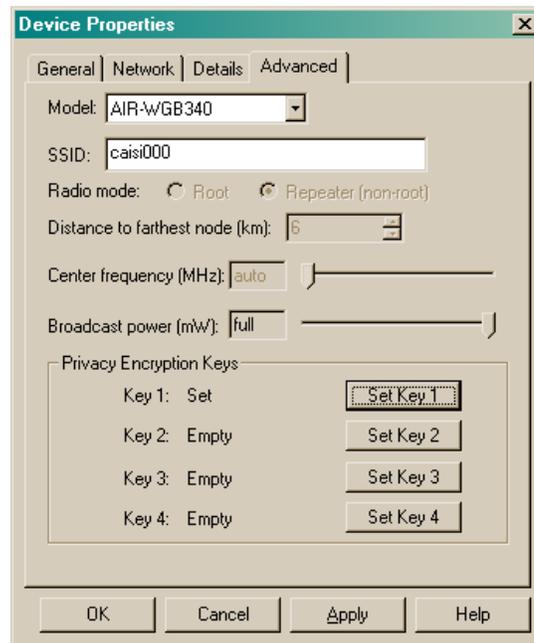


Figure 3-120 Multi-Client Radio Adapter Device Properties Advanced Tab

- (1) Click on “**Long 26 digits**” (Do not use short key.)
- (2) Under “**Enter Key**”, enter your 26 digit hexadecimal encryption key.



Figure 3-121 Multi-Client Radio Adapter Set WEP Key Screen

- (3) The CAISI default is **0123456789abcdef0123456789** for hardware testing and classroom training. *You must change the key before deploying the radio.*
- (4) Confirm the key by re-entering it into the “**Confirm Key**” field. Click on the “**OK**” button.
- e) If you have made changes within this tab, click on the “**Apply**” button and then click on the “**OK**” button.
- 10) The main CAISI Admin screen will appear where you should see the new device with the name you assigned it. The CAISI defaults are “**CCM-340-350**”.
- 11) Proceed to procedure **5. Send the configuration to the multi-client radio adapter on page 96.**

b. **“Device Wizard” Method**

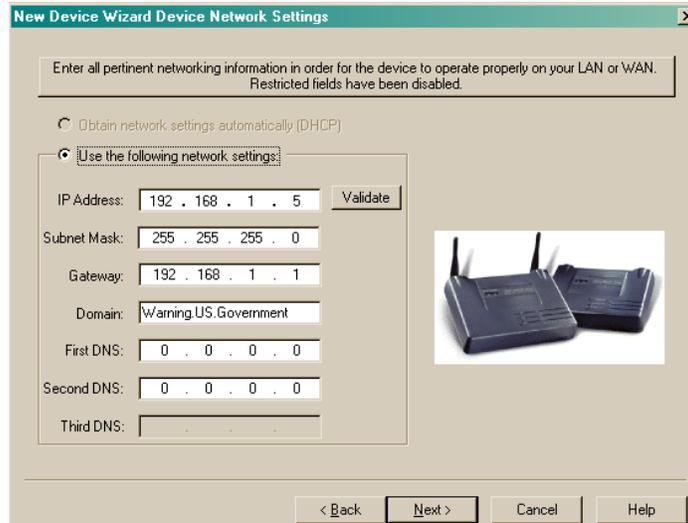
- 1) Select “**Device**” from the CAISI Admin menu and then select “**Device Wizard**” from the “Device” drop-down menu.
- 2) Set the “Device Type” button to **Cisco Aironet 340**. Click on the “**Next>**” button.
- 3) Set the “Network Type” to **Mixed Network**. Click on the “**Next>**” button.
- 4) Set “DNS Hostname” to “**CCM-340-350**”.
- 5) Create a “**Device Name:**” if you want it to be different from the “DNS Hostname:”
- 6) From the “**Available Device Templates**” drop-down menu, select **CCM-340/350**.

NOTE: *The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited.*

- 7) Click on the “**Next>**” button.

**Figure 3-122 Multi-Client Radio Adapter
New Device Wizard General Properties**

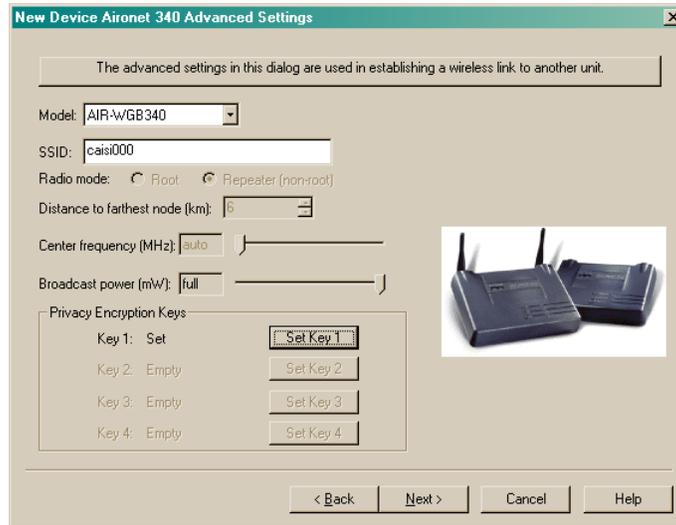
- 8) From the “**Use the following Network Settings**” enter the following parameters as assigned by your DOIM, S6 or CSSAMO.
 - a) IP Address: (**192.168.1.5** CAISI Default)
 - b) Subnet Mask: (**255.255.255.0** CAISI Default)
 - c) Gateway: (**192.168.1.1** CAISI Default)
 - d) Domain: (**Warning.US.Government** CAISI Default)
 - e) First DNS: (**leave at 0.0.0.0**)
 - f) Second DNS and Third DNS: (**leave at 0.0.0.0**)



**Figure 3-123 Multi-Client Radio Adapter
New Device Wizard Device Network Settings**

- 9) Click on the “**Validate**” button.
 - a) If the IP Address is unique, click on the “**OK**” button when prompted.
 - b) If the IP Address is not unique, a list box will pop up to show you the other device configurations that use that address. Click on the “**OK**” button to dismiss the list box. If necessary, enter a new IP Address, subnet mask, or both.
 - c) Click on the “**Next>**” button.
- 10) Verify that the “Model:” is “**AIR-WGB340**”. (Figure 3-124)
- 11) Enter your unit specific SSID. The CAISI default for hardware testing and classroom training is “**caisi000**”. **You must change the SSID before deploying the bridge.**
- 12) Verify “**Broadcast Power**” is set to “**full**”. OCONUS countries may require you to lower power setting, check with your local frequency manager upon arrival.
- 13) Under “Privacy Encryption Keys”, click on “**Set Key 1**” then click on “**Long 26 digits**”, (**Do not use short key.**)

- 14) Under “**Enter Key**” enter your 26 digit hexadecimal encryption key. The CAISI default is **0123456789abcdef0123456789** for hardware testing and classroom training. *You must change the key before deploying the radio.*
- 15) Confirm key by re-entering into the “**Confirm Key**” field. Click on the “**OK**” button.
- 16) If a value has been changed, click on the “**OK**” button.
- 17) Click on the “**Next>**” button.



**Figure 3-124 Multi-Client Radio Adapter
New Device Aironet 340 Advanced Settings**

- 18) The “**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience. Click on the “**Next>**” button.

- 19) Enter your new password in the “**Administrative (Write) Password:**” box and then reenter your password into the “**Confirm Administrative (Write) Password**” box. The CAISI default is “**system**”.



**Figure 3-125 Multi-Client Radio Adapter
New Device Wizard Password Validation**

- 20) Enter your new password in the “**Access (Read) Password:**” box and then reenter your password into the “**Confirm Access (Read) Password**” box. The CAISI default is “**access**”.

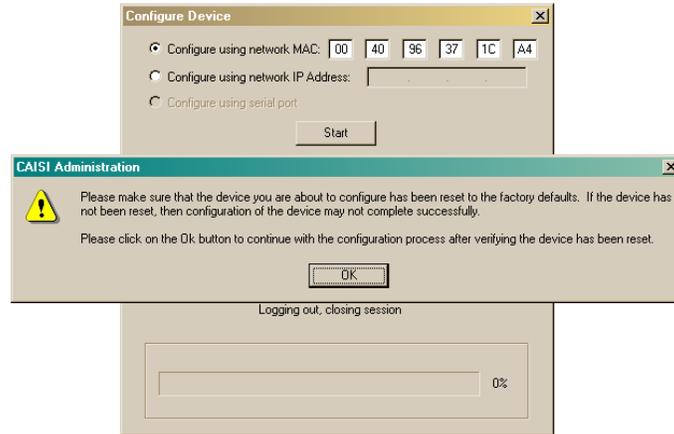
NOTE: *As you enter the password, asterisks appear. The password is not shown in the clear. You must change the password before deploying the bridge. You must change the password before you deploy the radio.*

- 21) Click on the **“Finish”** button.
- 22) Click on the **“OK”** button on the **“Important: Do not lose device passwords”** screen.
- 23) A dialog box will appear, click on the **“Done. No further action”** button.
- 24) Click on the **“OK”** button.



Figure 3-126 Multi-Client Radio Adapter CAISI Admin New Device Wizard

- 25) The main CAISI Admin screen will appear where you should see the new device with the name you assigned it. The CAISI defaults are **“CCM-340-350”**.
 - 26) Proceed to procedure **5. Send the configuration to the multi-client radio adapter.**
5. Send the configuration to the multi-client radio adapter.
 - a. Highlight the device you just created from the main screen. The CAISI defaults are **“CCM-340-350”**.
 - b. Select **“Device”** from the CAISI Admin toolbar and then select **“Properties”** from the **“Device”** drop-down menu.
 - c. Click on the **“Send Configuration”** button.
 - d. Select the **“Configure using network MAC”** button.
 - e. Enter the MAC address from the front of the Multi-Client Radio Adapter into the MAC address field.
 - f. Click on the **“Start”** button
 - g. Click on the **“OK”** button **ONLY** after resetting the Multi-Client Radio Adapter to factory defaults in response to the **“Please make sure that the device.....”** message. **The reset instructions are described below”** prompt.



**Figure 3-127 Multi-Client Radio Adapter
Configure Device Screen**

- h. Reset the multi-client radio adapter to factory defaults.
 - 1) With the radio powered, insert gently your CAISI reset tool into the reset button (very small hole located on the back of the radio next to the power input). You will feel or hear a small click.
 - 2) Press and hold the button for approximately 10-15 seconds. Continue to hold the reset button until:
 - a) The “**Status**” LED (middle) on the CCM turns to red or amber.
 - b) The “**Ethernet**” LED (top) flickers briefly.
 - 3) Remove the reset tool. The CCM radio will reboot and power itself back to a ready state.
- i. If the “**Administrative**” and “**Access**” passwords have not been entered previously, the entry boxes will appear. Enter the “**Administrative**” and “**Access**” passwords that your DOIM, S6 or CSSAMO has assigned. The CAISI defaults are “**system**” and “**access**”, respectively. Click on the “**OK**” button when completed. The CCM radio will now start to be configured. If the boxes don't appear, then skip this step.
- j. Click on the “**OK**” button when “**The device has been configured successfully**” message appears.
- k. Click on the “**Done**” button on the “**Configure Device**” screen.
- l. Click on the “**OK**” button to exit the “**Device Properties**” screen.
- m. The **CCM multi-client radio adapter** is now configured for operation. Click on the “**OK**” button on the “**Device Properties**” screen.
- n. Close CAISI Admin by clicking the (X) at the top right of the screen or by selecting “**Configuration**” from the main menu bar and then selecting “**Exit**”.

- o. At the CAISI Administration prompt, **“Do you want to save changes to the configuration before exiting the application?”** click on the **“Yes”** button.

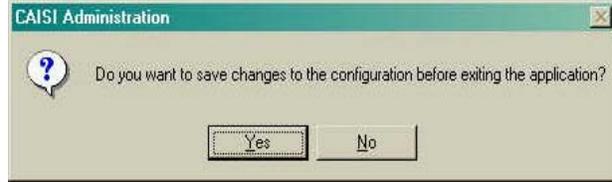


Figure 3-128 Multi-Client Radio Adapter Save Configuration Prompt

NOTE: You can use the *“Configure using network IP address”* option after you configure the multi-client radio adapter the first time with the MAC address.

3.7.3 Verify CCM Multi-Client Radio Adapter Operational Status

1. Open Internet Explorer.
2. In the address toolbar at the top of Explorer, enter the IP address with which you gave the radio adapter during configuration. In this case enter the CAISI default IP – **http://192.168.1.5**.
3. Click on **“Go”** on the Explorer toolbar or click on **“Enter”** on the notebook keyboard.
4. Click on **“Write Access”** at the top of the screen.
5. The **“Enter Network Password,”** screen will appear.
 - a. You will be prompted for a user name and password.
 - b. Enter **“ccm000”** in the **“User Name”** field. (This field can be left blank, user name does not matter).
 - c. Enter the password you assigned the device as prescribed by your DOIM, S6 or CSSAMO in the **“Password”** field. The CAISI default is **“system”**.
 - d. Click on the **“OK”** button.
6. Click on the **“Statistics”** menu select **“all”** next to **“Show Network Map.”**



Figure 3-129 Multi-Client Radio Adapter Enter Network Password Screen

- a. Locate the multi-client radio adapter you just configured by finding its MAC address in the list of devices on the network.
- b. Once you've located the multi-client radio adapter, verify the IP address is the one you assigned the device.
- c. Click on “Done”.

Device	Node Id	IP Address	Ver	Name
WGB340	00409648c898	192.168.001.005	8.58	WGB340_48c898
Enode	0010e49f8c53	192.168.001.002		

Figure 3-130 Multi-Client Radio Adapter Network Map

7. Close web browser.

3.7.4 Disconnect CCM Multi-Client Radio Adapter from the Notebook Computer

1. Disconnect the white straight-through Ethernet cable from the NIC in your SSR notebook and the RJ-45 straight-through adapter.
2. Disconnect the red crossover cable from the RJ-45 straight-through adapter and the “Ethernet” port on the back of the multi-client radio adapter.
3. Re-attach the short red crossover cable you initially removed from the “Encrypted” port on the back of inline encryptor.

NOTE: *If you have performed all necessary configuration procedures involving the Multi-client radio adapter and are ready to power down the equipment, refer to Paragraph 3.7.6 for procedures on disconnecting the Multi-Client Radio Adapter power cables.*

3.7.5 Configure the CCM Inline Encryptor (Firmware 1178W)

The process for configuring the Air Fortress Encryptor for the CCM is identical to the encryptor for the CBM. Please refer to Paragraph 3.6.5 of the configuration process for the CBM Encryptor.

3.7.6 CCM Power Cable Disconnection Procedures

1. Disconnect the male end of the 2-prong power cable from the external power source.
2. Disconnect the female end of the 2-prong power cable from power supply in the base of the chassis.

Section III CAISI ADMIN Management & Administration

3.8 CAISI ADMIN MANAGEMENT

With all applications, there are certain administrative functions that must be performed weekly, maybe even daily. This section covers the procedures for modifying devices, logging, configuration record keeping, how to perform backups and how to print.

3.8.1 Audit Logging

3.8.1.1 Purpose

The CAISI Admin application has a built-in audit logging facility. The primary purpose of audit logging is to gather information regarding usage activity and/or errors that might have occurred during device configuration or general use. There are many different levels and types of audit logging. They are listed in Table 3-10.

Table 3-10 Audit Logging Preferences

Preference	Description
Log informational messages	Informative messages provide the user with feedback as to what the application is doing at any particular instant. For instance, the user may want to know when the application has started to configure a device.
Log alert messages	Alert messages are critical interactive messages that alert the user to potentially disastrous errors or events. By checking this option, these interactive messages will also be written to the audit log.
Log error messages	Error messages indicate an unsuccessful attempt to perform a specific operation.
Log debug messages	Debug messages are used to output large amounts of low-level command data that is generally used by a support desk in troubleshooting a particular problem. Since these types of messages can dramatically increase the size of the audit log and <u>COMPROMISE SECURITY</u> by revealing device passwords, it is recommended that this option <u>ONLY</u> be selected when troubleshooting a problem.
Success/Failure audit	Success/failure audits are designed to provide an audit trail of application activity. These are designed to indicate when system parameters or settings have been changed; templates and devices have been added, deleted, or modified.

The audit log is stored as a regular ASCII (American Standard Code for Information Interchange) text file. The file can be viewed through the CAISI Admin application or through any text editor.

The location of the log file is determined by the location selected in the audit logging preferences dialog. The name of the log is of the format “<YYMM>.log” where <YY> is the two-digit designation for the current year, and MM is the current month. At the beginning of every month, a new log file is generated leaving the old one intact.

3.8.1.2 Viewing Details in the Audit Log

As stated in the previous section, the audit log can either be viewed through the application or through any COTS text editor. To view the log through the application:



Figure 3-131 View Audit Log - Main Menu Option

1. Click on the “**View**” main menu option.
2. Click on the “**Audit log**” sub-menu option. A dialog similar to the following will be displayed:

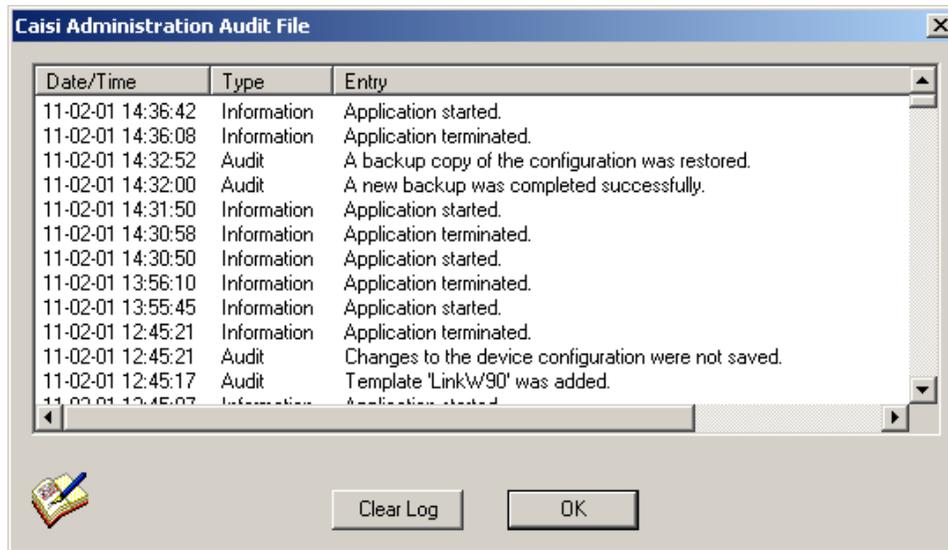


Figure 3-132 Audit Log Dialog Box

3. The contents of the audit log file are displayed. As can be seen in the above example, the log reflects the date and time a particular event occurred as well as the type of audit that was performed.

3.8.1.3 Deleting the Audit Log

Since the audit log grows with each use of the application, over time it may become too large to be effective. In other words, the log could at some point become cumbersome to read with a large number of entries. To delete the log file, follow the steps in the previous section and click on the “**Clear Log**” button. This will delete the contents of the log file.

3.8.2 Configuration File

All CAISI Admin template and device configurations and settings are stored in one centralized file named “CAISIAdmin.ccf”. This file is located in the CAISI Admin base directory path. This is the path where the application was installed. The path should be “C:\Net Tools\CAISIAdmin.ccf”.

Whenever a change to a template or a device configuration is made, the CAISI Admin application sets an internal flag that indicates a change has been made and the configuration file should be saved. This is done so that when the application is terminated, if the configuration file has not been saved, the application can prompt the user to save the file. If the application is terminated without saving the file, any changes made are not saved to disk and are lost.

3.8.2.1 Saving the Configuration File

The CAISI Admin configuration file can be saved at any time. To save the configuration file:

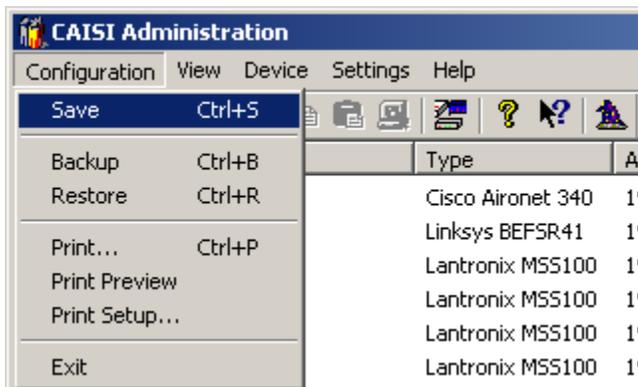


Figure 3-133 Configuration Save Menu Option

1. Click on the “**Configuration**” main menu option.
2. Click on the “**Save**” sub-menu option or Ctrl+S key combination, OR by using the CAISI Admin tool bar, click on the floppy diskette icon

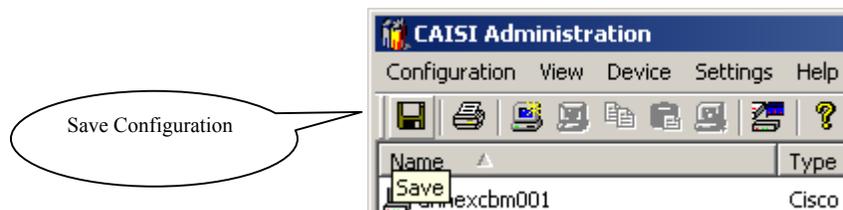


Figure 3-134 Configuration Save Toolbar Button

The configuration file will automatically be updated with the current template and device settings.

NOTE: Typically after a device has been configured, the configuration information will be modified with MAC address or IP address changes and the configuration file should be saved.

3.8.2.2 Backup and Restore

The CAISI Admin has built-in backup and restore capability to provide disaster recovery functionality. Backup and restore is performed on the CAISI Admin configuration file only, which will preserve all defined templates and devices as well as all of the defined attributes and configuration information. CAISI Admin preferences and settings are not backed up.

The CAISI Admin has the capability to store multiple backups. This capability opens the door for the “grandfathering” of backup files. This is achieved by sequentially numbering the backup files in order to maintain grandfathering integrity. The next section discusses how multiple backups are handled by the application.

3.8.2.3 Configuration Backup

In the event of a hard disk failure or for other disaster recovery reasons, a backup of the configuration file should be performed whenever possible. To backup the CAISI configuration:

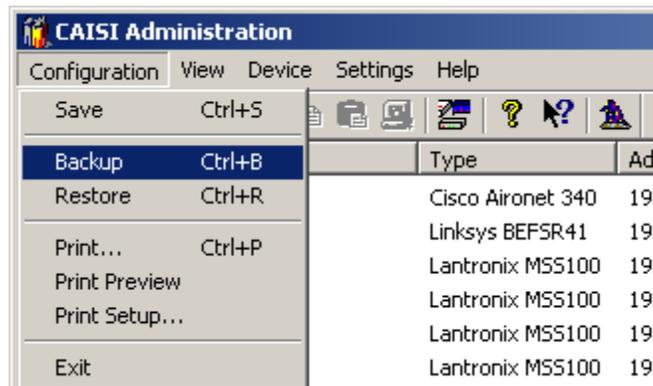


Figure 3-135 Configuration Backup Menu Option

1. Click on the “**Configuration**” main menu option.
2. Click on the “**Backup**” sub-menu option or depress the Ctrl+B keys. The “CAISI Configuration Backup” dialog will be displayed prompting for a location to backup the files to.

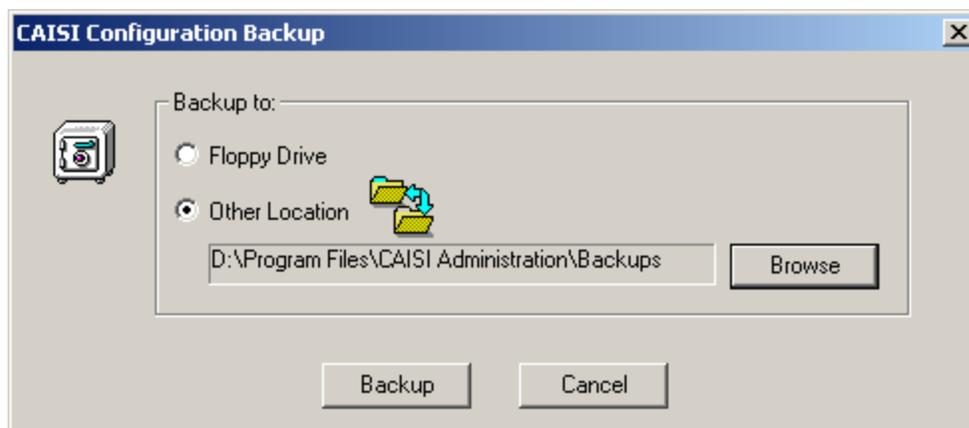


Figure 3-136 Configuration Backup Dialog Box

By default, the application pre-selects the floppy drive. This is generally the best method since it provides off-line storage of the configuration. In the event the local hard drive becomes corrupt and un-readable, a copy of the configuration file is stored onto floppy where it is easily recoverable. However, there are two available options:

- Floppy - Defaults to using the A: drive.
 - Other - Allows specification of a different drive and directory on the local computer or LAN.
3. Click on the backup location to use.
- If the selection is the “**Floppy Drive**”, make sure a floppy diskette has been inserted into the A: drive.
 - If the selection is “**Other Location**”, the last directory path used for backup/restore will be used. Click on the “**Browse**” button or select a different location. The following dialog will be displayed:

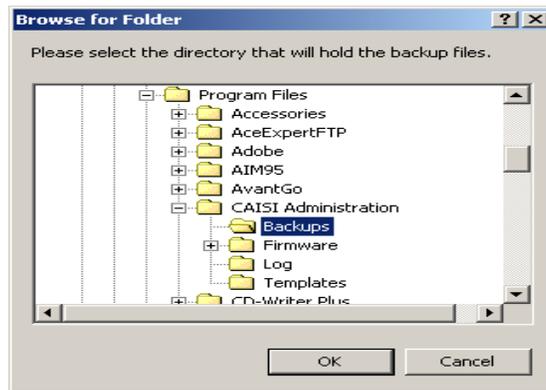


Figure 3-137 Browse for Folder Dialog Box

4. Select the drive and directory from the browse dialog and click on the “**OK**” button.
5. In the CAISI Admin Backup dialog, click on the “**Backup**” button to begin the backup.

NOTE: *The application maintains the naming of the backup files and will call the backup “CAISIAAdmin_bkp.ccf”.*

Refer to Figure 3-138, if a backup file already exists, the user will have the option of replacing the existing backup or creating a new backup file.



Figure 3-138 New or Replace Backup Dialog Box

- If the backup file is not replaced, a new file is created and will be named “CAISIAAdmin_bkp<x>.ccf” where <x> will be the next sequential number (ex. “CAISIAAdmin_bkp5.ccf”). The sequential numbering begins with 0. By creating a new backup file, the concept of backup grandfathering is introduced.

Note: *The backup will only take a few seconds and when complete a success dialog will be displayed.*



Figure 3-139 Backup Complete Prompt

- Click on “OK” button.

3.8.2.4 Configuration Restore

Restoration of the CAISI Admin configuration file may be required when the original configuration file is missing or has become corrupt. To restore a configuration file backup:

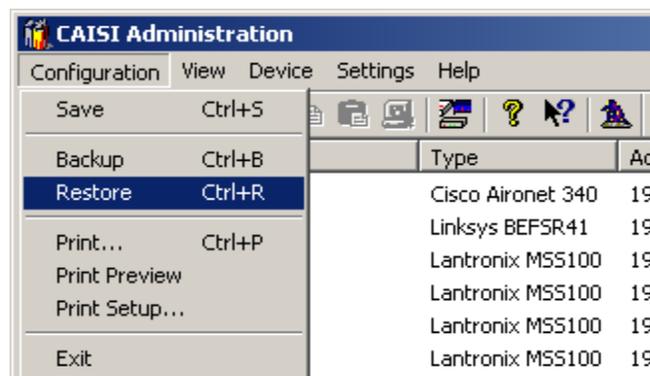


Figure 3-140 Configuration Restore Menu Option

- Click on the “**Configuration**” main menu option.
- Click on the “**Restore**” sub-menu option or depress the Ctrl+R keys. The CAISI Configuration Restore dialog will be displayed. The application needs to know where the configuration backups exist. The backup file can be on a floppy diskette in the Floppy Drive or in another location.

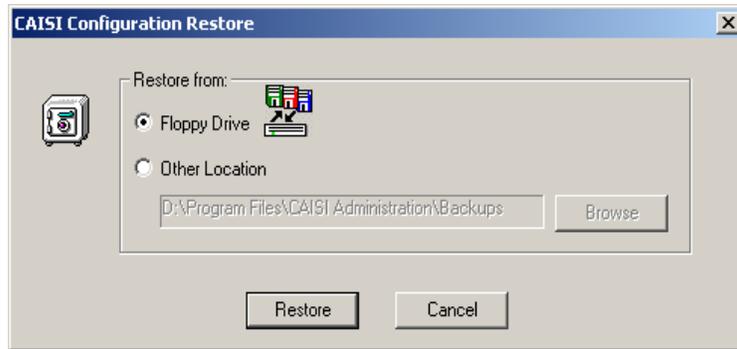


Figure 3-141 Configuration Restore Dialog Box

3. Click on the selection to tell the application where the backups are located.
4. Click on the “**Restore**” button.

If there is only one backup file, Figure 3-141 will continue to be displayed. If multiple backups exist, then the application will present a dialog listing all the available backups from which to select.

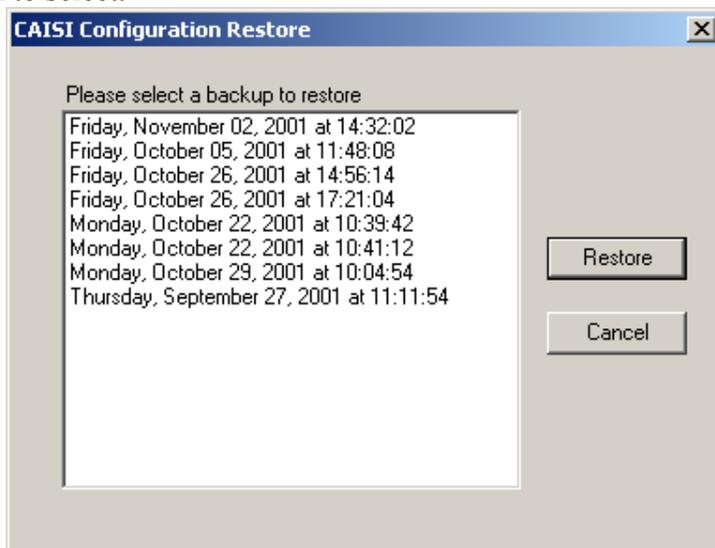


Figure 3-142 Configuration Restore Multiple Backups Dialog Box

5. Select the desired backup and click on the “**Restore**” button.

A confirmation dialog is then displayed.

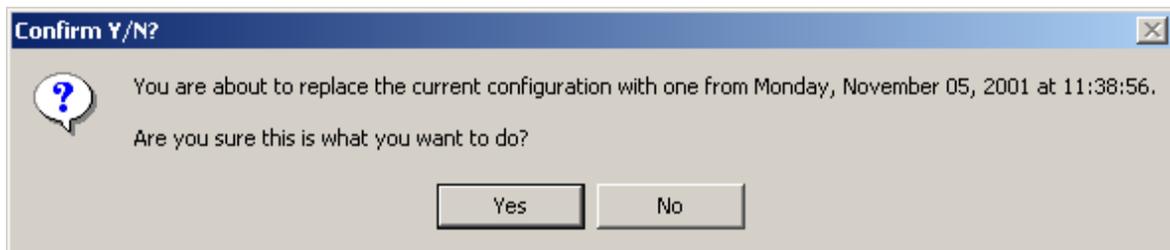


Figure 3-143 Configuration Restoration Confirmation Prompt

The “Confirm” dialog serves as a warning that the current configuration file will be replaced with a previous version.

NOTE: *Once a backup is restored, it cannot be undone.*

6. Click on the “Yes” button to restore the backup. A success dialog will then be displayed.

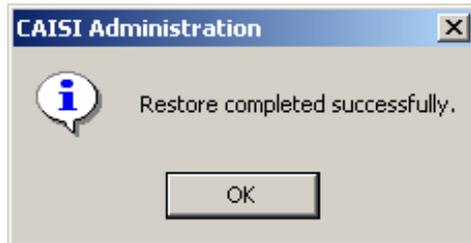


Figure 3-144 Restore Complete Dialog Box

7. Click on the “OK” button to return to the main view. At this point the main view will be updated with the configuration information that was stored in the backup.

3.8.3 Printing

This section covers the printing procedures, how to configure the printer, to use print preview and an overview of physical printing.

3.8.3.1 Print Setup

A facility to define print parameters was incorporated into the CAISI Admin application. Generally speaking, setting up a printer through the application is not an action that will normally be done, since the application will use the printing defaults as defined and setup through the operating systems.

To setup printing:

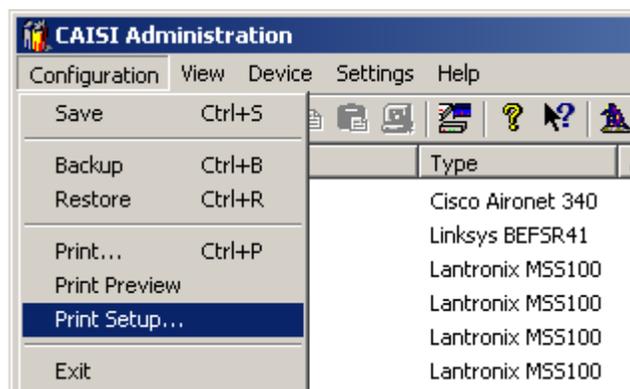


Figure 3-145 Print Setup Menu Option

1. Click on the “Configuration” main menu option.

- Click on the “**Print Setup**” sub-menu option. A standard print setup dialog will then be displayed:

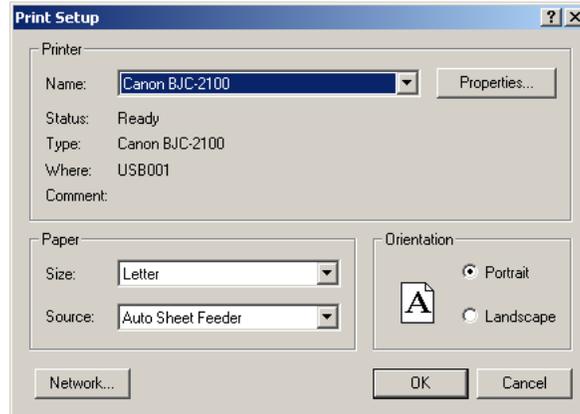


Figure 3-146 Print Setup Dialog Box

- Make the appropriate modifications to the print setup by selecting the printer to print to, adjusting the printer properties, selecting the paper size and source, or connect to another networked printer. One thing to note is that the CAISI Admin application always prints in landscape mode, so changing the orientation has no effect on printing.

NOTE: *The CAISI Admin application always prints in landscape mode.*

- Click on the “**OK**” button to save any changes for the current session. The next time data is sent to the printer during the active session, the configuration specified will be used.

