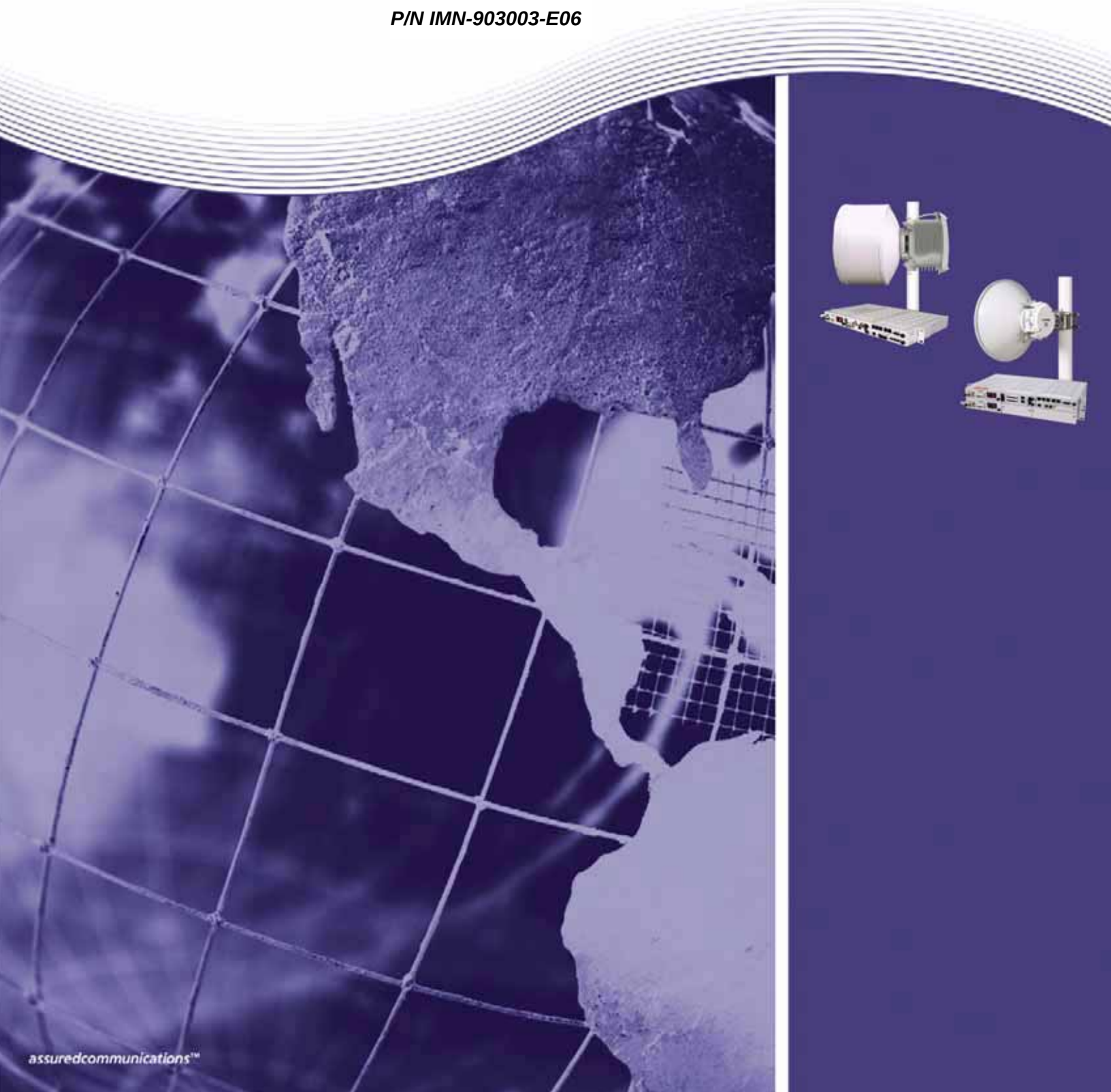
HARRIS

Microwave Digital Radios

TRuepoint® 5000 & TRuepoint® 4040 6 to 38 GHz

Operator's Interface

P/N IMN-903003-E06



assuredcommunications™

TRUEPOINT® 5000 SERIES

THE OPERATOR'S INTERFACE
PART NO. IMN-903003-E06
OCTOBER 2006

Revision history

Issue date	Status	Description of change / revision
March 2004	DRN C9650	• First issue of document
September 2004	ECO 22745	• TRuepoint software release 2
March 2005	ECO 24037	• TRuepoint software release 3
June 2005	ECO 24705	• TRuepoint software release 4
April 2006	PCO 25548	• TRuepoint software release 6 & 7
October 2006	PCO 26986	• 32E1 MUX capability; ROHS compliance; TR4040 support

Part Nº IMN-903003-E06

Harris Corporation -
Microwave Communications Division
637 Davis Drive
Morrisville, NC 27560
U.S.A.
1-800-4-HARRIS
FAX: 1-919-767-3233

Harris Corporation -
Microwave Communications Division
3, rue de l'Hôtel de Ville
Dollard-des-Ormeaux, Québec,
Canada H9B 3G4
1-800-227-8332 or 1-514-421-8400
FAX: 1-514-421-3555

WARNING

Making adjustments and/or modifications to this equipment that are not in accordance with the provisions of this instruction manual or other supplementary documentation may result in personal injury or damage to the equipment, and may void the equipment warranty.

AVERTISSEMENT

Tout réglage ou modification faits à cet équipement hors du cadre édicté par ce guide d'utilisation ou par toute autre documentation supplémentaire pourraient causer des blessures ou endommager l'équipement et peut entraîner l'annulation de sa garantie.

WARNUNG

Die an diesen Geräten gemachte Einstellungen und/oder Änderungen, welche nicht gemäß dieser Bedienungsanleitung, oder gemäß anderen zusätzlichen Anleitungen, ausgeführt werden, können Verletzungen oder Materialschäden zur Folge haben und eventuell die Garantie ungültig machen.

ATENCIÓN

Llevar a cabo ajustamientos y/o modificaciones a este equipo, sin seguir las instrucciones provistas por este manual u otro documento adicional, podría resultar en lesiones a su persona o daños al equipo, y anular la garantía de este último.

警告

不按该说明书有关条例或其它补充文件对该设备
所做的调整和/或改型可能会引起人身伤害
或损坏设备，并且设备保修也将失效。

CONTENTS

CHAPTER 4, UPGRADES

PREFACE

ROHS Compliance

Harris Corporation – Microwave Communications Division

Compliance with Restriction of the Use of Certain Hazardous Substances (RoHS) European Directive

TRuepoint® 4000 and TRuepoint® 5000

Harris MCD holds strong commitments to comply with the requirements of applicable environmental laws and regulations, including those of the Directive 2002/95/EC of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Harris MCD anticipates RoHS-compliant module releases of the TRuepoint® product family by no later than July 1, 2006, and has determined that non-RoHS compliant equipment cannot be shipped after the implementation date into countries which have adopted the directive.

In order to achieve this objective, Harris MCD has been working with its supply chain partners to eliminate the identified hazardous substances from its products and to secure vendor statements of compliance. Additionally, Harris MCD has assigned new part numbers in order to distinguish field replaceable units (FRUs) as RoHS-compliant.

Exemptions:

Harris MCD acknowledges that the "Directive does not apply to spare parts for the repair, or to the reuse, of electrical and electronic equipment put on the market before July 1, 2006", and may continue to support these existing products with non-RoHS-compliant product after the implementation date.

Harris MCD further recognizes that certain exemption criteria apply as defined in the Annex of Directive 2002/95/EC, according to Article 4.2, such as applications 5, 6, 7 and 8 (use of lead in glass, use of lead as an alloying element, lead used in high-melting temperature solders, and cadmium plating, respectively) or any other relevant Commission Decisions, amending for the purposes of adapting to technical progress, the Annex to Directive 2002/95/EC.

ISO 9001 Certification

The Harris Microwave Communications Division is committed to total customer satisfaction and is I.S. EN ISO 9001: 2000 registered for the design, manufacture, installation and service of microwave radio products and systems.

Technical Assistance Center

Our Technical Assistance Center (TAC) is staffed with factory trained and highly qualified Product Support staff whose task is to provide telephone support to resolve complex customer equipment problems quickly and accurately in a timely manner. Customers who completed product training given by Harris Microwave Communications Division and are equipped with proper test equipment and spare parts will experience quick resolution of their equipment problems.

Harris Corporation — Microwave Communications Division
350 Twin Dolphin Drive
Redwood Shores, CA
USA 94065-1421
Toll Free: 1-800-227-8332
Phone: 1-514-421-8333
Fax: 1-650-594-3621
Email: crcusa@harris.com

Harris Corporation — Microwave Communications Division
3 Hotel-de-Ville
Dollard-des-Ormeaux
Quebec, Canada H9B 3G4
Toll Free:1-800-227-8332
Phone: 1-514-421-8333
Fax: 1-514-685-4580
Email: crcmtl@harris.com (point-to-point)
bwa@harris.com (point-to-multipoint)

Coasin Communicaciones S.A.
Alsina 1322 - Codigo Postal (C1088AAJ)
Buenos Aires, Argentina
Phone: +54-11-4383-0074
Fax: +54-11-4383-0075
Email: coasin@coasincom.com.ar

Harris do Brasil
Edifício STADIUM
Al. Rio Negro 1030, Conjuntos 202/204/206
CEP 06454-000
Alphaville, Barueri 06454-000
Sao Paulo, Brazil
Phone: +55-11-4197-3201
FAX: +55-11-4197-3001
Email: crcbraz@harris.com

Harris Communications (Shenzhen) Limited
R3-B2, High Tech. Industrial Park
Nanshan District
Shenzhen, P.R. China 518057
Hotline:+86-13902996934
Phone: +86-755-2663-7928
Fax: +86-755-2663-7048
Email: service@harris.com.cn

DAGA SA
Autopista Norte #118-30
Bogota, Colombia
Phone: +571-603-1000 x3064
Fax: +571-603-1000 x3068
Email: wotero@harris.com

Harris Communication S.A.
Centrale Parc
Avenue Sully Prud'homme
92298 Chatenay-Malabry-France
Toll Free: 800-55-52-8080
Phone: +33- 1-55-52-8080
Fax: +33-1-55-52-8012
Email: crcemea@harris.com

Harris Asia Pacific (M) Sdn. Bhd.
Suite 803, Menara Amcorp,
Amcorp Trade Center
No. 18 Jalan Persiaran Barat
46050 Petaling Jaya, Selangor, Malaysia
Toll Free:1-800-88-0146
Phone: +60-3-7956-8908
Fax: +60-3-7956-5666
Email: custapac@harris.com

Harris S.A. de C.V.
Boulevard Manuel Avila Camacho #36 Piso 17
Col. Lomas de Chapultepec
C.P. 11000, Torres Esmeralda II
Mexico City, DF, Mexico
Toll Free:01-866-452-2054
Phone: +52-55-5249-3700
Fax: +52-55-5249-3701
Email: crcmex@harris.com

Harris Communication Systems Nigeria
Imperial Palace
Plot 274, Ajose Adeogun Street
Victoria Island, Lagos, Nigeria
Hotline: +234-1-850-5050
Phone: +234-1-4448888-9
Fax: +234-1-2701-888
Email: custng@harris.com

Telcon CA
Edif. Segre, 3a Transversal
Los Ruices Norte
Caracas 1071
Venezuela
Phone: +582-239-1211
Fax: +582-239-1866

Harris Microwave Customer Support

Harris provides world-class service for all our valued customers including 24/7 technical support. Your priority calls are handled through our Technical Assistance Center (TAC):

Call: +1-800-227-8332

Outside North America: +1-514-421-8333

You can also contact us through e-mail at:

crcusa@harris.com

Registered customers can obtain key product information on our Premier Web Site at: https://premier.harris/microwave

Service Registration Form

Dear Customer,
To facilitate warranty support and to receive product update information, please register on the Harris MCD Premier Customer website:

https://premier.harris.com/microwave

If you are unable to register online, please complete the form at the bottom of this page and return this page to our customer service department.

By Fax: 514-685-4580

By email: crcmtl@harris.com

By mail: Harris Corporation
Microwave Communications Division
3 Hotel de Ville
Dollard-des-Ormeaux, Quebec
CANADA H9B3G4

PLEASE PRINT:

Company Name: _____

Requestor's Name: _____

Title: _____ Dept: _____

Address: _____

City: _____ State/Province: _____

ZIP/Postal Code: _____ Country: _____

Telephone Number: _____ Fax Number: _____

Email: _____

Original Sales Order/PO Number: _____

Sales order numbers are found in your documentation and are stencilled on the equipment rack base plate, for example, A44044A1.

CHAPTER

1

INTRODUCTION

Scope of this Manual

This manual explains how to operate the TRuepoint® radio system. It describes the tools used to control and monitor the system as well as providing details on configuration, upgrades, and troubleshooting.

This manual explains how to accomplish the various tasks that the operator will be required to perform.

Using this Manual

This manual has been optimized for fast Web viewing, and text shown in this format identifies navigation links leading to locations that are internal or external to the manual.

You would normally use this manual after completing the ***RFU Installation and SPU Installation.*** This manual provides information specific to the Operator Interface.

Structure of this Manual

Besides this introductory Chapter, this Manual contains the following:

Chapter 2, Tools & Features

Identification and functional description of available tools for using the TRuepoint® system and software.

Chapter 3, Configuring and Operating the Radio

Provides steps for using the hand-held terminal, VT-100 emulation, or the Web-CIT to access and configure the software.

Chapter 4, Upgrades

Steps for upgrading software and firmware.

Chapter 5, Troubleshooting

Defines the LEDs and contains a list of alarms to aid in troubleshooting.

Chapter 6, Software Menu Tree

A complete list of the software menus in the hand-held terminal or VT-100 emulation.

Chapter 7, Menu Item Glossary

Provides a brief description of items in the software menu tree and/or Web-CIT.

Chapter 8, Glossary

Compilation of common and special terms — and their definitions, where appropriate — used throughout the TRuepoint™ user documentation.