NOTE: *Any changes made to the print setup are valid for the active CAISI Admin session only and are not used system wide.*

3.8.3.2 Physical Printing

Printing in the CAISI Admin is somewhat limited but can provide hardcopy output of one or more device configuration profiles. Not all configuration information is printed. All device information that is available in the main view through either the “Device View” or “Network View” options is printed in hardcopy format.

To print device information:

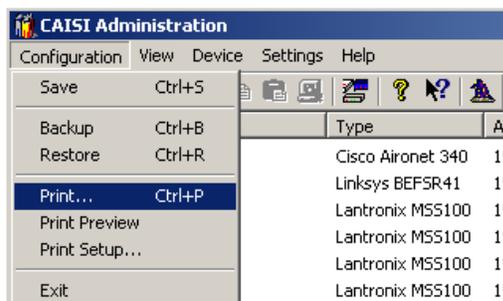


Figure 3-147 Configuration Print Main Menu Option

- Click on the “**Configuration**” main menu option.

2. Click on the “**Print**” sub-menu option or depress the Ctrl+P key combination.
3. In the print dialog that follows, make sure the proper printer has been selected.

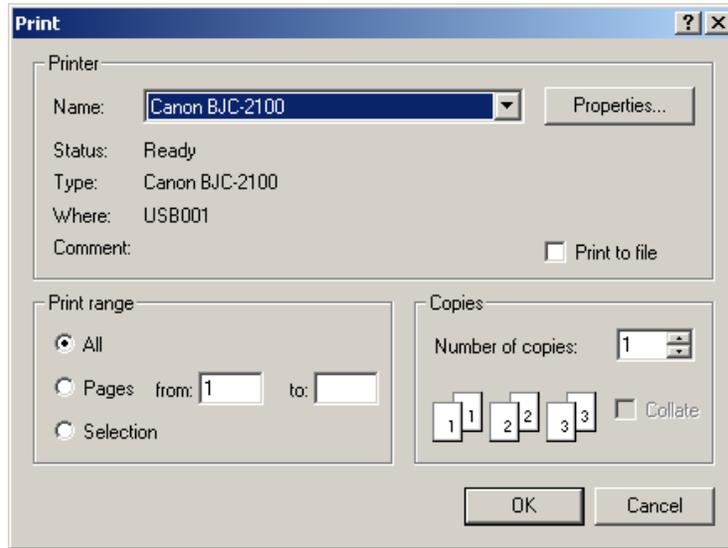


Figure 3-148 Print Dialog Box

4. Select the appropriate option in the “Print Range” box and the number of copies to print. The following table details the different print range options that are available:

Table 3-11 Print Range Options

Print option	Description
All	Selecting this option will print all defined devices.
Pages	This option allows printing one or more pages of information. To determine what devices will be included on a page, it is first necessary to select the print preview option. Please refer to the next section for details.
Selection	This option will be enabled if one or more devices were selected in the main view. When selected, this option will print only those devices that have been selected in the main view.

5. Click on the “**OK**” button. The application will then send the data to the printer. Shown below is a sample output.

CAISI Administration Devices
November 05, 2001

Device Name	Device Type	MAC Address	IP Address	Template	Location	Notes
annexchn001	Cisco Aironet 340	00-40-96-29-AC-8D	192.168.1.30	aironet-pri-root		
annexchn002	Linksys BEFSR41	00-20-78-DA-EB-92	192.168.1.1	linksys		
samlv90	Lantronix MSS100	00-80-A3-21-48-6C	192.172.19.5	derrick-mss		

Figure 3-149 Printer Output Sample

3.8.3.3 Print Preview

Print preview allows a preview of what the output will look like in “What You See Is What You Get” format before it is sent to the printer. The limitation in the preview offered by the application is that it cannot preview selected devices; rather all defined devices are displayed.

To preview the output:

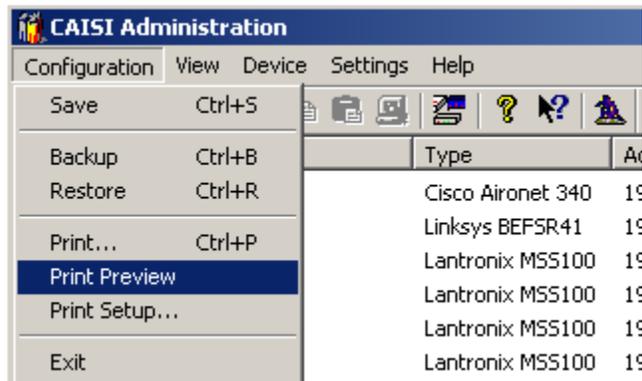


Figure 3-150 Print Preview Menu Option

1. Click on the “**Configuration**” main menu option.
2. Click on the “**Print Preview**” sub-menu option. The preview dialog will then be displayed.

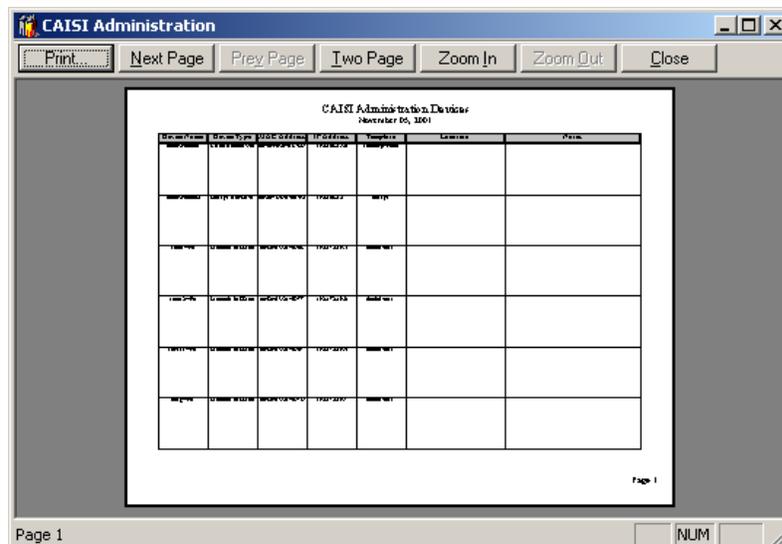


Figure 3-151 Print Preview Results

3. Click on the appropriate buttons at the top of the dialog to view each individual page, view the pages side by side, or zoom in and out.
4. Click on the “**Print**” button to send the output to the printer or
5. Click on the “**Close**” button to return to the CAISI Admin main view.

Chapter 4

ADVANCED TROUBLESHOOTING

4.1 GENERAL TROUBLESHOOTING PROCEDURES

There are basic steps in troubleshooting that you should attempt before performing advanced troubleshooting techniques. These general techniques include checking to see if the network is up, checking to see if the client next to you has communications and checking your power cables. If applying these techniques still does not solve your problem, then check your CBM or CCM. It may be down.

Troubleshooting is a three-step process.

- Identify (Realize that you have a problem and determine the symptoms.)
- Isolate (Isolate the problem - which component is causing it.)
- Correct (Fix the problem and test it to be sure it is fixed. If not, then start over.)

Perform the following troubleshooting steps in order and check to see if the problem has been resolved after each step.

Specific troubleshooting procedures are included in the following paragraphs for various CAISI components. This paragraph lists some general procedures, 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.**
 - a. If not, then verify the CBM/CCM is receiving power.
 - 1) To verify a CBM is receiving power verify the following:
 - a) 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.
 - b) Ensure the UPS is plugged into an operational external power source and the "I" (ON) side of the UPS rocker switch is pressed in.



**Figure 4-1 Troubleshooting
CBM Power Cables**

- 2) To verify the CCM is receiving power, ensure the power cord is seated firmly in the power adapter and the external power source.



**Figure 4-2 Troubleshooting
CCM Power Cables**

- b. If none of the computers connected to the CBM/CCM can communicate, then the problem probably lies in the CBM/CCM. Refer to Paragraph 4.3 for CBM troubleshooting procedures and Paragraph 4.4 for CCM troubleshooting procedures.
 - c. If the others can communicate, but one cannot, then the problem probably lies in the computer or connecting cables. Refer to Paragraph 4.1.
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, then the network is up – at least to the next closest CBM.
 4. **Reboot or Cycle Power.** Performing this procedure often 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.
 - 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 computer monitor and then press the power button on the Central Processing Unit (CPU).
 - b) Alternatively, unplug the CPU or computer power cord from the external power source.

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 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 may appear OK, but are probably not be plugged in tightly.

- 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. Sometime 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.



Figure 4-3 Troubleshooting Antenna Cables

- b. **10 BaseT (CAT-5) Ethernet cables**

- 1) Ensure the Ethernet cables are locked into their 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 connector.



Figure 4-4 Troubleshooting Ethernet Cables

- c. **10Base-2 coaxial 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.



Figure 4-5 Troubleshooting Coaxial Cables

- d. **Power cables**

- 1) Ensure power cables are firmly seated. They are held in by friction. Push it all the way in and wiggle the cable gently to make sure that it stays.



Figure 4-6 Troubleshooting Power Cables

6. Check your antenna and cable connectors.

There are three problems that sometimes occur with the antenna connectors.

- a. Water sometimes gets in the connectors and shorts 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 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 them back together.
 - 2) Insert your 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.

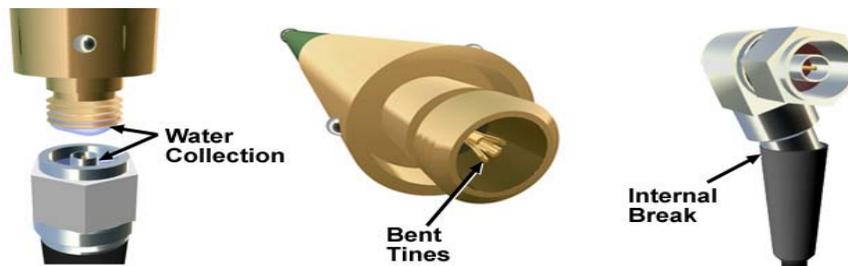


Figure 4-7 Troubleshooting Antenna & Cable Connectors

7. Check your antenna orientation.

a. Omni directional whip antennas

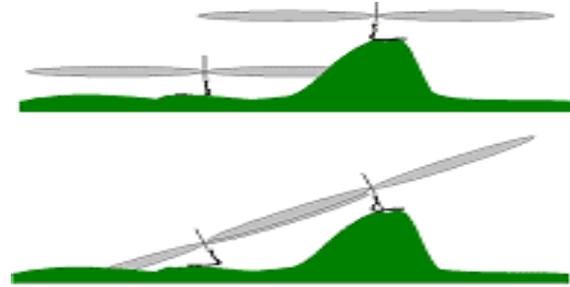
- 1) Ensure CAISI omni directional antennas are erected as vertical as possible. This is extremely important for good bandwidth and radio communications, especially for shots over a half-mile.
- 2) The omni-directional antenna is designed to provide a 360 degree radiation pattern. This antenna should be used when coverage in all directions from the antenna is required.



Figure 4-8 Troubleshooting Omni-Directional Antenna Radiation Pattern

- 3) The radio signal around the antenna resembles a flattened donut. Ensure the antenna is not tilted, if it is the donut is tilted and may be transmitting over the top of the other radio.

- 4) If there is a significant difference in elevation between the two radio sites, then you might need to deliberately tilt the antenna. Or use a panel antenna.



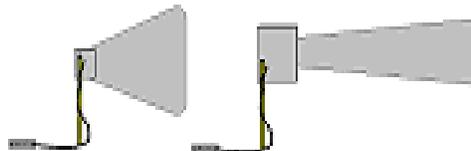
**Figure 4-9 Troubleshooting
Omni-directional Antenna Elevation
Difference**

b. Panel antennas

- 1) CAISI panel antennas are point to point antennas. When connecting two points or modules together the distance, obstructions and antenna location must be considered.
 - a) 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.
 - b) Ensure antennas are installed as high as possible and above obstructions such as trees.
 - c) Ensure antennas are aligned so that their main radiated power is directed at each other.
 - d) To verify directional antenna alignment/orientation perform the following procedures:

NOTE: *If the wired NIC is inserted in your notebook perform disconnection procedures IAW Paragraph 2.7.1 and insert your wireless NIC IAW procedures in TM 11-5895-1691-12 Paragraph 2.30.5.*

- Connect a 25' or 35' RF cable to the directional antenna and erect it IAW with procedures outlined in TM 11-5895-1691-12, Paragraphs 2.19.2, 2.18.1, 2.18.2, and 2.18.4.
- Connect the MMCX to N (F) cable from your RF antenna cable to the right port on the notebook wireless NIC.
- Use the Link Status Meter (LSM) to check signal quality.
- Select LSM from the CAISI toolbox.
- Watch the meter for about 15 seconds, and then turn the antenna a little to the left or right. Recheck the signal quality. Refer to paragraph 4.3.4 for picture.
- Continue to rotate the antenna as described above until signal quality is maximized.
- Close LSM utility and perform disconnection procedures.



**Figure 4-10 Troubleshooting
Panel Antenna Radiation Pattern**

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 not be able to associate with the distant CBM.

- a. Try reducing the data rate speed in the remote CBM/CCM by performing the following procedures:
 - 1) Ensure physical connection procedures for the module have been performed in accordance with (IAW) procedures outlined in Paragraph 2.11.1 for CBM physical connection or Paragraph 2.12.1 for CCM physical connection.
 - 2) Ensure module is receiving power. Refer to Paragraph 4.1.
 - 3) Open Internet Explorer on the notebook desktop.
 - 4) In the address toolbar at the top of Explorer, enter the IP address assigned to the multi-client radio adapter or the wireless bridge.
 - 5) Click on “GO” on the Explorer toolbar or click on “Enter” on the notebook keyboard.
 - 6) To reduce the “Data Rates (Mb/sec)” on the CBM wireless bridge perform the following:
 - a) At the “Enter Network Password” screen, enter the username and password you previously assigned the device. Click on the “OK” button.
 - b) Click on the “Setup” button near the top of the screen, or the “[Setup]” hyperlink near the bottom of the screen. The Setup Menu will appear.
 - c) From the “Express Setup” screen navigate to Network Ports, Root Radio/Bridge Radio “Hardware”.
 - d) Four fields appear below “Data Rates (Mb/sec)”. Begin reducing the “Data Rates (Mb/sec)” by changing the field next to “11.0” from basic to “no”.
 - e) Apply changes; click the “OK” button to approve.

BR350-51e531 Root Radio Hardware

Cisco 350 Series Bridge 12.01T

Map Help

Service Set ID (SSID): caisi000 more...

Allow "Broadcast" SSID to Associate?: yes no

Enable "World Mode" multi-domain operation?: yes

Data Rates (Mb/sec):

1.0 2.0 5.5 11.0

Transmit Power:

Frag. Threshold (256-2338): RTS Threshold (0-2339):

Max. RTS Retries (1-255): Max. Data Retries (1-255):

Beacon Period (19-5000 Kusec): Data Beacon Rate (DTIM):

Default Radio Channel: In Use: 1

Search for less-congested Radio Channel?: yes Restrict Searched Channels

Receive Antenna: Transmit Antenna:

If VLANs are *not* enabled, set Radio Data Encryption through the link below. If VLANs *are* enabled, Radio Data Encryption is set independently for each enabled VLAN through [VLAN Setup](#).

Radio Data Encryption (WEP)

Apply OK Cancel Restore Defaults

Figure 4-11 Troubleshooting Wireless Bridge Root Radio Hardware Screen

- f) To verify you are now associated to the remote CBM look at the lights on top of the wireless bridge, they should conform to the following:
 - The center **“Status”** LED is solid green the CBM is connected and has clients.
 - If the **“Status”** LED blinks 7/8 on and 1/8 off the CBM is connected to the root CBM but there are no CCMs connected to the wireless bridge.
 - If the **“Status”** LED blinks slowly, it is not connected to the root CBM and you need to continue to reduce the **“Data Rates (Mb/sec)”** until you are able to verify association status. Repeat procedure **d)** above by changing the next highest speed from basic to **“no”** until you are able to verify association status.
- 7) To reduce the **“Allowed bit rates in megabits/second”** on the **CCM** multi-client radio adapter perform the following:
 - a) Click on **“Write Access”**.
 - b) At the **“Enter Network Password”** screen, enter the username and password you previously assigned the device. Click on the **“OK”** button.
 - c) Click on **“Allow Config Changes”**.

- d) Select **“Radio”** from the **“Configuration”** menu.
- e) Try reducing the **“Allowed bit rates in megabits/second”** from **“1_11”** to **“1_5.5”**, **“1_2”** or even **“1”**.
- f) To verify you are now associated look at the lights on top of the multi-client radio adapter. The center **“Status”** LED will be lit solid green if you are associated to the remote CBM.

Item	Value
Service set identification	a string of at least 1 characters <input type="text" value="caisi000"/> <input type="button" value="Save"/>
Allowed bit rates in megabits/second	1_1_2 , 1_5.5 , 1_11 , 2_2_5.5 , 2_11 , 5.5 , 5.5_11 or 11
Basic bit rates in megabits/second	1_1_2 , 1_5.5 , 1_11 , 2_2_5.5 , 2_11 , 5.5 , 5.5_11 or 11
Enable world mode	<input type="checkbox"/> on or <input checked="" type="checkbox"/> off
RTS/CTS packet size threshold	a number of 2400 or less <input type="text" value="1024"/> <input type="button" value="Save"/>
Privacy configuration	
Parent node Id	our parent's network address <input type="text" value="any"/> <input type="button" value="Save"/> or any
Time to look for specified parent	<input type="checkbox"/> off or a time in seconds: <input type="text" value="off"/> <input type="button" value="Save"/>
Maximum number transmit retries	a number from 8 to 64 <input type="text" value="64"/> <input type="button" value="Save"/>
Refresh rate in 1/10 of seconds	a number from 5 to 150 <input type="text" value="100"/> <input type="button" value="Save"/>
Enable the diversity antennas	<input type="checkbox"/> on or <input checked="" type="checkbox"/> off
Transmit power level	1_5 , 15 , 30 or full
Maximum fragment size	a number from 256 to 2048 <input type="text" value="1024"/> <input type="button" value="Save"/>
Enable radio options	a password <input type="text"/> <input type="button" value="Save"/>

Figure 4-12 Troubleshooting CCM Radio Configuration Screen

- g) If you are not associated you need to continue to reduce the **“Allowed bit rates in megabits/second”** until you are able to verify association status. Repeat procedure **e)** above by reducing the value to the next highest speed until you are able to verify association status.

NOTE: *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 your 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.

- a. Ensure physical connection procedures for the module have been performed IAW procedures outlined in Paragraph 2.11.1.
- b. Ensure module is receiving power. Refer to Paragraph 4.1.
- c. Open Internet Explorer on the notebook desktop.
- d. In the address toolbar at the top of Explorer, enter the IP address assigned to the wireless bridge.
- e. Click on “GO” on the Explorer toolbar or click on “Enter” on the notebook keyboard.
- f. To check your root radio “Bridge Spacing” on the CBM wireless bridge perform the following:
 - 1) At the “Enter Network Password” screen, enter the username and password you previously assigned the device. Click on the “OK” button.
 - 2) Click on the “Setup” button near the top of the screen, or the “[Setup]” hyperlink near the bottom of the screen. The Setup Menu will appear.
 - 3) From the “Setup” screen navigate to Network Ports, Root Radio/Bridge Radio “Advanced”.
 - 4) In the “Bridge Spacing (km):” field, enter the distance of your longest shot.
 - 5) Apply changes; click on the “OK” button to approve.

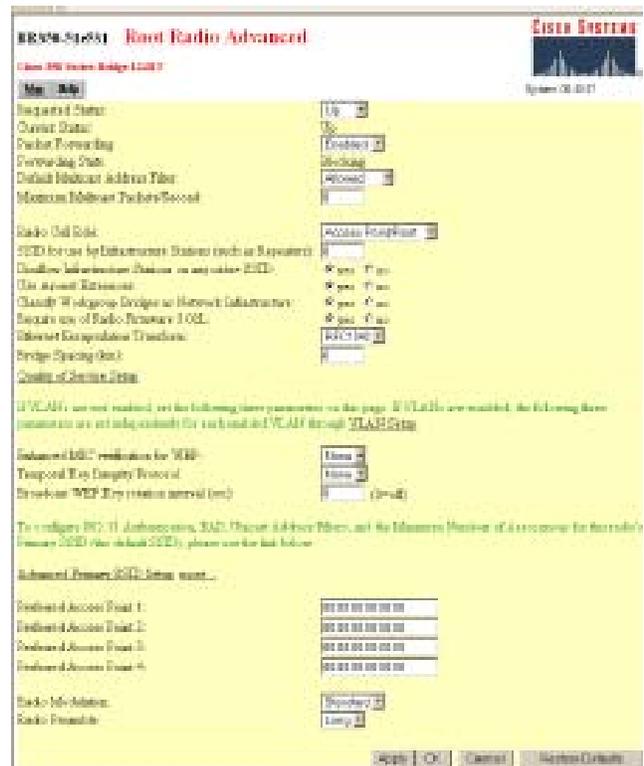


Figure 4-13 Troubleshooting Wireless Bridge Root Radio Advanced Screen

NOTE: If you have one very long shot and everything else is short, consider moving the long shot to a separate network, with its own root radio and SSID. This will make the rest of the network work much faster and improve throughput.

10. Check Your Configuration.

- a. Verify your parameters are set to their original values. Sometimes parameters were changed during some earlier troubleshooting session. If necessary, follow the configuration procedures in the preceding sections to reset them to their defaults. Then adjust them as necessary for the current deployment.
 - 1) Wireless Bridge: refer to Paragraph 2.11.2.2 or Paragraph 3.6.2.
 - 2) Encryptor: refer to Paragraph 2.11.6.
 - 3) Multi-client radio adapter: refer to Paragraph 2.12.2.2 or 3.7.2.
 - 4) LSA: refer to Paragraph 2.13.2.
 - b. Verify that parameters that were supposed to be changed to support deployment were changed.
 - c. Verify that there are no typographical errors, especially in the SSID or WEP key.
 - 1) Ensure physical connections procedures for the module have been performed. Refer to Paragraph 2.11.1 for CBM physical connection procedures or Paragraph 2.12.1 for CCM physical connection procedures.
 - 2) Ensure module is receiving power. Refer to Paragraph 4.1.
 - 3) Open Internet Explorer on the notebook desktop.
 - 4) In the address toolbar at the top of Explorer, enter the IP address assigned to the wireless bridge or the multi-client radio adapter.
 - 5) Click on “GO” on the Explorer toolbar or click on “Enter” on the notebook keyboard.
 - 6) To verify the SSID and WEP Key on the CBM wireless bridge perform the following:
 - a) At the “Enter Network Password” screen, enter the username and password you previously assigned the device. Click on the “OK” button.
 - b) From the “Summary Status” menu, select “Setup” then “Express Setup”. The “Express Setup” screen will appear.
- c) Verify the [Radio Service Set ID (SSID)] is set as required, for your network or as directed by your DOIM, S6 or CSSAMO.

- If the SSID is incorrect type the correct SSID in the [Radio Service Set ID (SSID)] field.
- Click on the “Apply” button. Click on the “OK” button to approve.

BR350-51e531 Express Setup

Cisco 350 Series Bridge 12.01T

Home Map Help

Uptime: 00:06:39

System Name: BR350-51e531

MAC Address: 00:40:96:51:e5:31

Configuration Server Protocol: None

Default IP Address: 192.168.1.3

Default IP Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

Root Radio:

Service Set ID (SSID): caisi000 more..

Role in Radio Network: Root Bridge

Optimize Radio Network For: Throughput Range Custom

Ensure Compatibility With: 2Mb/sec Clients

Security Setup

SNMP Admin. Community: root

Apply OK Cancel Restore Defaults

Figure 4-14 Troubleshooting Wireless Bridge Express Setup Screen

d) Click on the “**Back**” button to return to the “**Setup**” screen and then jump to Services, “**Security**”. From the security menu choose “**Radio Data Encryption (WEP)**”.

e) Verify the “**Key Size**” for Key 1 is set to “**128 bit**”.

f) Verify the “**Encryption Key**” is set to the key prescribed by your DOIM, S6 or CSSAMO by re-typing it in the field provided. Re-enter the key to confirm.

g) Click on the “**Apply**” button. Click on the “**OK**” button to approve.

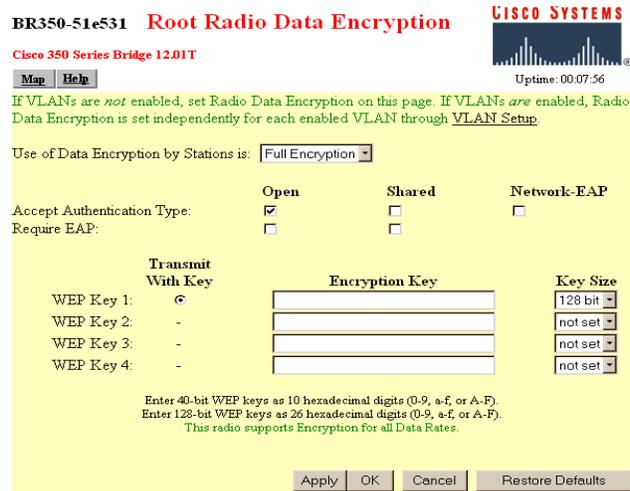


Figure 4-15 Troubleshooting Root Radio Data Encryption Screen

7) To verify the SSID and WEP key on the CCM multi-client radio adapter perform the following:

a) Click on “**Allow Config Changes**”.

b) Select “**Radio**” from the “**Configuration**” menu. The radio screen will appear.

c) Verify the SSID in the “**Service Set Identification**” field is set as required, for your network or as directed by your DOIM, S6 or CSSAMO. If the SSID is incorrect type the correct SSID in the “**Service Set Identification**” field and click the “**Save**” button.

d) Click on “**Privacy configuration**” on the radio screen and the privacy screen will appear.

e) Click on “**Set the keys**”.

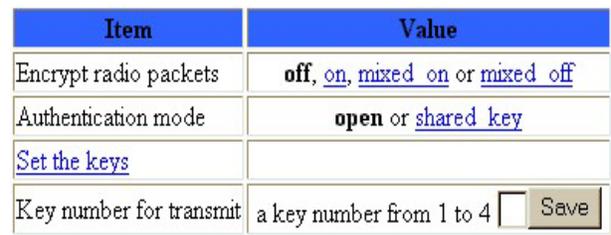
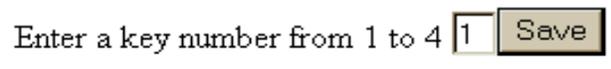


Figure 4-16 Troubleshooting CCM Radio Set the Keys Screen

f) Verify the key number is set to “1”. If not, enter “1” as the key number and click on the “**Save**” button.



[About](#)

Figure 4-17 Troubleshooting CCM Radio Set Key # Screen

- g) Verify the WEP key is set to the key prescribed by your DOIM, S6 or CSSAMO by re-typing it in the field provided. Click on the “**Save**” button.
- h) You will need to repeat this procedure to confirm the key.
- 8) Close Internet Explorer.

Enter a key of hex digits Save

[Abort](#)

Enter a key again Save

[Abort](#)

**Figure 4-18 Troubleshooting
CCM Radio Set Key Screen**

4.1.1 General Network Operation Rules

When diagnosing a problem with CAISI, the user should be aware of additional equipment on the network. Normally the addition of equipment would not cause any problems, unless the user failed to follow the rules.

Here are some rules that are most often violated and cause problems.

1. **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.

- a. The Air Fortress counts as one of the 8 clients. It communicates with other Air Fortresses 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.
- b. If a STAMIS computer has both a network card and an LSA connected, that’s two clients.
- c. If the user adds a “smart hub” or “smart switch”, that’s another client.
- d. If the user adds a dumb hub with three or four clients behind it, that’s three or four more clients.

2. **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.

- a. Every computer has to be within 100 meters of the hub.
- b. If you connect two cables together to make a long one, the total cannot exceed 100 meters.
- c. When you cascade hubs you are 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 to join the cables.

3. **The 5-4-3 Rule.** The 5-4-3 rule divides the network into two types of physical segments: populated (user) segments, and unpopulated (link) segments. User segments have users' systems connected to them. Link segments are used to connect the network's repeaters together. The rule mandates that between any two nodes on the network, there can only be a maximum of **five** segments, connected through **four** repeaters, or *concentrators*, and only **three** of the five segments may contain user connections.

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.

In CAISI, User segments include your connection, the gateway connection and the connection in the CBMs where the twisted pair hubs are joined by coaxial cable that could also contain users.

Symptoms: The network will see excessive collisions, outages, or slow communications.

- a. Ensure there are no more than two additional hubs connected to any CBM/CCM refer to the example outlined in Figure 4-19.
- b. Remove all power from the unit. Unplug power cables and disconnect them from the unit.

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.

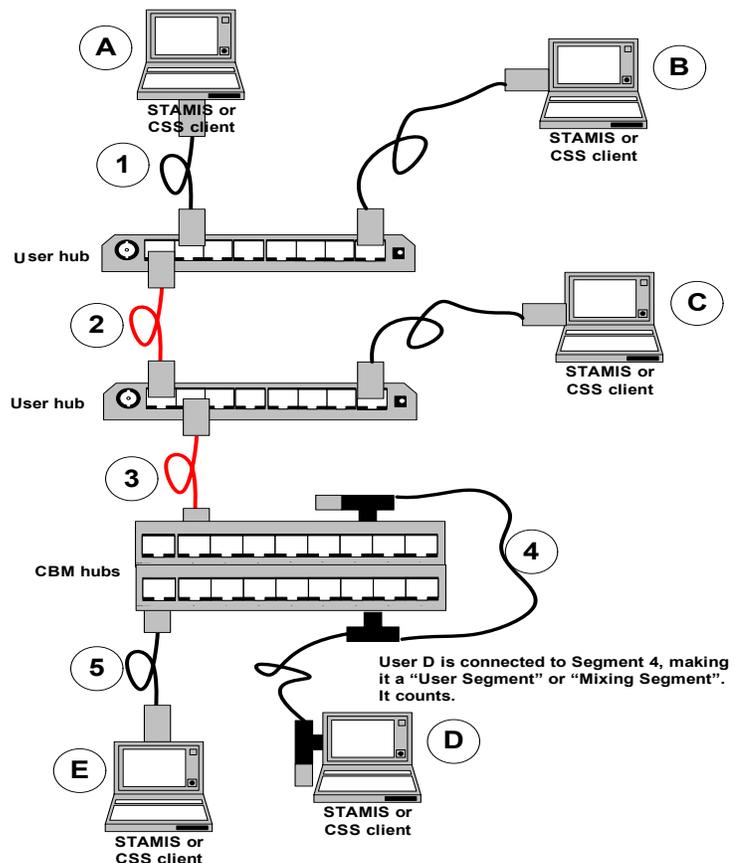


Figure 4-19 Troubleshooting Example 5-4-3 Rule

4. **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.

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.

- a. Commercial cables are acceptable.
- b. If you make your own cables ensure you use the correct pairs. To make a good straight through or crossover cable perform the following procedures:

NOTE: A good CAT-5 termination provides a proper wire crimp, a wire insulation strain relief crimp and a cable strain relief crimp. Do not unwind the wires more than necessary; maintaining the twists as far as possible is extremely important. Do not however, let this stop you from inserting the wires as far as possible.

- 1) Strip the cable’s jacket back one full inch.
- 2) Untwist the wires back to within 1/8" of the jacket.
- 3) Arrange the wires in the order in which you want to crimp them. Most cables use the 568B standard on both ends for straight cable but you can use the 568A as well. If you mix the standards you get a properly configured crossover cable.
 - a) For standard straight-through cables, wires 1 and 2 (orange-white and orange) must be connected to pins 1 and 2. Wires 3 and 4 (green-white and green) must be connected to pins 3 and 6.
 - b) 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.

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 4-20 Troubleshooting Cable Standards

- 4) 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.
 - 5) 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.
 - 6) Stuff the wires into the connector, making sure the wires stay lined up.
 - 7) 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.
 - 8) 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! All of this is very dependant on the tools you are using, the connectors you are using, and the cable you are using.
5. **The Uplink-Is-Not-An-Extra-Port Rule.** Many devices, such as the hubs in the CBMs and CCMs 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.

- a. The hubs in the CBMs 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.



**Figure 4-21 Troubleshooting
Hub Uplink Port**

- b. 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."
6. **The You're-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 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.

- a. 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.
- b. 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 too should be used for everything except STAMIS computers that require static addresses.

4.2 TROUBLESHOOTING THE SSR ACCESSORY KIT COMPONENTS

The SSR Accessory Kit includes many of the same components issued with the CBM/CCM, however it also contains some unique components.

Troubleshooting for the wireless bridge, multi-client radio adapter, encryptors, DSL Bridge, hubs, UPS, antennas, and cables are identical to the procedures for troubleshooting those components in the CBM/CCM. Refer to Paragraphs 4.3 *Troubleshooting the CBM* and 4.4 *Troubleshooting the CCM*, for component specific troubleshooting procedures.

This paragraph contains the procedures for troubleshooting the SSR notebook, the router and the 10BaseT Transceiver.

4.2.1 Troubleshooting the SSR Notebook

4.2.1.1 Troubleshooting the SSR Notebook Software

The SSR notebook is a standard personal computer, with the Windows 2000 operating system and the application software and utilities listed in Appendix A.



Figure 4-22 Troubleshooting SSR Notebook

If you have problems with the notebook or applications and cannot resolve them, perform the following procedures:

1. Check and adjust the CMOS settings by setting all the BIOS settings back to their original values, as listed in the "Notebook System Setup (BIOS Settings)" Paragraph 2.3.

2. Reload the hard disk image.
 - a. Reload the hard drive from CD, as instructed in the Paragraph 2.4.
 - b. If you cannot boot from hard disk, reload the CAISI Z13-4B-xx baseline from CD. Any accounts you have created will be lost and will have to be rebuilt.
 - c. If the baseline will not load, you have a hardware problem.
3. Replace hardware components by sending the notebook to the Forward Repair Activity (FRA) for replacement of components or the notebook.

If the computer boots properly, but you cannot log on because you forgot the password get the password envelope from the security officer. If that fails, reload from CD.

4. 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 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 computer will not soft boot, turn it off, by holding the OFF button for up to 10 seconds, wait a few seconds and turn it back on.
5. If any of the CAISI Toolbox utilities do not appear to be 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).*

4.2.1.2 Troubleshooting the SSR Notebook Utilities

This paragraph addresses communications problems you might encounter when using the notebook utilities. More information on these utilities is in Appendix A.

1. **Hyperterm.** Hyperterm is used in configuring and troubleshooting CAISI components. There are two Hyperterm shortcuts on the CAISI Toolbox menu. Select the appropriate one for the item you are configuring.

- a. If you connect and hit the Enter key a couple of times and nothing happens, check the cable. If you have the wrong cable it will not work.
 - 1) The wireless bridges require a 9-pin straight-through male-to-female cable. The cable issued with the SSR Accessory Kit is blue.
 - 2) The encryptors require a 9-pin null-modem female-to-female cable. The cable issued with the SSR Accessory Kit is beige.
 - 3) The LSA devices require a 9-to-25-pin null-modem cable. If you were issued LSA devices as part of your CAISI, there is a cable with each one and an additional cable in the SSR Accessory Kit.
 - b. If you have another application open that uses the serial port, such as BLAST, Hyperterm will not work. Close the other application, close Hyperterm, and reopen Hyperterm.
 - c. If you still get nothing, check your Hyperterm configuration to make sure that it is set to use COM1. It may have been changed somewhere along the line to another port or even TCP/IP.
 - d. If you connect and get gibberish, check the speed. The wireless bridges, routers, and LSA devices require 9600-baud connections. The encryptors require 38400. Close Hyperterm and reopen it, selecting the appropriate icon.
 - e. If you still get gibberish, check the settings. They may have been changed somewhere along the line. To change the settings, click on the “disconnect” icon, click on “**Properties**” make the change, save the change, then press the <Enter> key a couple of times to connect and get a login prompt.
2. **Ping.** An Internet utility wherein a computer, given another “host” computer’s Internet Protocol (IP) address, sends an “echo request” packet to the host across the network. If the host can be reached, it is required to send an echo reply. This is known as “pinging” and can quickly let you know if a host computer can be reached via TCP/IP.

The ping utility is extremely useful in determining the availability and quality of TCP/IP connections. To ping another device perform the following procedures:

- a. At the bottom of the notebook screen, click on the “**Command prompt**” icon. The command prompt screen will appear.
- b. Type the command “**ping xxx.xxx.xxx.xxx**”, where the x’s are the IP address of the distant host and press the <Enter> key. Example “ping 192.168.1.150”.

Sometimes the utility fails for no apparent reason when you know communications are up and good. This is often due to an IP address having just been changed somewhere in the system.

When you communicate by TCP/IP, the TCP/IP packet, addressed to an IP address, is actually wrapped inside an Ethernet packet that is addressed to a MAC address. The computer gets the MAC address by broadcasting an “arp” packet over the network asking “hey, who has this IP address?” The target computer answers with his MAC address and your computer caches that information in memory. From that point on,

no additional arp is required. But if an IP address changes, your MAC-to-IP address mapping in memory is wrong and you will not be able to communicate.

- c. If you are running a continuous ping, stop it. If you have a web browser open, close it. Then enter the command “**arp -d**” at a DOS prompt. This will clear the arp table. Now ping again and a new arp will be broadcast and you will be able to connect.
3. **Web Browser.** If you can ping a server or device, but cannot connect with your web browser, it may be because of a configuration parameter in the router, because of information cached in the browser, or because of security settings.
- a. If you have had the web browser open for a while, close it. Then open a new one. A lot of information, including connection status and usernames and passwords, is cached by the web browser. This information may be keeping you from connecting.
 - b. If your security settings in the web browser have been changed, you might not be able to connect. Open the browser. Go to **Tools/ Internet Options/Security** and set all of the zones back to defaults.
 - c. Check the server or device to which you are trying to connect.
 - 1) Connect through the serial port and check the configuration.
 - 2) Is there a setting that is keeping you from connecting? Radios, for instance, may have “non-console browsing” disabled, or have a management IP specified so that one can only connect from the specified address.
 - 3) The routers, similarly, may have a management address specified. If you cannot connect through the serial port, reset the device and reconfigure it.

4.2.1.3 Troubleshooting the SSR Notebook Wired NIC or Built-In NIC

Problems with the wired/built-in NIC are usually because of a bad cable, speed synchronization problems, network configuration problems, or having the encryption client turned on. Check the following:



Figure 4-23 Troubleshooting Wired NIC

1. **If you do not have a link light, or if communications are intermittent or slow.**
 - a. Verify the ends of the Ethernet cable are firmly seated in both the device and Wired/Built-In NIC ports.
 - b. Remove another cable from the SSR Accessory Kit and connect it into the device and Wired/Built-In NIC. Check for link lights.

- c. Verify the NIC card configuration parameters, speed and duplex should be set to auto.
 - 1) Right click on “**My Network Places**”, select “**Properties**”.
 - 2) Right click on “**CardBus II 10_100**” or “**Built-In Ethernet**” network card icon, select “**Properties**”.
 - 3) On the “General” tab, press the “**Configure**” button.
 - 4) Select the “**Advanced**” tab.

(Wired NIC)

- a) Under the “Property” field, select “**Line Configuration**”.
- b) Ensure the “Value” field is set to “**Auto Detect**”. Click on the “**OK**” button.

(Built-In NIC)

- a) Under the “Property” field, select “**Media Type**”.
- b) Ensure the “Value” field is set to “**Auto Config**”. Click on the “**OK**” button.

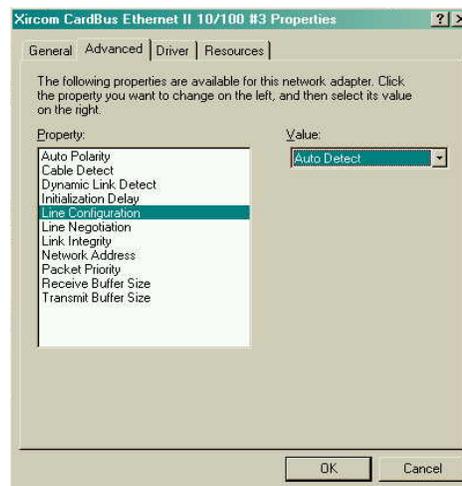


Figure 4-24 Troubleshooting Xircom Advanced Tab

- d. Refresh the NIC settings: Wired NIC – remove it, insert again.
Built-In NIC – disable, enable. (Right-click on NIC Icon).
 - e. Reboot the notebook. If that fails, reboot the devices to which you are connected.
2. **If you do have a link light, but cannot ping or communicate with any other host or network device.**
 - a. Verify the IP address, subnet mask, gateway, and DNS are set to values appropriate for the network.
 - 1) Right-click on “**My Network Places**”, select “**Properties**”.
 - 2) Right-click on the “**CardBus II 10_100**” or “**Built-In Ethernet**” network card icon, select “**Properties**”.
 - 3) Select “**Internet Protocol (TCP/IP)**”.
 - 4) Click on the “**Properties**” button.
 - 5) Select “**Use the following IP address**”, verify the IP address, subnet mask, gateway, and DNS values. Click on the “**OK**” button.
 - b. Verify the Air Fortress remote client is turned off.
 - 1) Look in the system tray for the small padlock icon.
 - 2) Double-click on the padlock icon and the Air Fortress Client screen will appear.
 - 3) On the “General” tab, verify “**Encryption/Security**” is set to “**Off**”. If not, select the “**Off**” option and then press the minimize icon on the Air Fortress Client menu screen.

4.2.1.4 Troubleshooting the SSR Notebook Wireless NIC

Problems with a wireless NIC are usually because of antenna problems, wireless configuration problems, network configuration problems, or remote encryption client configuration problems.

1. **If your radio is not associated, verify the following:**

- a. Verify the rabbit-ears antenna cable connectors are seated firmly into the holes on the end of the card.
- b. 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 4-25 Troubleshooting SSR Notebook with Rabbit Ears Antenna

- c. Inspect the RF cable, connectors, and antenna for damages and ensure the antenna is erected IAW procedures outlined in TM 11-5895-1691-12, Paragraph 2.17.4 for CBM component troubleshooting and Paragraph 2.20.4 for CCM component troubleshooting.
- d. Ensure that the Service Set Identifier (SSID), Wired Equivalent Privacy (WEP), and Authentication, are appropriate for the radio network.
 - 1) **Verify SSID.**
 - a) At the bottom of the notebook screen, click on the ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear. Select the "Aironet Client Utility" (ACU) utility to verify the wireless NIC SSID.
 - b) Select "Commands".
 - c) Select "Edit Properties".
 - d) Verify the SSID in the "SSID1" field is as required by your network. Click on the "OK" button.
 - e) Close the ACU tool.
 - 2) **Verify WEP key.**
 - a) Select the "Aironet Client Encryption Manager" (CEM) utility to verify the key for the wireless NIC.
 - b) Enter the default password, "Cisco", click on the "OK" button.
 - c) Select "Commands".
 - d) Select "Enter WEP key".
 - e) In the "WEP Key 1" field, enter the 26-character WEP key provided by your DOIM, CSS S6 or CSSAMO.
 - f) Click on the "OK" button. Close the CEM tool.

- 3) **Verify Authentication.**
 - a) Ensure physical connection procedures for the module have been performed IAW procedures outlined in Paragraph 2.11.1.
 - b) Ensure module is receiving power. Refer to Paragraph 4.1.
 - c) Open Internet Explorer on the notebook desktop.
 - d) In the address toolbar at the top of Explorer, enter the IP address assigned to the wireless bridge.
 - e) Click on “**GO**” on the Explorer toolbar or click on “**Enter**” on the notebook keyboard.
 - f) To check your radio “**Authentication**” on the CBM wireless bridge, perform the following:
 - At the “**Enter Network Password**” screen, enter the username and password you previously assigned the device. Click on the “**OK**” button.
 - Click on the “**Setup**” button near the top of the screen, or the “[Setup]” hyperlink near the bottom of the screen. The Setup Menu will appear.
 - From the “Setup” screen navigate to “Services” then “**Security**”.
 - Select “**Radio Data Encryption (WEP)**” on the “Security Setup” screen.
 - Verify “**Accept Authentication Type**” is set to “**Open**”. If necessary, apply changes and click on “**OK**” to approve.
 - Close Internet Explorer.

2. **If you are associated, but cannot ping or communicate with any other host or network device.**
 - a. Ensure that the IP address, subnet mask, gateway, and DNS are appropriate to network.
 - 1) Right-click on “**My Network Places**”, select “**Properties**”.
 - 2) Right-click on the “**Cisco**” network card icon, select “**Properties**”.
 - 3) Select “**Internet Protocol (TCP/IP)**”.
 - 4) Click on the “**Properties**” button.
 - 5) Select “**Use the following IP address**”, verify the IP address, subnet mask, gateway, and DNS values. Click on the “**OK**” button.
 - b. Ensure that the Air Fortress remote client AccessID is appropriate for the radio network.
 - 1) Ensure physical connection procedures for the module have been performed IAW procedures outlined in Paragraph 2.11.1.
 - 2) Ensure module is receiving power. Refer to Paragraph 4.1.
 - 3) At the bottom of the SSR notebook screen, double-click on the padlock icon and the Air Fortress Client screen will appear.
 - a) Click on the “**Utilities**” menu and select “**Update Access ID**”.
 - b) A dialog box will appear asking for your administrator’s password. Enter the CAISI default password “**fortress**” or the password you previously entered as prescribed by your DOIM, S6 or CSSAMO. Click on the “**OK**” button.
 - c) At the AirFortress Client “**Logon successful**”, prompt, click on the “**OK**” button.

- d) The “Change Access ID” menu will appear.
- e) Enter your current Access ID in the “**Current**” field.
- f) Enter your network’s pre-shared Access ID as prescribed by your DOIM, S6 or CSSAMO in both the “**New**” and “**Confirm**” fields. Click on the “**OK**” button.

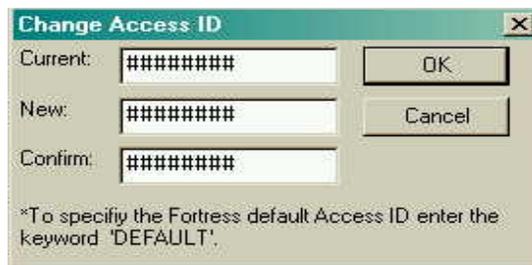


Figure 4-26 Troubleshooting Change Access ID Menu

- g) You will get a message saying that the AccessID was set and instructing you to please reset the device. Click on the “**OK**” button.
- h) Click on the “**Utilities**” menu and select “**Reset Connections**” then “**All Entries**”.



Figure 4-27 Troubleshooting Air Fortress Client Utilities Menu

- i) Close the AirFortress Client Utility by clicking on the minimize icon at the top of the AirFortress screen.

- c. Verify that the Air Fortress remote client is turned on if communicating with trusted network, and turned off if troubleshooting radios.
 - 1) Look in the system tray for the small padlock icon.
 - a) When you are in non-secure mode, it will be unlocked. When you are in secure mode, the icon will be a locked padlock.
 - 2) To turn Encryption/Security “**On**” or “**Off**”, perform the following procedures:
 - a) Double-click on the padlock icon and the Air Fortress Client screen with the “General” tab selected, will appear.
 - b) Select “**On**” or “**Off**” in the “Encryption/Security” section of the “General” tab of the Air Fortress Client screen. Selecting “On” will change your computer to secure mode, selecting “Off” will change your computer to non-secure mode.

NOTE: *The icon in your system tray will change from locked to unlocked and vice versa to indicate whether you are operating in secure or non-secure mode.*

If you can’t find anything wrong and have already cycled power, reset and reconfigure the notebook or application. If that fails, reload the notebook from CD, then reconfigure it to match your network. If all else fails, replace the notebook.

4.2.2 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 can not connect, you may not be able connect, or the router may just need rebooting.



Figure 4-28 Troubleshooting Router

Under Normal Conditions you should first, verify the Router has operational status by checking the Light Emitting Diode (LED).

4.2.2.1 Troubleshooting Router Light Emitting Diodes (LEDs)

CAISI router LEDs should be as follows:

1. LAN Indicators:
 - a. Power: Green. The Power LED illuminates when the Router is powered on.
 - b. Link/Act: Green. The Link/Act LED serves two purposes.
 - 1) If this LED is continuously illuminated, the Router is successfully connected to a device (STAMIS) through the corresponding port (1-8).
 - 2) If the LED is flickering, the Router is actively sending or receiving data over that port.
 - c. Full/COL: Green. The Full/Col LED also serves two purposes.
 - 1) If this LED is continuously illuminated, 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.
 - d. 100: Orange. The 100 LED illuminates when a successful 100Mbps connection is made through the corresponding port.
2. The WAN indicators:
 - a. Link: Green. The Link LED illuminates when a successful connection is made between the Router and your public network.
 - b. Act: Green. The Act LED flickers when the Router is sending or receiving data over the WAN Network.
 - c. Diag: Orange. The Diag LED illuminates when the Router goes through its self-diagnosis mode during boot-up. It will turn off upon successful completion of the diagnostic.

NOTE: *If this LED stays on for an abnormally long period of time, the device is not working properly and the unit may need to be replaced.*



Figure 4-29 Troubleshooting Router LEDs

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” (100 Base-TX) LEDs may be lit or not, depending on the equipment you connect.

4.2.2.2 Troubleshooting the Router Configuration

1. Briefly pressing the reset button will refresh the router’s connections, possibly clearing any jammed links.
 - a. Insert the CAISI reset tool into the reset buttonhole and hold for 2-3 seconds.



Figure 4-30 CAISI Reset Tool

2. **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, then you must set a new one.
 - a. Ensure router physical connection procedures have been performed IAW procedures outlined in Paragraph 2.10.1.
 - b. Ensure router and SSR notebook are receiving power. Refer to Paragraph 2.10.1.
 - c. To assign a new password to the router you will need to reset the router to its default configuration so that you can connect.

Version 1

- a. Insert the tip of the reset tool into the reset buttonhole on the back of the router and hold for 15 seconds.
- b. During this process the "**Diag**" light will light up, the "**Link**" light will light up momentarily, then both lights will go off, and the router will now be reset.
- c. If the green “**Link**” light does not flash, try again.

Version 2

- a. Insert the tip of the reset tool into the reset buttonhole on the back of the router and observe the following:
- b. The "**Diag**" light will light up red, all of the LEDs on the “100” level will blink twice, then all of the LEDs on the “Full/Col” level will blink twice, then all of the LEDs on the “Link/Act” level will blink twice. The “Diag” LED will then go out. The router will now be reset.
- c. If the “**Diag**” light does not go out, try again.

- d. Logon to the SSR notebook computer.
- e. Connect to the router and make sure that the configuration of the clients matches the configuration of the router.
 - 1) Open Internet Explorer.
 - 2) Enter the router's private address, **192.168.1.1** in your browser address bar and press the **<Enter>** key.
 - 3) The "**Enter Network Password**" screen will appear. You may leave the "User Name" field blank, however you must enter the password you previously assigned the device in the "Password" field. Click on the "**OK**" button.
 - 4) Click on the "**Password**" tab at the top of the screen.
 - a) Enter your new password. Re-enter your new password to confirm.
 - b) Click on the "**Apply**" button.
 - 5) Click on "**Continue**" on the "Settings are successful" screen.

Note: *If you reset and reconfigure the router, be sure to change the password. You do not want to leave the password set to the default value. Also, 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.*

3. If your clients cannot connect:

Clients on the private side of the router can only connect to each other and to servers on the public side.

- a. If one client cannot connect, check to see if others can. If so, then check the network card and configuration of the client that cannot communicate.
- b. If none of the clients can communicate, check the router configuration.
 - 1) Ensure router physical connection procedures have been performed IAW procedures outlined in Paragraph 2.10.1.
 - 2) Ensure router and SSR notebook are receiving power. Refer to Paragraph 2.10.1.
 - 3) Logon to the SSR notebook computer.
 - 4) Connect to the router and make sure that the configuration of the clients matches the configuration of the router.
 - a) Open Internet Explorer.
 - b) Enter the router's private address in your browser address bar and press the **<Enter>** key.
 - c) The "**Enter Network Password**" screen will appear. You may leave the "User Name" field blank, however you must enter the password you previously assigned the device in the "Password" field. Click on "**OK**".

d) On the Main Menu Setup tab:

- Verify the domain name, IP address and subnet mask are as required by your network.
- Verify the parameters for the WAN (the IP address, subnet mask, default gateway, and DNS server) are as required by your network.

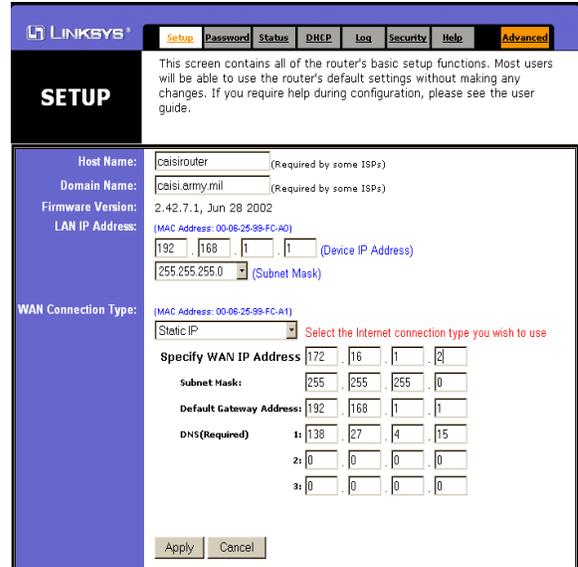


Figure 4-31 Troubleshooting Router Setup Tab

4. **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.
- b. If you are connected to the private side, you can only connect using the router’s private address.
- c. 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.

NOTE: *For security reasons, remote management is turned off on the Public side and should not be left on.*

5. If you still cannot connect to the router, try rebooting it. Deprive the router of power for four seconds. Unplug the router power cable. Then plug it back in.
6. To reset the router, follow procedures in step 2 above.
 - a. This will completely erase the current configuration, including the password.
 - b. Once you reset the router, you can connect to it from the private side and reconfigure it. The default password is “Admin” and the default IP address is “192.168.1.1” on the private segment.

NOTE: *After resetting the router, you will need to completely reconfigure the router. It will now be in the default state, as if it were brand new.*

7. If you still cannot connect to the router, you must replace it.

4.2.3 Troubleshooting the 10BaseT Transceiver

The SSR Accessory Kit contains a transceiver primarily for connecting to the INE or 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 auxiliary unit interface (AUI) port.

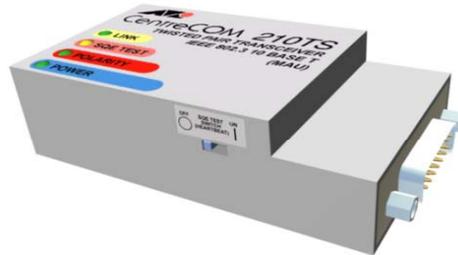


Figure 4-32 Troubleshooting 10BaseT Transceiver

During normal operations the CAISI transceiver LEDs should be as follows:

1. The “Power”, “Polarity” and “Link” LEDs should be lit (green).
 - a. The “Power” LED indicates that the transceiver is getting power (through the AUI port). If the transceiver has no lights, check the NES or connected equipment to make sure that it is on.
 - b. The Link LED blinks to indicate traffic.
2. The “SQE Test” LED should not be on.
3. If all indications are normal – you have all the right lights – but your clients cannot connect:
 - a. Check your cables. Sometimes the act of checking the cables (unplugging and inspecting each end and testing the cable) fixes the problem, because it makes the devices renegotiate their connection speeds when the cable is plugged back in.
 - b. Cycle power (unplug the transceiver from the AUI port for about ten seconds, then plug it back in).
 - c. Check the “SQE Test” switch. It should be all the way to the left inside the slot.
 - d. Cycle power or reboot (as appropriate) the item into which the Ethernet cable is connected (to force it to renegotiate its connection speed).
 - e. If you still have a problem, replace the transceiver.
4. If you still have a problem, replace the transceiver.

4.3 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. The procedures and rules in the preceding paragraphs will resolve most problems with the CBM. 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.

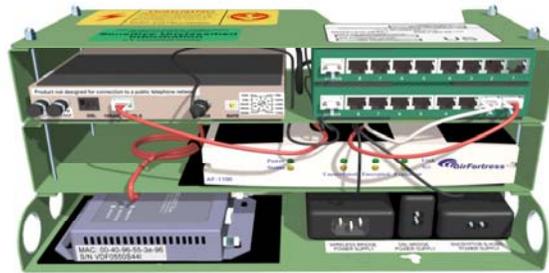


Figure 4-33 Troubleshooting CBM

4.3.1 CBM General Troubleshooting Procedures

1. Checked your cables IAW procedures outlined in 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:
 - 1) There are two LEDs built in to the top of the Ethernet port.
 - a) The right one should be solid green, to indicate the link to the encryptor.
 - b) The left one will flash to indicate traffic.



Figure 4-34 Troubleshooting Wireless Bridge Ethernet Port

- 2) The three lights on the top of the bridge should behave as follows:
 - a) 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, then go out. The center will then resume blinking and the activity lights will then begin to flicker.

3) Once the bridge is finished booting (The whole process takes about a three and a half minutes), the lights on 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.



Figure 4-35 Troubleshooting Wireless Bridge LEDs

b) The top LED “**Ethernet traffic**” represents data flowing on the Ethernet side of the bridge which hooks to the 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.

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.

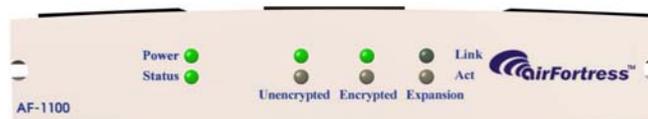


Figure 4-36 Troubleshooting Encryptor LEDs

b) The bottom “**Encrypted**” and “**Unencrypted**” Activity lights will flicker amber to indicate passing traffic.

c. DSL Bridge.

- 1) When the DSL Bridge is first powered on the lights should conform to the following:
 - a) The “**POWER**” light comes on and the “**SYNC**” light blinks twice.
 - b) 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.
 - c) 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.
 - d) 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 4-37 Troubleshooting 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.*

d. Hubs.

- 1) 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.
- 2) Port lights flicker to indicate outgoing traffic.

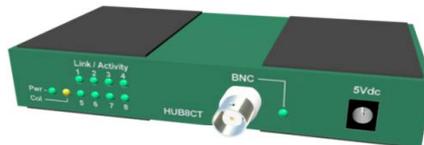


Figure 4-38 Troubleshooting Hub LEDs

4.3.2 Troubleshooting CBM Hubs

NOTE: The following procedures assume that you have already followed the general troubleshooting procedures outlined in Paragraph 4.1.

1. During normal operations the CBM hub lights should be as follows:
 - a. The “**Pwr**” light should be lit on both hubs to indicate the hubs are receiving power.
 - 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 backs of the hubs are seated properly. They sometimes vibrate loose.
 - b. The **Link/Activity** LEDs.
 - 1) 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.
 - 2) 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.
 - 3) 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.*

2. 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.
3. 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, which are also connected to the bottom hub, then only the top hub BNC light blinks.

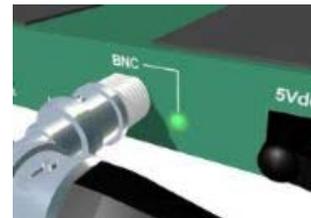


Figure 4-39 Troubleshooting Hub BNC Light

- 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.)

4. 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, 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.
5. If the hubs check out, but a connected computer doesn’t get a link light or cannot communicate, check the Ethernet cable from the computer to the hub.
6. 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.

4.3.3 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:
 - 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.
 - 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.
 - 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.
- d. **If you are not associated and you know the network is up**, either you do not have the right WEP key, or your radio is not reaching the next bridge in line.
- 1) Ensure physical connection procedures for the module have been performed IAW procedures outlined in Paragraph 2.11.1.
 - 2) Ensure module is receiving power. Refer to Paragraph 4.1.
 - 3) Ensure SSR notebook is receiving power.
 - 4) Ensure the AirFortress remote client padlock icon is unlocked and “Encryption/Security is turned **“Off”** since you are going to troubleshoot the wireless bridge using the wired NIC or built-in NIC.
 - 5) Open Internet Explorer on the SSR notebook desktop.
 - 6) In the address toolbar at the top of Explorer, enter the IP address assigned to the wireless bridge.
 - 7) Click on **“GO”** on the Explorer toolbar or click on **“Enter”** on the SSR notebook keyboard.
 - 8) At the **“Enter Network Password”** screen, enter the username and password you previously assigned the device. Click on the **“OK”** button.
 - a) Verify the SSID and WEP key:
 - From the “Summary Status” menu select **“Setup”** then **“Express Setup.”** The “Express Setup” screen will appear.
 - Verify the [Radio Service Set ID (SSID)] is set as required, for your network or as directed by your DOIM, S6 or CSSAMO. If the SSID is incorrect type the correct SSID in the [Radio Service Set ID (SSID)] field. Click on the **“Apply”** button. Click on the **“OK”** button to approve.
 - Click on the “Back” button to return to the “Setup” screen and then jump to Services, **“Security”**. From the security menu choose **“Radio Data Encryption (WEP)”**.
 - Verify the “Key Size” for key 1 is set to **“128 bit.”**
 - Verify the “Encryption Key” is set to the key prescribed by your DOIM, S6 or CSSAMO by re-typing it in the field provided. Re-enter the key to confirm.
 - Click on the **“Apply”** button. Click on the **“OK”** button to approve.

- b) Verify the following parameters:
 - From the “Summary Status” menu select “**Setup**”.
 - From the “**Setup**” screen navigate to Network Ports, Root Radio/Bridge Radio “**Hardware**”.
 - Four fields appear below “**Data Rates (Mb/sec)**” verify all four fields are set to “**basic**”. If not set all four fields to “basic,” apply changes; click the “**OK**” button to approve.
 - Ensure “**Transmit Power**” is set it to “**100mW**” or the maximum legal power for the area in which you are operating).
 - Ensure “**Search for Less Congested Radio Channel**” is set to “**yes**”.
 - Ensure both the “**Receive Antenna**” and “**Transmit Antenna**” values are set to “**Right**”.
 - If changes are made, apply changes; click on the “**OK**” button to approve.
 - Close Internet Explorer.
- c) If you still are not associated, check the antenna system IAW procedures outlined in Paragraph 4.3.4.
- e. **If you are associated and indications are normal**, connect your SSR notebook NIC to the hub in the CBM and attempt to pass traffic to a distant host that you know is up. Watch the lights.
 - 1) 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.
 - 2) 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.
 - 3) On the wireless bridge,
 - a) The amber activity light on the Ethernet port should flicker in time with the light on the encryptor.
 - b) 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.
 - 4) 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).
 - 5) 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) Verify you have the correct SSID and WEP key for the network.
 - a) Insert the wireless NIC in your SSR notebook.
 - Ensure the rabbit ears antenna cable connectors are seated firmly into the holes on the end of the card.
 - 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.
 - b) Open Internet Explorer on the notebook desktop.
 - c) In the address toolbar at the top of Explorer, enter the IP address assigned to the wireless bridge.
 - d) Click **“GO”** on the Explorer toolbar or Click **“Enter”** on the notebook keyboard.
 - e) At the **“Enter Network Password”** screen, enter the username and password you previously assigned the device. Click on the **“OK”** button.
 - f) To verify the SSID and WEP key perform the following:
 - From the “Summary Status” menu select “Setup” then **“Express Setup”**. The “Express Setup” screen will appear.
 - Verify the [Radio Service Set ID (SSID)] is set as required, for your network or as directed by your DOIM, S6 or CSSAMO. If the SSID is incorrect type the correct SSID in the [Radio Service Set ID (SSID)] field. Click on the **“Apply”** button. Click on the **“OK”** button to approve.
 - Click on the “Back” button to return to the “Setup” screen and then jump to Services, **“Security”**. From the security menu choose **“Radio Data Encryption (WEP)”**.
 - Verify the “Key Size” for key 1 is set to **“128 bit”**.
 - Verify the “Encryption Key” is set to the key prescribed by your DOIM, S6 or CSSAMO by re-typing it in the field provided. Re-enter the key to confirm.
 - Click on the **“Apply”** button. Click on the **“OK”** button to approve.
 - g) Turn your Air Fortress remote client on and Ping the user’s computer.
 - Double-click on the padlock icon and the Air Fortress Client screen with the “General” tab selected, will appear.
 - Select **“On”** in the “Encryption/Security” section of the “General” tab of the Air Fortress Client screen. Selecting “On” will change your computer to secure mode.
 - To ping the user’s computer first verify the computer is in an active communications mode if required. Then double click the DOS prompt icon on the notebook system tray. When the DOS window opens type the ping command followed by the user’s computer IP address, Ex... **“ping 192.168.1.25”**.
 - If you can communicate, the radio and encryptor are OK. Check the antenna system because you apparently have a sufficient signal to associate (or this is the root bridge), but not a sufficient signal to communicate over the radio.

- 9) **If you cannot communicate through the wireless NIC and this CBM is not the root**, make it the root and try again.
 - a) Remove the Wireless NIC IAW procedures outlined in Paragraph 2.7.1. Insert wired NIC or use built-in NIC and perform notebook to CBM connection procedures IAW Paragraph 2.11.1
 - b) Open Internet Explorer on the notebook desktop.
 - c) In the address toolbar at the top of Explorer, enter the IP address assigned to the wireless bridge.
 - d) Click on “**GO**” on the Explorer toolbar or click on “**Enter**” on the notebook keyboard.
 - e) At the “**Enter Network Password**” screen, enter the username and password you previously assigned the device. Click on the “**OK**” button
 - f) From the “Summary Status” menu select “Setup” then “**Express Setup**”. The “Express Setup” screen will appear.
 - g) Set the “**Role in Radio Network**” to “**Root Bridge**”, apply the changes and click “**OK**” to approve. If you can communicate, the radio and encryptor are OK. Set the role back to “**Non-Root Bridge w/Clients**”, apply the changes and click “**OK**” to approve. Close Internet Explorer.
 - h) Check the antenna system IAW procedures outlined in Paragraph 4.3.4 because you apparently have a sufficient signal to associate, but not a sufficient signal to communicate over the radio.
- 10) **If you cannot communicate through the wireless NIC**, leave the ping running while you perform the following:
 - a) Open Internet Explorer on the notebook desktop.
 - b) In the address toolbar at the top of Explorer, enter the IP address assigned to the wireless bridge.
 - c) Click on “**GO**” on the Explorer toolbar or click on “**Enter**” on the notebook keyboard.
 - d) At the “**Enter Network Password**” screen, enter the username and password you previously assigned the device. Click on the “**OK**” button
 - e) From the “Summary Status” menu select “Setup” then jump to Services, “**Security**”.
 - f) From the security menu choose “**Radio Data Encryption (WEP)**”.
 - Verify the “Key Size” for key 1 is set to “**128 bit**”.
 - Verify “Use of Data Encryption” is set to “**Full Encryption**”.
 - Verify the “Encryption Key” is set to the key prescribed by your DOIM, S6 or CSSAMO by re-typing it in the field provided. Re-enter the key to confirm.
 - Click on the “**Apply**” button. Click on the “**OK**” button to approve.
 - g) The bridge will be reset, traffic should resume and you can communicate. Close Internet Explorer.
- 11) If you still cannot communicate, perform a complete reset and reconfiguration on both the wireless bridge and encryptor IAW procedures outlined in Paragraph 2.11 or 3.6 for the wireless bridge configuration utilizing CAISI Admin.

4.3.4 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.

The antenna system consists of the antenna, RF antenna cable, lightning arrestor and the internal 12-in RF antenna cable (connecting the lightning arrestor to the wireless bridge). Easiest way to troubleshoot, is start on the outside and work in (try to isolate the problem) or vice versa – start inside and work out. First check the installation of the antenna itself.

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.
- 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 4-40 Troubleshooting Omni-Directional Antenna



Figure 4-41 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.

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 module chassis, ensure power to the radio is turned off.**

3. **Test the CBM antenna.**

NOTE: Remove the wireless NIC from the SSR notebook if inserted. Be careful when removing the rabbit ears antenna. Easiest way is to place the end of a flat end screwdriver underneath the wire of the connectors and pull straight off. Connectors are on tight. Make all the below connections, then insert the wireless NIC into the SSR notebook.

- a. Connect the MMCX to N (Female) adapter cable from the right port on the notebook wireless NIC to one side of the right angle (Double N) adapter.

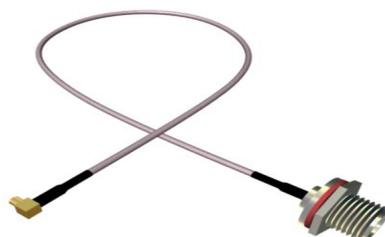


Figure 4-42 Troubleshooting MMCX to N (Female) Cable

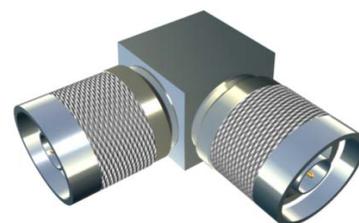


Figure 4-43 Troubleshooting Right Angle Adapter

- 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.
- d. Select LSM from the CAISI toolbox.
 - 1) Move/rotate the antenna to maximize signal strength and quality. Quality is more important than signal strength, but usually maximizing one will maximize the other.
 - 2) Compare the suspected antenna to the known good antenna.
 - 3) If the signal strength and quality are relatively close, your antenna is most likely not the problem.
 - 4) If the signal strength and quality are half as good as the known good antenna, the problem is most likely in the antenna.