Key Features of Harris' TRuepoint® 5000 Series

- SPU is RF independent
- RFU is capacity independent
- Fully programmable modem, from 4 QAM to 256 QAM[1] and Reed Solomon, or Reed Solomon concatenated with 2 or 4D TCM, depending on system gain and bandwidth requirements
- Optional application-specific modules
- 1 RMS SPU for 1+0 (Unprotected configuration)
- 2 RMS SPU for 1+1 (Protected configuration)
- Optional multiplexer protection, when using the 1+1 SPU
- In-service performance monitoring with parameters compliant to ITU-T G.826/828 recommendations
- Self-diagnostics/expert system to differentiate the path alarms from the equipment alarms
- Optional digital orderwire (Up to 2 in one SPU)
- Optional 64 kbit/s data interface (Up to 2 in one SPU)
- Built-in asynchronous data (19.2 kbit/s); standard offering
- Built-in agent to support SNMP protocol for IP interfaces
- FarScan™ support
- Programmable relay contacts for alarm indication or site control
- Site alarms monitoring
- Web-CIT interface for radio maintenance
- Telnet
- E-Keypad
- Tributary (local and remote), and IF loopback.
- Transmitter Reverse Channel Switching (RCS), Errorless Receiver Switching, Multiplexer Switching, Demultiplexer Switching
- ATPC and DTPC operation
- Capacity upgrade through software key or hardware key (for 16 x DS1/E1 module), MUX modules swap for other capacities
- Bandwidth selection by software

1. *Future availability*

Related Manuals

Manual P/N	Title	Comments
Top Level		
IMN-903000-Exx	System Description	Top level document providing a broad overview of the TRuepoint™ 5000 platform. Includes Theory of Operation, General Specifications, and Performance Tables.
IMN-904106-Exx	System Description	Top level document providing a broad overview of the TRuepoint™ 4040 platform. Includes Theory of Operation, General Specifications, and Performance Tables.
User Manuals: Hardware (recommended order of use)		
IMN-903001-Exx	RFU Installation	Provides instructions for installing the TR 5000 RFU. It also provides information on cabling connections to the SPU, grounding guidelines, and basic troubleshooting information.
IMN-903002-Exx	SPU Installation	Provides instructions for installing the TR 5000 SPU and its components (modules). It also provides general setup and basic troubleshooting information.
or		
IMN-904107-Exx	RFU Installation	Provides instructions for installing the TR 4040 radio terminal. It also provides information on cabling connections to the SPU, general setup, grounding guidelines, and basic troubleshooting information.
User Manuals: Software		
IMN-903003-Exx	Operator's Interface	This document.
QRC-903000-Exx	Quick Reference Card	Provides a graphical representation of the TRuepoint™ software menus.

CHAPTER

2

TOOLS & FEATURES

The following is an overview of some tools and features that are used in the TRuepoint® system and software.

System Configuration/Management

Web-CIT

The TRuepoint® Web-CIT provides for configuration, control, and administration of the radio as well as a display for alarms via an embedded web interface. The Web-CIT is available with a direct connection or remotely through the customer's TCP/IP network, and displays the current status of both the local and remote units.

The Web-CIT has five main sections:

- Fault Management
- Configuration
- Administration
- Performance
- Security

Harris Keypad or VT-100 Terminal

The Harris Keypad/Hand Held Terminal (HHT) provides for the configuration of the radio as well as a display for alarms. The same functionality is available using VT-100 emulation on a standard PC terminal.

You can use the Keypad or a VT-100 terminal to:

- Configure and control the system
- Review system status
- Review system alarms
- Implement password control

Netcom

The Netcom protocol carries information inside a Harris equipment network. Its minimum capacity (or bandwidth) allocated in the overhead of the radio is 6 x 64 kbit/s = 384 kbit/s (depending on the capacity of the radio) up to 8 x 64 kbit/s + 20 kbit/s = 532 kbit/s for higher bit rates (3DS3).

This protocol encapsulates all the functions such as SCAN (System Control and Alarm Network), Network Management, O/W, and Data Channel. The payload or bandwidth is dynamically allocated to any of these services; this means that if the O/W and 19.2 kbit/s data channels are not used this capacity is then allocated to Netcom to assign to the remaining services such as NMS or SCAN. This will increase the speed of the Network Management System and SCAN.

Netcom is carried in the auxiliary channel of the RF link (radio overhead, except in the case of SONET and SDH). On that link, it is encapsulated in HDLC-like frames.

The physical interface of Netcom is available on the two Ethernet (repeater) 10/100 Base-T ports to connect to other Harris equipment. The two connectors allow for daisy chain and NMS connections.

Netcom is available over HDLC links (HDLC Port) as well to connect to MicroStar® equipment and supports the following applications:

- Local and remote login
- SCAN
- IP and ARP
- Data Channel
- Service channel digital bridge
- Object exchange
- Orderwire signalling
- Network topology

StarView™

The StarView™ Element Management System provides tools to manage your Harris radio networks from a single-operator Windows NT or Windows 2000 workstation. StarView allows you to communicate directly with legacy Harris radio equipment by means of an SNMP proxy agent and with newer Harris radio equipment by means of embedded SNMP agents. StarView's features include:

- A graphical interface
- Network status that allows up to the minute feedback on network performance
- Alarm status that allows immediate feedback on your network's health
- Local and remote connectivity with Harris radio equipment
- Online help for easy access to StarView operation information

NetBoss EM™

NetBoss EM™ is a scalable, cross platform Element Management System that supports distributed network architectures. It has the flexibility to support a wide range of network topologies and network element protocols, and provides the ability to model your network and monitor its components in real time.

NetBoss EM™ provides a complete management solution for the Harris TRuepoint 4040 PDH/Ethernet digital radio. SNMP management and Web based management of the radios is provided. Complete fault and configuration capabilities with graphical network representations to the radio component level are supported as well.

FarScan™

FarScan™ is a user-friendly Windows® based SCAN/SNMP proxy which monitors and controls Harris microwave radio alarms directly via a standard serial communications port using Harris' proprietary SCAN (System Control and Alarm Network) protocol or SNMP protocol.

SNMP protocol allows remote connectivity through use of IP Networking to an SNMP based network management system. The SNMP module is optionally available and can be co-hosted on the same computer as FarScan.

FarScan performs the following primary functions:

- Manual commands
- Polling (AutoPoll and SelectPoll)
- Reporting
- FarScan networking
- Paging

E-Keypad

E-Keypad is an application that is integrated within the FarScan™ software running on a PC. This application displays a pop-up window that shows the HHT, allowing a user from a given site, to control and monitor a remote TRuepoint™ 5000 radio, or any other radio that supports the ESCAN protocol on a Harris Microwave network.

Paperless Chart Recorder (PCR)

Paperless Chart Recorder (PCR) is a software-based diagnostic tool that permits remote access to the operational data that is stored on the radio. The radio's computer is capable of storing selected alarms and events as well as tracing the received signal power level (RSL) of the radio for set periods of time. PCR provides the ability to upload and view this history of alarms, events and RSL activity using SNMP and FTP protocols.

PCR is an optional package. Please contact your local Harris Sales representative to purchase the PCR software and training package. More information about PCR can be found in the ***PCR Instruction*** manual, IMN-112951-Exx.

Event Log Viewer

The Event Log Viewer is part of the Web-CIT and provides the ability to monitor and log events for further analysis. It captures key events that occur on the radio such as alarms, configuration changes, attempted logins, etc. Events can then be filtered and/or sorted for further diagnosis. See Chapter 5 for more information.

Software Download/Upgrade

Software Keys

In software system 6.x and above, two types of software keys are utilized: Software Feature Keys and Software Capacity Keys.

Software Feature Keys include optional features to the system such as Event Logger and Strong Security that customers may choose to include in their system.

Software Capacity Keys allow customers to upgrade the capacity of their system quickly and easily by purchasing a software key and performing the upgrade remotely.

Microwave Software Upgrade Utility

The Microwave Software Upgrade Utility (MSUU) allows customers to upgrade the radio with a software upgrade pack. The MSUU provides a user-friendly interface for connecting to the radio and initiating the upgrade process. It provides the ability to do a direct upgrade to an individual radio, a direct flash upgrade through a MMC card reader, or an upgrade utilizing the radio's ESCAN interface.

The MSUU is designed to work with a PC running Microsoft Windows® 2000, Service Pack 4 or later.

Configuration Transfer Utility

The Configuration Transfer Utility (CTU) allows customers to upgrade from a Version 1 Controller running software 4.x or lower to a Version 2 Controller running software 6.x or higher without losing their configuration data.

CHAPTER

3

CONFIGURING AND OPERATING THE RADIO

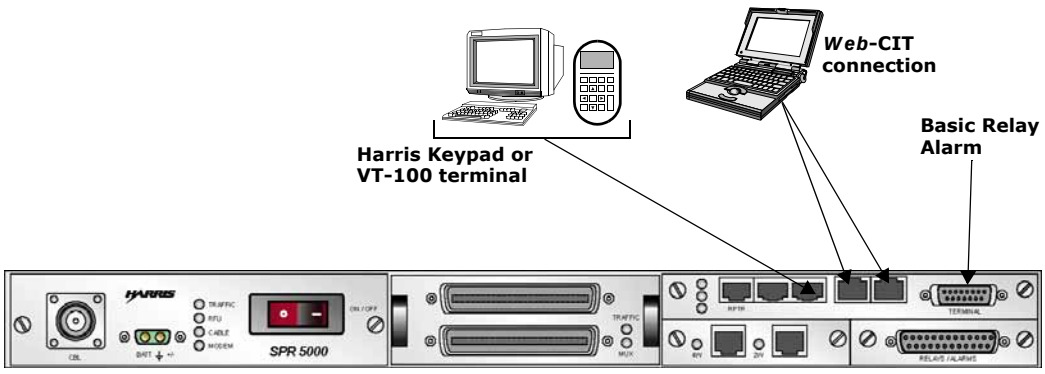
Control and Monitoring

Figure 3-1 shows the connections that can be made to control and monitor the equipment.

The Web-CIT is the preferred method and uses a 10/100 Base-T ethernet connection; there are two provided allowing for a repeater configuration. For instructions on how to use the Web-CIT please turn to page 3-9.

The Harris Keypad/Hand-Held Terminal or another VT-100 compatible terminal connects to the radio via the RS-232 Port 2. If you are using FarScan to monitor legacy equipment, it connects through Port 1.

Figure 3-1: Truepoint monitoring connections



Software Compatibility & Features

In order to run Software Version 6.x.x. or higher you must have the Version 2 Controller Card (101-903460-501). Please see the **SPU Installation Manual** for more information about the Controller cards.

The following table lists the features that are available with the Controller models.

Table 3-1: V1 vs. V2 Controller

Feature	Version 1	Version 2
Software Version	4.x or lower	6.x and higher
Security	Basic	Basic; Strong available w/purchase of software key
Web-CIT	Included	Included[a]
Time Synchronization (SNTP)	Included in 4.x software	
Event Log Viewer	Not available	
VT-100 over Telnet		

a. *These features are available via a software key and will be included unless otherwise noted.*

Software keys are available for both features and capacities. For more information on how to purchase a software key, contact Harris Customer Service. For information on installing and/or upgrading your software key, go to Chapter 4.

To see what features and capacities you have available, go to CONFIGURATION > INVENTORY > SW KEY in the Web-CIT.

Using the hand-held/VT-100 terminal

The hand-held terminal/Harris keypad or any other VT-100 compatible terminal interacts with the embedded control software in the radio and connects to the radio through Port 2 on the Controller module. Once connected, a user will see a number of menus and managed object screens that are linked together in a tree. The operator uses key strokes to move from menu to menu and to change parameters. To order a Harris keypad, see the part list in the ***SPU Installation*** manual, IMN-903002-Exx.

Connecting to the Radio: Hand-Held or PC/VT-100 Terminal

Hand-Held Terminal Unit (HHT)

Connect the HHT to Port 2 on the IDU as shown in Figure 3-1.

As shown in Figure 3-2, the HHT has an 11-key keypad, four function keys, and a 4-line by 20-column alphanumeric readout (display).

The numeric keys (keys 0 through 9) are used for keying in numeric values. They are also used for the following functions:

- The 2, 4, 6, and 8 numeric keys are also used as arrow keys and are used to scroll up (8 key), down (2 key), page-up (4 key), and page-down (6 key) through the menus. Page-up and page-down move the display four lines up and down respectively.
- The 5 numeric key is used as a HOME key, which closes the existing menu and returns to the MAIN menu.
- To enter letters, hold down the appropriate numeric key (0-9) and wait for the letter you want to appear. Only capital letters are supported.

The ENTER key is used to initiate the execution of a selected menu function or register a numeric value.

The function keys (F1, F2, F3, and F4) are used to execute menu functions that appear as “soft keys” on the last line in applicable menus. Function key F1 corresponds to the first “soft key” selection, F2 to the second, F3 to the third, and F4 to the fourth. Refer to Figure 3-4 for the location of the “soft keys” in the display.

Figure 3-2: The Hand-held Terminal Unit

VT-100 Terminal or PC

Connect the VT-100 terminal or PC to Port 2 on the IDU as shown in Figure 3-1. You will need an RJ-45 to RS-232 cable or a RJ-45 cable with a RS-232 adapter. Port 2 is pre-configured at 9600 baud.

All Windows PCs have HyperTerminal which will allow you to emulate a VT-100 terminal. To use HyperTerminal, go to Programs > Accessories > Communication > HyperTerminal from the Windows Start menu.

The VT-100 or PC communications port must be configured as follows:

	VT-100	PC
Mode	ANSI	ANSI
Local echo	OFF	OFF
Control	INTERPRET	N/A
Host port	RS232C (modem port)	RS232C (modem port)
Port speed	9600 baud	9600 baud
Data bits	8	8
Stop bit	1	1
Parity	NONE	NONE

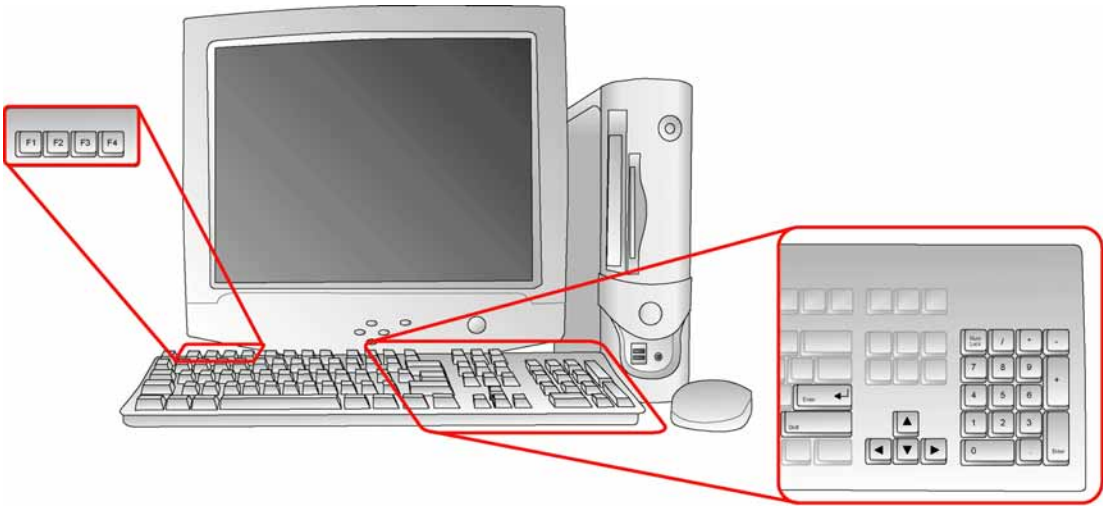
The layout of a typical PC keyboard is shown in Figure 3-3. You will need to use the numeric keys for entering numeric values and the arrow keys to scroll up and down.