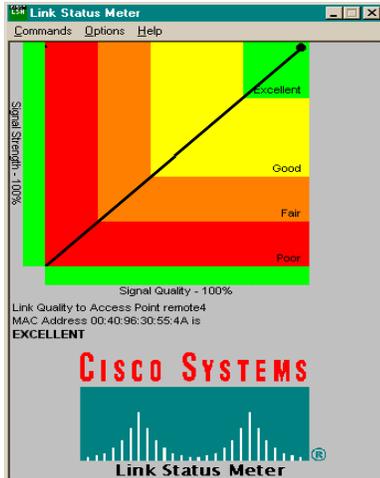


Figure 4-44 Troubleshooting LSM Results Known Good Antenna

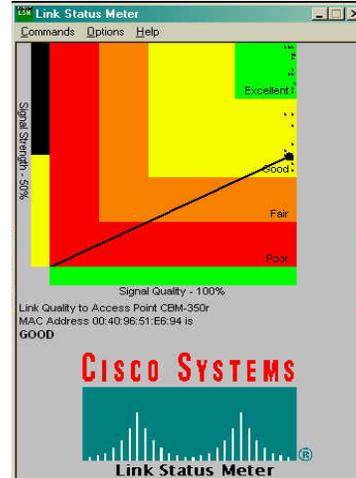


Figure 4-45 Troubleshooting LSM Results Suspected Bad Antenna

- 5) Disconnect the MMCX to N (Female) adapter cable from the notebook wireless NIC and the right angle (Double N) adapter.
- 6) Disconnect the other end of the right angle adapter from the antenna.
- 7) Reconnect the antenna to the chassis and apply power to the radio.

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.

4. Test the CBM antenna and RF Antenna cable.

- a. Disconnect the RF antenna cable from the outside of the CBM lightning arrestor.
- b. Connect your MMCX to N (female) to the N (male) antenna cable connector you just disconnected from the lightning arrestor.
- c. Connect the other end of your MMCX cable to the right port of the wireless NIC installed in the SSR notebook.
- d. Use the Link Status Meter (LSM) to check signal quality IAW procedures outlined in Paragraph 4.3.1.2.
- e. Disconnect the MMCX to N (female) cable from notebook wireless NIC and the N (male) antenna cable.
- f. Reconnect all components and cables.

5. Troubleshoot the CBM lightning arrestor.

- a. Disconnect the small RF cable inside the CBM 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 Link Status Meter (LSM) to check signal quality.
- f. If there is a substantial difference in signal quality from the previous test, the lightning arrestor 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 CBM internal 12” RF antenna cable.

- a. Disconnect the small RF antenna 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.

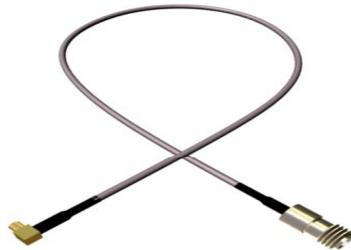


Figure 4-46 Troubleshooting MMCX to RPTNC Cable



Figure 4-47 Troubleshooting 12” RF Antenna Cable

- c. Use the Link Status Meter (LSM) to check signal quality.
- d. If there is a substantial difference in signal quality from the previous test, the small RF antenna cable inside the CBM 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.

4.3.5 Troubleshooting CBM DSL Bridge

1. During normal operations the DSL Bridge lights should be as follows:
 - a. The “PWR”, “LINK”, “SYNC” and “MAR” lights should be lit (green). The others should flicker.
 - 1) “PWR” the center light indicates that the DSL Bridge is getting power. If the DSL Bridge has no lights, check the power cord connections to the power adapter and from the power adapter to the DSL Bridge.
 - 2) “LINK” the leftmost light indicates that the Link from the DSL Bridge to the hub is good.
 - 3) LAN “TX” and “RX” light blink to indicate traffic on the LAN (Ethernet) connection.
 - 4) “COL” light may also blink occasionally to indicate collisions on the network. This is normal.
 - 5) “SYNC” light blinks several times when you first connect the field wire. As soon as the DSL Bridges on each end synchronize, the “SYNC” light comes on steady.
 - 6) Usually the “MAR” light comes on at the same time as the “SYNC” light, to indicate that the modems have a strong enough signal to provide a margin for error for reliable operations over time. 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.

2. **If you connect the field wire and do not get a “SYNC” light**, then the distant end is not yet connected or has a problem, or there is a problem with the field wire.
 - a. Contact the distant end to be sure that the wire is connected.
 - b. Ensure that both ends have the same speed setting. The speed should normally be set to “8”.
 

The image shows a DSL bridge device with a speed dial on the front panel. The dial is a circular gauge with numbers 0 through 9. A yellow needle points to the number 8. The dial is labeled 'SPEED' and 'RATE'.
 - c. Try changing both ends to the slowest speed (“1”) to see if they sync up.
 - d. If so, then try progressively faster speeds until you lose the “MAR” LED. Then set the speed back to the fastest speed at which the “MAR” LED lights. Both ends have to work together. The speed settings must match.
 - e. Check for a good metal-to-metal connections at each end. The bare wire ends of the wire must be firmly clamped in the jaws of the binding posts.
 

The image shows a DSL bridge device with a field wire connected to a binding post. The wire is inserted into the binding post and is held in place by a metal clamp. The device is labeled 'DSL BRIDGE' and 'FIELD WIRE'.

Figure 4-48 Troubleshooting DSL Bridge Speed Setting

Figure 4-49 Troubleshooting Field Wire Connection

- f. If you are using WF-16 field wire, check that both ends are connected to the *same color* pair of the WF-16.
- g. 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.
- h. Check the field wire for shorts, breaks, or bad splices. Usually you can detect problems by visual inspection.
- i. 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.

4.3.6 Troubleshooting CBM UPS



**Figure 4-50 Troubleshooting
CBM UPS**

1. During normal operations the CBM UPS lights should be as follows:
 - a. The only one lit should be the “**PWR ON/OFF**” light to indicate that the UPS is getting power. If the power light is not lit, check the external power source into which the UPS is connected.

NOTE: *The UPS must be plugged in and getting good power before it will turn on. This is a safety, to keep it from turning on by accident during transit.*

 - b. During power outages, the “**Using Battery**” LED will light to indicate that you are on battery power. There will also be a beeping signal that you are using the battery. You have between ten and twenty minutes of power available in a fully charged UPS.
2. If any of the other lights are lit, you have a problem.
 - a. The “**Check Battery**” light indicates that the internal battery has failed or will soon fail. Return to Forward Repair Activity (FRA).
 - b. The “**UPS Overload**” light indicates that you have too much stuff plugged into the “Battery Backup Protected Outlets.” You should have nothing except your CBM plugged into these outlets. The other outlets may be used for other authorized computers, but not your printer, coffee pot, or any other high current draw device. If this light comes on and stays on when you have only the CBM plugged in, contact the FRA. The internal circuits are failing.
 - c. The red “**Building Wiring Fault**” light is there to alert you to a wiring problem with the external outlet the UPS is plugged into. An ungrounded outlet is by far the most common condition that causes this indicator to come on.

4.4 TROUBLESHOOTING THE CCM

The CCM includes a multi-client 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 4.1 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 4-51 Troubleshooting 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. CCM recognizes each user by the Media Access Control (MAC) address – 12 digit hexadecimal.

If there are more than 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.

All of the following procedures assume that you have already followed the general troubleshooting procedure outlined in Paragraph 4.1. In particular that you have:

4.4.1 CCM General Troubleshooting Procedures

1. Checked your cables IAW procedures outlined in 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 CCM is first powered on, the lights should conform to the following:
 - a. Multi-client radio adapter.

- 1) There are two LEDs built in to the top of the Ethernet port.
 - a) The right one should be solid green, to indicate the link to the hub.
 - b) The left one will flash to indicate traffic.



Figure 4-52 Troubleshooting Multi-Client Radio Adapter Ethernet Port

- 2) The three lights on the top of the multi-client radio adapter should behave as follows:
 - a) 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.



Figure 4-53 Troubleshooting Multi-Client Radio Adapter LEDs

- b) Once the multi-client 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 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.

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.

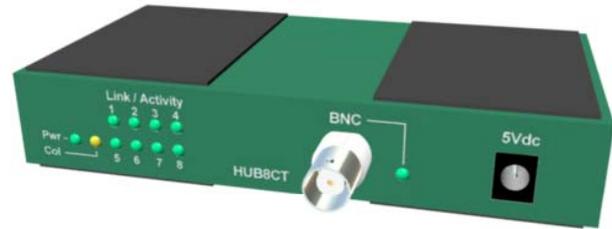


Figure 4-54 Troubleshooting Hub LEDs

- 2) Port lights flicker to indicate outgoing traffic.
4. Cycled power or rebooted (as appropriate) the next item in line at each end (switches, hubs, PCs etc).

4.4.2 Troubleshooting the CCM Hub

NOTE: *The following procedures assume that you have already followed the general troubleshooting procedures outlined in Paragraph 4.1.*

1. During normal operations the CCM hub lights should be as follows:
 - a. The “**Pwr**” light should be lit on both hubs to indicate the hubs are receiving power.
 - 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 CCM.
 - a) If the encryptor and radio also have no power, the power supply is the problem, since the hub, radio and encryptor share the same power supply.
 - b) If the encryptor and radio have power but the hub does not, make sure that the power lead in the back of the hub is seated properly. They sometimes vibrate loose.
 - b. The **Link/Activity** LEDs.
 - 1) Port number “1” light should be lit (green) on the hub. This corresponds to the white straight through Ethernet cable coming from the encryptor.
 - 2) 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.*

2. 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.

3. 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.
4. If the hubs check out, but a connected computer doesn’t get a link light or cannot communicate, check the Ethernet cable from the computer to the hub.
5. 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.

4.4.3 Troubleshooting CCM Encryptor and Multi-Client Radio Adapter

The Air Fortress 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:
 - 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.
 - 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:
 - 1) The center “**Status**” LED should be steady.
 - 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 2.12.1 for CCM physical connection procedures.
 - b. Ensure module is receiving power. Refer to Paragraph 4.1.1.
 - c. Open Internet Explorer on the notebook desktop.
 - d. In the address toolbar at the top of Explorer, enter the IP address assigned to the multi-client radio adapter.
 - e. Click on “**GO**” on the Explorer toolbar or click on “**Enter**” on the notebook keyboard.
 - f. Click on “**Write Access**” and enter the password you previously assigned the device when prompted.
 - g. Click on “**Allow Config Changes**”.
 - h. Verify the following configuration parameters for the CCM multi-client radio adapter are as required for your network.

- 1) Select “**Radio**” from the “**Configuration**” menu. The radio screen will appear.
- 2) Verify the SSID in the “**Service Set Identification**” field is set as required, for your network or as directed by your DOIM, S6 or CSSAMO.
- 3) If the SSID is incorrect type the correct SSID in the “**Service Set Identification**” field and click on the “**Save**” button.

Item	Value
Service set identification	a string of at least 1 characters caisi000 Save
Allowed bit rates in megabits/second	1, 1_2, 1_5_5, 1_11, 2, 2_5_5, 2_11, 5_5, 5_5_11 or 11
Basic bit rates in megabits/second	1, 1_2, 1_5_5, 1_11, 2, 2_5_5, 2_11, 5_5, 5_5_11 or 11
Enable world mode	on or off
RTS/CTS packet size threshold	a number of 2400 or less 1024 Save
Privacy configuration	
Parent node Id	our parent's network address any Save or any
Time to look for specified parent	off or a time in seconds off Save
Maximum number transmit retries	a number from 8 to 64 64 Save
Refresh rate in 1/10 of seconds	a number from 5 to 150 100 Save
Enable the diversity antennas	on or off
Transmit power level	1, 2, 15, 30 or full
Maximum fragment size	a number from 256 to 2048 1024 Save
Enable radio options	a password Save

Figure 4-55 Troubleshooting CCM Radio Configuration Screen

- 4) Verify the “**Allowed bit rates in megabits/second**” is set to “**1_11**”.
 - 5) Verify “**Basic bit rates in megabits/second**” is set to “**1**”.
 - 6) Click on “**Privacy configuration**” on the radio screen and the privacy screen will appear.
 - a) Click on “**Set the keys**”.
 - b) Verify the key number is set to “**1**” If not, enter “**1**” as the key number and click on the “**Save**” button.
 - c) Verify the WEP key is set to the key prescribed by your DOIM, S6 or CSSAMO by re-typing it in the field provided. Click on the “**Save**” button. You will need to repeat this procedure to confirm the key.
 - 7) Verify “**Parent Node ID**” is set to “**any**”.
 - 8) Verify “**Enable the Diversity Antennas**” is set to “**off**”.
 - 9) Verify “**Transmit Power Level**” is set to “**full**” or the maximum legal power for the area in which you are operating.
 - 10) To verify you are now associated look at the lights on top of the multi-client radio adapter. The center “**Status**” LED will be lit solid green if you are associated to the remote CBM.
 - 11) Close Internet Explorer.
4. If you still are not associated, check the antenna system IAW procedures outlined in Paragraph 4.4.4.
 5. If you are associated and indications are normal, connect your SSR notebook NIC to the hub in the CCM and attempt to pass traffic to a distant host that you know is up. Watch the lights.
 - 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.
6. 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.”
 7. 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.
 8. 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.
 9. 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.
 10. If you still cannot communicate perform the following procedures:
 - a. Connect your beige nine-pin null modem cable to the SSR notebook and the encryptor.
 - b. At the bottom of the SSR notebook screen, click on ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear. Select “**Hyperterm COM1 (38,400)**”.
 - c. When the Com1 38400 HyperTerminal screen appears, press the <Enter> key.
 - d. At the Air Fortress login prompt, enter the administrator username “**sysadm**” and press the <Enter> key.
 - e. At the password prompt, type in the password you previously assigned the device and press the <Enter> key.
 - f. Enter the **set engine accessid** command and press the <Enter> key.
- NOTE:** *You may be prompted for the old key. If you don’t know the old key, reset the encryptor and configure it from scratch.*
- g. At the “**New Access ID**” prompt set the key to the new 16-digit hexadecimal number Access ID prescribed by your DOIM, S6 and CSSAMO and re-enter to confirm.
 - h. Enter the **exit** command and press the <Enter> key.
 - i. When you log out, traffic should resume and you should be able to communicate.
 - j. Disconnect the cable and exit Hyperterm. If you had a continuous ping running, stop it, wait 2 minutes, and try again.
11. Open Internet Explorer on the notebook desktop.
 - a. In the address toolbar at the top of Explorer, enter the IP address assigned to the multi-client radio adapter.

- b. Click on “**GO**” on the Explorer toolbar or click on <**Enter**> on the notebook keyboard.
 - c. Click on “**Write Access**” and enter the password you previously assigned the device when prompted.
 - d. Click on “**Allow Config Changes**”.
 - e. Select “**Radio**” from the “Configuration” menu. The radio screen will appear.
 - f. Click “**Privacy configuration**” on the radio screen and the privacy screen will appear.
 - 1) Verify “**Encrypt Radio Packets**” is set to “**on**” and the “Authentication Mode” is set to “**open**”.
 - 2) Click on “**Set the keys**”.
 - a) Verify the key number is set to “**1**” If not, enter “1” as the key number and click on the “**Save**” button.
 - b) Verify the WEP key is set to the key prescribed by your DOIM, S6 or CSSAMO by re-typing it in the field provided. Click on the “**Save**” button. You will need to repeat this procedure to confirm the key.
12. If you still cannot communicate, connect follow procedures outlined in Paragraph 4.3.3 to verify the wireless bridge WEP key matches the radio adapters.
13. Check the antenna system IAW procedures outlined in Paragraph 4.4.4 because you apparently have a sufficient signal to associate, but not a sufficient signal to communicate over the radio.
14. 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 for the multi-client radio adapter configuration utilizing CAISI Admin.

4.4.4 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.

The antenna system consists of the antenna, RF antenna cable, lightning arrestor and the internal 12-in RF antenna cable (connecting the lightning arrestor to the multi-client radio adapter). Easiest way to troubleshoot, is start on the outside and work in (try to isolate the problem) or vice versa – start inside and work out. First check the installation of the antenna itself.

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.
 - 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.



Figure 4-56 Troubleshooting Erected CCM 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.

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 module chassis ensure power to the radio is turned off.**

3. Test the CCM antenna.

NOTE: Remove the wireless NIC from the SSR notebook if inserted. Be careful when removing the rabbit ears antenna. Easiest way is to place the end of a flat end screwdriver underneath the wire of the connectors and pull straight off. Connectors are on tight. Make all the below connections, then insert the wireless NIC into the SSR notebook.

- a. Connect the MMCX to N (Female) adapter cable from the right port on the notebook wireless NIC 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.

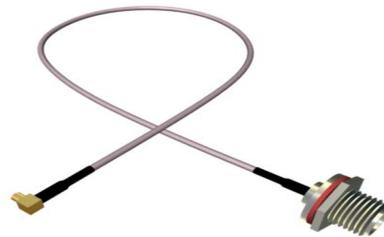


Figure 4-57 Troubleshooting MMCX to N (Female) Cable

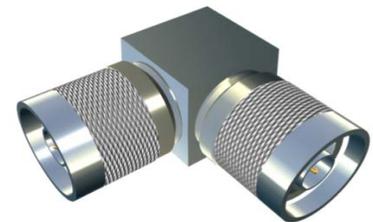


Figure 4-58 Troubleshooting Right Angle Adapter

- c. Use the Link Status Meter (LSM) to compare and check the signal quality.

- d. Select “Link Status Meter” from the CAISI toolbox.
 - 1) Move/rotate the antenna to maximize signal strength and quality. Quality is more important than signal strength, but usually maximizing one will maximize the other.
 - 2) Compare the suspected antenna to the known good antenna.
 - 3) If the signal strength and quality are relatively close, your antenna is most likely not the problem.
 - 4) If the signal strength and quality are half as good as the known good antenna, the problem is most likely in the antenna.

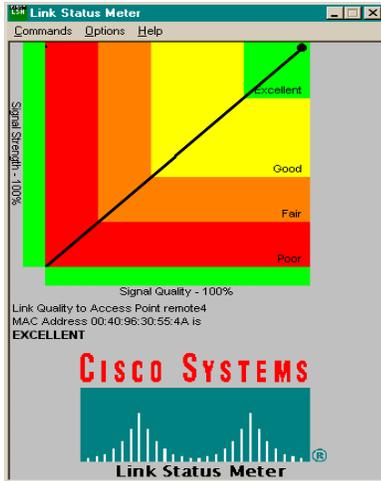


Figure 4-59 Troubleshooting LSM Results Known Good Antenna

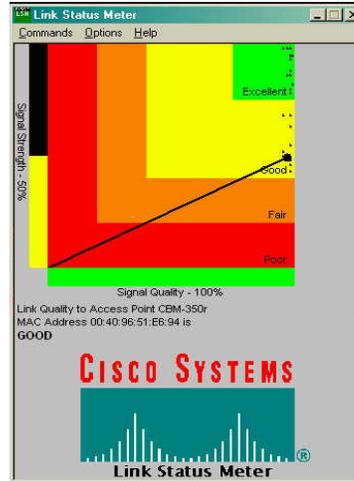


Figure 4-60 Troubleshooting LSM Results Suspected Bad Antenna

- 5) Disconnect the MMCX to N (Female) adapter cable from the notebook wireless NIC and the right angle (Double N) adapter.
- 6) Disconnect the other end of the right angle adapter from the antenna.
- 7) Reconnect the antenna to the chassis and apply power to the radio.

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.

4. Test the CCM antenna and RF antenna cable.

- a. Disconnect the RF antenna cable from the outside of the CCM lightning arrestor.



Figure 4-61 Troubleshooting CCM Lighting Arrestor and RF Antenna Cable

- b. Connect your MMCX to N (female) to the N (male) antenna cable connector you just disconnected from the lightning arrestor.
- c. Connect the other end of your MMCX cable to the right port of the wireless NIC installed in the SSR notebook.
- d. Use the Link Status Meter to check signal quality outlined in step 3 above.
- e. Disconnect the MMCX to N (female) cable from notebook wireless NIC and the N (male) antenna cable.
- f. 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 Link Status Meter (LSM) to check signal quality. (Step 3 above)
- f. If there is a substantial difference in signal quality from the previous test, the lightning arrestor 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 Antenna cable.

- a. Disconnect the small RF cable inside the CCM from the radio.

NOTE: *Be careful when removing the rabbit ears antenna and the MMCX cables from the wireless NIC. Connectors are delicate.*

- 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.

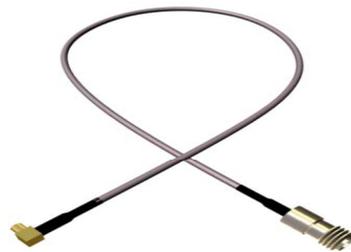


Figure 4-62 Troubleshooting MMCX to RPTNC Cable



Figure 4-63 Troubleshooting 12” RF Antenna Cable

- c. Use the Link Status Meter to check signal quality.
- 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.

4.5 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.

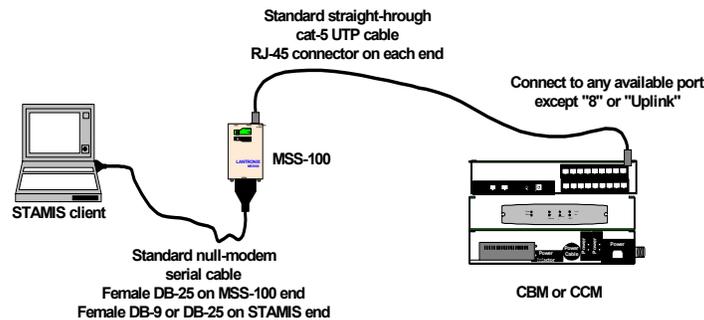


Figure 4-64 Troubleshooting Physical Connections of LSA

1. During normal operations, the LSA LEDs indicate Ethernet, serial links and traffic.
2. The MSS-100 device has five LEDs:
 - a. "Link" light to indicate that the CAT-5 Ethernet connector is linked to a hub or switch.
 - b. "100" light to indicate that the Ethernet link is at 100MB. If the LED is not lit, the link is at 10MB.
 - c. "Serial" LED to indicate that traffic is flowing through the serial connection.
 - d. If you have a solid red "Serial" light or if it's solid red for three seconds followed by one second of another color, the unit must be replaced.
 - e. "OK" light to indicate that the device booted successfully and is operating normally. If you have a solid red "OK" light or if it's solid red for three seconds followed by one second of another color, the unit must be replaced.
 - f. "Power" LED that is lit whenever power is applied.
 - g. During normal operations, the "OK" LED is on and blinks about once every two seconds.
 - h. If you have a rapidly blinking "OK" light, cycle power (remove power cord and then reconnect it to the LSA) to force it to reboot. If it still blinks rapidly, then the unit must be replaced.
 - i. If the MSS-100 is not operating normally and there are no lights at all, the device or its power supply must be replaced.

NOTE: *If basic troubleshooting procedures fail, perform advanced troubleshooting and diagnostic procedures.*

3. If all indications are normal, but your clients cannot connect:

- a. If you get a **Boot>** prompt, check the network cable, just as if you have no green Link LED (above), then cycle power.
- b. 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.
- c. 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 (remove power cord and then reconnect it to the LSA) to force it to reboot and restart the CAISI VEE program. Then try again to communicate. The STAMIS will need to be registered, because registration is lost when power is lost. Watch the Blast screen to ensure that the warning and TS> prompt appear. If they do not, contact the system administrator to remotely attempt to restart the CAISI VEE program in your LSA.
 - 3) If you still don't see any prompts, replace the cable.
 - 4) If the cable doesn't help reset the LSA to factory and reconfigure the LSA.
 - 5) 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.
 - 6) Check the HOSTS and CAISIVEE.CFG files to ensure that they match your current deployment. If, for instance, CAISIVEE.CFG says to go to files before DNS and your HOSTS file is wrong, the STAMIS will constantly try to connect to the wrong address contained in the HOSTS file.
- d. If you still cannot connect, contact the system administrator, network control, or CSS S6 to ensure that the network is actually up the whole way.
- e. If you still cannot communicate, you need to check the configuration. Reload the HOSTS file, CAISIVEE.CFG file, or program files if necessary.

NOTE: *STAMIS users will not need or be able to access the programs or configuration settings inside the LSA. The SSR can, but will need both the login and privileged passwords to access the LSA for configuration. If the password is lost, then the LSA can be reset and reconfigured from scratch, following instructions in Paragraph 2.13.2.*

4. You can use telnet to check the configuration and make changes on the fly without stopping the CAISIVEE program.
 - a. At the bottom of the SSR notebook screen, click on the **Command Prompt (C:\)** screen. The Command Prompt menu will appear.
 - b. Type the command, **telnet xxx.xxx.xxx.xxx** where the xxx's is the IP address of the LSA. Example: telnet 192.168.1.150
 - c. There are four commands that you need to check the configuration. They are as follows:
 - 1) "**show server**" - checks the firmware version, the inactivity timer, and the IP address information.

- 2) “**show server boot**” - checks the boot flags.
- 3) “**show ports**” -
 - a) Checks the Flow control and baud rate.
 - b) Checks the characteristics. They must include:
 - Autobaud
 - Inactive Limit
 - Password
 - Telnet Pad
 - IncPassword
- 4) “**ping xxx.xxx.xxx.xxx**” (replaces x’s with IP address)
 - a) Use the ping command to check outgoing network connectivity.
 - b) You can ping IP addresses or hostnames.

Note: *The local HOSTS file is not used, however, so you can only ping names that are in the DNS server.*

If you reset and reconfigured the LSA, and still cannot communicate, you will need to replace the LSA.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

CAISI MANUAL TOOLS AND SYSTEM UTILITIES

A.1 CAISI SYSTEM UTILITIES

The following is a guide explaining the utilities needed to manually configure the components of the CAISI.

A.1.1 BLAST

Blocked Asynchronous Transmission (BLAST) is 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. The configuration menu is shown below:

```

BLAST  Offline                               C:\UTIL\BLAST
Configure New Modify Tag Remove Directory Local Learn Online
... load the selected setup and dial/logon the remote system

----- ESC-exit -----
Dialing Directory                               Telephone #
ALLPPP... Configure some or all CSMIM2 for 9600 81N .....
CSMIM2... CSMIM2 Setup using DTE Connector 9600 81N .....
DEFAULT...                               9600 81N .....
DIALUP... dialup..... 9600 81N 35840.....
EMME... EMME Setup using PC Connector... 9600 81N .....
LINEDRIV.. Connection using line drivers... 9600 81N .....
NULLMODM.. Connection using null modem cabl 9600 81N .....

-----
F1-help | | | | | 00:00:00 | | | | | 81N 09:48 am
  
```

Figure A-1 BLAST Configuration Menu

You will in most cases be using the DEFAULT settings for configuring most components in BLAST. Press \downarrow Enter to view the default settings:

```

BLAST  Offline                               C:\UTIL\BLAST
... <|>-up <|>-down <=>-right <=>-left <PgUp>-first <PgDn>-last
... press AT to clear or enter new text

----- ESC-exit -----
Setup for: DEFAULT
Description: CAISI Terminal
Phone Number:
System Type:
User ID:
Password: XXXXXXXXXXXXXXXX
Attention Key: AK
Connection: COM1
Emulation: VT100...
Connection T/O: 60
Full Screen: YES
Originate/Answer: ORIGINATE
Local Echo: NO
Modem Type: Hardwire
AutoLF In: NO
Pulse Dialing: NO
AutoLF Out: NO
Baud Rate: 9600
Wait for Echo: NO
Parity: NONE
Prompt Char: NONE
Data/Stop Bits: 8/1
Char Delay: 0
Line Delay: 0
Keyboard File:
XON/XOFF Pacing: NO
Script File:
RTS/CTS Pacing: YES
Log File:
Protocol: BLAST...
Translate File:
Packet Size: 256_
  
```

Figure A-2 BLAST Defaults

A terminal emulator makes your computer act like one of the remote console terminals originally hard-wired directly to the mainframe computers before there were any personal

computers. One of the most common terminals was the VT-100. That is what BLAST is set to emulate. All of the early terminals were character based – they did not do graphics and had no mice. All pictures were produced by printing characters on the screen, and all input was from the keyboard.

A.1.2 HyperTerminal

HyperTerminal (HyperTerm) is a Windows based terminal emulation program. The processes used will be discussed in the next section. This section addresses the configuration aspects of HyperTerminal.

1. Once you have opened HyperTerminal from the CAISI Toolbox menu, click on “**File**” and highlight “**Properties**”, press the <Enter> key:

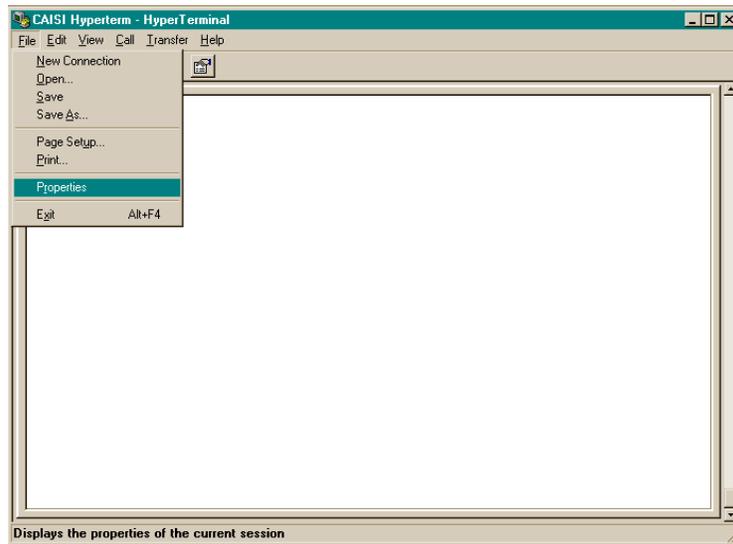


Figure A-3 HyperTerm - Select Properties Screen

The following screen will appear:



Figure A-4 HyperTerm - Properties Screen

2. Ensure the “Connect using” option is set to “**Direct to Com 1**”. Click on “**Configure**”.

The following screen will appear:

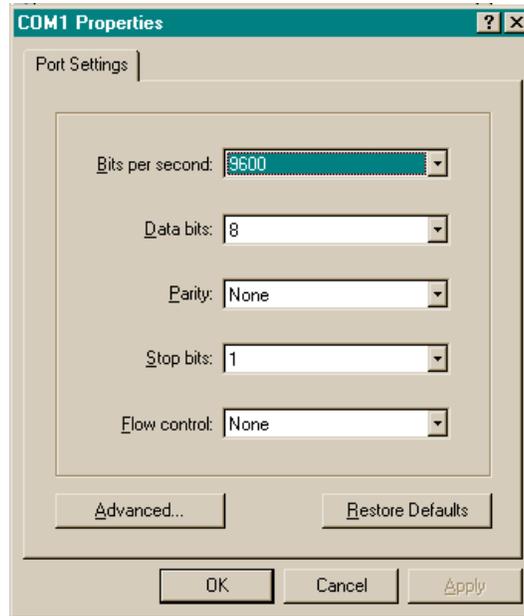


Figure A-5 HyperTerm - Port Settings Screen

3. Ensure the values are as shown. Click on “**OK**”.
4. On the CAISI Hyperterm Properties screen, click on “**Settings**” tab.

The following screen will appear showing the default values:

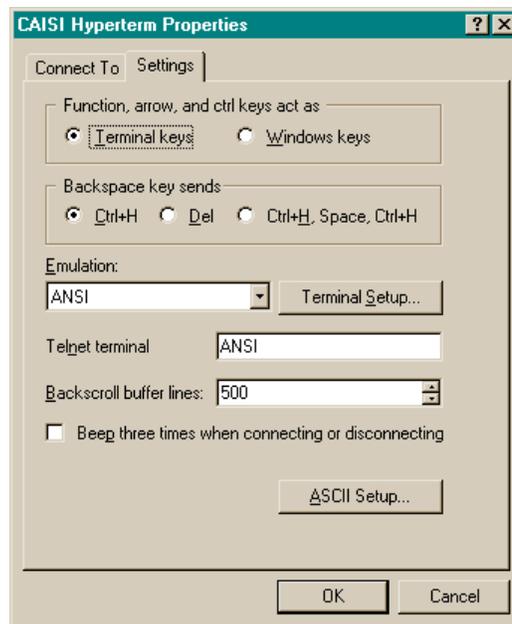


Figure A-6 Hyperterm – Settings Tab Screen

A.1.4 Telnet

Telnet is a remote logon terminal emulator program. The term Telnet stands for “Telecommunications Network”. It is a terminal emulation over TCP/IP. The Telnet program allows you to establish a terminal type connection to a remote device. A terminal is a monitor connected to a server. The server feeds information to a dummy terminal and the terminal displays the data. In computing terms, a terminal is a monitor and keyboard; there is no CPU or hard disc drive. The central computer or server controls everything.

Telnet is often used as a means of configuring a device over the network. The idea is that you remotely log into the device and change its configuration. You will also find Telnet type connections running in commercial environments, especially in stock control systems. The user logs into the computer via Telnet and then selects options from menus in the software. The data that the user enters is transmitted to the host computer, which then processes the information.

Once the computer has processed the instructions, updated information is transmitted to the client terminal. This type of approach ensures that all processing is carried out on the server.

The Telnet protocol can be used to configure the Cisco Wireless Bridges, Cisco client adapters, and the LSA. This is done via the Ethernet connector on each of the devices. To initiate a Telnet session, the user will open a command line window from the CAISI notebook. Once the user has opened the command line, they will type the command Telnet and the IP address of the device they want to configure. (Example, “**Telnet 172.16.1.10**”).

Once in a Telnet session, the user is ready to configure the device. To check the configuration, open Telnet, click on “**Terminal**”, and highlight “**Preferences**” and press the <Enter> key. The following telnet screen will appear.

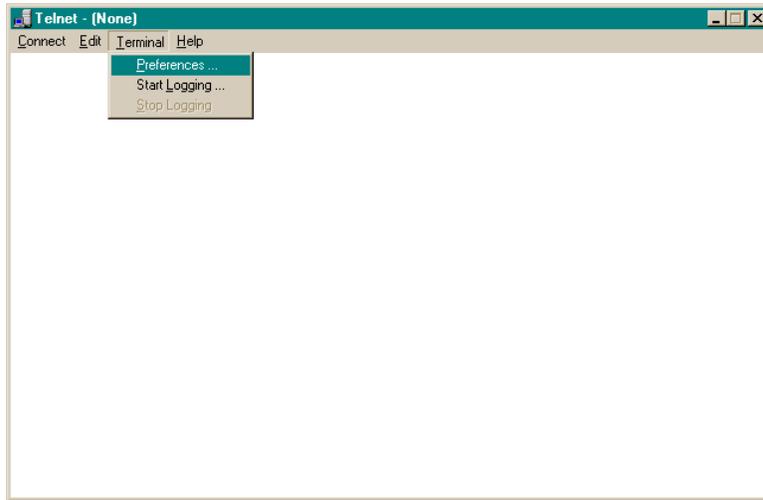


Figure A-7 Telnet – Main Screen

The terminal preference screen is shown below:

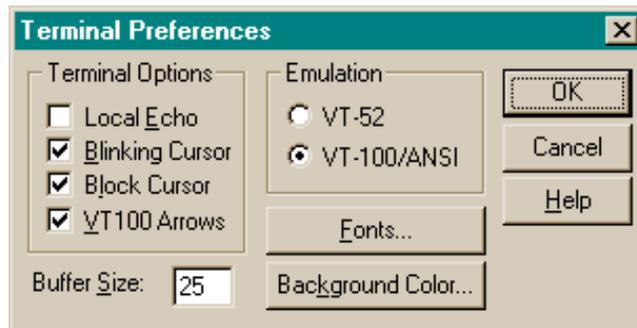


Figure A-8 Telnet – Terminal Preferences Screen

Do not turn on “**Local Echo**”. Virtually every application on every computer you log into using Telnet will perform an echo, displaying your keystrokes as you type. Turning on Local Echo would result in double echoes. Double echos slow data transmission and cause slow response from the network.