The RETURN key is used to initiate the execution of a selected menu function or to register a numeric value.

The period key (.) is used as the HOME key.

The F1, F2, F3, and F4 keys serve as the four function keys that represent the "soft keys" in the display. The soft key EXIT will return the display back to the previous menu.

Figure 3-3: A typical PC keyboard

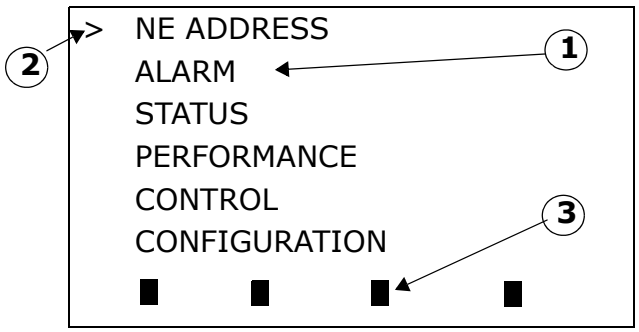


Configuring and Operating the Radio: Hand-Held or PC/VT-100 Terminal

Moving from Menu to Menu

Once a terminal is connected the operator simply uses certain keys to move from menu to menu. The starting point is the main menu as seen in Figure 3-4 when using a VT-100 terminal or a PC emulation. If you are using the hand-held keypad, only three lines will appear at a time so you will need to use the arrow keys to scroll down. To access the sub-menus, use the arrow-key to scroll through the menu until the desired sub-menu is aligned with the cursor. Then press the return or enter key to display the selected menu. Repeat this procedure on the item that you wish to view or change. To return to the previous menu press F4 (EXIT). To return to the MAIN menu press HOME (.).

Figure 3-4: The Main Menu



1 Menu item.
2 Cursor.
3 Soft key spaces (key functions appear when applicable). These soft key spaces correspond to function keys F1, F2, F3, and F4 on the keyboard.

For more information on menus, please refer to Chapter 6 and Chapter 7. The entire menu tree is listed in Chapter 6; Chapter 7 contains explanations of many of the menu items arranged in alphabetical order.

Path Notation

This manual uses a short-form notation convention to designate menu items. To designate a particular item, the item name is given plus the names of all the menus between the MAIN menu and the item. For example, ALARM > PATH > RSL A LOW designates the RSL A LOW menu item in the ALARM branch.

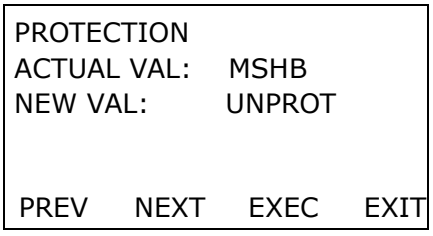
Selecting menu options

Many of the menus provide a number of optional operations. For example the CONTROL > TRANSMIT > TX MUTE item provides two options: ON (normal) and OFF.

In the CONTROL branch these options are shown on the display. Also shown on the display is the standard EXIT option as a soft key position on the bottom line of the screen. To select a soft key option, press the F key that corresponds to the option (see Figure 3-2 or Figure 3-3).

In the CONFIGURATION branch, options appear in the NEW VAL field of a selection screen (see Figure 3-5) that appears when the corresponding parameter is selected from the menu. The operator uses the PREV and NEXT keys to bring the required value into the NEW VAL field, then presses EXEC to select it as the new configuration value.

Figure 3-5: Configuration Option Selection Screen



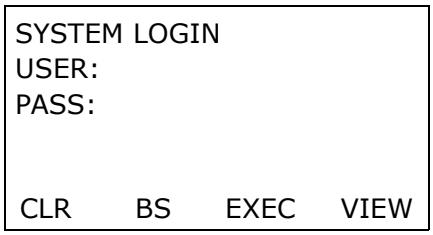
User Authorization

The TRuepoint® radio has a user authorization feature that limits access to multiple features including the control and configuration menus.

In order to restrict access to the menus in the HHT, you will need to go to CONFIGURATION > ENABLE LOGIN and turn it ON. You will then need to logout of the system. Once ENABLE LOGIN is turned ON, when you go to use the HHT a new screen (see Figure 3-6) will appear asking for your user name and password.

When you receive your radio, the default user name is "admin" and the default password is "12345" for software version 4.5 or lower or "12345678" for software version 6.x and higher.

Figure 3-6: ENABLE LOGIN screen



In this screen, CLR and BS are used to edit the field, EXEC will show you a list of user names that you can select instead of typing one in, and VIEW puts the keypad in read-only mode.

If you want to limit access to the control and configuration menus for a particular user account, go to the CONFIGURATION > SECURITY > LOCAL USERS menu item, create or select the appropriate user, and then select NO under CONTROL ACCESS and CONFIG ACCESS.

If you forget or lose your password you can use the FORGOT PASSWORD? feature on the main menu. In order to access the FORGOT PASSWORD? menu, when the screen appears asking for your user name and password you will need to select VIEW in the bottom right hand corner (F4). Selecting VIEW will allow you into the system as a guest. Once you have logged in as a guest, FORGOT PASSWORD? will appear in the menu after CONFIGURATION. Select it, and an access code will appear. You must then call Customer Service with this access code. Customer Service will give you a 1 time use only password that will allow you to login to the system and fix your password.

The NE address

The network element (NE) address is ***unique*** to each radio in the network. The embedded control software and FarScan™ network control software use this address to select remote radios for control and monitoring operations. The embedded control software uses the NE ADDRESS item in the main menu to enter the address of the remote radio to be operated. The NE ADDRESS item in the configuration menu is used to set the NE ADDRESS of the local radio.The selection screen for configuring the NE address is similar to the one shown in Figure 3-5, with the difference that it allows the operator to enter an NE address value in the NEW VAL field before pressing EXEC.

Using the Web-CIT

The Web-CIT is an embedded Web based CIT providing the ability to configure, control, and administer the system. This tool utilizes web technology to control and monitor the radio system through a direct connection, or remotely through the customers' TCP/IP network. Radio pairs, both local and remote, are visible to the operator from the same screen.

On the TRuepoint® SPU, either of the 10/100 Base-T ports on the Controller module allows you to connect a PC to the radio in order to access the Web-CIT. The Web-CIT will work with either Microsoft® Internet Explorer 6.0 and higher or Netscape Navigator 7.0 and higher.

The Web-CIT is powered by the GoAhead Web Server.

Security Considerations

Depending on the security measures at a given site, a customer may need to adjust their security permissions in order to use the Web-CIT. If this is the case, users should be aware that configuring a web browser to run the Web-CIT could create a security breach when accessing the Internet if the security settings are lowered. Users should reset their security levels back to the higher levels before using the same computer to access the Internet for usage other than the Web-CIT.

In no event shall HARRIS CORPORATION, its staff and/or partners be liable to the user for any special, consequential, indirect or similar damages, including any lost profits or lost data arising out of such a security breach. The user is solely responsible for taking all protection measures necessary for achieving a secure connection before, during, and after the use of the Web-CIT software.

Connecting to the Radio: TRuepoint Web-CIT

There are two ways to connect to the radio with the TRuepoint Web-CIT.

Option 1:

1. Connect a PC to a 10/100 Base-T port on the IDU as shown in Figure 3-1. You will need a standard ethernet cable. Make sure that the computer you are using is in the same subnet as the radio; if it is not, go to Start > Settings > Network and Dial-up Connections on your PC. Then click on Local Area Connection and then the Properties tab. Select Internet Protocol (TCP/IP) and then the Properties tab. Select "Use the following address" and enter an IP address that is in the same subnet as the radio. For examples, see Step 7.
2. Go to your internet browser and type in the IP address that corresponds to the NE address; the IP address is always 10.x.xx.1, where the first digit of the NE address comprises the first x, and the second and third digits comprise the second and third x. The default NE address of a new radio is 999 so the IP address will be 10.9.99.1.
3. You will be prompted to enter your user name and password. If this is the first time you are connecting to the system, the default user name is **admin** and the default password is **12345** if you have software version 4.5 or lower or **12345678** if you have software version 6.x or higher. If you have both a local and a remote site, you will need to login to both sites.
4. Once you have entered your user name and password, Figure 3-7 will appear. Note that the local radio is on the left side of the main frame and the remote radio is on the right side.

   If the local and the remote system do not have the same software version, the remote site will display a notification message. The functionality of the local window in the Web-CIT will not be affected. If this occurs, open a separate Web-CIT session to access the remote site.
5. Go to CONFIGURATION > SYSTEM and enter a new NE address. Make sure you click the APPLY button. Once you have done this, you will need to reboot the Controller.
6. The defaults for the TRuepoint ethernet interface are ENABLED, and AUTO mode. **Auto** mode automatically generates the Ethernet IP address and subnet mask for each radio based on the NE address. In order to make sure that you will connect correctly, you should go to Start > Settings > Network and Dial-up Connections on your PC. Then click on Local Area Connection and then the Properties tab. Select Internet Protocol (TCP/IP) and then the Properties tab. Make sure that "Obtain an IP address automatically" is selected.

If at a later date you change the ETHERNET MODE to **Manual**, you should follow these same steps except make sure that "Use the following IP address" is selected.
See "Network Configuration" on page 3-49 for more information on the ETHERNET MODE.

7. Once this is done and the system has rebooted, go to your internet browser and type in the IP address that corresponds to the number you entered as the NE address.

   Examples: NE Address is 232, IP address is 10.2.32.1
   NE Address is 1, IP address is 10.0.1.1
   NE Address is 20, IP address is 10.0.20.1
   NE address is 800, IP address is 10.8.0.1

Option 2:

1. Using the Harris Keypad or another VT-100 compatible terminal, enter the NE ADDRESS in the CONFIGURATION > NETWORK MANAGEMENT menu. The NE ADDRESS must be a number from 001 to 999.
2. Connect a PC to a 10/100 Base-T port on the IDU as shown in Figure 3-1. You will need a standard ethernet cable.
3. The defaults for the TRuepoint ethernet interface are ENABLED, and AUTO mode. **Auto** mode automatically generates the Ethernet IP address and subnet mask for each radio based on the NE address. The DHCP server should be enabled as well.

If you use the PC you are using to connect to the radio for other purposes and the radio is DHCP enabled, you should release and renew your IP connection before entering the IP address of the Web-CIT. To do this, go to the DOS prompt and type in ipconfig/release and then ipconfig/renew.

In order to make sure that you will connect correctly, you should go to Start > Settings > Network and Dial-up Connections on your PC. Then click on Local Area Connection and then the Properties tab. Select Internet Protocol (TCP/IP) and then the Properties tab. Make sure that "Obtain an IP address automatically" is selected.
See "Network Configuration" on page 3-49 for more information on the ETHERNET MODE.

4. Once this is done, go to your internet browser and type in the IP address that corresponds to the number you entered as the NE address.

   Examples: NE Address is 232, IP address is 10.2.32.1
   NE Address is 1, IP address is 10.0.1.1
   NE Address is 20, IP address is 10.0.20.1
   NE address is 800, IP address is 10.8.0.1

5. You will be prompted to enter your user name and password. If this is the first time you are connecting to the system, the default user name is **admin** and the default password is **12345/12345678** depending on your software version. If you have both a local and a remote site, you will need to login to both sites.

   If the local and the remote system do not have the same software version, the remote site will display a notification message. The functionality of the local window in the Web-CIT will not be affected. If this occurs, open a separate Web-CIT session to access the remote site.

6. Once you have entered your user name and password, Figure 3-7 will appear. Note that the local radio is on the left side of the main frame and the remote radio is on the right side.

Figure 3-7: TRuepoint CIT main page

Notes

It is our recommendation that you keep a Web-CIT session open for no longer then 12 hours. If you have a session open for that long, please logout, close your web browser, re-open the browser, and login again.

If you are using the Web-CIT while connected to a V1 Controller on one side of the hop, and the remote terminal has a V2 Controller, the remote side of the screen may not show properly if the screen contains information that is not supported by the V1 Controller. If you need to see this information it is recommended that you connect to the remote site as if you were local.

Configuring and Operating the Radio: TRuepoint Web-CIT

Expanding Menus

Once the Web-CIT is connected the operator simply uses the navigator bar on the far left hand side to move from menu to menu. To expand a menu, click on the appropriate menu item in the black bar and the rest of that menu will appear as shown in Figure 3-8. In this example, the Configuration menu has been expanded, while the Fault Management, Administration, Performance, and Security menus have not.

Selecting menu options

Once you have expanded a menu, you can move from screen to screen simply by clicking on the appropriate option. Figure 3-8 and Figure 3-9 shows the screen that appears when you click on CONFIGURATION > SYSTEM.

Figure 3-8: System Configuration Menu Example 1

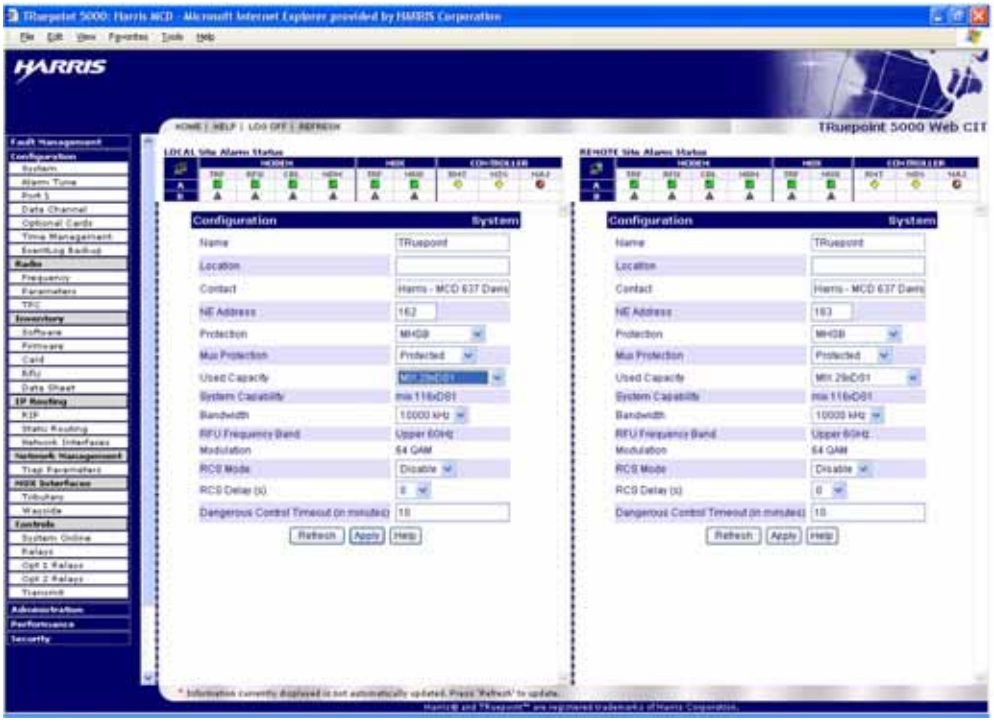
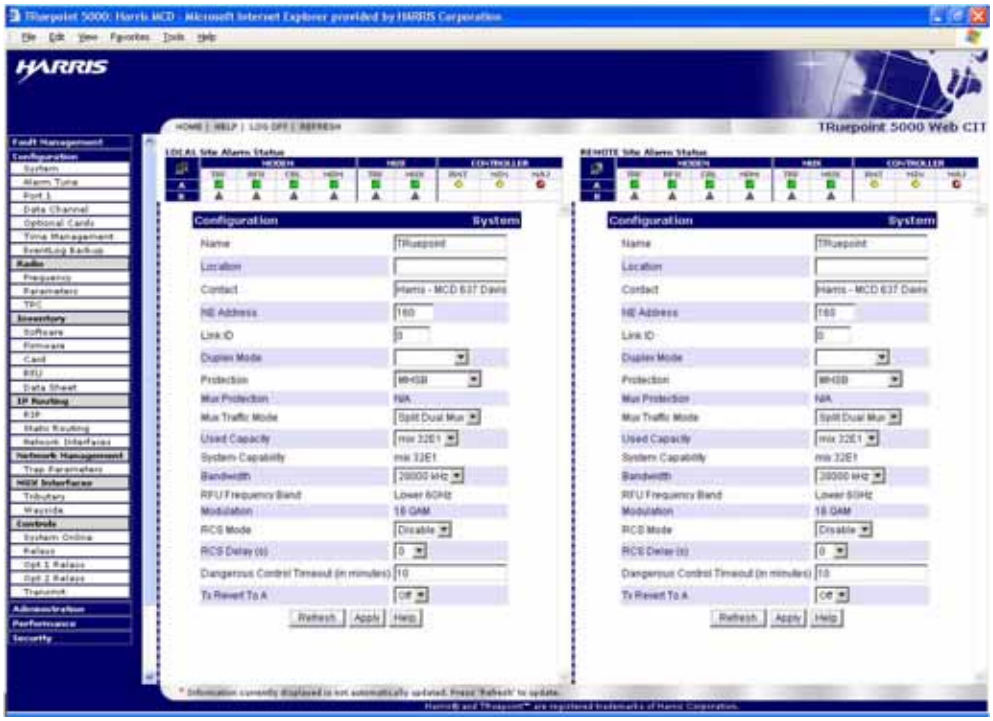


Figure 3-9: System Configuration Menu Example 2



Many of the menus provide a number of optional operations. For example the CONFIGURATION > SYSTEM screen provides multiple drop down menus as seen in Figure 3-8 and Figure 3-9.

If you make a change, you must click the APPLY button at the bottom of each frame for that change to take effect.

Other Features

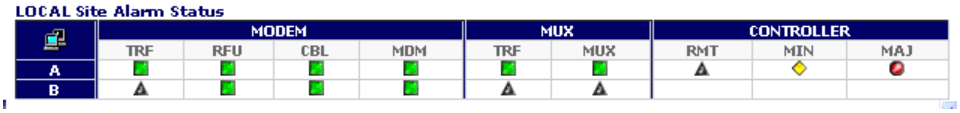
The TRuepoint Web-CIT offers many other features to assist you in operation of the system.

1. At the top of the window is a set of commands (Figure 3-10) that do not change as you navigate from screen to screen.
   - Home: At any time you can click on Home to return to the main screen.
   - Help: A new window will pop up containing the HELP database.
   - Log off: When you are finished, click on log off to be logged out of the system.
   - Refresh: Reloads the window.

Figure 3-10: Web-CIT top menu

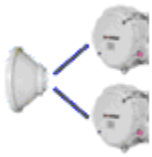
2. A graphical representation of the LEDs that are on the physical units appears at the top of the main frame for both the Local and Remote site. Note that if the computer icon below “Local” or “Remote” is flashing blue, the connection is up (see Figure 3-11). If the computer icon is red, the connection has been lost. You can mouse over the icon as well to get a message telling you whether you are connected or not.

Figure 3-11: Web-CIT LEDs

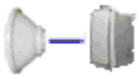


3. On the main page, when you first log in to the system, a graphical representation of the hardware for both the local and remote site appears. See Figure 3-12 for examples of the graphics.

Figure 3-12: Web-CIT hardware graphics



TR4040 MHSB protected system with Mixed Mode MUX



TR5000 unprotected system with Mixed Mode MUX

4. When you select an item from the menu bar such as CONFIGURATION > SYSTEM as seen in Figure 3-8, a HELP button appears at the bottom of the page. If you want help for this particular screen, clicking on the HELP button will take you directly to that information in the HELP database.

5. To change, the color scheme, go to ADMINISTRATION > COLOR SCHEME. The choices are blue, red, and green; blue is the default. When you change the color on the local side, it changes the color on the local window and the navigation bars. When you change the color on the remote side, it changes the remote window. See Figure 3-23 for an example of using two different color schemes.

Configuration Details

Once you have connected to the radio you will need to configure the system. The following instructions are for using the Web-CIT to configure the system; the menu path in the HHT will be listed at the end of each section.

If at any point you lose the connection to the remote site you will need to refresh the window.

NE Address

If you have not entered a unique IP address for the radio, do so at this time. See "Connecting to the Radio: TRuepoint Web-CIT". For more information on the NE Address, refer to "Network Configuration" on page 3-49.

Tx & RX Frequencies

Go to CONFIGURATION > RADIO > FREQUENCY and set your Tx and Rx frequencies. If you have a 4040 system, the Rx frequency will be calculated based on the Tx frequency.

The default frequency for both Tx and Rx is 0 kHz so it is important that you enter a correct frequency in the appropriate box. Entries should be made in kHz.

The following frequencies are available for the existing RFU bands:

Table 3-2: TR 4040 Frequency Ranges

RFU Band (GHz)	Frequency Range (GHz)
7	7.10 - 7.90
8	7.73 - 8.5
13	12.75 - 13.25
15	14.40 - 15.35
18	17.70 - 19.70
23	22.00 - 23.62
26	24.25 - 26.45
32	31.82 - 33.83
38	37.00 - 40.10

Table 3-3: TR 5000 Frequency Ranges

RFU Band (GHz)	Frequency Range (kHz)
6L	5.915 - 6.425
6U	6.425 - 7.125
7	7.100 - 7.900
8	7.725 - 8.500
10/11	10.500 - 11.710
13	12.700 - 13.243
15	14.500 - 15.350
18	17.700 - 19.705
23	21.200 - 23.600
38	37.000 - 40.000

HHT: CONFIGURATION > SYSTEM > RFU > TX A/B FREQ, RX A/B FREQ

Capacity

Go to CONFIGURATION > SYSTEM.

For every system, the software will detect from the MUX the maximum capacity of the system. This number is displayed as a non-editable entry in CONFIGURATION > SYSTEM as System Capability.

If you have a DS1 or E1 system, however, you can reduce the number of tributaries that will be used by the system. This is available in the USED CAPACITY drop-down menu. You can see an example of this in Figure 3-8.

If you set the USED CAPACITY to a lower number than the SYSTEM CAPABILITY, then the actual capacity of the system will be equal to the lower number. For example, if you have a MUX with a hardware key of 16DS1, but you only want to use 8 tributaries at this time, then you would set your USED CAPACITY at 8 DS1. Your SYSTEM CAPABILITY will still appear as 16DS1.

If you are connected to a remote site and you want to change the USED CAPACITY you should always change the remote end first.

HHT: CONFIGURATION > SYSTEM > SPU > USED CAPACITY for setting the Used Capacity, STATUS > SYSTEM > CAPABILITY for viewing the System Capability.

Capacities can be limited by a hardware key (V1 Controller and 2-16 E1 or 4-16 DS1 MUX) or by a software key (V2 Controller and 2-16 E1, 4-16 DS1, or NxE1/DS1+2x10-100BASE-T MUX). If you have a system with both types of keys, the system will detect and enable the highest value. To find out the value of your hardware key, go to CONFIGURATION > INVENTORY > CARD. To find out the value of your software key, go to CONFIGURATION > INVENTORY > SW KEY.

To purchase a software capacity key, please contact Harris Customer Service.

32E1 Capacity

If order to use 32E1, you must have 2 NxE1+2x10-100BASE-T MUXes and have purchased a software key for Split Dual Mux (32E1). You must also have a SPU shelf with the 202-902595-511 backplane.

The 32E1 configuration will not work unless you have the proper backplane. If you do not have the correct backplane, there will be a loss of synchronization on one of the MUXes.

Please note that if you have purchased a software key for a capacity other than 32E1, that software key will co-exist with the 32E1 software key. They will both show as Available on the CONFIGURATION > INVENTORY > SW KEY page if you have both.

To enable 32 E1, go to CONFIGURATION > SYSTEM > MUX TRAFFIC MODE. Select SPLIT DUAL MUX from the drop-down menu. Once you have selected this, mix 32E1 in the USED CAPACITY menu should appear as shown in Figure 3-9.

When you change the traffic mode from Single Mux to Split Dual Mux or vice versa, you should always reboot the Controller software.

Protection

Stay on the CONFIGURATION > SYSTEM page. The following protection schemes are available under the PROTECTION drop-down menu.

Selection	Explanation
UNPROTECTED	Nonprotected radio
UNPROTECTED-2[a]	2+0 nonprotected radios
MHSB	Monitored Hot Standby
FD	Frequency Diversity
SD	Space Diversity
FD/SD[a]	Hybrid Diversity

a. Not available with TR4040.

If your system protection is MHSB, FD, SD, or FD/SD, you also have the option of protecting the MUX. Select Protected from the MUX PROTECTION drop-down menu.

You can see an example of this in Figure 3-9, which shows MHSB protection.

HHT: SYSTEM > SPU > PROTECTION, SYSTEM > SPU > MUX PROTECTION.

If you select Frequency Diversity or Hybrid Diversity, it is recommended that you select Manual or DTPC for your **TPC Mode**. In a FD or HD configuration with ATPC mode, when there is selective fading of the current online channel, boosting of the output power of both transmitters will increase the output power of another channel. A high level of output power of this second channel might cause unneeded interference with other systems and will consume High Output Power allowance time if such a restriction is enforced.

Channel Bandwidth

Stay on the CONFIGURATION > SYSTEM page. Under the BANDWIDTH drop-down menu there are corresponding bandwidths that may be selected for each capacity. Table 3-5 displays these options. When you select the appropriate bandwidth, the corresponding MODULATION will automatically appear.

Table 3-4: Bandwidth-Capacity Pairs, TR4040

Capacity	Bandwidth (MHz)	Modulation	System Frequency Band (GHz)
2E1 or mix2E1	3.5	QPSK	7, 8, 13, 15, 18, 23, 26
4E1 or mix 4E1	7.0	QPSK	7, 8, 13, 15, 18, 23, 26, 38
8E1 or mix8E1	14.0	QPSK	7, 8, 13, 15, 23, 26, 38
	13.75	QPSK	18
	7.0	16QAM	7, 8, 13, 15, 18, 23, 26, 38
16E1 or mix16E1	28.0	QPSK	7, 8, 13, 15, 23, 26, 38
	27.5	QPSK	18
	14.0	16QAM	7, 8, 13, 15, 23, 26, 38
	13.75	16QAM	18

Table 3-5: Bandwidth-Capacity Pairs, TR5000

Capacity[a]	Bandwidth (MHz)	Modulation	System Frequency Band (GHz)
4DS1 or mix4DS1	5.0	QPSK	11, 15, 18, 23, 38
	2.5	16QAM	6L, 6U, 7, 8, 11, 15, 18, 23, 38
8DS1 or mix8 DS1	10.0	QPSK	15, 18, 23, 38
	5.0	16QAM	7, 15, 18, 23, 38
	3.75	32QAM	6L, 6U, 7, 8, 11, 15
12DS1 or mix12DS1	5.0	32QAM	6L, 6U, 7, 8, 11, 15, 18, 23, 38
16DS1 or mix16DS1	20.0	QPSK	15, 18, 23, 38
	10.0	16QAM	11, 15, 18, 23, 38
	5.0	128QAM	6L, 6U, 7, 8, 11
2E1 or mix2E1	3.5	QPSK	6L, 6U, 7, 8, 10, 11, 13, 15, 18, 23, 26, 38