A.1.5 Web Browser

Internet Explorer is the web browser pre-loaded on the SSR notebook computer. Once the network is operational, Internet Explorer or Hypertext Transfer Protocol (HTTP) may be used to connect to the radios for configuration and troubleshooting. It is the protocol used by the World Wide Web to format and transmit messages. For example, when you type a Web address into your browser, an HTTP command is sent to the Web server, telling it how to access and transmit the desired Web page.

The HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems. A feature of HTTP is the typing and negotiation of data representation, allowing systems to be built independently of the data being transferred.

As with Telnet, HTTP can also be used to configure the Cisco wireless bridges, Cisco multi-client radio adapters, Linksys router and the LSA. This process is also done via the Ethernet connection to each of the devices.

To configure or manage the devices (Cisco wireless bridge, multi-client radio adapter, LSA or the Linksys Router), the user needs to open Microsoft Internet Explorer. Once opened, the user is able to type in the IP address of the device to be configured in the address block window.

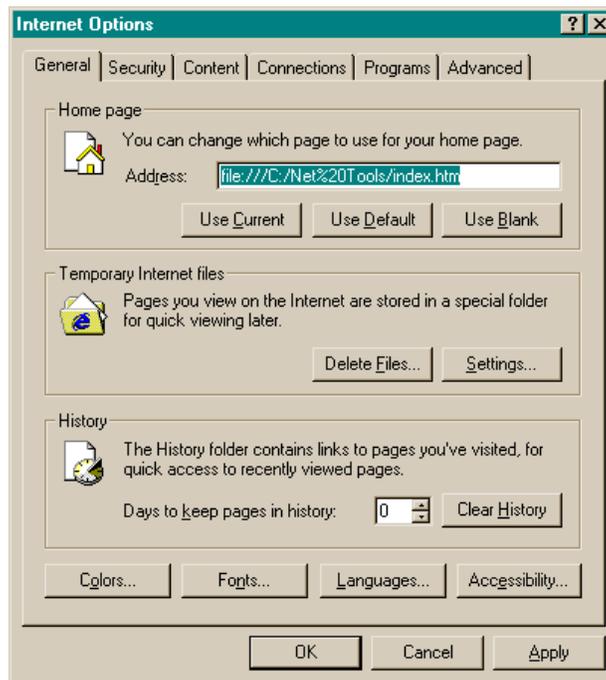


Figure A-9 Internet Explorer Configuration Options

A.2 USING THE MANUAL CONFIGURATION TOOLS

Components can be configured using either manual procedures or the CAISI Admin software application (for auto-configuration). The manual method can be used over the network or by connecting directly with the provided tools (Utilities). The following information describes the utilization of the configuration tools discussed in the previous section.

A.2.1 Wireless NIC Utilities

There are three utilities used in conjunction with the CAISI notebook wireless NIC:

- Aironet Client Encryption Manager (CEM)
- Aironet Client Utility (ACU)
- Link Status Meter (LSM)

A.2.1.1 Aironet Client Encryption Manager (CEM).

The CEM is used to set the Wired Equivalent Privacy (WEP) key on the wireless card by performing the following steps:

1. Insert the wireless NIC in the SSR notebook computer. Attach rabbit ears antenna to the velcro patch on the left corner of the notebook cover.
2. Click on the “CAISI Toolbox” icon on the task bar or the “Start” – “Programs” menu.
3. Select **CEM** and press the <Enter> key. The following screen will appear that shows the latest utility version, as of 4-01-2002 is v 4.15:



Figure A-10 Client Encryption Manager (CEM) - Login Screen

3. Enter your password. If you have not set a password, the default password is “Cisco”. A screen similar to the following will appear:

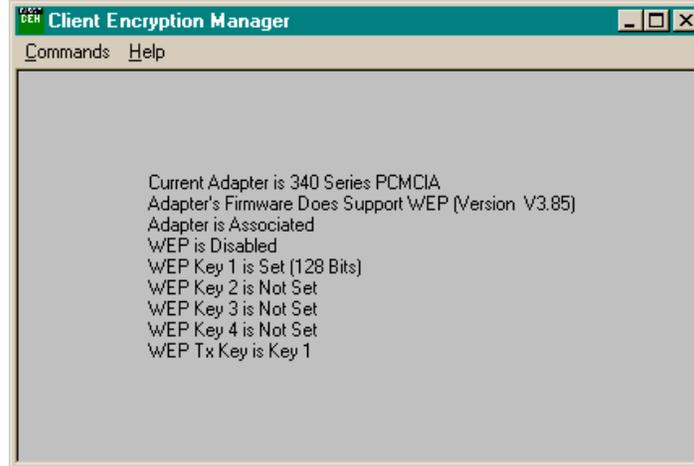


Figure A-11 WEP Key Screen

4. Click on “**Commands**” and Select “**Enter WEP Key**” from the pull-down menu. The following screen will appear:

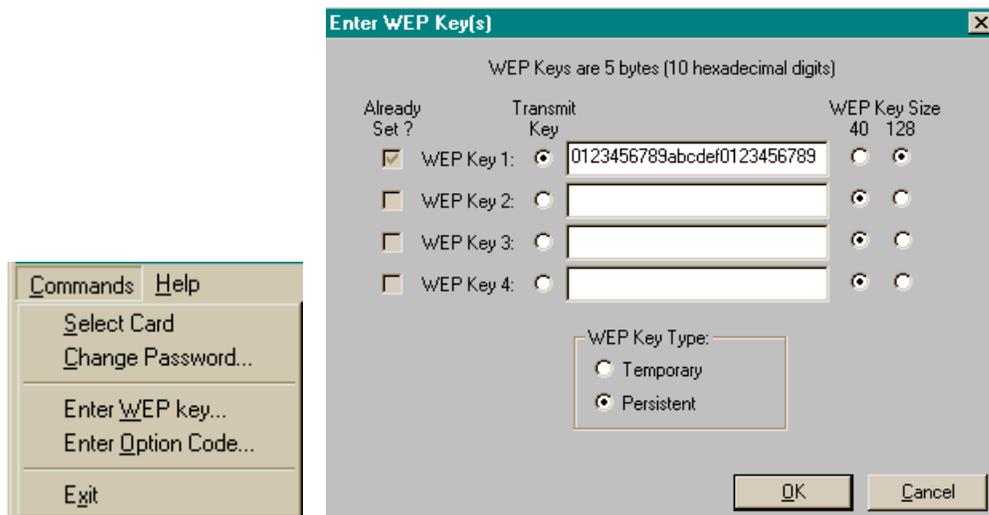


Figure A-12 Setting the WEP Key

Enter the Key or Keys as provided by the CSSAMO or S-6. The key will be 128-bit. This means that you must enter twenty-six hexadecimal characters and they must be exactly right.

NOTE: *Some users, such as the S-6 or CSSAMO, who must travel from one CAISI node support area to another, may have more than one key loaded. The typical STAMIS or CSS user will have only one key.*

Actual step by step instruction in setting the WEP key and changing the password is covered in Section 2.8.

A.2.1.2 Aironet Client Utility (ACU).

The ACU is used to set the Service Set Identification (SSID) and to run diagnostics.

From the CAISI Toolbox, open the “**Aironet Client Utility**”. The following screen will appear:

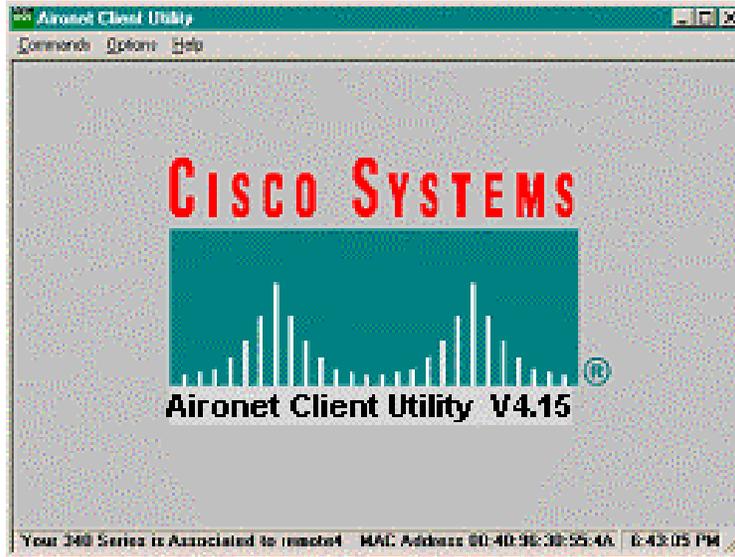


Figure A-13 Aironet Client Utility (ACU) – Main Screen

Click on **Commands** and click on **Edit Properties**. The properties screen will open on the System Parameters tab:

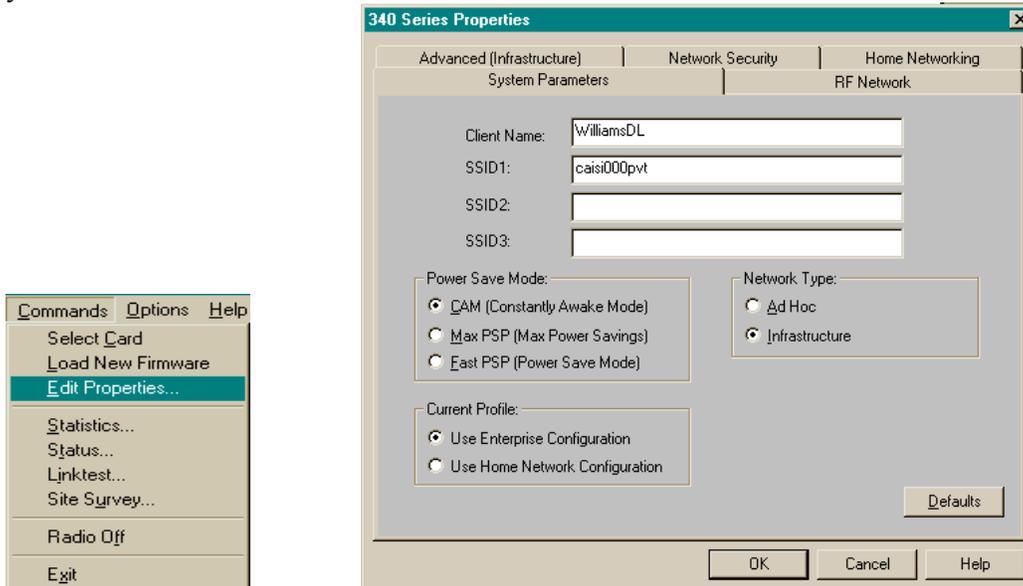


Figure A-14 ACU - System Parameters Screen

Enter the Computer Host Name and assigned SSID. CAISI default is “caisi000”. Set Power Save Mode to “CAM”, Network Type to “Infrastructure”, and Current Profile to “Use Enterprise Configuration”.

Click on the “RF Network” tab to get the following screen:

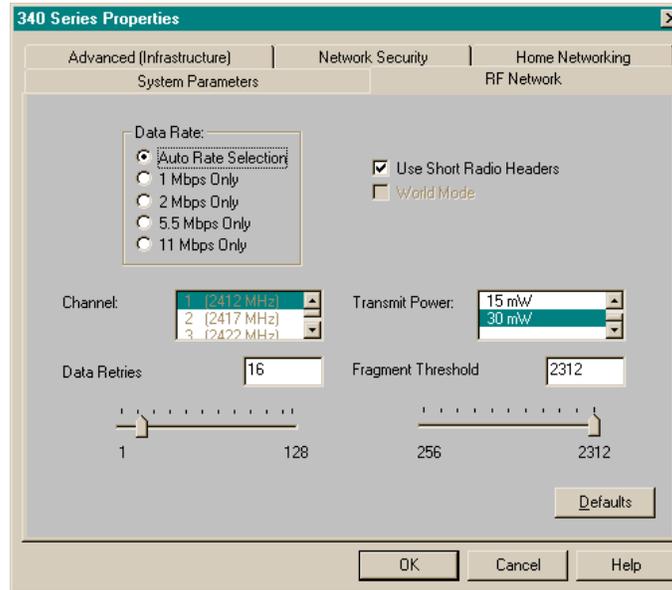


Figure A-15 ACU - RF Network Tab

Set the Data Rate to “Auto” and ensure the “Use Short Radio Headers” box is checked. Set the Transmit Power as directed by S-6, DOIM, or CSSAMO.

Click on the “Advanced (Infrastructure)” tab:

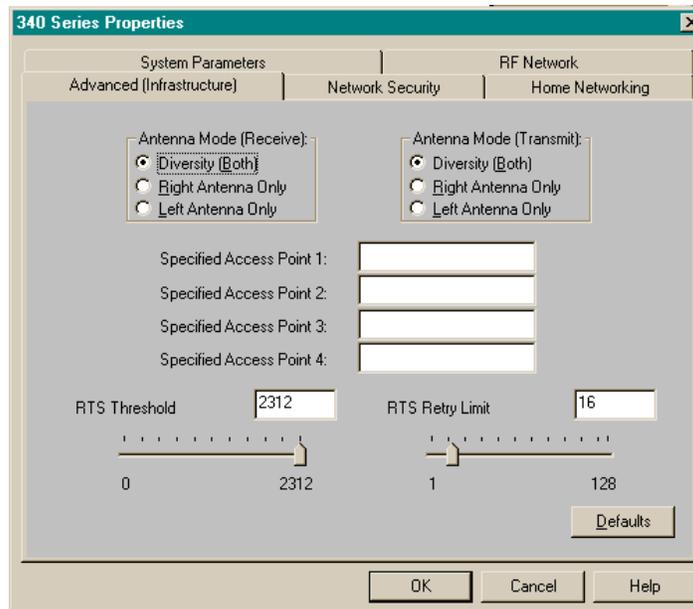


Figure A-16 ACU - Advanced (Infrastructure) Tab

Set both Antenna Modes to “**Diversity**” if you are using the rabbit ears antenna or the tab antenna on the notebook computer. If you are using the small whip antenna on a PCI or ISA adapter, in a desktop, then choose “**Right**”. Do not enter a Specified Access Point at this point unless directed to do so.

Click on the next tab, “**Network Security**”.

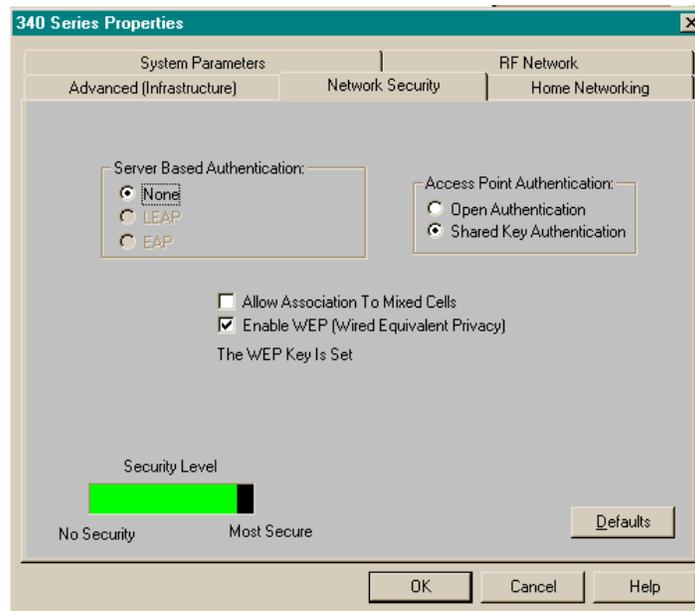


Figure A-17 ACU - Network Security Tab

Set Access Point Authentication to “**Open Authentication**” and check the “Enable WEP” box. Click on “**OK**”. The wireless card will now be configured.

A.3 NETWORK MONITORING TOOLS

The SSR Notebook Computer has several tools loaded on it to assist in network monitoring. These are detailed below.

A.3.1 Link Status Meter (LSM)

The Link Status Meter on the SSR notebook computer can be used to aim the antenna. It provides a graphical representation of relative signal strength:

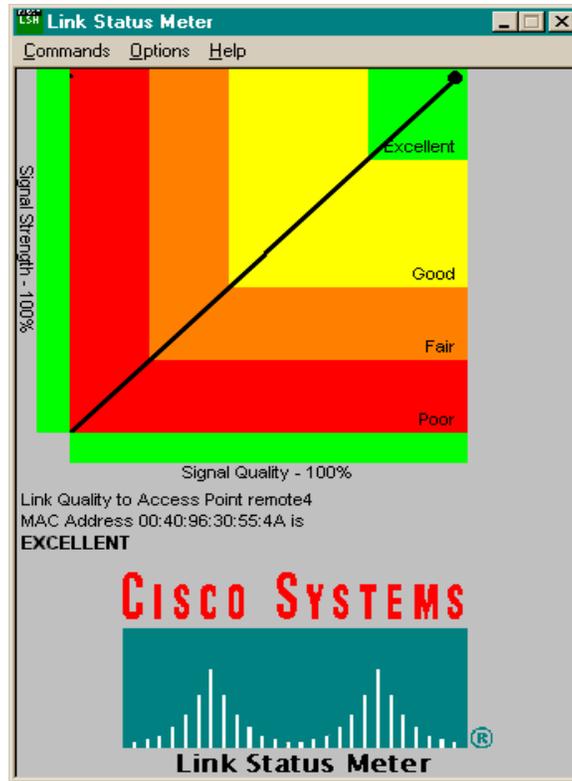


Figure A-18 Link Status Meter (LSM)

For information on how to use the LSM, refer to Section 4.3.4.

A.3.2 WS_Watch

WS_Watch is a tool that allows you to graphically monitor the network. It is extremely limited, but useful. It is a visual tool, that is an icon on the screen represents the various computers and network devices you are interested in. Any device with an IP address can be placed on the screen and WS_Watch will periodically ping each address, changing the color of the icon to represent the ability to reach the IP address. Below is an example of a network diagram in WS_Watch:

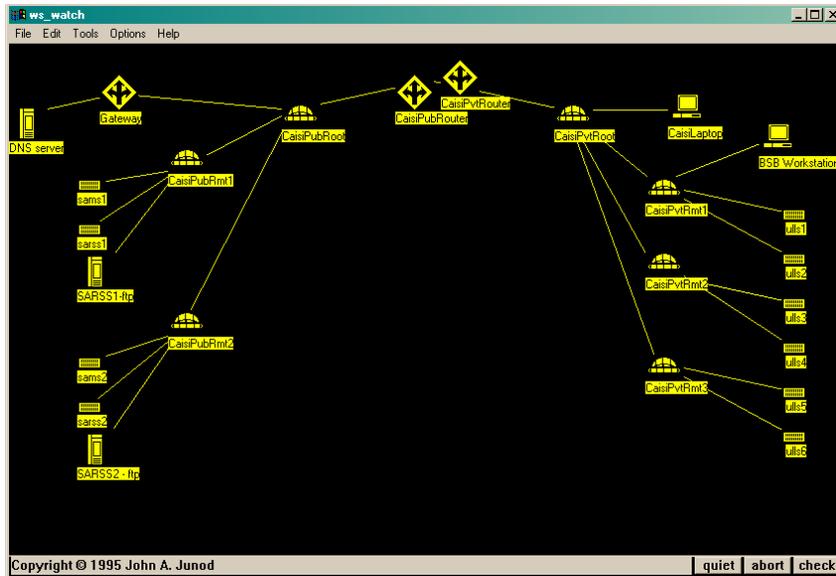


Figure A-19 Sample WS_Watch Screen

Although you see lines interconnecting the icons on the above screen, the lines are just graphics. They are just there to visualize the network.

The Icons available when diagramming a network are shown below. You must set attributes for each device when you create it.

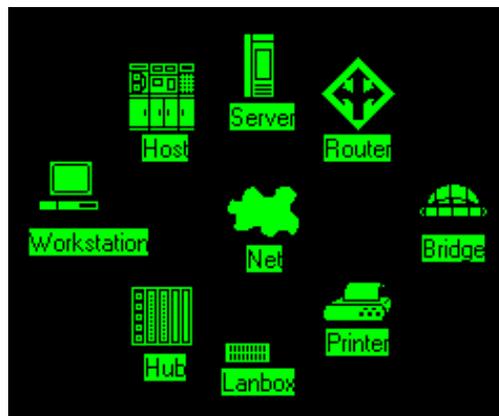


Figure A-20 WS_Watch Icons

Follow the steps below to diagram your network:

1. If a default diagram is on your screen, click on “**File**”, click on “**New**”, Click on “**Network**”.
2. At the top of the screen, click on “**Edit**”. The screen will display a grid format and Edit will change to End Edit.
3. To add an Icon to the diagram, Click on **Add** and Click on **Host**. A default Icon will appear that you can click and drag into position. When you release the mouse the following configuration screen for the Icon will appear:

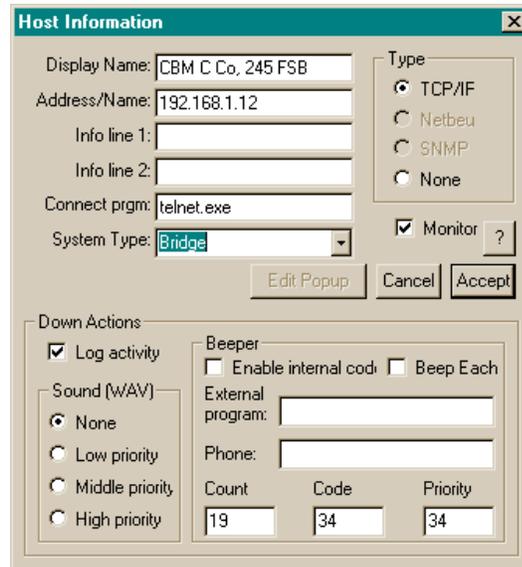


Figure A-21 WS-Watch - Icon Configuration Screen

4. The following values must be entered.
 - a) Display Name. The Display Name can be anything you want it to be, the type of device, the owning unit, or some combination.
 - b) Address/Name. This field must contain the exact IP address of the device the Icon represents.
 - c) Connect prgm. Leave this at the default telnet.exe.
 - d) System Type. The designation selected here will determine the type of Icon that is displayed. The Icons are shown above in Figure A-20. Note there is a Bridge Icon available.

NOTE: *There is a Net Icon available (the cloud). In this instance, it would be used to designate an MSE/TPN network, and will not have an IP address assigned to it, as there is no single IP for MSE.*

- e) Type. Ensure TCP/IP is selected.
- f) Monitor. Ensure this is checked.

- g) Log Activity. This is optional.
 - h) Sound. If this is checked, an audible sound will occur whenever WS_Watch loses contact with an IP address.
5. Once you have all your Icons on the screen, you can draw lines between the Icons to establish the relationship between the network components. To do so:
- a) Click on Add and click on Line.
 - b) Holding down the right mouse button, place the cursor over the start point of the line. Move the cursor to the end of the line and release the mouse button.
 - c) Once all of the lines have been drawn, click on End_Edit. The grid will disappear and WS_Watch will begin monitoring the network.

NOTE: *The lines will not change color, as the Icons will. They are merely placed on the diagram to establish relationships between elements of the network.*

Should WS_Watch fail in an attempt to ping one of the IP addresses, it will gradually change the color of the icon to yellow, and then red. Should WS_Watch reestablish contact (through ping) with the destination IP address, it will gradually change the icon back to green.

A.3.3 TJPing

Pinging involves sending a small data packet to a destination IP address and receiving a response, if you are able to reach that IP. It is a simple means of testing network connectivity and availability. TJPing is a method of pinging and receiving more information than a basic DOS ping. Three functions are Ping, Lookup and Trace.

1. **Ping:** Verify that a distant host is currently on the network and responding to ping (echo) commands.

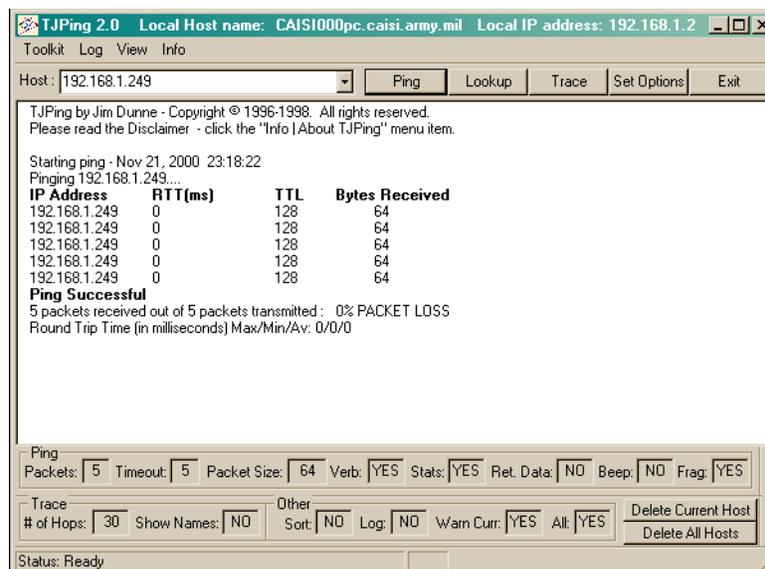


Figure A-22 TJPing – Ping Screen

To ping a host you type in the destination IP address and click on Ping. A series of small data packets will be sent to the destination and the results will be displayed as shown above.

2. **Lookup:** If you have a host name but do not know the IP address, you can ask the DNS for this information using the Lookup function of TJPing:

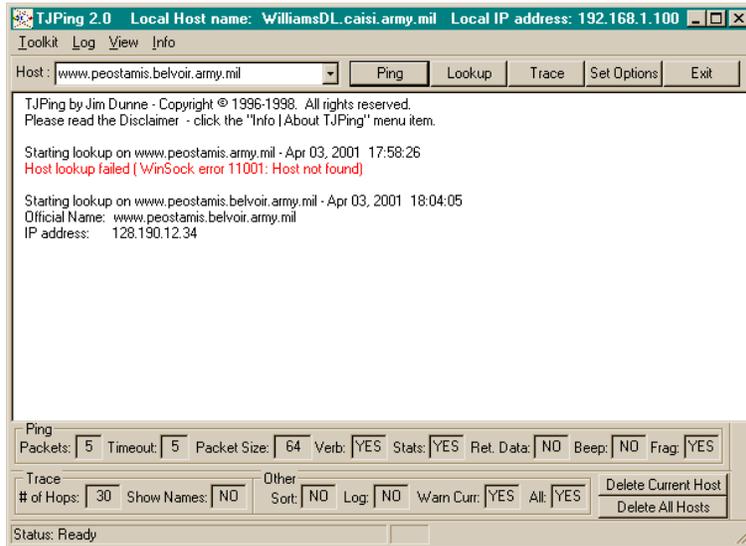


Figure A-23 TJPing – Lookup Screen

Type the destination host name in the Host field and click on Lookup. TJPing will query the DNS and return with the IP address associated with that host name in the DNS.

3. **Trace:** You can also trace the path your ping takes through the network to the destination IP address using the Trace function of TJPing:

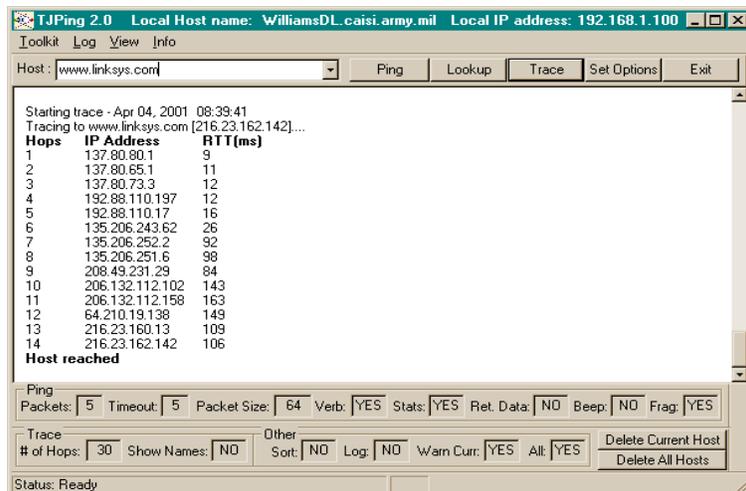


Figure A-24 TJPing – Trace Screen

As shown above, TJPing will show the “points” that the ping is routed through in the network as it reaches the destination host. You can use the Lookup function to determine the host name of any of the hops.

TJPing options are the defaults. You can change any parameters that you like.

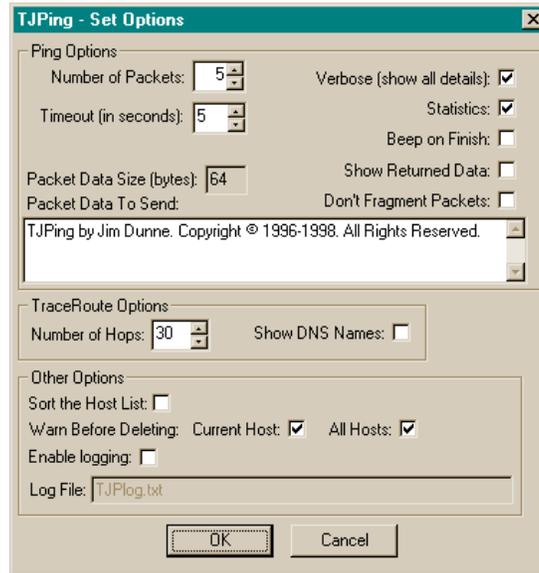


Figure A-25 TJPing – Set Options Screen

A.3.4 IP Address Assistant

There are two versions of the IP Address Assistant on the SSR notebook. Their functionality is essentially the same, however, the older version, on the left below, contains a Help function.

The Address Assistant is designed to help in splitting a network into subnets. Below is the result of splitting the 255.255.255.192 subnet of 192.168.1.0 into four segments with 62 possible hosts:

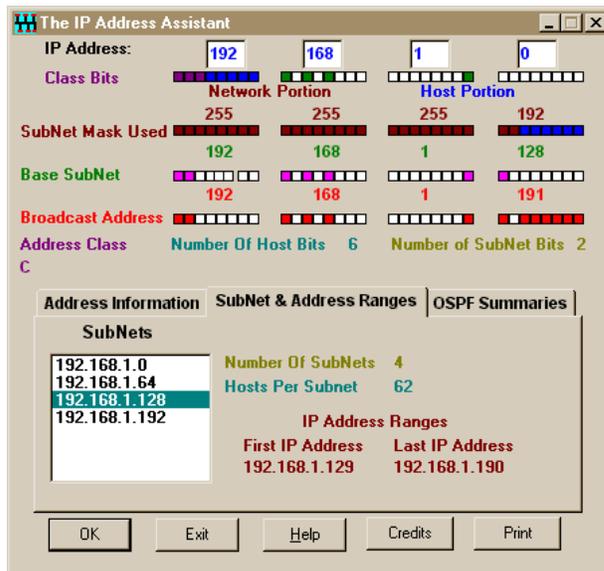


Figure A-26 IP Address Assistant

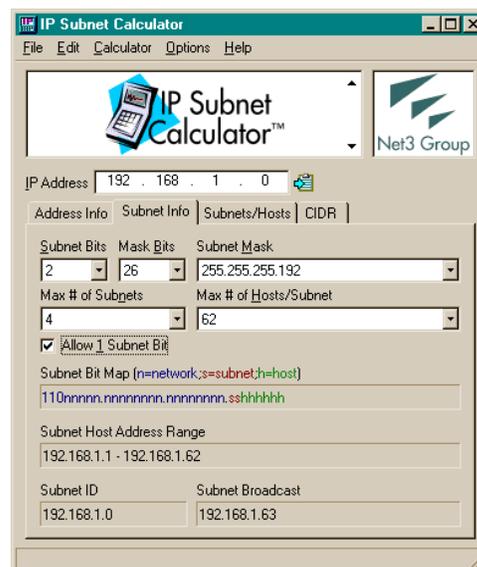


Figure A-27 IP Subnet Calculator

A.3.5 WS_FTP

WS_FTP is used to transfer files from one computer to another. You will need it to update the configuration files on the LSAs.

When you open WS_FTP you will see a Session Profile screen:

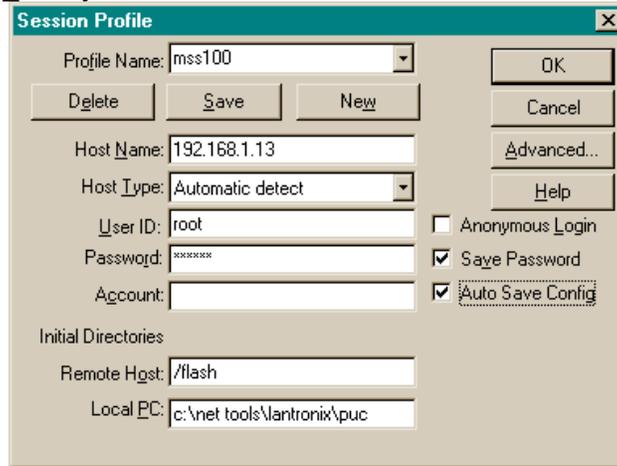


Figure A-28 WS_FTP - Session Profile Screen

Connect: Enter the name or address of the computer you wish to connect to. Click on “OK” and the following screen will appear:

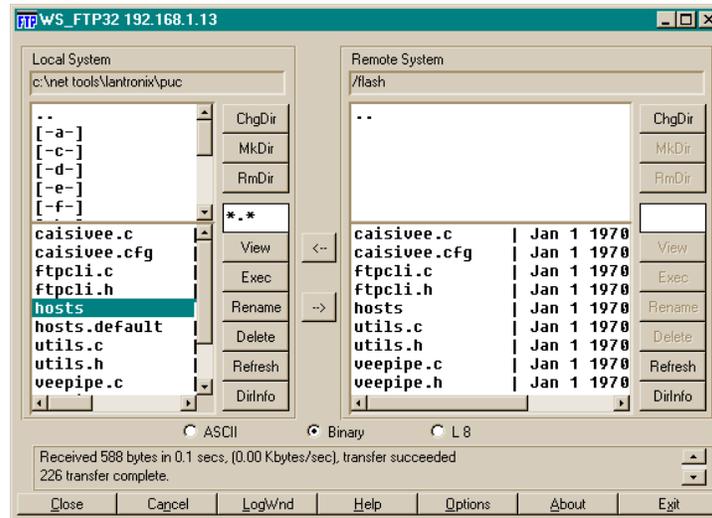


Figure A-29 WS_FTP - File Transfer Screen

Transfer Files: Navigate to the correct directory on the local and remote systems. Select the files to be transferred by clicking on the <-> buttons.