Table 3-5: Bandwidth-Capacity Pairs, TR5000

Capacity[a]	Bandwidth (MHz)	Modulation	System Frequency Band (GHz)
4E1 or mix4E1	7.0	QPSK	6L, 6U, 7, 8, 10, 11, 13, 15, 18, 23, 26, 38
	3.5	16QAM	6L, 6U, 7, 8, 10, 11, 13, 15, 18, 23, 26, 38
8E1 or mix8E1	14.0	QPSK	6L, 6U, 7, 8, 10, 11, 13, 15, 23, 26, 38
	13.75	QPSK	18
	7.0	16QAM	6L, 6U, 7, 8, 10, 11, 13, 15, 18, 23, 26, 38
16E1 or mix16E1	28.0	QPSK	6L, 6U, 7, 8, 10, 11, 13, 15, 23, 26, 38
	27.5	QPSK	18
	27.0	QPSK	7, 15
	29.65	QPSK	6L, 6U, 8
	11.66	16QAM	8
	14.0	16QAM	6L, 6U, 7, 8, 10, 11, 13, 15, 23, 26, 38
	13.75	16QAM	18
	7.0	64QAM	7
21E1 (Sub 155 Mb)	56.0	QPSK	23, 26, 38
	40.0	QPSK	11, 26
	30.0	32QAM	6U
	29.65	32QAM	6L, 8
	28.0	32QAM	6L, 7, 8, 10, 11, 13, 15, 23, 26, 38
	27.5	32QAM	18
	27.0	32QAM	7, 15
	14.0	32QAM	7, 8, 10, 11, 13, 15, 23, 26, 38
	13.75	32QAM	18
OC-3/ STS-3 or SMX A (84DS1)	50.0	32QAM	23, 38
	40.0	64QAM	11, 15, 18, 23
	18.0	128QAM	7, 15
	29.65	128QAM	6L
	30.0	128QAM	6L, 6U, 7, 8, 11, 15, 18, 23, 38

Table 3-5: Bandwidth-Capacity Pairs, TR5000

Capacity[a]	Bandwidth (MHz)	Modulation	System Frequency Band (GHz)
STM-1	56.0	32QAM	23, 26, 38
	55.0	32QAM	18
	40.0	64QAM	6L, 6U, 11, 26
	27.5	128QAM	18
	27.0	128QAM	7, 15
	28.0	128QAM	6L, 7, 8, 10, 11, 13, 15, 23, 26, 38
	29.65	128QAM	6L, 8
	30.0	128QAM	6U
3DS3+ 3DS1	50.0	16QAM	23, 38
	40.0	32QAM	11, 15, 18, 23
	29.65	128QAM	6L
	30.0	128QAM	6L, 6U, 7, 8, 11, 15, 18, 38
DS3 or 100BT or 28 DS1	15.0	16QAM	15, 23, 38
	10.0	64QAM	6L, 6U, 7, 8, 11, 13, 15, 18, 23, 38
DS3+DS1 or 100BT+ DS1 or 28DS1 +DS1	30.0	QPSK	6L, 11, 18, 38
	40.0	QPSK	11, 15, 18, 23
	15.0	16QAM	15, 23, 38
	20.0	16QAM	6L, 6U, 13, 15, 18, 23, 38
	28.0	16QAM	10[b]
	10.0	64QAM	6L, 6U, 7, 8, 11, 13, 15, 18, 23, 38
E3+E1 or 100BT+E1	27.0	QPSK	7, 15
	27.5	QPSK	18
	28.0	QPSK	6L, 6U, 7, 8, 10, 11, 13, 15, 23, 26, 38
	29.65	QPSK	6L, 6U, 8
	14.0	16QAM	6U, 7, 8, 10, 11, 13, 15, 23, 26, 38
	13.75	16QAM	18
Mix29DS1	30.0	QPSK	6L, 11, 18, 38
	40.0	QPSK	11, 15, 18, 23
	15.0	16QAM	15, 23, 38
	20.0	16QAM	6L, 13, 15, 18, 23, 38
	10.0	64QAM	6L, 6U, 7, 8, 11, 13, 15, 18, 23, 38

Table 3-5: Bandwidth-Capacity Pairs, TR5000

Capacity[a]	Bandwidth (MHz)	Modulation	System Frequency Band (GHz)
Mix58DS1	30.0	16QAM	6L, 11, 18, 38
	40.0	16QAM	11, 15, 18, 23
	20.0	64QAM	6L, 6U, 7, 13, 15, 18, 23, 38
Mix87DS1	50.0	16QAM	23, 28
	40.0	32QAM	11, 15, 18, 23
	29.65	64QAM	6L
	30.0	64QAM	6L, 6U, 7, 8, 11, 15, 18, 38
Mix100 DS1	50.0	32QAM	23, 38
	40.0	64QAM	11, 15, 18, 23
	30.0	128QAM	6L, 6U, 7, 8, 11, 15, 18, 23, 38
	29.65	128QAM	6L
Mix100BT +4DS1	40.0	16QAM	11, 15, 18, 23
	20.0	128QAM	6L, 6U, 7, 15, 18, 23, 38
Mix35E1	29.65	16QAM	6L, 8
	28.0	16QAM	6L, 7, 8, 10, 11, 13, 15, 23, 26, 38
	27.5	16QAM	18
	27.0	16QAM	7, 15
	14.0	128QAM	7, 8, 10, 11, 13, 15, 23, 26, 38
	13.75	128QAM	18
Mix50E1	29.65	32QAM	6L, 8
	28.0	32QAM	6L, 7, 8, 10, 11, 13, 15, 23, 26, 38
	27.5	32QAM	18
	27.0	32QAM	7, 15
Mix75E1	56.0	32QAM	23, 26, 38
	55.0	32QAM	18
	40.0	64QAM	6L, 6U, 11, 26
	30.0	128QAM	6U
	29.65	128QAM	6L, 8
	28.0	128QAM	6L, 7, 8, 10, 11, 13, 15, 23, 26, 38
	27.5	128QAM	18
	27.0	128QAM	7, 15

Table 3-5: Bandwidth-Capacity Pairs, TR5000

Capacity[a]	Bandwidth (MHz)	Modulation	System Frequency Band (GHz)
Mix100BT +4E1	29.65	32QAM	6L, 8
	28.0	32QAM	6L, 7, 8, 10, 11, 13, 15, 23, 26, 38
	27.5	32QAM	18
	27.0	32QAM	7, 15
32E1	29.65	16QAM	6L, 8
	28.0	16QAM	6L, 7, 8, 10, 11, 13, 15, 23, 26, 38
	27.5	16QAM	18
	27.0	16QAM	7, 15
SMX A (28DS1/ subSTS3)	50.0	QPSK	23, 38
	40.0	QPSK	11, 15, 18, 23
	30.0	16QAM	6L, 6U, 7, 8, 11, 15, 18, 23, 38
	20.0	16QAM	6L, 6U, 7, 8, 15, 18, 23, 38
	15.0	32QAM	23, 38
	12.5	64QAM	38
SMX A (56DS1/ subSTS3)	50.0	16QAM	23, 38
	40.0	16QAM	11, 15, 18, 23
	30.0	32QAM	6L, 6U, 7, 8, 11, 15, 18, 23, 38
	20.0	128QAM	6L, 6U, 7, 8, 15, 18, 23, 38

a. A Mix capacity applies to Mux cards that allow a mix of DS1/E1 & Ethernet traffic for a total of over the air capacity equivalent to the number of DS1s/E1s listed.

b. Applies to DS3+DS1 only.

HHT: CONFIGURATION > SYSTEM > SPU > CHANNEL BW.

Tributaries/Wayside

Depending on your system you will need to go to CONFIGURATION > MUX INTERFACES > TRIBUTARY or CONFIGURATION > MUX INTERFACES > WAYSIDE.

Table 3-6: Tributary/Wayside Options

Option	Tributary	Wayside
INDEX	Lists the Tributary number.	N/A
STATUS	Ensure that the box is checked (i.e. ENABLE) for each tributary that you want to carry traffic.	Ensure that the box is checked (i.e. ENABLE) for each wayside channel that you want to carry traffic.
STATE (MODE)	N/A	Select DS1, E1, or DISABLE.
CODE	Applicable to DS1 rates only. Select the appropriate line code for each tributary used: AMI or B8ZS. The code should be the same for both sides of a hop.	N/A if the Wayside Mode is E1. Select the appropriate line code for the wayside channel: AMI or B8ZS.
EQUALIZER	Applicable to DS1 or DS3 rates only. Select the appropriate range in feet: 0-133, 133-266, 266-399, 399-533, 533-655	
FRAMING	Applicable to 28DS1 or DS3 rates. Select the appropriate framing format: m1-3 asynchronous or C-bit parity. If DS3, the format should be the same for both sides of a hop.	N/A
TERMINATION	N/A	Applicable to E1 rate only. Select E1 for unbalanced (75 ohms); E1bal for balanced (120 ohms).

HHT: CONFIGURATION > TRIBUTARIES.

Figure 3-13: Tributary Example 1: 28DS1, 2+0 protection

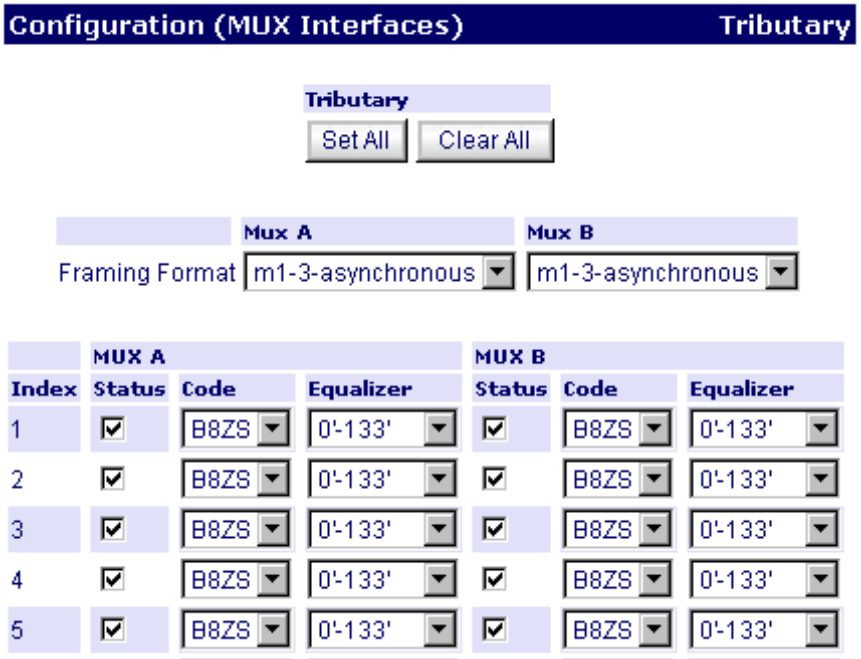
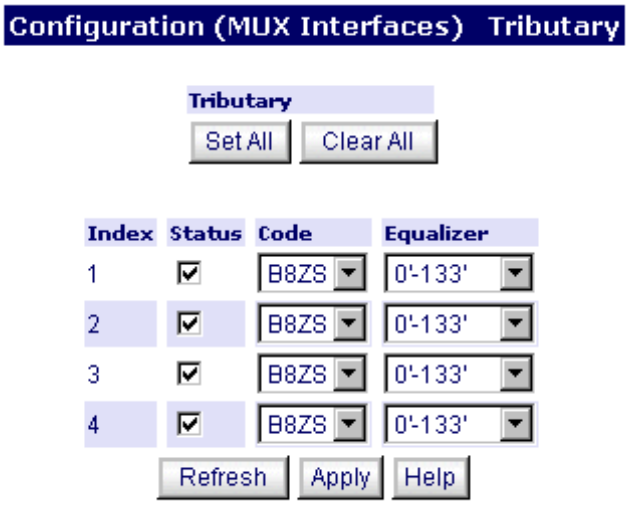


Figure 3-14: Tributary Example 2: 4DS1



CONFIGURING AND OPERATING THE RADIO

Tributaries with a 21E1 MUX

If you have a 21E1 MUX, your options are slightly different as seen in Figure 3-15. The options are described in Table 3-7.

Figure 3-15: Tributary Example 3: 21E1 MUX

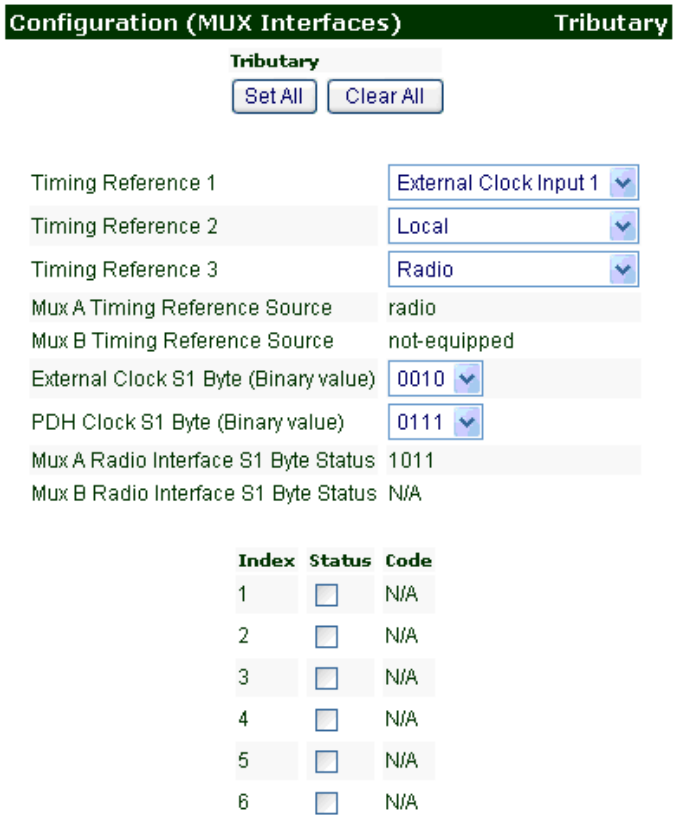


Table 3-7: 21E1 Tributary Options

Option	Action
TIMING REFERENCE (1-3)	Allows you to prioritize the timing reference of the MUX.
EXTERNAL CLOCK S1 BYTE	Allows you to specify a synchronization quality level for the timing reference of the external clock input 1.
PDH CLOCK S1 BYTE	Allows you to specify a synchronization quality level for the timing reference derived from the PDH (E1) incoming signal.
INDEX	Lists the Tributary number.
STATUS	Ensure that the box is checked (i.e. ENABLE) for each tributary that you want to carry traffic.