WS_FTP Options: Default options are shown below:

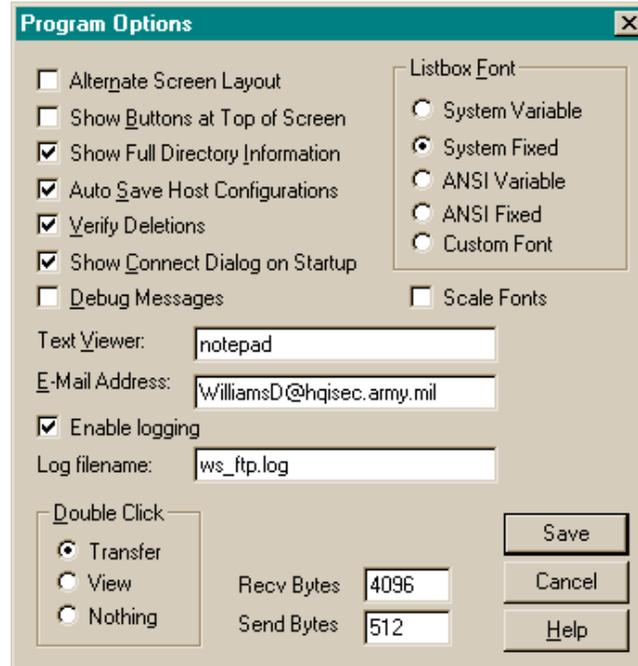


Figure A-30 WS_FTP – Program Options Screen

A.3.6 Show IP Configuration

This tool is a simple batch file to give you a quick and easy way to see your IP address and parameters. It executes two commands:

```
ipconfig /all | more
```

```
pause
```

```

C:\WINNT>ipconfig /all | more
Windows 2000 IP Configuration

Host Name . . . . . : CAISI004pc
Primary DNS Suffix . . . . . : caisi.army.mil
Node Type . . . . . : Broadcast
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : caisi.army.mil
                                army.mil

Ethernet adapter Cisco 342 wireless:

   Connection-specific DNS Suffix  . : caisi.army.mil
   Description . . . . . : Cisco Systems 340 Series Wireless LAN Adapter
   Physical Address. . . . . : 00-40-96-36-F0-1F
   DHCP Enabled. . . . . : No
   IP Address. . . . . : 192.168.1.2
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 192.168.1.1
   DNS Servers . . . . . : 138.27.4.15
                           172.16.1.10

C:\WINNT>pause
Press any key to continue . . .

```

Figure A-31 Show IP Configuration Screen

You can add similar batch files for tasks you frequently perform. If you often switch back and forth between two networks, for instance, and are using DHCP, you might create a batch file to release and renew your address, as follows. Use pauses to keep your screens from disappearing before you have a chance to read them.

```
ipconfig /release
```

```
ipconfig /renew
```

```
pause
```

Appendix B

GLOSSARY/ACRONYM LIST

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.

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.

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 bit encryption .

Address Resolution Protocol (ARP). A TCP/IP protocol used to obtain a node's physical address. A client station broadcasts an ARP request onto the network with the IP address of the target node it wishes to communicate with, and the node with that address responds by sending back its physical address so that packets can be transmitted. Wireless Bridge and Multi-client radio adapter have an ARP table.

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). 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.

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.

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.

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.

In-Line 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 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.

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.

Packet. A collection of bits comprising data and control information formatted for transmission from one **node** to another.

Point-to-Point (PTP). A BLAST data transmission protocol that utilizes the limited voice circuit of Mobile Subscriber Equipment (MSE).

Point-to-Point Protocol (PPP). A protocol for communication between two computers using a serial interface. Means of transferring TCP/IP packets over a dial-up or direct connections (serial).

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.

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.

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.

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).

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.

SUI. Sensitive unclassified information.

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 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
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
ARP	Address Resolution Protocol
ASB	Aviation Support Battalion
ASCII	American Standard Code for Information Interchange
AUI	Auxiliary Unit Interface
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)
BSA	Brigade Support Area
BSN	Brigade Subscriber Node
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
COL	Collision
COMSEC	Communication Security
CONUS	Continental United States
COTS	Commercial Off-The-Shelf
CSS	Combat Service Support
CSSAMO	Combat Service Support Automation Management Office

DA	Department of the Army
dB <i>i</i>	Decibel
DHCP	Dynamic Host Configuration Protocol
DIAG	Diagnostics
DISA	Defense Information Systems Agency
DISCOM	Division Support Command
DNS	Domain Name Server
DoD	Department of Defense
DOIM	Directorate of Information Management
DSA	Division Support Area
DSB	Division Support Battalion
DSL	Digital Subscriber Line
DSU	Direct Support Unit
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
FSB	Forward Support Battalion
FTP	File Transfer Protocol
GUI	Graphical User Interface
GMT	Greenwich Mean Time
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
LAN	Local Area Network
LED	Light Emitting Diode
LEN	Large Extension Node
LOS	Line of Sight
LRU	Line Replaceable Unit
LSA	Legacy Support Adapter
LSM	Link Status Meter
MAC	Media Access Control
MAR	Margin of Error
MB	Megabyte
Mbps	Megabits per second
MDI	Media Dependent Interface
MDI-X	Media Dependent Interface - crossover
METT-T	Mission, Enemy, Terrain, Troops and Time Available
Mhz	Megahertz
MISC	Miscellaneous
MMCX	Multimedia Communication Exchange
MOS	Military Occupational Specialty
MSE	Mobile Subscriber Equipment
MTU	Maximum Transmission Unit
MW	Milli-Watt
NAT	Network Address Translation
NAV	Norton Anti-Virus
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
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
PDSS	Post-Deployment Software
PEO EIS	Program Executive Office Enterprise Information Systems
PMCS	Preventive Maintenance Checks and Services
PO	Project Officer
POC	Point of Contact
PWR	Power
QTY	Quantity
RAU	Radio Access Unit
RCVD	Received
REC	Receive
RF	Radio Frequency
RPTNC	Reverse Polarity TNC
RX	Receive
SA	System Administrator
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
SEN	Small Extension Node
SIDPERS-3	Standard Installation/Division Personnel System-3
SINGARS	Single Channel Ground and Airborne Radio System
SIPRNET	Secure Internet Protocol Router Network
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedures
SPI	Stateful Packet Inspection
SPBS-R	Standard Property Book System - Redesign

SRU	System Replaceable Unit
SSID	Service Set Identification
SSA	Supply Support Activity
SSR	System Support Representative
STAMIS	Standard Army Management Information Systems
SUI	Sensitive Unclassified Information
SUM	Software User Manual
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/IP	Transmission Control Protocol/Internet Protocol
TFSA	Task Force Support Area
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TM	Technical Manual
TNS	Tactical Name Service
TPN	Tactical Packet Network
TRI-TAC	Tri-services Tactical
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
VDC	Voltage Direct Current
VEE	Virtual End-to-End
WAN	Wide Area Network
WEP	Wired Equivalent Privacy

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

QUICK CONFIGURATION GUIDE



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 07703-5000.
DESTRUCTION NOTICE – Destroy by any method that will prevent disclosure of contents or reconstruction of this document.

CAISI QUICK CONFIGURATION GUIDE

HEADQUARTERS, DEPARTMENT OF THE ARMY

APRIL 2003

**QUICK CONFIGURATION GUIDE
TABLE OF CONTENTS**

CONFIGURE NOTEBOOK COMPUTER, WIRED/BUILT-IN NIC & WIRELESS NIC4

Notebook Computer Configuration 4

Configuration Properties for the Wired NIC or Built-In NIC 5

Configuration Properties for the Wireless NIC 6

Air Fortress Remote Client for use with the wireless NIC 7

QUICK CONFIGURATION PROCEDURES USING CAISI ADMIN8

Set up Linksys Router BEFSR41/81 (Firmware 2.40.2) 8

Perform Linksys Router Connection Procedures..... 8

Configure the Linksys Router Device 8

Add Option Method 9

Device Wizard Method 11

Send the Configuration to the Linksys Router..... 13

Perform Disconnection Procedures..... 13

QUICK CONFIGURATION: SET UP OF A CBM USING CAISI ADMIN14

Perform CBM Wireless Bridge Connection Procedures 14

Configure the CBM Wireless Bridge Device 14

Add Option Method 14

Device Wizard Method 17

Send the Configuration to the CBM Wireless Bridge 19

Perform Disconnection Procedures..... 20

Perform CBM Inline Encryptor Connection Procedures 21

Configure the CBM Inline Encryptor 21

Add Option Method 21

Device Wizard Method 23

Send the Configuration to the Inline Encryptor 24

Perform Disconnection Procedures..... 25

QUICK CONFIGURATION: SET UP OF A CCM USING CAISI ADMIN26

Perform CCM Multi-client Radio Adapter Connection Procedures..... 26

Configure the CCM 340 Radio Device..... 26

Add Option Method 26

Device Wizard Method 29

Send the Configuration to the Multi-Client Radio Adapter 31

Perform Disconnection Procedures..... 32

QUICK CONFIGURATION PROCEDURES USING MANUAL TOOLS & UTILITIES

.....**32**

QUICK CONFIGURATION: SET UP A CBM USING MANUAL PROCEDURES ..32

Configure the CBM Wireless Bridge Using Manual Procedures32

Perform CBM Wireless Bridge Connection Procedures32

Configure the CBM Wireless Bridge32

Disable Remote Access to the Bridge.....37

Verify the Wireless Bridge is Operational with your Network.....37

Perform Disconnection Procedures.....37

Configure A CBM Encryptor38

Perform Encryptor Connection Procedures38

Configure the Encryptor through the Serial Port38

Perform Disconnection Procedures.....41

QUICK CONFIGURATION: SET UP OF A CCM USING MANUAL PROCEDURES

.....**42**

Configure A CCM Multi-Client Radio Adapter Using Manual Procedures.....42

Perform Multi-Client Radio Adapter Connection Procedures.....42

Configure the CCM Multi-Client Radio Adapter.....42

Verify the Multi-Client Radio Adapter is Operational with your Network.....45

Disable Remote Access to the Multi-client Radio Adapter45

Perform Disconnection Procedures.....46

Configure a CCM Encryptor46

1. CONFIGURE NOTEBOOK COMPUTER, WIRED/BUILT-IN NIC & WIRELESS NICs

1) Notebook Computer Configuration

- a) Verify your notebook computer has the current baseline loaded.
 - i) If the CAISI configuration baseline is **not loaded** or needs to be restored perform the following procedures:
 - (1) Ensure notebook computer is powered on.
 - (2) Insert installation CD #1 into the CD disk drive.
 - (3) Shutdown notebook computer.
 - (4) Turn the notebook power on. The computer will reboot.
 - (5) At the “Startup” menu, select “**Option 1-Load CAISI Image to Hard Drive**” and press the <Enter> key.
 - (6) When prompted, “insert next media”, remove CD #1 and replace it with CD #2.
 - (7) Wait 15 seconds for the disk to spin up and then press the <Enter> key. The load will resume.
 - (8) When CD #2 install is complete, the installation screen will clear and a message will inform you that the load is complete.
 - (9) Remove CD #2 and close drive.
 - (10) Reboot the CAISI notebook. **Ctrl-Alt-Delete**
 - (11) When prompted enter the username and password, the CAISI defaults are **caisadmin** and **BS_69dlw**.
 - (12) A message will inform you that Windows has finished installing new device, it will prompt you to restart the computer, Click “**Yes**”.
 - ii) If the CAISI configuration baseline **is loaded**, and you need to change the name of the notebook proceed as follows.

NOTE: *The name of the computer and IP needs to be unique if used on the same network.*

- (1) Log on to the notebook, using the default administrator account. The username is **caisadmin** and the password is **BS_69dlw**.
- (2) Answer “**No**” when asked if you want to change the password.

NOTE: *Answer “No” only during class instruction. Change your usernames and passwords according to your security officer.*

- (3) Right-click on “**My Computer**”.
- (4) Choose “**Properties**”.
- (5) Click on the “**Network Identification**” tab.
- (6) Click on the “**Properties**” button.
- (7) Change the Computer name as appropriate for your network.
- (8) Change the Workgroup as appropriate for your network.

- (9) Click on the “**More**” button to enter your primary fully qualified DNS domain name. An example of a fully qualified DNS domain name will be caisi.army.mil.
- (10) Enter your primary fully qualified DNS domain name.
- (11) Click “**OK**” on the “DNS suffix” pop-up screen.
- (12) Click “**OK**” on the “Identification Changes” pop-up screen.
- (13) Click on the “**Start**” button on the system task bar, then select “**Shut Down**” and click on the “**OK**” button when the shutdown screen pops up.

2) Configuration Properties for the Wired/Built-In NIC.

- a) To configure the Network Parameters for the wired NIC or built-in NIC:
 - i) Ensure only the wired NIC is inserted in the PCMCIA slot. (Only wired NIC)
 - ii) Power on the CAISI notebook.
 - iii) Log on to the notebook. The CAISI default username is **caisadmin** and the password is **BS_69dlw**.
 - iv) Right-click on “**My Network Places**”.
 - v) Choose “**Properties**”.
 - vi) Right-click on the “**CardBus II 10_100**” or “**Built-In Ethernet**” network card icon.
 - vii) Choose “**Properties**”.
 - viii) Select “**Internet Protocol (TCP/IP)**”.
 - ix) Click on the “**Properties**” button.
 - x) Select “**Use the following IP address**” and then enter:
 - (1) IP address CAISI default=192.168.1.2
 - (2) Subnet mask CAISI default=255.255.0.0
 - (3) Default Gateway CAISI default=192.168.1.1
 - xi) Select “**Use the following DNS server addresses**” and then enter:
 - (1) Preferred DNS server CAISI default=138.27.4.15
 - (2) Alternate DNS server.

NOTE: *If you left the default private IP address, a pop-up box will inform you that the address is the same as the wired NIC or Built-In NIC. It asks if you want to enter a different IP.*

- xii) You need to:
 - (1) Click on the “**No**” button when it asks you if you want a different IP address.
 - (2) Click on the “**OK**” button on the Properties screen.
 - (3) Exit out of the “Network and Dial-up Connections” window

NOTE: *Only users with a Wired NIC need to do steps xiii – xv.*

- xiii) Click the NIC card icon on the menu tray at the bottom of the notebook screen.
- xiv) Click “**Stop Xircom CreditCard Ethernet Adapter 10/100.**”
- xv) At the “Safe to remove hardware” message prompt, click “**OK**”.
- xvi) Reboot the computer.

3) Configuration Properties for the Wireless NIC.

- a) To configure the Network Parameters for the wireless NIC:
 - i) Ensure only the wireless NIC is inserted in the PCMCIA slot.
 - ii) Power on the CAISI Notebook.
 - iii) Log on to the notebook, The CAISI default username is **caisiadmin** and the password is **BS_69dlw**.
 - iv) Right-click on “**My Network Places**”.
 - v) Choose “**Properties**”.
 - vi) Right-click on the “**Cisco**” network card icon.
 - vii) Choose “**Properties**”.
 - viii) Select “**Internet Protocol (TCP/IP)**”.
 - ix) Click on the “**Properties**” button.
 - x) Select “**Use the following IP address**” and then enter:
 - (1) IP address CAISI default=192.168.1.251
 - (2) Subnet mask CAISI default=255.255.0.0
 - (3) Default Gateway CAISI default=192.168.1.1
 - xi) Select “**Use the following DNS server addresses**” and then enter:
 - (1) Preferred DNS server CAISI default=138.27.4.15
 - (2) Alternate DNS server.

NOTE: *If you left the default private IP address, a pop-up box will inform you that the address is the same as the wired/built-in NIC. It asks if you want to enter a different IP.*

- xii) You need to:
 - (1) Click on the “**No**” button when it asks you if you want at different IP address
 - (2) Click on the “**OK**” button on the “Properties” screen.
 - (3) Exit out of the “Network and Dial-up Connections” window
 - (4) Click on the “**CAISI Toolbox**” icon on the task bar or the “Start” menu.
 - (5) Select the “**Aironet Client Encryption Manager**” (CEM) tool.
 - (6) Enter the default password, **Cisco**.
 - (7) Click on the “**OK**” button.
 - (8) Select “**Commands**”.
 - (9) Select “**Change Password**”.
 - (10) Enter a new password.
 - (11) Make sure to write it down, seal it in an envelope and give it to your security officer.
 - (12) Select “**Commands**”.
 - (13) Select “**Enter WEP key**”.
 - (14) Select the 128 bit key size
 - (15) In the “WEP Key 1” field, enter the new 26-character WEP key provided by the CSS S6. The CAISI default is 0123456789abcdef0123456789
 - (16) Click on the “**OK**” button.

NOTE: *You must change this field. Do not use the CAISI default WEP key and make sure the key you assign the NIC is a 128-bit key and not a 40-bit key.*

- (17) Close the CEM tool.

- (18) Select the “**Aironet Client Utility**” (ACU) tool from the CAISI Toolbox.
- (19) Select “**Commands**”.
- (20) Select “**Edit Properties**”.
- (21) Enter your assigned host name in the “Client Name” field. The CAISI default is Caisi000pc.
- (22) Enter your assigned SSID in the “SSID1” field. The CAISI default is caisi000.
- (23) Click on “**Network Security**”.
- (24) Ensure WEP is enabled.
- (25) Ensure level of security is set to “**open**”.
- (26) Click “**OK**”.
- (27) Close the ACU tool.
- (28) Click the NIC card icon on the menu tray at the bottom of the notebook screen.
- (29) Select the wireless NIC and click on the “**Stop Cisco Systems 340 Series Wireless LAN Adapter**” button.
- (30) At the “Safe to remove hardware” message prompt, click “**OK**”.
- (31) Reboot the computer.

4) **Air Fortress Remote Client (for use with the wireless NIC)**

- a) To configure the Parameters for the Air Fortress remote client:
 - i) Look in the system tray for the small padlock icon. When you are in secure mode, the icon will be a locked padlock. When you are non-secure, it will be unlocked.
 - ii) Double-click on the icon and the Air Fortress Client screen will appear.
 - iii) Click on the “**Utilities**” menu and select “**Update Access ID**”. A dialog box will pop up, asking for your administrator’s password. The CAISI default is “**fortress**”.
 - iv) An AccessID dialog will pop up. Enter the old key in the “current” field. **0123456789abcdef** is the default on the encryptors coming from Tobyhanna. If the encryptor is new from the factory, enter the word **default** instead.
 - v) Enter your network’s preshared Access ID key in both the “new” and “confirm” fields. It must be 16 hexadecimal digits and must match the one you entered in the AF-1100s.
 - vi) Click “**OK**”. You will get a message saying that the AccessID was set and instructing you to please reset the device. Click “**OK**”.
 - vii) Click on the “**Utilities**” menu and select “**Reset Connections**” then “**All Entries**”.
 - viii) To change the administrator’s password, click on the “**Configure Password**” button. Enter and confirm the new password. Write it down and turn it in for safekeeping. If you lose the password, reinstalling the client is not enough to reset it – you’d need to reload the notebook from CD.
- b) To turn the Air Fortress remote client on or off:
 - i) Look in the system tray for the small padlock icon.
 - ii) Double-click on the icon and the Air Fortress Client screen will appear.
 - iii) On the “General” tab, select encryption “**On**” if you are going to use your wireless NIC to get onto the SBU CAISI network. If you are going to troubleshoot the wireless network or if you are going to use the wired/built-in NIC instead of the wireless NIC, turn encryption “**Off**”.

NOTE: *You must have encryption turned off any time you use the wired NIC or built-in NIC. If you are having trouble communicating, check the Air Fortress Remote Client icon.*

NOTE: *You must have encryption turned on any time you use the wireless NIC (the Cisco) to access the CAISI LAN.*

2. QUICK CONFIGURATION PROCEDURES USING THE CAISI ADMIN APPLICATION

2.1 Set Up of Linksys Router BEFSR41/81 (Firmware 2.40.2)

A standard CAISI SSR notebook, configured as follows is required for router configuration.

- It 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 or built-in network card installed. Its wireless network card *must not* be installed.

Version 1 has an uplink switch for port 8. Port 8 can be used for crossover “X” or straight-through “=” connections. Power supply consists of a power adapter and a 3-prong power cord.

Version 2 has an automatic senser for crossover or straight-through connections, therefore all 8 ports can be used for connection. Power supply consists of a wall-style power adapter.

1) Perform Linksys Router connection procedures:

- a) Connect your laptop NIC to the router using a white straight-through Ethernet cable into LAN port 1. (Any port).
- b) ONLY Version 1 router. Alternatively, use a red crossover cable connected to port 8, with the uplink switch set to crossover mode where “straight” (“=”), “crossover” (“X”). The uplink switch is located next to the power cord input at the back of the router. Do not connect to the WAN port.

2) Configure the Linksys Router device.

- a) Reset the router to factory settings

Version 1

1. Insert the tip of the reset tool into the reset buttonhole on the back of the router and hold for 15 seconds.
2. During this process the "**Diag**" light will light up, the "**Link**" light will light up momentarily, then both lights will go off, and the router will now be reset.
3. If the green “**Link**” light does not flash, try again.

Version 2

1. Insert the tip of the reset tool into the reset buttonhole on the back of the router and observe the following:
2. The "**Diag**" light will light up red, all of the LEDs on the "100" level will blink twice, then all of the LEDs on the "Full/Col" level will blink twice, then all of the LEDs on the "Link/Act" level will blink twice. The "Diag" LED will then go out. The router will now be reset.
3. If the "**Diag**" light does not go out, try again.

NOTE: *Both lights are located on the right front panel of the router.*

- b) At the bottom of the SSR notebook screen, click on ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear. Click on the "**CAISI Admin**" menu selection.
- c) To configure the Router choose one of the following configuration methods: Select either the 1) "Add" option or 2) "Device Wizard" option from the "Device" drop down menu.
 - i) **"Add" Option Method.**
 1. Select "**Device**" from the CAISI Admin menu and then select "**Add**" from the "**Device**" drop-down menu. Set "**DNS Hostname:**" (Where "DNS Hostname:" = the host name of the router) to the name provided by your DOIM, S6 or CSSAMO. The CAISI default is **caisirouter**.
 2. Create a "**Device Name:**" if you want it to be different from the "DNS Hostname." From the "**Template**" drop-down menu select **caisirouter-DHCP** or **caisirouter-nonDHCP**, as prescribed by your DOIM, S6 or CSSAMO. These settings apply to the WAN side of the router.
 3. For classroom training, set "Template" to **caisirouter-nonDHCP** from the drop down menu.
 4. Click on the "**Edit Properties**" button. The "**Device Properties**" screen will appear with the "**General**" tab selected.
 - (a) Set the "**Administrative Password**" to the password provided by your DOIM, S6 or CSSAMO.
 - (b) Click on the "**Change**" button. The Set Password screen will appear.
 - (c) Enter your new password in the "**Enter Password**" dialog box.
 - (d) For classroom training, set the password to the CAISI default "**system**".

NOTE: *As you enter the password, asterisks will appear. The password is not shown in the clear. You must change the password before you deploy the router.*

- (e) Press on the <Tab> key and confirm the new password by entering the password in the "**Confirm Password**" dialog box.
- (f) Click on the "**OK**" button.

NOTE: *Until you actually send the configuration to the router, the administrative password field may indicate “empty” even though you entered it earlier. If you have previously sent this configuration to the router, it will indicate a status of “set”. However, the application does not store user names or passwords. They are cached during the current session, but are lost as soon as you exit from the application. An asterisk to the left of the field name indicates that the password is cached. If there is no asterisk, you must reenter the password.*

- (g) If you have made changes to values on the “**General**” tab, click on the “**Apply**” button.
5. Click on the “**Network**” tab.
 - (a) If you selected **caisirouter-nonDHCP** perform the following procedure, otherwise you may skip to (5) (d).
 - (b) Click on the “**Validate**” button.
 - (i) If the IP Address is unique, click on the “**OK**” button when prompted.
 - (ii) If the IP Address is not unique, a list box will pop up to show you the other device configurations that use that address. Click on the “**OK**” button to dismiss the list box. If necessary, enter a new IP Address.
 - (c) Validate or change the following settings in the “**Use the following Network Settings**” as assigned by your DOIM or S6.
 - (i) IP Address: (**172.16.1.2** CAISI Default)
 - (ii) Subnet Mask: (**255.255.255.0** CAISI Default)
 - (iii) Gateway: (**192.168.1.1** CAISI Default)
 - (iv) Domain: (**caisi.army.mil** CAISI Default)
 - (v) First DNS: (**138.27.4.15** CAISI Default)
 - (vi) Second DNS and Third DNS: (**0.0.0.0** CAISI Default)
 - (vii) If you have made changes within this tab, click on the “**Apply**” button and proceed to Step (6).
 - (d) Verify that the “**Obtain network settings automatically (DHCP)**” box is selected.
 6. Click on the “**Details**” tab.
 - (a) “**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience.
 - (b) If you make changes to values on the “**Details**” tab, click on the “**Apply**” button.
 7. Click on the “**Advanced**” tab.
 - (a) Validate or change the following settings as assigned by your DOIM, S6 or CSSAMO.
 - (i) Private IP Address: (**192.168.1.1** CAISI Default)
 - (ii) Private Subnet Mask: (**255.255.255.0** CAISI Default)
 - (iii) Enable DHCP Serving: (**box is checked** CAISI Default)
 - (iv) From: (**192.168.1.100** CAISI Default)
 - (v) To: (**192.168.1.249** CAISI Default)

- (vi) Port Forwarding: (**no values assigned** CAISI Default)
 - (vii) If you have made changes within this tab, click on the “**Apply**” button.
8. Click on the “**OK**” button. The main CAISI Admin screen will appear where you should see the new device-with the name you assigned it. The CAISI default is “**caisirouter**”.
 9. Proceed to procedure **d) Send the configuration to the router on page 13**.

ii. **“Device Wizard” Method**

1. Select “**Device**” from the CAISI Admin menu and then select “**Device Wizard**” from the “**Device**” drop-down menu.
2. Set the “**Device Type**” button to **Linksys BEFSR41/81**.
3. Click on the “**Next>**” button.
4. Set the “**Network Type**” to **Mixed Network**.
5. Click on the “**Next>**” button.
6. Set “**DNS Hostname:**” (Where “**DNS Hostname:**” = the host name of the router) to the name provided by your DOIM, S6 or CSSAMO. The CAISI default is **caisirouter**.
7. Create a “**Device Name:**” if you want it to be different from the “**DNS Hostname.**”
8. From the “**Template**” drop-down menu select **caisirouter-DHCP** or **caisirouter-nondHCP**, as prescribed by your DOIM, S6 or CSSAMO. These settings apply to the WAN side of the router.
9. For classroom training, set “**Template**” to **caisirouter-nondHCP** from the drop down menu.
10. Click on the “**Next>**” button.

<p>NOTE: <i>The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited.</i></p>
--

11. The “**New Device Wizard Network Settings**” screen will appear. If you selected **caisirouter-nondHCP** perform the following procedure, otherwise you may skip to step **(11) (c)**.
 - (a) Click on the “**Validate**” button.
 - (i) If the IP Address is unique, click the on the “**OK**” button when prompted.
 - (ii) If the IP Address is not unique, a list box will pop up to show you the other device configurations that use that address. Click on the “**OK**” button to dismiss the list box. If necessary, enter a new IP Address.
 - (b) Validate or change the following settings in the “**Use the following Network Settings**” as assigned by your DOIM, S6 or CSSAMO.

- (i) IP Address: **(172.16.1.2 CAISI Default)**
 - (ii) Subnet Mask: **(255.255.255.0 CAISI Default)**
 - (iii) Gateway: **(192.168.1.1 CAISI Default)**
 - (iv) Domain: **(caisi.army.mil CAISI Default)**
 - (v) First DNS: **(138.27.4.15 CAISI Default)**
 - (vi) Second DNS and Third DNS: **(0.0.0.0 CAISI Default)**
 - (vii) Click on the “**Next>**” button and proceed to Step 12.
- (c) Verify that the “**Obtain network settings automatically (DHCP)**” box is selected and click on the “**Next>**” button.
12. The “**New Device Wizard Linksys Advanced Settings**” screen will appear.
- (a) Click on the “**Validate**” button.
 - (i) If the IP Address is unique, click on the “**OK**” button when prompted.
 - (ii) If the IP Address is not unique a list box will pop up to show you the other device configurations that use that address. Click on the “**OK**” button to dismiss the list box. If necessary, enter a new IP Address, subnet mask, or both.
 - (b) Validate or change the following settings as assigned by your DOIM, S6 or CSSAMO.
 - (i) Private IP Address: **(192.168.1.1 CAISI Default)**
 - (ii) Private Subnet Mask: **(255.255.255.0 CAISI Default)**
 - (iii) Enable DHCP Serving: **(box is checked CAISI Default)**
 - (iv) From: **(192.168.1.100 CAISI Default)**
 - (v) To: **(192.168.1.249 CAISI Default)**
 - (vi) Port Forwarding: **(no values assigned CAISI Default)**
 - (vii) Click on the “**Next>**” button.
13. The “**New Device Wizard Device Details**” screen will appear.
- (a) “**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience.
 - (b) Click on the “**Next>**” button.
14. The “**New Device Wizard Password Validation**” screen will appear.
- (a) Set the “**Administrative Password**” to the password provided by your DOIM, S6 or CSSAMO.
 - (i) Enter the password in the “**Administrative (Write) Password:**” box.
 - (ii) For classroom training, set the password to the CAISI default “**system**”.

NOTE: *As you enter the password, asterisks will appear. The password is not shown in the clear. You must change the password before you deploy the router.*

- (iii) Press on the “**Tab**” key and confirm the new password by entering the password in the “**Confirm Administrative (Write) Password:**” box.
 - (iv) Click on the “**Finish**” button.
15. The “**CAISI Admin New Device Wizard**” screen will appear. Select “**Done. No further action**” in the “Next step” box.
- (a) Click on the “**OK**” button.
 - (b) The main CAISI Admin screen will appear where you should see the new device- with the name you assigned it. The CAISI default is “**caisirouter**”.
16. Proceed to procedure **d) Send the configuration to the router.**

d) Send the configuration to the router.

- (i) Highlight the newly created device. The CAISI default is **caisirouter**.
- (ii) Select “**Device**” from the CAISI Admin toolbar and then select “**Properties**” from the from the “Device” drop-down menu.
- (iii) Click on the “**Send Configuration**” button.
- (iv) Select the “**Configure using IP Address:**” button and set the IP Address to the address you assigned the router. The CAISI default is **192.168.1.1**
- (v) Click on the “**Start**” button on the “**Configure Device**” screen.
- (vi) If the “**Enter Password**” screen appears, enter the password you assigned to the router. The CAISI default is “**system**”.
- (vii) Click on the “**OK**” button.
- (viii) Click on the “**OK**” button when the “**The device has been configured successfully**” message appears.
- (ix) Click on the “**Done**” button on the “**Configure Device**” screen.
- (x) Click on the “**OK**” button on the “**Device Properties**” screen.
- (xi) The Router is now configured.

<p>NOTE: <i>Ensure you save the device before exiting CAISI Admin.</i></p>

3) **Perform disconnection procedures.**

- a) Disconnect the straight-through Ethernet cable from the NIC on the SSR laptop.

2.2 QUICK CONFIGURATION: SET UP OF A CBM

2.2.1 Configure a CBM Wireless Bridge using CAISI Admin (Firmware V12.01T)

A standard CAISI SSR notebook, configured as follows is required for wireless bridge configuration.

- It 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**.
- Wired NIC or Built-in NIC must be used. Its wireless network card *must not* be installed.

1) **Perform CBM wireless bridge connection procedures.**

- a) Disconnect the red crossover cable from the port labeled “Encrypted” on the back of the encryptor.
- b) Remove the RJ-45 straight-through adapter and a straight-through Ethernet cable from your SSR Accessory Kit 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 NIC.
- e) You are now connected from your NIC to the “Network” port on the power injector.

NOTE: *If you connect to the “AP/Bridge” port, you can damage your 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.*

NOTE: *If the wireless bridge is not installed in a CBM, connect a white straight-through Ethernet cable from the “AP/Bridge” port on the Ethernet power injector to the “Inline Power Ethernet” port on the bridge.*

- f) Connect the blue straight-through nine pin serial cable from your laptop serial port to the serial port on the wireless bridge.
- g) Connect an antenna to the CBM.
- h) Ensure you connect the power cord to the wireless bridge power supply.

2) **Configure the CBM wireless bridge device**

- a) At the bottom of the SSR notebook screen, click on ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear. Select “**CAISI Admin**”.
- b) To configure the wireless bridge, choose one of the following configuration methods: Select either the 1) “**Add**” option or 2) “**Device Wizard**” option from the “Device” drop down menu.
 - i) **“Add” Option Method.**
 - (1) Select “**Device**” from the CAISI Admin toolbar and then select “**Add**” from the “**Device**” drop-down menu.

- (2) Set “**DNS Hostname:**” (Where “DNS hostname” = the host name of the wireless bridge) to the name provided by your DOIM, S6 or CSSAMO. The CAISI defaults are “**CBM-350r**” for a root bridge and “**CBM-350nr**” for a non-root bridge.
- (3) Create a “**Device Name:**” if you want it to be different from the “DNS Hostname:”
- (4) From the “**Template**” drop-down menu select **CBM-350-root** if the radio is designated a “root” or **CBM-350-nonroot** if the radio is designated a repeater.

NOTE: *The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited.*

- (5) Click on the “**Edit Properties**” button. The “**Device Properties**” screen will appear with the “**General**” tab selected.
- (6) Verify the “**Device Name**” (the host name you assigned the wireless bridge) is correct. The CAISI defaults are “**CBM-350r**” for a root bridge and “**CBM-350nr**” for a non-root bridge.
 - (a) To set the “**User Name:**”, click on the “**Change**” button.
 - (i) Enter your new User Name into the “**Enter User Name:**” dialog box.
 - (ii) The CAISI default is “**root**”.

NOTE: *You must change the User name before you deploy the radio.*

- (iii) Click on the “**OK**” button.
 - (b) Set the “**Administrative Password**” to the password provided by your DOIM, S6 or CSSAMO.
 - (i) Click on the “**Change**” button. The Set Password screen will appear.
 - (ii) Enter your new password in the “**Enter Password**” dialog box.
 - (iii) For classroom training, set the password to the CAISI default “**system**”.

NOTE: *As you enter the password, asterisks will appear. The password is not shown in the clear. You must change the password before you deploy the radio.*

- (iv) Press on the <Tab> key and confirm the new password by entering the password in the “**Confirm Password**” dialog box.
 - (v) Click on the “**OK**” button.
 - (c) Set the “**Access Password**” to the password provided by your DOIM, S6 or CSSAMO.
 - (i) Click on the “**Change**” button. The Set Password screen will appear.
 - (ii) Enter your new password in the “**Enter Password**” dialog box.
 - (iii) For classroom training set the password, to the CAISI default “**access**”.
 - (iv) Press on the <Tab> key and confirm the new password by entering the password in the “**Confirm Password**” dialog box.
 - (v) Click on the “**OK**” button.

- (d) If you have made changes to values on the “**General**” tab, click on the “**Apply**” button.