Tributaries with a NxE1/NxDS1+2x10-100BASE-T MUX

When you have a NxE1+2x10-100BASE-T or NxDS1+2x10-100BASE-T MUX, the tributary page in the Web-CIT has three tabs: Tributaries, Ethernet Ports, and QoS Map. There are many different ways you can distribute the traffic between the Tributaries and the two Ethernet Ports. The following steps are designed to walk you through setting up this type of MUX.

1. Go to CONFIGURATION > SYSTEM. Select the capacity you want from the USED CAPACITY drop-down menu. Please note that if you select a capacity higher than 16 DS1/E1, such as mix58DS1, you will only have 16 tributaries and the rest of the capacity will be allocated to the Ethernet Ports.
2. Go to CONFIGURATION > MUX INTERFACES > TRIBUTARIES. The options on the Tributary tab remain the same as tributaries for other MUX options; see Table 3-6. If you have selected a USED CAPACITY that is less than 16DS1/E1 then you will only see that number of tributaries. Otherwise you will see 16 as long as your software key is not limited to a lower capacity. In the example in Figure 3-16, you can see the 16 tributaries listed, with 12 being enabled and 4 disabled. The capacity of the 4 disabled tributaries is then available for ethernet traffic.

Figure 3-16: Tributary Ex. 4: NxDS1+2x10-100BASE-T MUX

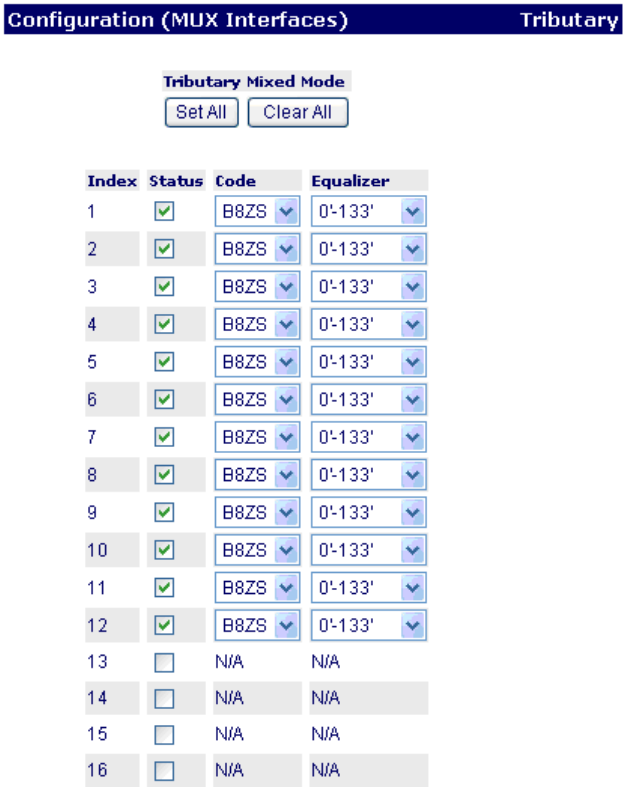
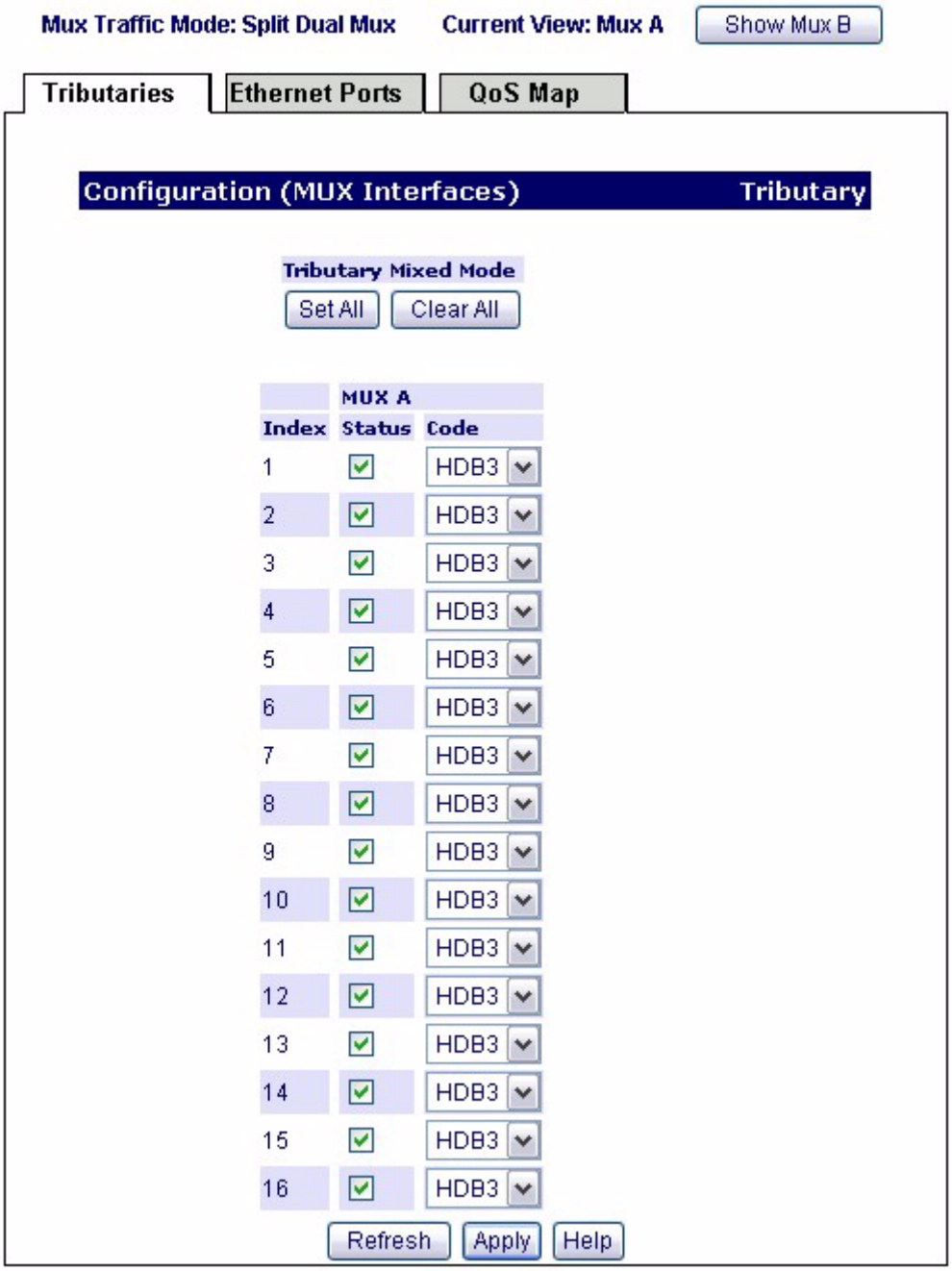
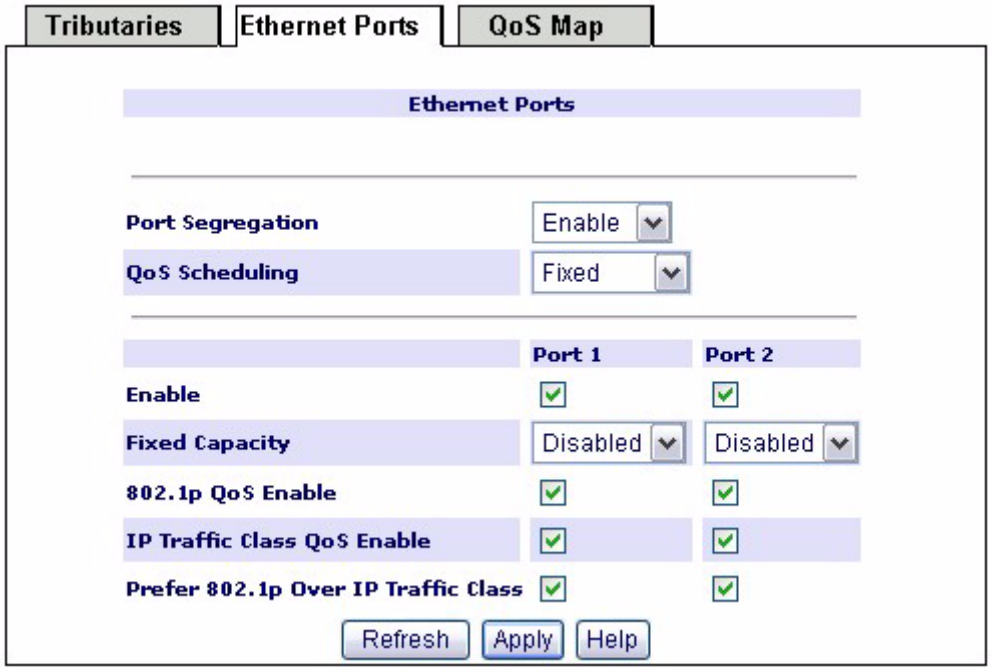


Figure 3-17: Tributary Ex. 5: NxE1+2x10-100BASE-T, Split Dual MUX



3. Click on the Ethernet Port tab. Figure 3-18 will appear. For definitions of each line, see Table 3-8.

Figure 3-18: Ethernet Ports Tab



4. Depending on how many tributaries you have enabled, the remaining capacity will appear in FIXED CAPACITY. Note that in Figure 3-16, 12 tributaries are enabled. The remaining capacity can be allocated by using the FIXED CAPACITY drop-down menu. If you want traffic to go on both Ports 1 & 2, ENABLE Port Segregation and then ENABLE the ports.

5. Once you have enabled the ports, you have a choice of defining the traffic. Select the appropriate number from the FIXED CAPACITY drop-down menu. If you chose mix58DS1, for example, and you have enabled all 16 tributaries on the Tributaries tab, then you will have 42 DS1 allocated to the Ethernet ports. This can then be distributed evenly between the two ports, or you can put more on one and less on the other. For example, if the Used Capacity is 29DS1 and 12 tributaries are enabled, that will leave 17 DS1 available to split between Port 1 and Port 2. **If you have both a local and a remote site, the number of Enabled tributaries MUST BE THE SAME for the maximum number of tributaries to appear**.

For an ethernet connection, Harris recommends that all external device(s) you use support auto-negotiation. If the external devices does not support auto-negotiation, then the external device should be configured as 100 Mbits/s full-duplex. Also, if only one connection is being made, Harris recommends that you disable Port Segregation.

Table 3-8: Ethernet Ports Options

Option	Action
PORT SEGREGATION	Select ENABLE if you want the port traffic segregated. This setting must be the same for the local and remote site.
QOS SCHEDULING	Select FIXED or WEIGHTED.
ENABLE	Select the appropriate check box to ENABLE Port 1 and/or Port 2.
FIXED CAPACITY	Select a DS1 or E1 capacity or leave it as DISABLED. This setting must be the same for the local and remote site.
802.1p QOS ENABLE	Select the appropriate check box for Port and/or Port 2. When enabled, an 802.1p QoS map appears under the QoS Map tab allowing different priorities to be set for each priority field level.
IP Traffic Class[a] QOS ENABLE	Select the appropriate check box for Port 1 and/or Port 2. When enabled, an IP Traffic Class QoS map will appear under the Qos Map tab allowing different priorities to be set for different groups of IP classes.
Prefer 802.1p Over IP Traffic Class	Select the appropriate check box for Port 1 and/or Port 2. This sets the order of preference when prioritizing Ethernet traffic.

a. This can be referred to as IP DiffServ as well.

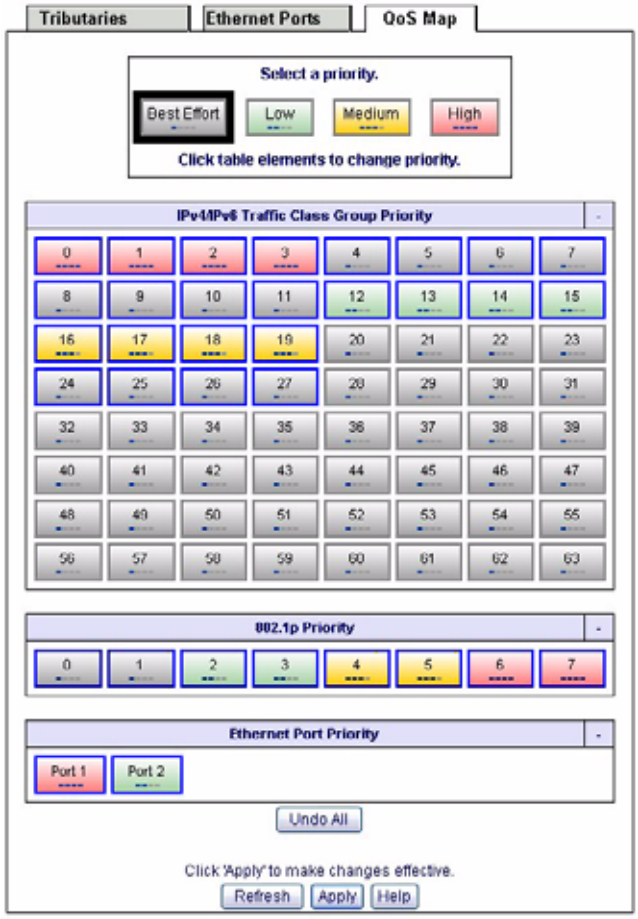
6. For further segregation, click on the QoS Map tab. The QoS Map allows Ethernet traffic quality of service priorities to be set. If you want to set these traffic priorities, make sure that the appropriate priorities are enabled on the Ethernet Ports tab (see Figure 3-18).

7. To change a priority, select a priority level by clicking on it. The choices are Best Effort, High, Medium, or Low. A black frame will show which priority has been chosen (see Figure 3-19). Click within each of the tables to change the priority of that group, level or port. The color for the group, level or port will change to show the new priority. To save your changes, press Apply.

Table 3-9: Priority Tables in the QoS Map

Priority Table	Description
Ethernet Port	Displays when one of the Ethernet ports has been enabled. By highlighting Port 1, for example, you designate that the traffic on Port 1 will always take priority over the traffic on Port 2.
802.1p	Displays when 802.1p QoS is enabled for one of the Ethernet ports and works at the media access control (MAC) framing layer. There are eight levels (0-7) of priority that can be set. For example, you might want to give your network-critical traffic a priority of 7, while streaming multimedia might get a priority of 3.
IPv4/IPv6	Displays when IPTC QoS is enabled for one of the Ethernet ports and works at the IP packet layer. This gives one group of IP classes a higher priority over another group. The table segments IP classes into 64 groups that can have different priorities.

Figure 3-19: QoS Map Tab



Tributaries with a Add-Drop MUX

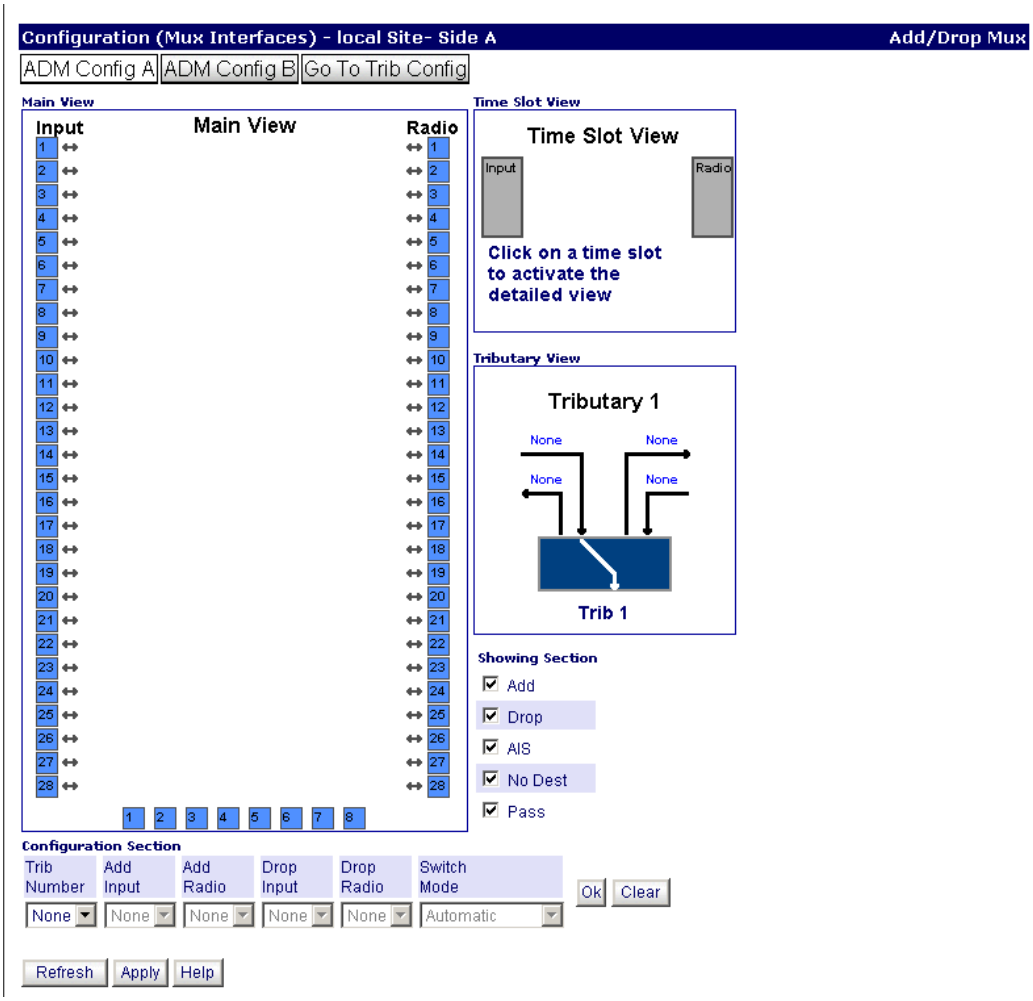
When you have an Add-Drop MUX, you will see a different screen with several sections as seen in Figure 3-20. The add/drop screen allows you to select which time slot of the DS3 signal will be dropped to one of the DS1 tributaries and allows you to select which DS1 tributary will be added to the DS3 signal.

Since the ADM screen is large, you can look at the header to see which site (local or remote) is shown, and if you have a 2+0 system, which side is shown. The buttons directly below the header allow you to browse to the other site and/or side.

Table 3-10: ADM Options

Screen Area	Available Action
Main View	Shows the overall status. Click on a time slot or tributary to activate a sub view.
Time Slot View	Shows the last clicked time slot.
Tributary View	Select a tributary by clicking on it in the Main view or by selecting the number from the drop-down menu in the Configuration section.
Showing Section	Select the appropriate box show or hide the options in the Main View.
Configuration Section	Select the appropriate tributary from the drop-down menus. The OK button will apply the latest user inputs to the screen; the Clear button will erase all user inputs since Apply was last used.

Figure 3-20: ADM Tributary screen



TPC Mode

Transmit Power Control (TPC) allows you to adjust the TX output power to the necessary level in order to provide reliable signal reception at the remote end of the RF link.

Go to CONFIGURATION > RADIO > TPC and select the TPC mode: Manual Control, ATPC, or DTPC. The configuration points mentioned below can be entered on this page as well.

HHT: CONFIGURATION > SYSTEM > OUTPUT POWER > TPC MODE.

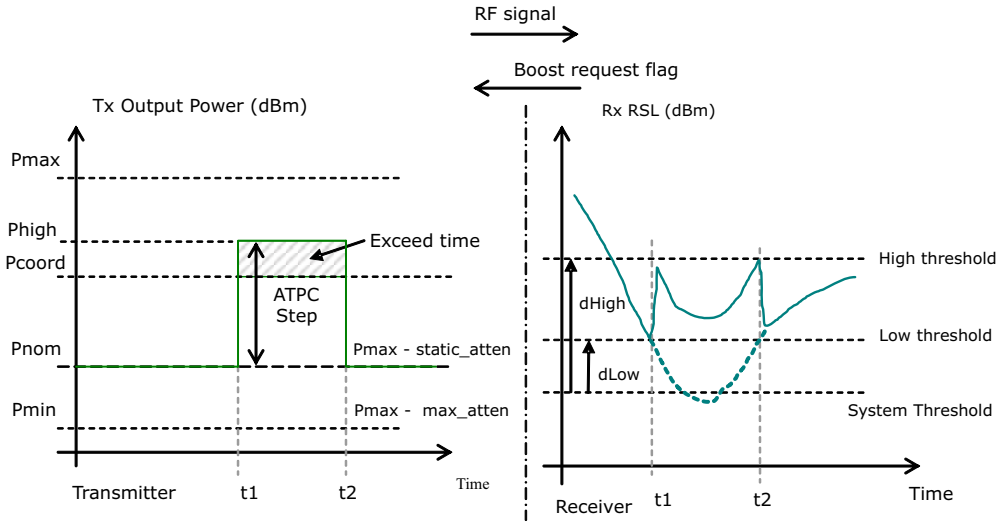
Manual Control is the default mode, and allows you to adjust the Tx output power to the desired level by setting the Tx Static Attenuation for RFU A and RFU B. The range is from 0-30 dB, in 0.5 dB increments.

ATPC mode allows the radio to operate at a low output power that is enough to provide reliable signal reception at the remote end of the RF link. However, when a fading condition occurs and the RSL at the remote end is approaching the system threshold, the Tx output power increases to a predetermined high output power level. When the fading condition is over and the RSL at the remote end is far enough below the system threshold, the Tx output power returns to the low level.

To set up ATPC, you must set the nominal power level using Tx Static Attenuation. Then you define the Remote ATPC Low Threshold Offset (0-25 dB) and the Boost Step (0-15 dB). When the RSL level drops below the system threshold plus the ATPC low threshold, the receiver will set the boost request flag and send it to the transmitter. If allowed, the transmitter will increase the Tx output power by the number set in the Boost Step. When the RSL at the receiver increases above the system threshold plus the ATPC high threshold, the receiver clears the boost request flag and sends it back to the transmitter, which in turn returns Tx output power bock to the nominal power level.

Figure 3-21 illustrates various parameters related to ATPC mode; the dashed line shows that without ATPC, the RSL would go below the system threshold.

Figure 3-21: ATPC Parameters

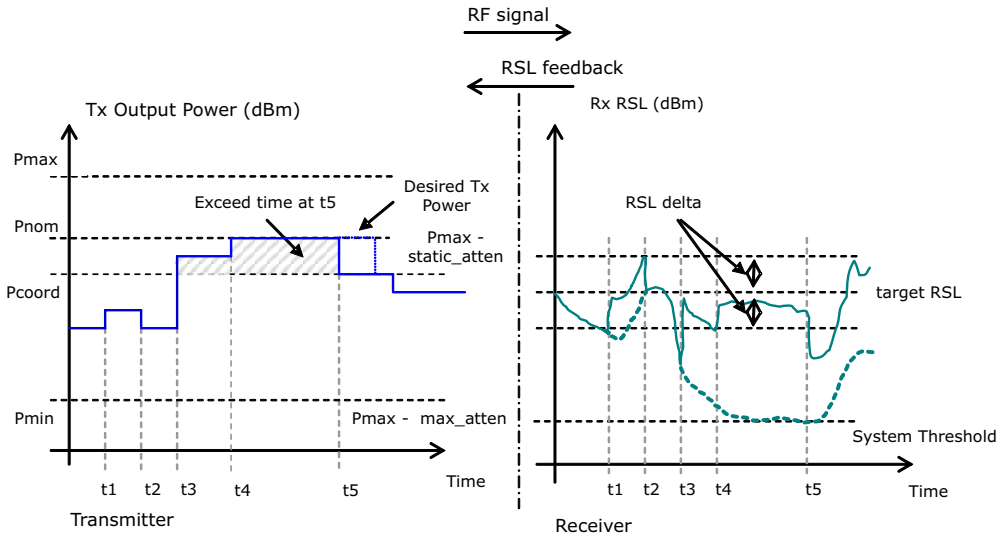


DTPC mode allows you to specify a target remote end RSL value that provides reliable signal reception. Tx output power is automatically adjusted to maintain this specified target remote end RSL, by comparing the received remote RSL with the Remote Nominal RSL value and adjusting accordingly.

The nominal power level set via Tx Static Attenuation serves as a starting point. Tx output power can be decreased if nominal power is not needed to maintain the Remote Nominal RSL value, but the Tx output power will never go above the nominal power level.

Figure 3-22 illustrates various parameters related to DTPC mode; the dashed line shows RSL as it would be without DTPC.

Figure 3-22: DTPC Parameters



For definitions of all TPC Mode configurable parameters, please see Chapter 7.

Security

If you have software version 6.x.x or higher, you will have the option of selecting BASIC or STRONG security. The BASIC security mode supports SNMPv1; the STRONG security mode supports SNMPv3, HTTPS and FTPS over TSL, and a RADIUS Server. BASIC is the default. Both modes support an Attack Prevention Mechanism.

Local Users

To create a new user, go to SECURITY > USER AUTHORIZATION.

As noted before, the default user is **admin** and the default password is **12345** if you have software version 4.5 or lower/**12345678** if you have software version 6.x or higher. This screen allows you to change your default user name and password as well as set up additional users.

To change the default name, click on the word **admin** so it is highlighted and click the EDIT button. Then you can enter a new name longer than 3 but no greater than 10 alphanumeric characters.

To add a new user, click on the CREATE button. Once you have done that, enter the user NAME (up to 10 alphanumeric characters) and PASSWORD (longer than 8 but no greater than 32 characters), confirm the PASSWORD, and select the appropriate permission level. Click ADD to add that user.

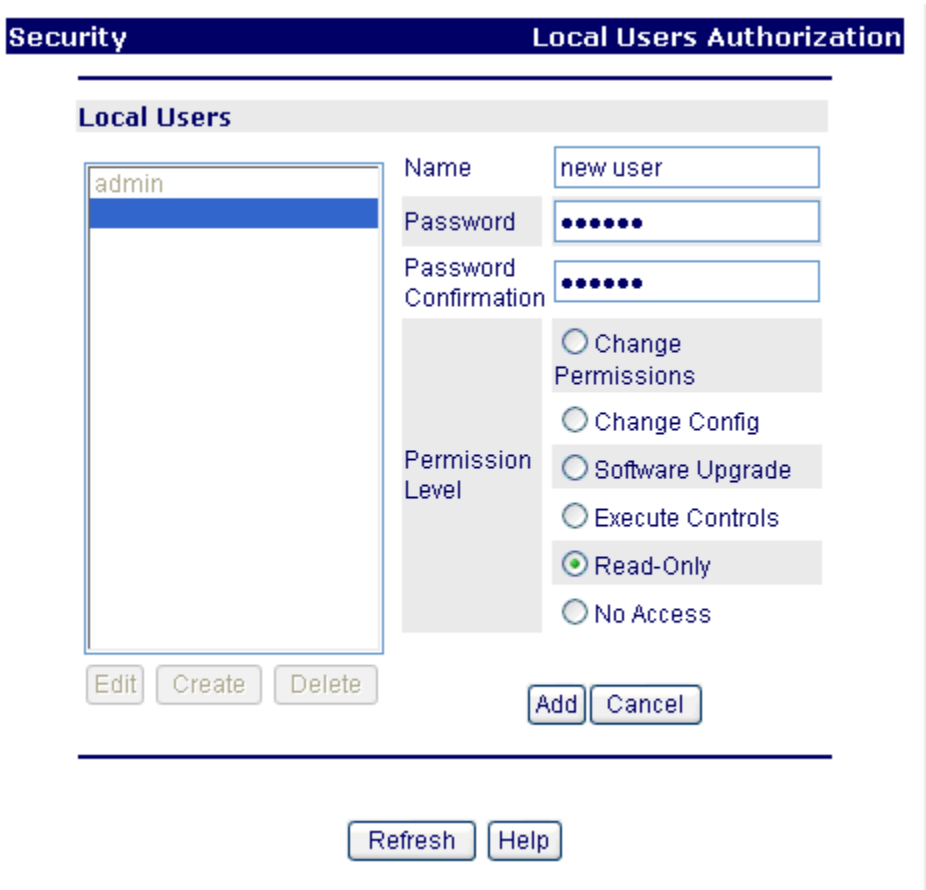
To change a user's access privileges, simply select a different permission level. Click UPDATE to make the appropriate changes. The available permission levels are listed in Table 3-11.

Table 3-11: Permission Levels

Level	Capability
No Access	The user cannot access the radio.
Read-Only	The user can access the radio but only to monitor the status, control, performance and configuration values.
Execute Controls	The user has all the privileges of the Read-Only level plus the ability to change the control values.
Software Upgrade	The user has all the privileges of the Execute Controls level plus the ability to upgrade the software running in the system.
Change Config	The user has all the privileges of the Software Upgrade level plus the ability to change the configuration of the system except for user authorization parameters.
Change Permissions	The user has all the privileges of the Change Config level plus the ability to change the user authorization parameters.