NOTE: *Until you actually send the configuration to the radio, the administrative password and access password fields may indicate “empty” even though you entered it earlier. If you have previously sent this configuration to the radio, it will indicate a status of “set”. However, the application does not store user names or passwords. They are cached during the current session, but are lost as soon as you exit from the application. An asterisk to the left of the field name indicates that the password is cached. If there is no asterisk, you must reenter the password.*

- (7) Click on the “**Network**” tab.
 - (a) Select “**Use the following Network Settings**” and enter the following parameters as assigned by your DOIM, S6 or CSSAMO.
 - (i) IP Address: (**192.168.1.3** root or **192.168.1.4** non-root CAISI Default)
 - (ii) Subnet Mask: (**255.255.255.0** CAISI Default)
 - (iii) Gateway: (**192.168.1.1** CAISI Default)
 - (iv) Domain: (**leave blank** or **Warning.US.Government** CAISI Default)
 - (v) First DNS: (**leave at 0.0.0.0**)
 - (vi) Second DNS and Third DNS: (**leave at 0.0.0.0**)

NOTE: *Since there is not a DHCP server on the Untrusted Network (the radio portion of the network is on the “Encrypted” side of the encryptors and cannot see any host or server on the “Unencrypted” side), the user is advised not to select “**Obtain network settings automatically (DHCP).**”*

- (b) Click on the “**Validate**” button.
 - (i) If the IP Address is unique, click on the “**OK**” button when prompted.
 - (ii) If the IP Address is not unique, a list box will pop up to show you the other device configurations that use that address. Click on the “**OK**” button to dismiss the list box. If necessary, enter a new IP Address, subnet mask, or both.
- (c) If you have made changes to values on the “**Network**” tab, click on the “**Apply**” button.
- (8) Click on the “**Details**” tab.
 - (a) “**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience.
 - (b) If you have made changes to values on the “**Details**” tab, click on the “**Apply**” button.

- (9) Click on the “**Advanced**” tab.
 - (a) Enter your unit specific SSID. The CAISI default for hardware testing and classroom training is “**caisi000**”. *You must change the SSID before deploying the bridge.*
- (10) Set the radio mode to “**root**” if the radio is designated a “root” or click on “**non-root**” if the radio will serve as a repeater.
 - (a) Set “**Distance to farthest node**” to the approximate distance, in kilometers, of your longest expected radio link anywhere in the network. The CAISI default is set to **6**.
 - (b) Verify “**Center Frequency**” is set to “**auto**”. OCONUS countries may require a different frequency, check with your local frequency manager upon arrival.
 - (c) Verify “**Broadcast Power**” is set to “**100**”. OCONUS countries may require you to lower power setting, check with your local frequency manager upon arrival.
 - (d) Under “**Privacy Encryption Keys**”, click on the “**Set Key 1**” button.
 - (e) Click on “**Long 26 digits**”. (Do not use short key.)
 - (f) Under “**Enter Key**”, enter your 26 digit hexadecimal encryption key.
 - (g) The CAISI default is **0123456789abcdef0123456789** for hardware testing and classroom training. *You must change the key before deploying the bridge.*
 - (h) Confirm the key by re-entering it into the “**Confirm Key**” field. Click on the “**OK**” button.
 - (i) If you have made changes within this tab, click on the “**Apply**” button and then click on the “**OK**” button.
- (11) The main CAISI Admin screen will appear where you should see the new device with the name you assigned it. The CAISI defaults are “**CBM-350r**” for a root bridge and “**CBM-350nr**” for a non-root bridge.
- (12) Proceed to procedure **c)**. **Send the configuration to the wireless bridge on page 19.**

ii) **Device Wizard** Method

- (1) Select “**Device**” from the CAISI Admin menu and then select “**Device Wizard**” from the “**Device**” drop-down menu.
- (2) Set the “**Device Type**” button to **Cisco Aironet 350**. Click on the “**Next>**” button.
- (3) Set the “**Network Type**” to **Mixed Network**. Click on the “**Next>**” button.
- (4) Set “**DNS Hostname**” to “**CBM-350r**” for a root bridge or “**CBM-350nr**” for a non-root bridge.
- (5) Create a “**Device Name:**” if you want it to be different from the “**DNS Hostname:**”
- (6) From the “**Available Device Templates**” drop-down menu, select **CBM-350-root** if the radio is designated a “root” or **CBM-350-nonroot** if the radio is designated a repeater. Click on the “**Next>**” button.

NOTE: *The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited.*

- (7) From the “**Use the following Network Settings**” enter the following parameters as assigned by your DOIM, S6 or CSSAMO.
 - (a) IP Address: (**192.168.1.3** root or **192.168.1.4** non root CAISI Default)
 - (b) Subnet Mask: (**255.255.255.0** CAISI Default)
 - (c) Gateway: (**192.168.1.1** CAISI Default)
 - (d) Domain: (**leave blank or Warning.US.Government** CAISI Default)
 - (e) First DNS: (**leave at 0.0.0.0**)
 - (f) Second DNS and Third DNS: (**leave at 0.0.0.0**)
- (8) Click on the “**Validate**” button.
 - (a) If the IP Address is unique, click on the “**OK**” button when prompted.
 - (b) If the IP Address is not unique, a list box will pop up to show you the other device configurations that use that address. Click on the “**OK**” button to dismiss the list box. If necessary, enter a new IP Address, subnet mask, or both.
 - (c) Click on the “**Next>**” button.
- (9) Enter your unit specific SSID. The CAISI default for hardware testing and classroom training is “**caisi000**”. **You must change the SSID before deploying the bridge.**
- (10) Set the radio mode to “**root**” if the radio is designated a “root” or click on “**non-root**” if the radio will serve as a repeater.
- (11) Verify “**Center Frequency**” is set to “**auto**”. OCONUS countries may require a different frequency, check with your local frequency manager upon arrival.
- (12) Verify “**Broadcast Power**” is set to “**100**”. OCONUS countries may require you to lower power setting, check with your local frequency manager upon arrival.
- (13) Under “**Privacy Encryption Keys**”, click on the “**Set Key 1**” button then click on “**Long 26 digits**”. (**Do not use short key.**)
 - (a) Under “**Enter Key**”, enter your 26 digit hexadecimal encryption key. The CAISI default is **0123456789abcdef0123456789** for hardware testing and classroom training. **You must change the key before deploying the bridge.**
 - (b) Confirm key by re-entering into the “**Confirm Key**” field. Click on the “**OK**” button.
 - (c) If a value has been changed, click on the “**OK**” button.
- (14) Click on the “**Next>**” button.
- (15) The “**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience. Click on the “**Next>**” button.
- (16) Enter your new User Name into the “**User Name:**” box. (The CAISI default is “**root**”. **Note: you must change it before you deploy the radio.**)

- (17) Enter your new password in the “**Administrative (Write) Password:**” box and then reenter your password into the “**Confirm Administrative (Write) Password**” box. The CAISI default is “**system**”.

NOTE: *As you enter the password, asterisks appear. The password is not shown in the clear. **You must change the password before deploying the bridge.** You must change the password before you deploy the radio.*

- (18) Click on the “**Finish**” button.
- (19) A dialog box will appear, click on the “**Done. No further action**” button.
- (20) Click on the “**OK**” button.
- (21) The main CAISI Admin screen will appear where you should see the new device with the name you assigned it. The CAISI default is “**CBM-350r**” for a root bridge.
- (22) Proceed to procedure c) **Send the configuration to the wireless bridge.**
- c) **Send the configuration to the wireless bridge.**
- i) Highlight the device you just created from the main screen. The CAISI defaults are “**CBM-350r**” for a root bridge and “**CBM-350nr**” for a non-root bridge.
- ii) Select “**Device**” from the CAISI Admin toolbar and then select “**Properties**” from the “Device” drop-down menu.
- iii) Click on the “**Send Configuration**” button.
- iv) Select the “**Configure using serial port**” button.
- v) Click on the “**Start**” button on the “**Configure Device**” screen.
- vi) At the “**Do you want to reset the device to factory defaults at this time**” prompt, click on the “**Yes**” button.
- vii) The “**Please COLD RESTART the device by power cycling the unit.**” prompt will appear.
- (1) At this time, physically disconnect either the white Ethernet cable attached to the “**To AP/Bridge**” port on the CBM radio's power injector or the power cord into the bridge's power adapter. Reconnect it. This will perform a Cold Restart of the CBM radio.
- (2) Click on the “**OK**” button on the screen prompt immediately after performing this process.

NOTE: *Do not wait for the bridge to finish rebooting before clicking the on “**OK**” button.*

- viii) After the CBM radio reboots and restarts (approximately 4 1/2 minutes, the prompt “**The Aironet 350 has been reset to factory defaults**” will appear. Click on the “**OK**” button.

NOTE: *To see what the wireless bridge is doing when it is resetting, press the <Ctrl> <Shift> keys to bring up the output debug window.*

- ix) If the User Name has not been entered previously, the “**Set User Name**” entry box will appear. If the box doesn't appear, then skip this step.
 - (1) Enter the assigned User Name that your DOIM, S6 or CSSAMO has assigned.
 - (2) The CAISI default is “**root**”. Click on the “**OK**” button when completed. The CBM radio will now start to be configured.
- x) When the Windows dialog box appears stating the “The device has been configured successfully”, click on the “**OK**” button.
- xi) Click on the “**Done**” button on the “**Configure Device**” screen.
- xii) Click on the “**OK**” button on the “Device Properties” screen.

<p>NOTE: <i>Ensure you save the device before exiting CAISI Admin.</i></p>

3) **Perform disconnection procedures.**

- a) Disconnect the standard serial cable from the serial port on the CBM wireless bridge and the serial port on the laptop.
- b) Disconnect the white straight-through cable from the NIC and the RJ-45 straight-through adapter.
- c) Disconnect the red crossover cable from the RJ-45 straight-through adapter.
- d) Re-attach the red crossover Ethernet cable to the “Encrypted” port on the back of the encryptor.

2.2.2 Configure a CBM Encryptor Using CAISI Admin (Firmware 1178W)

A standard CAISI SSR notebook, configured as follows is required for the Inline Encryptor configuration.

- It 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**.
- Wired NIC or Built-in NIC must be used. Its wireless network card *must not* be installed.

1) Perform CBM Inline Encryptor Connection Procedures.

- a) Plug one end of a straight-through cable into the CBM hub and the other end to the NIC.
- b) Connect the beige crossover nine-pin serial cable from your laptop serial port to the serial port on the inline encryptor.
- c) Ensure you connect the power cord to the far right power supply labeled “**Encryptor/Hubs**”.

2) Configure the CBM encryptor.

- a) At the bottom of the SSR notebook screen, click on ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear. Select “**CAISI Admin**”.
- b) To configure the wireless bridge choose one of the following configuration methods: Select either the 1) “**Add**” option or 2) “**Device Wizard**” option from the “Device” drop down menu.

i) “Add” Option Method.

- (1) Select “**Device**” from the CAISI Admin toolbar and then select “**Add**” from the “**Device**” drop-down menu.
- (2) Set “**DNS Hostname:**” (Where “DNS hostname” = the host name of the wireless bridge) to the name provided by your DOIM, S6 or CSSAMO. The CAISI default is “**CBM-AF-1100**”.
- (3) Create a “**Device Name:**” if you want it to be different from the “DNS Hostname:”
- (4) From the “**Template**” drop-down menu select a template from the list of CAISI Admin defined templates.

NOTE: *The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited.*

- (5) For classroom training, set “Template” to “**AirFortress-Web Enable**”.
- (6) Click on the “**Edit Properties**” button. The “Device Properties” screen will appear with the “**General**” tab selected.
 - (a) Verify the “**Device Name**” (the host name you assigned the wireless bridge) is correct. The CAISI defaults is “**CBM-AF-1100**”.
 - (b) Set the “**Administrative Password**” to the password provided by your DOIM, S6 or CSSAMO.

- (i) Click on the “**Change**” button. The “Set Password” screen will appear.
- (ii) Enter your new password in the “**Enter Password**” dialog box.
- (iii) For classroom training, set the password to the CAISI default “**system00**”.

NOTE: *As you enter the password, asterisks will appear. The password is not shown in the clear. You must change the password before you deploy the inline encryptor.*

- (iv) Press on the <Tab> key and confirm the new password by entering the password in the “**Confirm Password**” dialog box.
- (v) Click on the “**OK**” button.

NOTE: *Until you actually send the configuration to the encryptor, the administrative password and access password fields may indicate “empty” even though you entered it earlier. If you have previously sent this configuration to the encryptor, it will indicate a status of “set”. However, the application does not store user names or passwords. They are cached during the current session, but are lost as soon as you exit from the application. An asterisk to the left of the field name indicates that the password is cached. If there is no asterisk, you must reenter the password.*

- (c) If you have made changes to values on the “**General**” tab, click on the “**Apply**” button.
- (7) Click on the “**Network**” tab.
- (a) Select “**Use the following Network Settings**” and enter the following parameters as assigned by your DOIM, CSSAMO or S6.
 - (b) IP Address: (**192.168.254.254** CAISI Default)
 - (c) Subnet Mask: (**255.255.255.0** CAISI Default)
 - (d) Gateway: (**192.168.254.254** CAISI Default)
 - (e) Do **Not** click on the “**Validate**” button, as there may be multiple encryptor devices with the same IP.
 - (f) If you have made changes to values on the “**Network**” tab, click on the “**Apply**” button.
- (8) Click on the “**Details**” tab.
- (a) “**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience. Click on the “**Apply**” button if any changes were made.
- (9) Click on the “**AirFortress AF-1100**” tab.
- (a) Ensure the “**Crypto Algorithm:**” is set to **AES**.
 - (b) Enter your unit specific “**Access ID:**”. The CAISI default is **0123456789ABCDEF**. (Case does not matter)

NOTE: *You must change the Access ID before deploying the encryptor.*

- (c) Change the “**Re-Keying Interval:**” to **2**.

(d) Serial number can be left blank.

NOTE: *A hole can be created in the “Firewall” by utilizing the “Access Point:” feature. This allows the user to communicate to a device on the untrusted (radio) Network from the Trusted (STAMIS) network. This feature should only be utilized on the same CCM or CBM due to security measures. Be very careful when using this feature, as we do not encourage its use unless implemented under special circumstances.*

(e) If you have made changes to values on the “**AirFortress AF-1100**” tab, click on the “**Apply**” button.

- (10) Click on the “**OK**” button to exit the “**Device Properties**” screen.
- (11) The main CAISI Admin screen will appear where you should see the new device with the name you assigned it. The CAISI default is “**CBM-AF-1100**.”
- (12) Proceed to procedure **c) Send the configuration to the encryptor on page 24.**

ii) **Device Wizard**” Method

- (1) Select “**Device**” from the CAISI Admin menu and then select “**Device Wizard**” from the “**Device**” drop-down menu.
- (2) Set the “**Device Type**” button to **AirFortress AF-1100**. Click on the “**Next>**” button.
- (3) Set the “**Network Type**” to **Mixed Network**. Click on the “**Next>**” button.
- (4) Set “**DNS Hostname**” to **CBM-AF-1100**.
- (5) Create a “**Device Name:**” if you want it to be different from the “**DNS Hostname:**”.
- (6) From the “**Available Device Templates**” drop-down menu select **AirFortress – Web Enabled**. Click on the “**Next>**” button
- (7) From the “**Use the following network settings:**” enter the following parameters as assigned by your DOIM or S6.
 - (a) IP Address: (**192.168.254.254** CAISI Default)
 - (b) Subnet Mask: (**255.255.255.0** CAISI Default)
 - (c) Gateway: (**192.168.254.254** CAISI Default)
 - (d) Do **Not** click on the “**Validate**” button, as there may be multiple encryptor devices with the same IP.
 - (e) Click on the “**Next>**” button.
 - (f) Make sure the “**Crypto Algorithm:**” is set to **AES**.
 - (g) Enter your unit specific “**Access ID:**”. The CAISI default is **0123456789ABCDEF**. (Case does not matter).

NOTE: *You must change the Access ID before deploying the encryptor.*

- (h) Change the “**Re-Keying Interval:**” to **2**.
- (i) Serial number can be left blank.

NOTE: *A hole can be created in the “Firewall” by utilizing the “Access Point:” feature. This allows the user to communicate to a device on the untrusted (radio) Network from the Trusted (STAMIS) network. This feature should only be utilized on the same CCM or CBM due to security measures. Be very careful when using this feature, as we do not encourage its use unless implemented under special circumstances.*

- d) Click the on the “**Next>**” button.
- (8) The “**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience. Click on the “**Next>**” button.
- (9) Set the “**Administrative (Write) Password**”.
 - (a) Enter your new password in the “**Administrative (Write) Password:**” box.
 - (b) Reenter your password into the “**Confirm Administrative (Write) Password:**” box.
 - (c) For classroom training, set the password to the CAISI default “**system00**”.

NOTE: *As you enter the password, asterisks will appear. The password is not shown in the clear. **You must change the password before you deploy the inline encryptor.***

- (d) Click on the “**Finish**” button.
 - (10) The main CAISI Admin screen will appear where you should see the new device with the name you assigned it. The CAISI default is “**CBM-AF-1100**”.
 - (11) Proceed to procedure **c) Send the configuration to the encryptor.**
- c) Send the configuration to the encryptor.**
- (1) Highlight the device you just created from the main screen. The CAISI default is **CBM-AF-1100**.
 - (2) Select “**Device**” from the CAISI Admin toolbar and then select “**Properties**” from the “**Device**” drop-down menu.
 - (3) Click on the “**Send Configuration**” button.
 - (4) Select the “**Configure using serial port**” button.
 - (5) Click on the “**Start**” button.
 - (6) At the “**Do you want to reset the device to factory defaults at this time?**” prompt, click on the “**Yes**” button.
 - (7) The “**Please COLD RESTART the device by power cycling the unit.**” prompt will appear.
 - (a) At this time, physically disconnect either the power cable attached to back of the encryptor or on the main power supply labeled “**Encryptor/Hubs**”. Reconnect it. This will perform a Cold Restart of the encryptor.

NOTE: *Do not wait for the encryptor to finish rebooting before clicking on the “**OK**” button.*

- (8) When the Windows dialog box appears stating that “**The device has been configured successfully**”, click on the “**OK**” button.
- (9) Click on the “**Done**” button on the “**Configure Device**” screen.
- (10) Click on the “**OK**” button to exit the “**Device Properties**” screen. The encryptor is now configured for operation.

NOTE: <i>Ensure you save the device before exiting CAISI Admin.</i>
--

- 3) **Perform disconnection procedures.**
 - a) Disconnect the white straight-through Ethernet cable from the NIC in the SSR notebook and the CBM hub.

2.3 QUICK CONFIGURATION: SET UP OF A CCM

2.3.1 Configure A CCM 340 or 350 Multi-Client Radio Adapter Using CAISI Admin (Firmware V8.65)

A standard CAISI SSR notebook, configured as follows is required for multi-client radio adapter configuration.

- It 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**.
- Wired NIC or Built-In NIC must be used. Its wireless network card *must not* be installed.

1) Perform CCM Multi-Client Radio Adapter connection procedures.

- a) Disconnect the red crossover cable from the port labeled “Encrypted” on the back of the inline encryptor.
- b) Remove the RJ-45 straight-through adapter and a white straight-through Ethernet cable from the 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 Ethernet cable into the RJ-45 straight-through adapter and the other end into the NIC of the SSR Notebook.
- e) Connect an antenna to the CCM.

2) Configure the CCM 340 Radio device.

- a) Apply power to the CCM.
- b) Reset the CCM 340 radio to factory settings by inserting your CAISI reset tool into the reset button (very small hole located on the back of the radio next to the power input). Hold it for 10 to 15 seconds, until the middle light on the CCM 340 turns to red or amber. Continue to hold the reset button until you see the Ethernet light (the one closest to the connectors side of the radio) flicker briefly. The CCM 340 radio will reboot and power itself back to a ready state. The middle light should be lit green.
- c) If the CAISI Admin is not already running, run the CAISI Admin by clicking on the ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear. Click on the "**CAISI Admin**" menu selection.
- d) To configure the multi-client radio adapter choose one of the following configuration methods: Select either the 1) “Add” option or 2) “Device Wizard” option from the “Device” drop down menu.
 - i) “Add” Option Method.
 - (1) Select “**Device**” from the CAISI Admin menu and then select “**Add**” from the “**Device**” drop-down menu.
 - (2) Set “**DNS Hostname:**” (Where “DNS hostname” = the host name of the wireless bridge) to the name provided by your DOIM, S6 or CSSAMO. The CAISI default is “**CCM-340-350**”.
 - (3) Create a “**Device Name:**” if you want it to be different from the “DNS Hostname:”.

- (4) From the “**Template**” drop-down menu select a template from the list of CAISI Admin defined templates.

NOTE: *The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited.*

- (5) For classroom training, set “Template” to **CCM-340/350**.
- (6) Click on the “**Edit Properties**” button. The “**Device Properties**” screen will appear with the “**General**” tab selected.
- a) Verify the “**Device Name**” (the host name you assigned the multi-client radio adapter) is correct. The CAISI default is “**CBM-340-350**”.
 - b) Set the “**Administrative Password**” to the password provided by your DOIM, S6 or CSSAMO.
 - (i) Click on the “**Change**” button. The Set Password screen will appear. Enter your new password in the “**Enter Password**” dialog box.
 - (ii) For classroom training, set the password to the CAISI default “**system**”.

NOTE: *As you enter the password, asterisks will appear. The password is not shown in the clear. **You must change the password before you deploy the radio.***

- (iii) Press on the <Tab> key and confirm the new password by entering the password in the “**Confirm Password**” dialog box.
 - (iv) Click on the “**OK**” button. . Click on the “**OK**” button on the “**Important: Do not lose device passwords**” screen.
- c) Set the “**Access Password**” to the password provided by your DOIM, S6 or CSSAMO.
- (i) Click on the “**Change**” button. The “Set Password” screen will appear. Enter your new password in the “**Enter Password**” dialog box.
 - (ii) For classroom training set the password, to the CAISI default “**access**”.
 - (iii) Press on the <Tab> key and confirm the new password by entering the password in the “**Confirm Password**” dialog box.
 - (iv) Click on the “**OK**” button.
 - (v) Click on the “**OK**” button on the “**Important: Do not lose device passwords**” screen.
- d) If you have made changes to values on the “**General**” tab, click on the “**Apply**” button.

NOTE: *Until you actually send the configuration to the radio, the administrative password and access password fields may indicate “empty” even though you entered it earlier. If you have previously sent this configuration to the radio, it will indicate a status of “set”. However, the application does not store user names or passwords. They are cached during the current session, but are lost as soon as you exit from the application. An asterisk to the left of the field name indicates that the password is cached. If there is no asterisk, you must reenter the password.*

- (7) Click on the “**Network**” tab.
 - (a) Select “**Use the following Network Settings**” and enter the following parameters as assigned by your DOIM, CSSAMO or S6.
 - (i) IP Address: (**192.168.1.5** CAISI Default)
 - (ii) Subnet Mask: (**255.255.255.0** CAISI Default)
 - (iii) Gateway: (**192.168.1.1** CAISI Default)
 - (iv) Domain: (**leave blank** or **Warning.US.Government** CAISI Default)
 - (v) First DNS: (**leave at 0.0.0.0**)
 - (vi) Second DNS and Third DNS: (**leave at 0.0.0.0**)

NOTE: *Since there is not a DHCP server on the Untrusted Network (the radio portion of the network is on the “Encrypted” side of the encryptors and cannot see any host or server on the “Unencrypted” side), the user is advised not to select “**Obtain network settings automatically (DHCP).**”*

- (b) Click on the “**Validate**” button.
 - (i) If the IP Address is unique, click on the “**OK**” button when prompted.
 - (ii) If the IP Address is not unique, a list box will pop up to show you the other device configurations that use that address. Click on the “**OK**” button to dismiss the list box. If necessary, enter a new IP Address, subnet mask, or both.
 - (c) If you have made changes to values on the “**Network**” tab, click on the “**Apply**” button.
- (8) Click on the “**Details**” tab.
 - (a) “**Location**” and “**Notes**” fields are provided for you to enter any additional comments for your convenience. Click on the “**Apply**” button if changes were made.
- (9) Click on the “**Advanced**” tab.
 - (a) Verify that the “Model:” is “**AIR-WGB340**”.
 - (b) Enter your unit specific SSID. The CAISI default for hardware testing and classroom training is “**caisi000**”. ***You must change the SSID before deploying the radio.***

- (c) Verify “**Broadcast Power**” is set to “**full**”. OCONUS countries may require you to lower power setting, check with your local frequency manager upon arrival.
- (d) Under “**Privacy Encryption Keys**”, click on the “**Set Key 1**” button. Click on “**Long 26 digits**”. (**Do not use short key.**)
 - (i) Under “**Enter Key**”, enter your 26 digit hexadecimal encryption key.
 - (ii) The CAISI default is **0123456789abcdef0123456789** for hardware testing and classroom training. *You must change the key before deploying the radio.*
 - (iii) Confirm the key by re-entering it into the “**Confirm Key**” field. Click on the “**OK**” button.
- (e) If you have made changes within this tab, click on the “**Apply**” button and then click on the “**OK**” button.
- (10) The main CAISI Admin screen will appear where you should see the new device with the name you assigned it. The CAISI defaults are “**CCM-340-350**”.
- (11) Proceed to procedure e) **Send the configuration to the multi-client radio adapter on page 31.**

ii) **“Device Wizard” Method**

- (1) Select “**Device**” from the CAISI Admin menu and then select “**Device Wizard**” from the “Device” drop-down menu.
- (2) Set the “Device Type” button to **Cisco Aironet 340**. Click on the “**Next>**” button.
- (3) Set the “Network Type” to **Mixed Network**. Click on the “**Next>**” button.
- (4) Set “DNS Hostname” to “**CCM-340-350**”.
- (5) Create a “**Device Name:**” if you want it to be different from the “DNS Hostname:”
- (6) From the “**Available Device Templates**” drop-down menu select **CCM-340/350**.

NOTE: *The template selected will be the one used to initially define the device. All attributes and properties from the template will immediately be inherited.*

- (7) Click on the “**Next>**” button.
- (8) From the “**Use the following Network Settings**” enter the following parameters as assigned by your DOIM, S6 or CSSAMO.
 - (a) IP Address: (**192.168.1.5** CAISI Default)
 - (b) Subnet Mask: (**255.255.255.0** CAISI Default)
 - (c) Gateway: (**192.168.1.1** CAISI Default)
 - (d) Domain: (**leave blank** or **Warning.US.Government** CAISI Default)
 - (e) First DNS: (**leave at 0.0.0.0**)
 - (f) Second DNS and Third DNS: (**leave at 0.0.0.0**)

- (9) Click on the **“Validate”** button.
 - (a) If the IP Address is unique, click on the **“OK”** button when prompted.
 - (b) If the IP Address is not unique, a list box will pop up to show you the other device configurations that use that address. Click on the **“OK”** button to dismiss the list box. If necessary, enter a new IP Address, subnet mask, or both.
- (10) Click on the **“Next>”** button.
- (11) Verify that the **“Model:”** is **“AIR-WGB340”**.
- (12) Enter your unit specific SSID. The CAISI default for hardware testing and classroom training is **“caisi000”**. **You must change the SSID before deploying the bridge.**
- (13) Verify **“Broadcast Power”** is set to **“Full”**. OCONUS countries may require you to lower power setting, check with your local frequency manager upon arrival.
- (14) Under **“Privacy Encryption Keys”**, click on **“Set Key 1”** then click on **“Long 26 digits”**. **(Do not use short key.)**
 - (a) Under **“Enter Key”** enter your 26 digit hexadecimal encryption key. The CAISI default is **0123456789abcdef0123456789** for hardware testing and classroom training. **You must change the key before deploying the radio.**
 - (b) Confirm key by re-entering into the **“Confirm Key”** field.
 - (c) Click on the **“OK”** button.
 - (d) If a value has been changed, click on the **“OK”** button.
 - (e) Click on the **“Next>”** button.
- (15) The **“Location”** and **“Notes”** fields are provided for you to enter any additional comments for your convenience. Click on the **“Next>”** button.
- (16) Enter your new password in the **“Administrative (Write) Password:”** box and then reenter your password into the **“Confirm Administrative (Write) Password”** box. The CAISI default is **“system”**.
- (17) Enter your new password in the **“Access (Read) Password:”** box and then reenter your password into the **“Confirm Access (Read) Password”** box. The CAISI default is **“access”**.

NOTE: *As you enter the password, asterisks appear. The password is not shown in the clear. **You must change the password before deploying the bridge.** You must change the password before you deploy the radio.*

- (18) Click on the **“Finish”** button.
- (19) Click on the **“OK”** button on the **“Important: Do not lose device passwords”** screen.
- (20) A dialog box will appear, click on the **“Done. No further action”** button.
- (21) Click on the **“OK”** button. The main CAISI Admin screen will appear where you should see the new device with the name you assigned it. The CAISI defaults are **“CCM-340-350”**.

(22) Proceed to procedure e) **Send the configuration to the multi-client radio adapter.**

e) **Send the configuration to the multi-client radio adapter.**

- i) Highlight the device you just created from the main screen. The CAISI defaults are “**CCM-340-350**”.
- ii) Select “**Device**” from the CAISI Admin toolbar and then select “**Properties**” from the “Device” drop-down menu.
- iii) Click on the “**Send Configuration**” button.
- iv) Select the “**Configure using network MAC**” button.
- v) Enter the MAC address from the front of the Multi-Client Radio Adapter into the MAC address field.
- vi) Click on the “**Start**” button.
- vii) Click on the “**OK**” button **ONLY** after resetting the Multi-Client Radio Adapter to factory defaults in response to the “**Please make sure that the device.....**” message. **The reset instructions are described below** prompt.
 - (1) Reset the multi-client radio adapter to factory defaults.
 - (2) With the radio powered, insert gently your CAISI reset tool into the reset button (very small hole located on the back of the radio next to the power input). You will feel or hear a small click.
 - (3) Press and hold the button for approximately 10-15 seconds. Continue to hold the reset button until:
 - (a) The “**Status**” LED (middle) on the CCM turns to red or amber.
 - (b) The “**Ethernet**” LED (top) flickers briefly.
 - (4) Remove the reset tool. The CCM radio will reboot and power itself back to a ready state.
- viii) If the “**Administrative**” and “**Access**” passwords have not been entered previously, the entry boxes will appear.
 - (1) Enter the “**Administrative**” and “**Access**” passwords that your DOIM, S6 or CSSAMO has assigned.
 - (2) The CAISI defaults are “**system**” and “**access**”, respectively. Click on the “**OK**” button when completed. The CCM radio will now start to be configured. If the boxes don't appear, then skip this step.
- ix) Click on the “**OK**” button when “**The device has been configured successfully**” message appears.
- x) Click on the “**Done**” button on the “**Configure Device**” screen.
- xi) Click on the “**OK**” button to exit the “**Device Properties**” screen.
- xii) The **CCM multi-client radio adapter** is now configured for operation. Click on the “**OK**” button on the “Device Properties” screen.

<p>NOTE: <i>Ensure you save the device before exiting CAISI Admin.</i></p>

3) **Perform disconnection procedures.**

- a) Disconnect the white straight-through Ethernet cable from the laptop's NIC and the RJ-45 straight-through adapter.
- b) Disconnect the red crossover cable from the RJ-45 straight-through adapter.
- c) Re-attach the red crossover Ethernet cable to the "Encrypted" port on the back of the inline encryptor.

2.3.2 Configure a CCM Encryptor Using CAISI Admin (Firmware 1178W)

The procedures to configure the CCM encryptor are the same as those to configure a CBM encryptor. Refer to the procedures outlined in paragraph **2.2.2** to configure the CCM encryptor

3. QUICK CONFIGURATION PROCEDURES USING MANUAL TOOLS & UTILITIES

3.1 QUICK CONFIGURATION: SET UP OF A CBM.

3.1.1 Configure a CBM Wireless Bridge using manual procedures.

A standard CAISI SSR notebook, configured as follows is required for wireless bridge configuration.

- It 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**.
- Wired NIC or Built-In NIC must be used. Its wireless network card *must not* be installed.

1) Perform CBM Wireless Bridge connection procedures.

- a) Disconnect the red crossover cable from the port labeled “Encrypted” on the back of the 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 NIC.
- e) You are now connected from your NIC to the “Network” port on the power injector.

NOTE: *If you connect to the “AP/Bridge” port, you can damage your 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.*

NOTE: *If the wireless bridge is not installed in a CBM, connect a white straight through Ethernet cable from the “AP/Bridge” port on the Ethernet power injector to the “Inline Power Ethernet” port on the bridge.*

- f) Connect the blue straight-through nine-pin serial cable from your terminal serial port to the serial port on the bridge.
- g) Connect an antenna to the CBM and apply power.

2) Configure the CBM Wireless Bridge.

- a) From CAISI toolbox select “**Hyperterm COM1 (9,600)**”.
- b) Apply power to the wireless bridge and watch the lights.
- c) Watch the terminal screen. When the “Please enter your username” message appears on the console or the “Summary Status” screen, press the <Enter> key. If you get the “Express Setup” screen, the bridge is at factory defaults and you can skip the next step. Otherwise proceed as follows.

- i) Immediately enter the command “:**resetall**” (a colon and the words “reset” and “all” – all run together with no spaces between) then press the <Enter> key.
- ii) Type “**yes**” at the “Are you sure?” prompt. If you get a message telling you that the “:**resetall**” command timed out, cycle power and try again.
- iii) To cycle power, unplug the Ethernet cable between the power injector and the bridge, wait five seconds, then plug it back in. Sometimes a bridge takes so long to boot (because of DHCP timeouts) that there is very little time left for you to sneak the “:**resetall**” command in before the two-minute time limit. Keep trying until you see the radio’s response, “**Rebooting system due to resetting factory defaults.**”
- d) Set the IP Address, as required for your network or as directed by the S-6 or DOIM, as follows:
 - i) Type “**Add**” and press the <Enter> key.
 - ii) At the “Enter Address” prompt, enter the address provided by the DOIM or S-6, or enter “**192.168.1.4**” the default IP for the CAISI non-root wireless bridge.
 - iii) Press the <Enter> key.
- e) Turn DHCP off, as follows: Type “**pr**” and press the <Enter> key. Type “**n**” then press the <Enter> key.
- f) Apply changes, as follows: Type “**ap**” and press the <Enter> key.

NOTE: Before Proceeding - From this point forward, all configurations can be done in a web browser instead of the console if you prefer. The screens are identical. In your web browser enter the IP address assigned to the radio. The non-root default from Tobyhanna is **192.168.1.4**

NOTE: If using the web browser you will need to navigate to the “**Express Setup**” screen. From the “**Summary Status**” menu select “**Setup**” then “**Express Setup**”. The “**Express Setup**” screen will appear.

- g) At the “Express Setup” Screen.
 - i) Set the IP [Subnet Mask], as required for your network or as directed by the DOIM, S6 or CSSAMO. The default for a CAISI bridge is “**255.255.255.0**”.
 - ii) Set the Default [Gateway], as required for your network or as directed by the DOIM, S6 or CSSAMO. The default for a CAISI bridge is “**192.168.1.1**”.
 - iii) Set the [Radio Service Set ID (SSID)] as required, for your network or as directed by the DOIM, S6 or CSSAMO. The default for a CAISI bridge is “**caisi000**” for hardware testing and classroom training. **You must change the SSID before deploying the radio.**
 - iv) Set the [Role in Radio Network] to “**Non-Root Bridge w/Clients**” unless this will be the root bridge. In that case, set it to “**Root Bridge**”.
 - v) Apply changes. Click the “**OK**” button to approve.

- h) Click the “**Back**” button to return to the “Setup” screen and then jump to Services, “**Security**”.
 - i) Choose “**User Information**” then “**Add New User**”.
 - ii) Create a **root** user: Change the **root** password, write it down, seal it in an envelope, and turn it into your security officer. For this user select all capabilities (select all the check boxes). The default **root** password is “**system**” for hardware testing and classroom training. **You must change the password before deploying the radio.** Apply changes.
 - iii) Create a **monitor** user. Change the **monitor** password, write it down, seal it in an envelope, and turn it into your security officer. The default **monitor** password is “**access**” for hardware testing and classroom training. **You must change the password before deploying the radio.** For this user only, select the “**Admin**” capability. Apply changes.
- i) Click the “**Back**” button to return to the “Security Setup” screen and then jump to “**User Manager**”.
 - i) Set “User Manager” to “**Enabled**”.
 - ii) Set “Allow Read-Only browsing without Login” to “**no**”.
 - iii) Leave “Protect Legal Credit Page” set to “**no**”.
 - iv) Apply changes. Click the “**OK**” button to approve. When you do so, the screen will clear and you will be asked to log in. Log in as **root** (with your new or default **system** password). The “User Manager” screen will return.

NOTE: *You must have defined the users before you can enable the user manager. Otherwise you would lock yourself out of the radio, since there would be no authorized root user.*

- j) Click the “**Back**” button to return to the “Security Setup” screen and then choose “**WEP**”.
 - i) Set the “Key Size” for Key 1 to “**128 bit**”.
 - ii) Set the “Encryption Key” to a new key, write it down, seal it in an envelope, and turn it into your security officer. The default WEP key is “**0123456789abcdef0123456789**”.
 - iii) Apply changes. Click the “**OK**” button to approve.

NOTE: *You must set the key size before you set the encryption key, but if you attempt to apply just the key size it does not take.*

- iv) Set “Use of Data Encryption by Stations” to “**Full Encryption**”. Leave all other settings at their defaults. “Accept Authentication type” is set “**open**” by default. All the others are unset.
- v) Apply changes. Click the “**OK**” button to approve.

NOTE: *You must set and apply the WEP key size and WEP key before you can turn encryption on. “Full encryption” will not be an option until you apply the key.*

- k) Click on the **“Back”** button to return to the **“Setup”** screen and jump to Network Ports, Root Radio/Bridge Radio **“Hardware”**.
 - i) Set **“Allow Broadcast SSID to Associate”** to **“no”**.
 - ii) Set **“World Mode”** to **“yes”**.
 - iii) Set **“Frag Threshold”** to **“1024”**.
 - iv) Set **“RTS Threshold”** to **“1024”**.
 - v) Set **“Search for less-congested Radio Channel”** to **“yes”**.
 - vi) Set both the **“Receive Antenna”** and **“Transmit Antenna”** values to **“Right”**.
 - vii) Apply changes. Click the **“OK”** button to approve.
- l) Click the **“Back”** button to return to the **“Setup”** screen and then jump to Services, **“Name Server”**.
 - i) Set **“Domain Name System (DNS)”** to **“Disabled”**.
 - ii) Apply changes. Click on the **“OK”** button to approve.
- m) Click the **“Back”** button to return to the **“Setup”** screen and then jump to Network Ports, Ethernet, **“Hardware”**.
 - i) Set **“Loss of Backbone Connectivity Action”** to **“No Action”**.
 - ii) Apply changes. Click on the **“OK”** button to approve.
- n) Click the **“Back”** button to return to the **“Setup”** screen and then jump to Network Ports, Root Radio/Bridge Radio **“Advanced”**.
 - i) Set **“Disallow Infrastructure Stations on any other SSID”** to **“yes”**.
 - ii) Set **“Require use of Radio Firmware 5.02L”** to **“yes”**.
 - iii) Make sure that **“Ethernet Encapsulation Transform”** is set to **“RFC1042”**.
 - iv) Set **“Bridge Spacing (km)”** to **“6”**.
 - v) Set **“Radio Preamble”** to **“long”**.
 - vi) Apply changes. Click the **“OK”** button to approve.
- o) Click the **“Back”** button to return the **“Setup”** screen and jump to Event Log, **“Notifications”**.
 - i) At **“Should Notify-Disposition Events SNMP Generate Traps”**, click on **“No”**.
 - ii) At **“Should Notify-Disposition Events Generate Syslog Messages”**, click on **“No”**.
 - iii) Leave all other settings at their defaults.
 - iv) Apply changes. Click the **“OK”** button to approve.
- p) Click the **“Back”** button to return to the **“Setup”** screen and jump to Services, **FTP**.
 - i) Set the protocol to **“FTP”**.
 - ii) Set Default File Server to **“192.168.1.2”** or the address if your CAISI notebook.
 - iii) Set the FTP directory to **“C:\net tools\aironet\firmware”**.
 - iv) Set the user name to **“caisiadmin”**.
 - v) Set the password to your password or the default. The default is **“BS_69dlw”**.
 - vi) Apply changes. Click the **“OK”** button to approve.
- q) At this time the CAISI default configuration for the wireless bridge is complete.

3) **Verify the Wireless Bridge is operational with your network.**

- a) Open the Internet Explorer on the notebook desktop.
- b) In the address toolbar at the top of the Explorer, enter the IP address with which you gave the wireless bridge during configuration. In this case, enter the IP – **192.168.1.3** (CBM root) or **192.168.1.4** (non-root).
- c) Click on the “**Go**” on the Explorer toolbar or click on “**Enter**” on the notebook keyboard.
- d) If the “Enter Network Password” screen appears:
 - i) Enter the user name and password you previously assigned the device. THE CAISI default user name is “**root**” and the default password is “**system**”.
 - ii) Click on the “**OK**” button.
- e) To confirm that the wireless bridge is configured, navigate to the “**Express Setup**” screen.
 - i) If you successfully configured the wireless bridge, you should see the SSID you assigned it or the CAISI default SSID, **caisi000**.
 - ii) At factory defaults, the SSID is tsunami.

IMPORTANT PROCEDURAL NOTE: *As a security precaution, after initial configuration, all remote configurations to a wireless bridge should be turned off.*

4) **Disable Remote Access to the Bridge.**

- a) Use your browser’s “**Back**” button to get back to the “Setup” screen.
- b) Click on “**Web Server**” and the “Web Server Setup” screen will appear.
- c) Click on the “**no**” button next to “Allow Non-Console Browsing” and click on the “**Apply**” button.
- d) Nothing will appear to happen. This means that it worked – you lose contact with the bridge because it no longer allows access except through the console port.

5) **Perform Disconnection Procedures.**

- a) Disconnect the standard serial cable from the serial port on the CBM wireless bridge and the serial port on the laptop.
- b) Disconnect the white straight-through cable from the NIC and the RJ-45 straight-through adapter.
- c) Disconnect the red crossover cable from the RJ-45 straight-through adapter.
- d) Re-attach the red crossover Ethernet cable to the external or “Encrypted” port on the back of the encryptor.

3.1.2 Configure a CBM encryptor using manual procedures.

A standard CAISI SSR notebook, configured as follows is required for encryptor configuration.

- It 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**.
- Wired NIC or Built-In NIC must be used. Its wireless network card *must not* be installed.

To configure the encryptor through the serial port, proceed as follows.

1) Perform encryptor connection procedures.

- a) Connect your notebook to the serial port of the encryptor with a nine-pin female to nine-pin female null modem (crossover) serial cable from the SSR Accessory Kit.

2) Configure the encryptor through the serial port.

- a) At the bottom of the SSR notebook screen, click on ">>" to the right of the "CAISI Toolbox" button. The CAISI Toolbox menu will appear. Select "**Hyperterm COM1 (38,400)**".
- b) When the Com1 38400 HyperTerminal screen appears, press the <Enter> key.
- c) A username prompt will appear, enter the CAISI default username, "**sysadm**" and press the <Enter> key.
- d) A password prompt will appear, type in the CAISI default password: "**system**" or "**system00**" (if the firmware version on the encryptor is 1178W or later), "**sysadm**" (factory default) or the password you previously assigned the device and press the <Enter> key.
- e) Traffic at this point will stop flowing as soon as you log in.

NOTE: *If the password has been lost, reset the encryptor to factory default. To set the encryptor to factory defaults: cycle power, log in with "**default_reset**" as both the username and password. When the Air Fortress has finished rebooting, log back in with the factory default username and password, "**sysadm**" (THIS PROCEDURE MUST BE COMPLETED WITHIN 2 MINUTES OF CYCLING POWER.)*

- f) Type the "**set engine crypto aes**" command and press the <Enter> key.
- g) Type the "**set engine accessid**" command and press the <Enter> key.
- h) You will be prompted for the new access ID.
 - i) Set it to the CAISI default, "**0123456789abcdef**", re-type "**0123456789abcdef** to confirm and press the <Enter> key. (16 Hexadecimal numbers, case does not matter.)
 - ii) The CAISI default key may only be used for hardware testing or classroom training. **The key must be changed before the encryptor is deployed.** 
 - iii) You may be prompted for the old key. If the encryptor is fresh from Tobyhanna, use the CAISI default. If you don't know the old key, reset the encryptor and configure it from scratch.

REMINDER: In order to communicate, all encryptors and remote clients that will be on the same net (where the radios have the same SSID) must have the same key.

- i) Type the “**set engine rekey 2**” (CAISI default) command and press the <Enter> key.
- j) Type the “**passwd sysadm**” command and press the <Enter> key.
 - i) Enter your new password when prompted. Reenter it when prompted.
 - ii) The console username is “sysadm” and cannot be changed. You can only change the password.

NOTE: *Write down the new password, seal it in an envelope and turn it in to your security officer for safekeeping. If you lose it, you will have to reconfigure the encryptor from scratch.*

- k) Optionally, enter the “**set device ip n.n.n.n**” command, where “n.n.n.n” is the IP address to be assigned to the device. The default address is **192.168.254.254**. You may leave it set to this address.
- l) Enter the **exit** command to log out and press the <Enter> key.

NOTE: *If you forget to logout, the https procedures in the following steps will not work.*

- m) Minimize Hyperterm.
- n) Connect your notebook NIC to the hub in a CBM or CCM with a white straight-through CAT-5 Ethernet cable. Or connect directly to the encryptor “Unencrypted” port with a red crossover cable.
- o) Use the secure web browser to connect to the encryptor, as follows.
- p) Enter the factory default IP address “**https://192.168.254.254**” or your own previously assigned encryptor address in the browser address bar. Notice that using the browser in secure mode (**https** instead of **http**) means that you must type in the entire command, not just the address.
- q) When the Security Alert appears click “**OK**”.
- r) A second Security Alert will appear click “**Yes**”.

NOTE: To access the encryptor from the web, a different username and password than that which you used in the console is required. The web access username is “admin” and cannot be changed. You can only change the password.

- s) Enter “**admin**” (factory default) as the username and one of the following passwords: “**admin**” (the factory default password), “**system00**” (CAISI default), or your own previously assigned encryptor password. Click “**OK**”. The welcome screen will appear. If the password is lost, reset the encryptor to factory defaults and begin again at step 2). You will need to redo the console settings as well as the web settings.
- t) Click on the “**User Access**” button in the menu panel on the left side of the screen. The User Access screen will appear.
- u) Enter the old password “**admin**” (factory default), “**system00**” (CAISI default) or your current one, as appropriate in the “Old Password” field. Enter your new password in the “**New Password**” and “Retype New Password” fields. Click “**OK**”.

- v) Click on the “**OK**” button. Click on “**Help**”, a login menu prompting you to enter your password will appear. Enter your new password to verify it has successfully been changed.

NOTE: *Write down the new password, seal it in an envelope and turn it in to your security officer for safekeeping.*

- w) Close web browser.
- x) Maximize Hyperterm.
- y) Log back in using the following procedures:
 - i) A username prompt will appear, enter the CAISI default username, “**sysadm**” and press the <**Enter**> key
 - ii) A password prompt will appear, type in the CAISI default password: “**system**” or “**system00**” (if the firmware version on the encryptor is 1178W or later), “**sysadm**” (factory default) or the password you previously assigned the device, and press the <**Enter**> key.
- z) Enter the “**enable fips**” command and press the <**Enter**> key. You are required to operate in FIPS mode.

NOTE: *When you enable FIPS mode, you also automatically disable ssh and snmp access to the encryptor.*

IMPORTANT PROCEDURAL NOTE: *After all or any actions involving “https” you should disable web access to the encryptor.*

- aa) Disable remote access to the encryptor.
 - i) Enter the “**disable ssh**” command and press the <**Enter**> key.
 - ii) Enter the “**disable afweb**” command and press the <**Enter**> key.
- bb) Enter the “**exit**” command and press the <**Enter**> key to log out. The encryptor will restart and traffic will begin to flow as soon as you log out.

IMPORTANT PROCEDURAL NOTE: *As long as you are logged in to the encryptor console port, traffic will not flow through the encryptor. You must log out when you are finished with configuration.*

NOTES

If you immediately try to connect to another encryptor device using the same default IP address, you will likely get a “not found” error. Your computer actually connects to the device by its MAC address. And your computer thinks that it knows the MAC address of the encryptor because you just tried to connect to the same IP address. But it’s wrong, because you just changed encryptors and the new one has the same IP address as the old one but its MAC is different.

NOTES Continued

Confusion can also arise when you change the IP address of the encryptor or any device. Your computer still thinks that the MAC is valid for the old IP address. But when it tries to contact the new IP address it gets the same MAC for it. Now it gets confused, because there are two entries in memory (the arp (address resolution protocol) cache) with the same MAC.

If either situation occurs, it will be short lived. Arp entries are automatically deleted as they time out. Wait a few minutes and try again. If you are curious or in a hurry, open a DOS window on the laptop and enter the command “**arp -a**” to see the arp cache. To fix the problem enter the command “**arp -d 192.168.254.254**” (or whatever the old or duplicate address is) to delete the offending entry. This will clear the address from your arp cache and force your computer to rediscover the MAC address corresponding to the IP address.

3) Perform disconnection procedures.

- a) Disconnect the nine-pin female to nine-pin female null model (crossover) serial cable from your notebook and from the serial port of the encryptor.
- b) Disconnect the white straight-through Ethernet cable from the NIC in the SSR notebook and the CBM hub.

3.2 QUICK CONFIGURATION: SET UP OF A CCM

3.2.1 Configure a CCM Multi-Client radio adapter using manual procedures.

A standard CAISI SSR notebook, configured as follows is required for Multi-Client Radio Adapter set up.

- It 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**.
- Wired NIC or Built-In NIC must be used. Its wireless network card *must not* be installed.

1) Perform Multi-Client radio adapter connection procedures.

The multi-client radio adapter does not have a console port. You can only configure it over the network.

- a) Disconnect the red crossover cable from the port labeled “Encrypted” on the back of the inline encryptor.
- b) Remove the RJ-45 straight-through adapter and a straight-through Ethernet cable from the 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 white straight-through Ethernet cable into the RJ-45 straight-through adapter and the other end into the NIC on the SSR notebook.
- e) You are now connected from your NIC to the “Ethernet” port on the multi-client radio adapter.

2) Configure the CCM Multi-Client radio adapter.

- a) Use the radio adapter’s *hardware*-reset button to reset the radio.
 - i) With the radio powered, insert your CAISI reset tool into the tiny unlabeled hole next to the power connector (labeled “5VDC”).
 - ii) You will feel or hear a small click. Press and hold the button for about ten seconds. All the lights on the adapter will go out. After a few seconds, the Association light (the center one) will flash red or amber, then immediately go out.
 - iii) Continue to hold the reset button until you see the Ethernet light (the one closest to the connectors side of the radio) flicker briefly. The CCM 340 radio will reboot and power itself back to a ready state.
 - iv) The reset button sets the adapter to the following “factory default” parameters.

Setting Name	Default Value
IP address	192.168.200.1
SSID	tsunami
Authentication type	open
WEP level	off
Node name	AIR-WGB340_XXXXXX (the last six characters of the unit's MAC address)

- b) When the radio adapter is at the defaults, you can use the IP Setup (IPSU) utility to set its IP address and SSID. The MAC address is on the label.
- i) Start the Cisco Aironet IPSU on the notebook.
 - ii) Enter the MAC address of the radio into the “Device MAC ID:” field (no dashes).
 - iii) Click on the “**Get IP Addr**” button. The IP address field should fill in with the address 192.168.200.1. If it does not, try the reset procedure again until it does.
 - iv) Click on “**Set Parameters**” button. The IP address field will change from gray to white.
 - v) Enter the desired IP address into the “IP Address” field, and press the “**Set Parameters**” button.
 - vi) The Cisco factory default address is **192.168.200.1**. If the device already has some other address, such as if the device was previously configured or if a DHCP server assigned one, you will see that address instead, *but the change will fail*. No error will be displayed; the address will just not change.
 - vii) If you get a “Device does not answer” message, press and hold the Reset button on the radio for about 10 seconds, then try again by starting back at step b).
- c) You must initially use the Ethernet port to communicate from your notebook to the multi-client radio adapter. Open Internet Explorer and connect to 192.168.200.1 (Cisco default) or 192.168.1.5 (CAISI default) or the new IP you just entered by IPSU.
- i) Click on “**Allow Config Changes**”.
 - ii) Select “**Radio**” from the top menu.
 - iii) When the radio configuration screen appears enter your SSID in the “Service Set Identification” field. It must match the root radio’s SSID in order to know what network to join. The default on radios issued by Tobyhanna is “**caisi000**”. This SSID should only be used in classroom training and hardware testing. **You must change the SSID before deploying the radio.**
 - iv) Click on the “**Save**” button. You can make only one change at a time. If the field has a “Save” button next to it, you must use the button to save changes to that field. If you make several changes at once, only the one whose button you use will be changed. The other changes will be lost.

- v) Enable “World Mode” by clicking on “**on**”. (The word “on” will now be bold.)
- vi) Change the “RTS/CTS packet size threshold” from the default 2048 to **1024**. Click the “**Save**” button.
- vii) While still on this screen, click “**off**” next to “Enable the diversity antennas.”
- viii) Leave the “transmit power level” set to **full**, unless directed to reduce it for overseas areas.
- ix) Change the “Maximum fragment size” from 2048 to **1024**.
- x) Leave all the other fields at their defaults.
- xi) Click on “**Privacy configuration**” located in the middle of the radio screen. The privacy screen will appear.
- xii) Click on “**Set the keys**” then enter “**1**” as the key number. Click on “**Save**”. Enter your WEP key and click “**Save**”, you will need to repeat this procedure to confirm.

NOTE: *The default CAISI WEP key on radios from Tobyhanna is “0123456789abcdef0123456789”. This key should only be used in classroom training and hardware testing. You must change the SSID before deploying the radio.*

- xiii) Once your key is set, set “Encrypt Radio Packets” to “**on**”. Leave the “Authentication mode” set to “**open**”.
- xiv) Select “**Ethernet**” from the top menu. The Ethernet configuration screen will appear.
 - (1) Reduce the “Wired LAN node stale out time” from the default 700 to **300** and click on “**Save**”.
 - (2) Turn “Do not stale out client nodes” **off**. The default is “on”.
 - (3) If the DOIM, S-6 or CSSAMO has specified an MTU size for your network, enter it in the “Maximum frame size” field.
 - (4) Select “**Filter**” from the top menu.
 - (5) Under “Packet direction by filters”, Click on “**Both**”.
- xv) Select “**Logs**” from the top menu.
 - (1) Go to “A community name of at least 1 character” located midway down the screen under the “Value” column.
 - (i) Delete “**Public**”.
 - (ii) Enter a space (null) by tapping on the keyboard spacebar.
 - (iii) Click on “**Save**”.
 - (2) Scroll down to “**Enable Reception of Syslog Messages**” then Click on “**Off**”.
 - (3) Leave all the other fields at their defaults.
- xvi) Select “**Console**” from the Configuration menu. Console configuration screen will appear.
 - (1) Select “**Set write privilege password**” and enter your new password as prescribed by your DOIM, S6 or CSSAMO.
 - (2) CAISI default is “**system**”.
 - (3) Click on the “**Save**” button and repeat procedure to confirm.

NOTE: *The CAISI default password is for hardware testing and classroom training only. You must change the password before deploying the radio.*

At this point the radio adapter is fully configured and ready to use. You should test it with your network.

3) **Verify the Multi-client radio adapter is operational with your network.**

- a) Open the Internet Explorer on the notebook desktop.
- b) In the address toolbar at the top of the Explorer, enter the IP address with which you gave the multi-client radio adapter during configuration. During classroom training, use the default IP – **192.168.1.5**
- c) Click on the “Go” on the Explorer toolbar or click on “Enter” on the notebook keyboard.
- d) Click on the “Statistics” menu, select “all” next to the “Show Network Map” field.
 - i) Locate the multi-client radio adapter you just configured by finding its MAC address in the list of devices on the network.
 - ii) Verify the IP address is the one you assigned the device.
 - iii) Click on the “Done” button.
- e) Close Internet Explorer.

IMPORTANT PROCEDURAL NOTE: *As a security precaution, after initial configuration, all remote configurations to the multi-client radio adapter should be turned off.*

4) **Disable Remote Access to the Multi-Client Radio Adapter.**

- a) Select “Write Access” from the top menu. The “Enter Network Password” screen will appear.
- b) In the User Name field, enter “**ccm000**”. This field is optional and can be left blank.
- c) Enter the password you assigned the device as prescribed by your DOIM, S6 or CSSAMO in the “Password” field. CAISI default is “**system**”.
- d) Click on the “OK” button.
- e) Select “Allow Config Changes” from the top menu.
- f) Select “Identity” from the “Configuration” menu.
 - i) Make sure that “Use BOOTP/DHCP on startup” is **off**.
 - ii) Set the Internet Address to **0.0.0.255**. Click on the “Save” button.
 - iii) Nothing will appear to happen because you will lose contact with the multi-client radio adapter. Without a valid address, no one can talk to it. Not even intruders, even if they have managed to penetrate the WEP key.

NOTE: *Set the IP address to 0.0.0.255. Do not set it to 0.0.0.0 because this would automatically re-enable DHCP.*

NOTE: *Once the radio’s IP address is removed, you will no longer have access to the radio. If you need to make a change to your configuration at a later time, you will need to reset the multi-client radio adapter and reconfigure it.*

- g) Close Internet Explorer.

5) **Perform disconnection procedures.**

- a) Disconnect the straight-through Ethernet cable from the NIC and the RJ-45 straight-through adapter.
- b) Disconnect the RJ-45 straight-through adapter from the short red crossover cable.
- c) Re-attach the short red crossover cable you initially removed from the “Encrypted” port on the back of inline encryptor.

3.2.2 Configure a CCM encryptor using manual procedures.

The procedures to configure the CCM encryptor are the same as those to configure a CBM encryptor. Refer to the procedures outlined in paragraph **3.1.2** to configure the CCM encryptor.

Index

Subject	Paragraph	Page
10Base-2 Cable (RG-58)		
Troubleshooting	4.1	4-3
10Base-T Cable (CAT-5)		
Troubleshooting	4.1	4-3
How to make 10Base-T cables?	4.1.1	4-13
10Base-T Transceiver		
Troubleshooting	4.2.3	4-27
Access ID		
Inline Encryptor	2.11.6 / 3.6.5	2-66/3-77 3-80
Wireless NIC	2.9.1	2-26
Acronyms	Appendix B	B-8
Add Device Method	3.4.9.1	3-25
Administrative Instructions	1.1 – 1.2	1-1
Advanced Properties	3.4.10.4	3-37
Aironet Client Utility (ACU)	2.8	2-20
Overview	Appendix A	A-9
Wireless NIC (Sets SSID)	2.8	2-24
Antennas		
General Troubleshooting	4.1	4-4
Troubleshoot CBM Antenna System	4.3.4	4-37
Troubleshoot CCM Antenna System	4.4.4	4-49
Attributes		
Device Attributes	3.4.1	3-16
Modify Attribute Properties	3.4.3	3-19
Audit Logging		
Deleting The Audit Log	3.8.1.3	3-101
Purpose	3.8.1.1	3-100
Viewing Details	3.8.1.2	3-101
BIO Settings	2.3	2-2
Mitac 7020	2.3.1	2-3
Mitac 7521T	2.3.2	2-7
CAISI		
Configuration Overview	1.5	1-10
Equipment	1.4	1-6
CAISI Bridge Module (CBM)	1.4.1	1-7
CAISI Client Module (CCM)	1.4.2	1-8
Legacy Support Adapter (LSA)	1.4.3	1-9

Subject	Paragraph	Page
CAISI (Continued)		
System Support Representative (SSR)	1.4.4	1-9
Accessory Kit		
Supported Components	1.5.1	1-11
CAISI Administration Software Application (CAISI Admin)		
Commands		
Configuration		
Inline Encryptor	3.6.5	3-73
Multi-Client Radio Adapter	3.7.2	3-88
Router	3.5	3-39
Wireless Bridge	3.6.2	3-60
Devices	3.3	3-8
Creating A Device	3.4.9	3-25
Add Device Method	3.4.9.1	3-25
Device Wizard Method	3.4.9.2	3-26
Delete a Device	3.4.10.5	3-38
Device Attributes vs. Template Properties	3.4.1	3-16
Device Information Fields	3.2.4	3-6
Device List	3.2.3	3-5
Device Properties	3.3.1	3-8
General	3.3.1.1	3-10
Network	3.3.1.2	3-11
Details	3.3.1.3	3-12
Advanced	3.3.1.4	3-12
Device Templates	3.4	3-16
Create A Device Template	3.4.2	3-17
Template Properties	3.4.3	3-19
General	3.4.4	3-20
Network	3.4.5	3-20
Specific (Advanced)	3.4.6	3-21
Device Views	3.2.5	3-7
Modifying Device Properties	3.4.10	3-31
General	3.4.10.1	3-32
Network	3.4.10.2	3-34
Details	3.4.10.3	3-36
Advanced	3.4.10.4	3-37
Management and Administration	3.8	3-100
Audit Logging	3.8.1	3-101
Deleting The Audit Log	3.8.1.3	3-101
Purpose	3.8.1.1	3-100
Viewing Details	3.8.1.2	3-101

Subject	Paragraph	Page
CAISI Administration Software Application (CAISI Admin) (Continued)		
Configuration File	3.8.2	3-102
Backup	3.8.2.3	3-103
Restore	3.8.2.4	3-105
Saving The Configuration File	3.8.2.1	3-102
Printing	3.8.3	3-107
CAISI Bridge Module (CBM)		
Overview	1.4.1	1-7
Component Configuration (CAISI Admin)		
Inline Encryptor	3.6.5	3-73
Wireless Bridge	3.6.2	3-60
Component Configuration (Manual)		
Inline Encryptor	2.11.6	2-65
Wireless Bridge	2.11.2	2-48
Minimum Configuration	2.11.2.1	2-48
Full Configuration from Scratch	2.11.2.2	2-56
Physical Connection	2.11.1/3.6.1	2-47/3-59
CAISI Client Module (CCM)		
Overview	1.4.2	1-8
Component Configuration (CAISI Admin)	3.7	3-85
Inline Encryptor	(Same as CBM) 3.6.5	3-73
Multi-Client Radio Adapter	3.7.2	3-88
Component Configuration (Manual)	2.12	2-75
Inline Encryptor	(Same as CBM) 2.11.6	2-65
Multi-Client Radio Adapter	2.12.2	2-78
Minimum Configuration	2.12.2.1	2-78
Full Configuration from Scratch	2.12.2.2	2-81
Physical Connection	2.12.1/3.7.1	2-77/3-87
Client Encryption Manager (CEM)		
Overview	2.8	2-20
	Appendix A	A-7
Configuration (CAISI Admin)		
Inline Encryptor	3.6.5	3-73
Multi-Client Radio Adapter	3.7.2	3-88
Router	3.5	3-39
Wireless Bridge	3.6.2	3-60

Subject	Paragraph	Page
Configuration (Manual)	2	
Built-In NIC	2.7	2-17
Inline Encryptor	2.11.6	2-65
LSA	2.13	2-91
Verify Operation	2.13.3	2-105
Multi-Client Radio Adapter	2.12.2	2-75
Minimum Configuration	2.12.2.1	2-78
Full Configuration from Scratch	2.12.2.2	2-81
Verify Operation	2.12.3	2-88
Notebook Computer	2.1	2-1
BIOS Settings	2.3	2-3
Mitac 7020	2.3.1	2-3
Mitac 7521T	2.3.2	2-7
Computer Name	2.6	2-15
Create and Maintain User Accounts	2.5	2-10
Router	2.10	2-31
Wired NIC	2.7	2-17
Wireless Bridge	2.11.2	2-48
Minimum Configuration	2.11.2.1	2-48
Full Configuration from Scratch	2.11.2.2	2-56
Verify Operation	2.11.3	2-63
Wireless NIC	2.8	2-20
Details Properties	3.3.1.3/3.4.10.3	3-12/3-36
DSL		
Troubleshooting	4.3.5	4-41
General Properties	3.3.1.1/3.4.10.1	3-10/3-32
Glossary of Terms	Appendix B	B-1
Hubs		
Troubleshooting	4.3.2/4.4.2	4-31/4-45
Inline Encryptors (AirFortress)		
Configuration (Manual)	2.11.6	2-2-65
Configuration (CAISI Admin)	3.6.5	3-73
Troubleshooting	4.3.3/4.4.3	4-32/4-46
IP Setup (IPSU)	2.12.2.2	2-82
Legacy Support Adapter (LSA)		
Connections	2.13.1	2-91
Configuration (Manual)	2.13.2	2-92
Verify Operation	2.13.3	2-105
Troubleshooting	4.5	4-53

Subject	Paragraph	Page
Link Status Meter (LSM)	4.3.4 / 4.4.4	4-37/4-49
Manual Configuration (See Configuration (Manual))		
Multi-Client Radio Adapter		
Connections	2.12.1/3.7.1	2-77/3-87
Configuration (Manual)		
Minimum Configuration	2.12.2.1	2-78
Full Configuration from Scratch	2.12.2.2	2-81
Verify Operation	2.12.3	2-88
Configuration (CAISI Admin)	3.7.2	3-88
Troubleshooting	4.4.3	4-46
Network Monitoring Tools		
Link Status Meter (LSM)	Appendix A	A-12
	4.3.4 /	4-37 /
	Appendix A	A-12
WS_Watch	Appendix A	A-13
TJPing	Appendix A	A-15
IP Address Assistant/Subnet Calculator	Appendix A	A-17
WS_FTP	Appendix A	A-18
Show IP Configuration	Appendix A	A-19
Network Operation Rules	4.1.1	4-11
Network Properties	3.3.1.2/3.10.1.2	3-11/3-32
Notebook Computer		
BIOS Settings		
Mitac 7020	2.3.1	2-3
Mitac 7521T	2.3.2	2-7
Computer Name	2.6	2-15
Create and Maintain User Accounts	2.5	2-10
Overview	2.1	2-1
Software		
Inventory	1.3	1-3
Reload	2.4	2-9
Troubleshooting	4.2.1	4-15
Software	4.2.1.1	4-15
Utilities	4.2.1.2	4-16
BLAST	Appendix A	A-1
HyperTerminal	4.2.1.2 /	4-16 /
	Appendix A	A-2
Ping	4.2.1.2	4-17
Telnet	Appendix A	A-4
Web Browser	4.2.1.2 /	4-18 /
	Appendix A	A-6
Wired NIC or Built-In NIC	4.2.1.3	4-18
Wireless NIC	4.2.1.4	4-20

Subject	Paragraph	Page
Passwords	2.5	2-10
Printing		
Physical Printing	3.8.3.2	3-108
Print Preview	3.8.3.3	3-110
Print Setup	3.8.3.1	3-107
Quick Configuration Guide	Appendix C	C-1
Configure Notebook	Appendix C	C-4
Configure Wired/Built-In NIC	Appendix C	C-5
Configure Wireless NIC	Appendix C	C-5
Air Fortress Remote Client	Appendix C	C-7
Configure Router using CAISI Admin	Appendix C	C-8
Configure Wireless Bridge using CAISI Admin	Appendix C	C-14
Configure Inline Encryptor using CAISI Admin	Appendix C	C-21
Configure Multi-Client Radio Adapter using CAISI Admin	Appendix C	C-26
Configure Wireless Bridge using Manual procedures	Appendix C	C-32
Configure Inline Encryptor using Manual procedures	Appendix C	C-38
Configure Multi-Client Radio Adapter using Manual procedures	Appendix C	C-42
Reload Software	2.4	2-9
Router, Linksys		
Configuration (Manual)	2.10	2-31
Configuration (CAISI Admin)	3.5	3-39
Troubleshooting	4.2.2	4-23
Save Configuration File	3.8.2.1	3-102
Software Developer/Maintainers and Support Engineers	1.3.2	1-5
Software Inventory	1.3	1-3
Software Security	1.3.1	1-5
Service Set Identification (SSID)		
Wireless NIC	2.8	2-24
Wireless Bridge	2.11.2.1 /	2-53/2-58
	2.11.2.2 / 3.6.2	3-64/3-66
Multi-Client Radio Adapter	2.12.2.1 /	2-79/2-84
	2.12.2.2 / 3.7.2	3-92/3-94
SSR Accessory Kit		
Overview	1.4.4	1-9
Templates	3.4	3-16
Create a Device Template	3.4.2	3-17
Template Properties	3.4.3	3-19
General	3.4.4	3-20
Network	3.4.5	3-20

Subject	Paragraph	Page
Templates (Continued)		
Specific (Advanced)	3.4.6	3-21
Delete a Template	3.4.8	3-24
TJPing	Appendix A	A-15
Troubleshooting		
General Troubleshooting Procedures	4.1	4-1
Cables	4.1	4-3
Network Operation Rules	4.1.1	4-11
SSR Notebook	4.2.1	4-15
Software	4.2.1.1	4-15
Utilities	4.2.1.2	4-16
Wired NIC or Built-In NIC	4.2.1.3	4-18
Wireless NIC	4.2.1.4	4-20
Router	4.2.2	4-23
10Base-T Transceiver	4.2.3	4-27
CBM	4.3	4-28
General	4.3.1	4-28
Hubs	4.3.2	4-31
Encryptor and Wireless Bridge	4.3.3	4-32
Antenna System	4.3.4	4-37
DSL Bridge	4.3.5	4-41
UPS	4.3.6	4-42
CCM	4.4	4-43
General	4.4.1	4-43
Hub	4.4.2	4-45
Encryptor and Multi-Client Radio Adapter	4.4.3	4-46
Antenna System	4.4.4	4-49
LSA	4.5	4-53
UPS		
Troubleshooting	3.7.6	3-38
User Account	2.5	2-10
User Profile	2.5	2-11
Wired Equivalent Privacy (WEP)		
Wireless NIC	2.8	2-22
Wireless Bridge	2.11.2.1 /	2-53/2-60
	2.11.2.2 / 3.6.2	3-64/3-67
Multi-Client Radio Adapter	2.12.2.1 /	2-80/2-86
	2.12.2.2 / 3.7.2	3-92/3-95
Wired NIC/Built-In NIC		
Configuration	2.7	2-17
Troubleshooting	4.2.1.3	4-18

Subject	Paragraph	Page
Wireless Bridge		
Physical Connection	2.11.1/3.6.1	2-47/3-59
Manual Configuration	2.11.2	2-48
Minimum Configuration	2.11.2.1	2-48
Full Configuration from Scratch	2.11.2.2	2-56
CAISI Admin Configuration	3.6.2	3-60
Troubleshooting	4.3.3	4-32
Wireless NIC		
Configuration	2.8	2-20
Wired Equivalent Privacy (WEP)	2.8	2-22
Access ID	2.9	2-26
Troubleshooting	4.2.1.4	4-20