To delete a user, click on the user you want to delete so that the user is highlighted and then click the DELETE button.

Figure 3-23: User Authorization

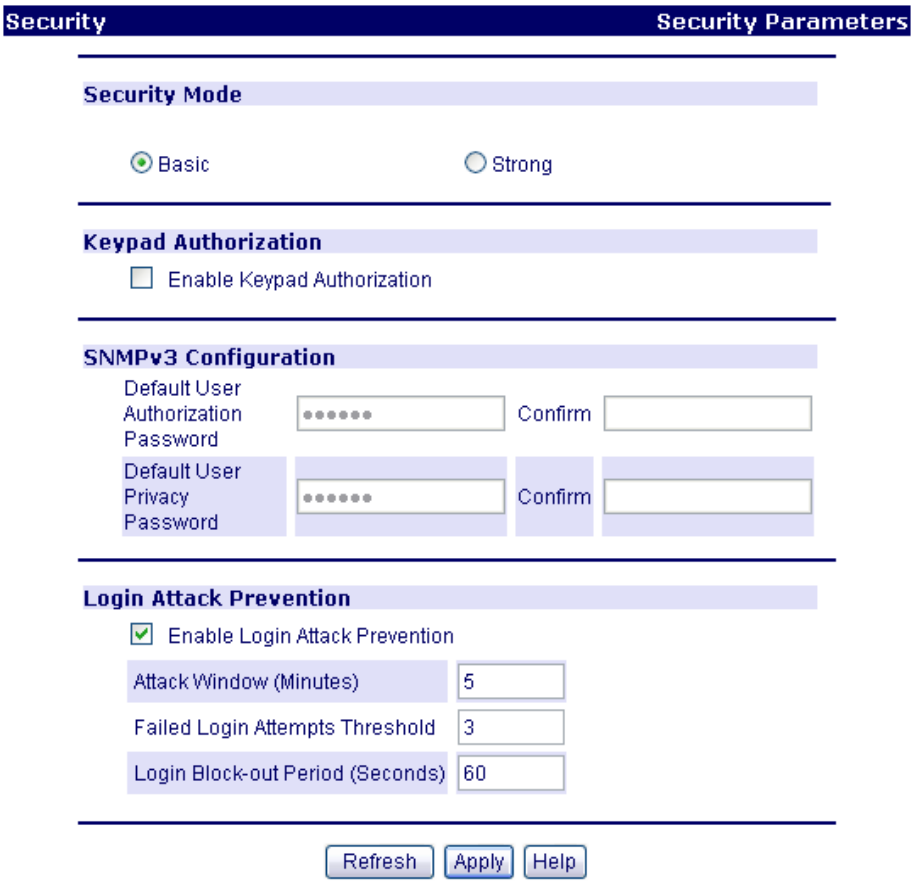


HHT: CONFIGURATION > SECURITY > LOCAL USERS.

Attack Prevention

Go to SECURITY > SECURITY PARAMETER (see Figure 3-24). Login Attack Prevention is available in both BASIC and STRONG modes, and is designed to prevent problems due to an attack from an unauthorized user. When this feature is ENABLED, once the FAILED LOGIN ATTEMPTS THRESHOLD (a number between 1 and 255) has been reached within the ATTACK WINDOW time period (0-2880 min.), any further authorization attempts will be locked out for the LOGIN BLOCK-OUT PERIOD (0-60 sec.). The default values appear in Figure 3-24.

Figure 3-24: Security Parameters



STRONG Security Option

If you want stronger security, go to SECURITY > SECURITY PARAMETER, change the security mode to STRONG, and click APPLY. The strong security option requires a software key.

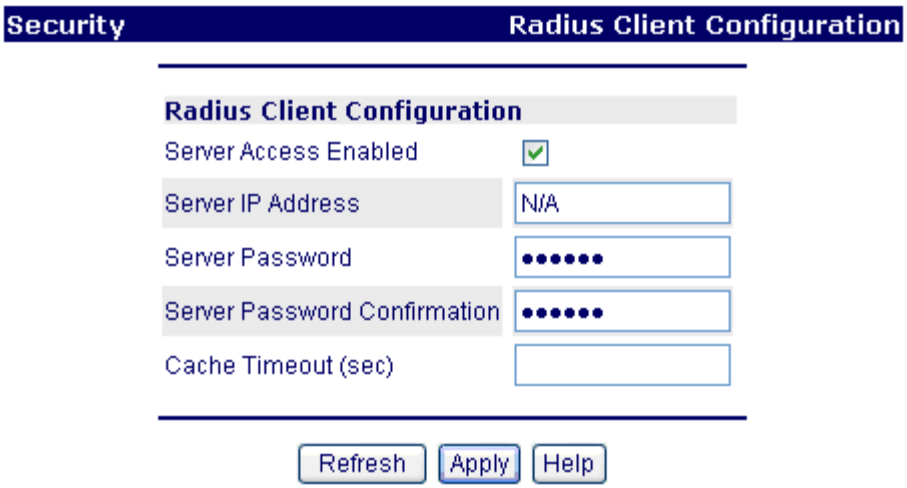
The STRONG security mode uses encryption, so when you change the mode from BASIC to STRONG, you may need to reload the Web-CIT using https rather than http.

Once you have selected STRONG, you will be able to set up SNMPv3 Configuration by entering the default user authorization and privacy passwords. These passwords must be from 8-18 characters.

Radius Client

STRONG security also allows you to access Radius Client Configuration, which allows you to access the Radius server, which in turn allows you to create a user on the server. This information is then disseminated to all radios on the server so you do not have to go to each radio and add a specific user. If you ENABLE Server Access, as seen in Figure 3-25, then the system will get its' information from the Radius Server, and a user can login to any radio from any interface if that user is in the server list. If it is not enabled, then only local users can access the system.

Figure 3-25: Radius Client Configuration



HHT: CONFIGURATION > SECURITY > RADIUS CLIENT.

Cached Accounts

Cached accounts contain information obtained from the RADIUS server that is cached locally for authentication and user authorization during a temporary absence of access to the server. A user name and password can be entered as required; the default user name and password fields contain an empty string. The user name and password obtained from the RADIUS server is cached for a configurable length of time. This function is not available when the radiusClient is disabled.

Configuration File Protection

In software version 6.x and higher, a configuration file is used which contains sensitive information. In addition, this file is encrypted so that an unauthorized user cannot gain information which would allow remote access to the system. The encryption is linked to the memory card.

Additional Web-CIT Options

Transmitter Switching

Transmitter switching is a protective mechanism which is triggered automatically in the event of a hardware failure. It can also be initiated manually. The following limitations apply:

- When the revertive transmitter switching option is enabled the Reverse channel switching option is disabled by the software.
- When the Reverse channel switching option is enabled the revertive transmitter switching option is disabled.

Revertive Transmitter Switching

Revertive switching automatically switches back to the original configuration when the fault is resolved (no alarm) and the channel becomes available.

Go to CONFIGURATION > CONTROLS > SYSTEM ONLINE and turn Tx Revert to A Switch ON.

HHT: CONTROL > SWITCH

Transmitter Reverse Channel Switching (RCS)

Reverse Channel Switching (RCS) allows you to protect the system against a transmitter silent failure and is available with MHSB or SD protection.

In a 1+1 protected MHSB system or SD system, RCS is a method of automatically switching to a standby transmit channel initiated by the corresponding receive end when the traffic outage occurs at the receive end. When only one transmitter is transmitting, the controller at the receive end issues a request to the transmit end to initiate transmitter switching when the online demultiplexer at the receive end experiences a synchronization alarm. If there is no higher switching priority for transmitter switching, the controller at the transmit end initiates switching to the standby channel.

RCS is useful for preventing a prolonged traffic outage in the event of a silent failure at the transmit end.

Go to CONFIGURATION > SYSTEM and select the RCS mode: Simple or Smart. You can also choose DISABLE, which will exclude the RCS state machine from the switching algorithm.

Both SIMPLE and SMART provide protection against a transmitter silent failure. SMART will switch back and forth to check if the problem is a path or an equipment failure while SIMPLE will not.

RCS Delay allows you to set a value between 0-20 seconds (in increments of 2 seconds) which determines how fast RCS will occur after the switching condition is detected.

When a Remote Sync Loss alarm appears in the system, the system waits the RCS delay time to see if the traffic has recovered. If the traffic has recovered, no switching occurs. It the traffic has not recovered, then the system switches the traffic from TxA (or B) to TxB (or A). In SIMPLE mode, this pattern continues until the traffic has recovered. Once the traffic is recovered no more switching occurs.

In SMART mode, the same pattern occurs at first. However, if the Remote Sync Loss Alarm clears after the first switch takes place and the traffic is recovered, the system then does another switch to check for a path failure. If the traffic is still recovered after the second switch, no more switching takes place. If the traffic is still lost, a third switch takes place and a Tx Silent Failure alarm is raised.

HHT: CONFIGURATION > SYSTEM > SPU > RCS MODE/RCS DELAY.

Receiver Switching

Receiver switching is a protection mechanism triggered automatically in the event of a hardware failure or in the event of path failure (flat fading or selective fading). It can also be initiated manually.

Go to CONFIGURATION > CONTROL > SYSTEM > Rx Decoder or Rx Dade/Demux and select SWITCH.

HHT: CONTROL > SWITCH and select RX/DECDR OR RXD/DMUX.

Optional Cards

Go to CONFIGURATION > OPTIONAL CARDS.

If you do not have any Optional cards in your system, a N/A will appear next to the Option Card box on the screen.

If you do have Optional cards, the type of Optional Card will appear on the screen and you will have the option of whether to use it or not by clicking on the check box next to the name of the card.

HHT: Depending on the type of Optional card you have, CONFIGURATION > RELAYS or CONFIGURATION > EXTERNAL ALARMS or CONFIGURATION > ORDERWIRE.

System Information

The first three entries on the CONFIGURATION > SYSTEM page are NAME, LOCATION, and CONTACT. Please note that these fields can contain up to 126 characters only.

Data Sheet

Go to CONFIGURATION > INVENTORY > DATA SHEET.

The Data Sheet page displays inventory information about the radio, as seen in Figure 3-26. If you want to print this information, select the “Save Page as File” button as seen on the right hand side of Figure 3-26. The information will be saved as a Comma Separated Value file which can then be imported into applications such as Microsoft Excel.

There are four data fields that you can fill out as seen on the left hand side of Figure 3-26 for printing purposes only. These fields are Customer Name, Rack Number, Site Name, and AGC voltage.

Figure 3-26: Data Sheet

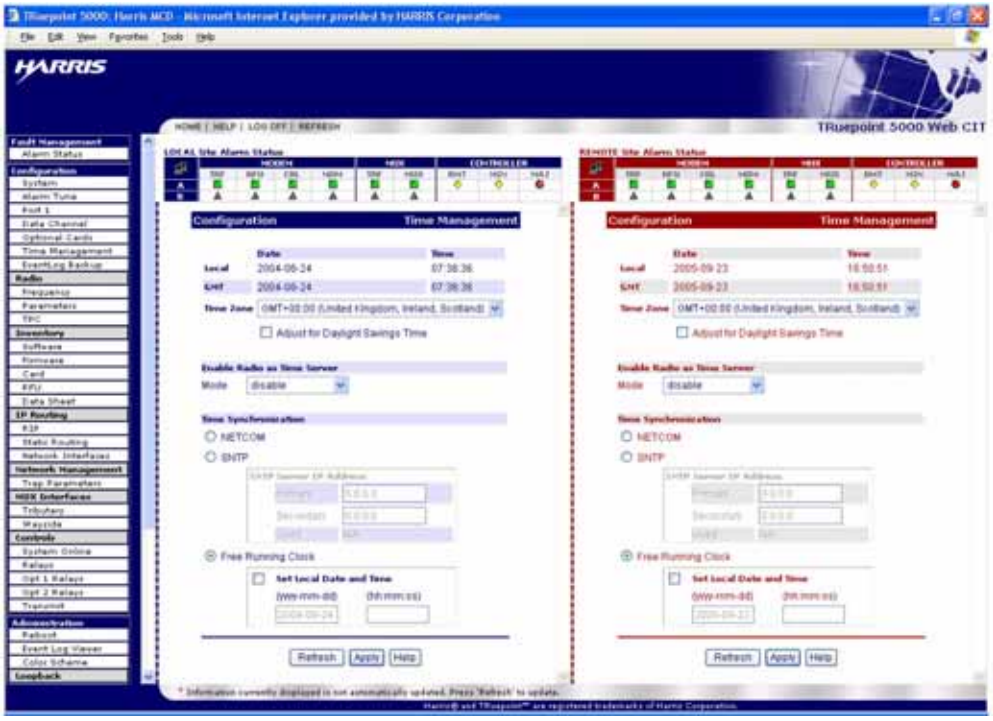
There is no equivalent to the Data Sheet in the HHT. However, the STATUS branch contains most of the same information.

Time Management

Go to CONFIGURATION > TIME MANAGEMENT.

The time management screen allows you to configure the radio's clock. The clock can be set independently or can be synchronized with a SNTP (Simple Network Time Protocol) server. This insures that its clock is in sync with other network elements sharing the same SNTP server.

Figure 3-27: Time Management Screen



HHT: CONFIGURATION > TIME MANAGEMENT.

Network Management

Harris point-to-point equipment is designed to work with standard protocols over standard media and with Harris legacy products using the proprietary SCAN and Netcom protocols. TRuepoint supports an IP network (the Web-CIT, SNMP, FTP), a Netcom network, and a SCAN network.

You can connect a TRuepoint radio to other Harris point-to-point radios via the NTWRK or LAN port to another Ethernet port (another TRuepoint, MicroStar Type II, or Constellation), via the HDLC serial port to a RPTR_OUT serial port (MicroStar Type I or Type III), or via Port 1 to a SPUR (AUX) port (MegaStar - Farscan only).

Furthermore, in a TRuepoint 5000 network, a mix of links using the V1 Controller and links using the V2 Controller are possible without any restrictions. It is also possible to mix both a V1 and a V2 on a hop, but the capability of the link will be driven by the least powerful Controller.

Figure 3-28: Example of a network with connections to other Harris radios

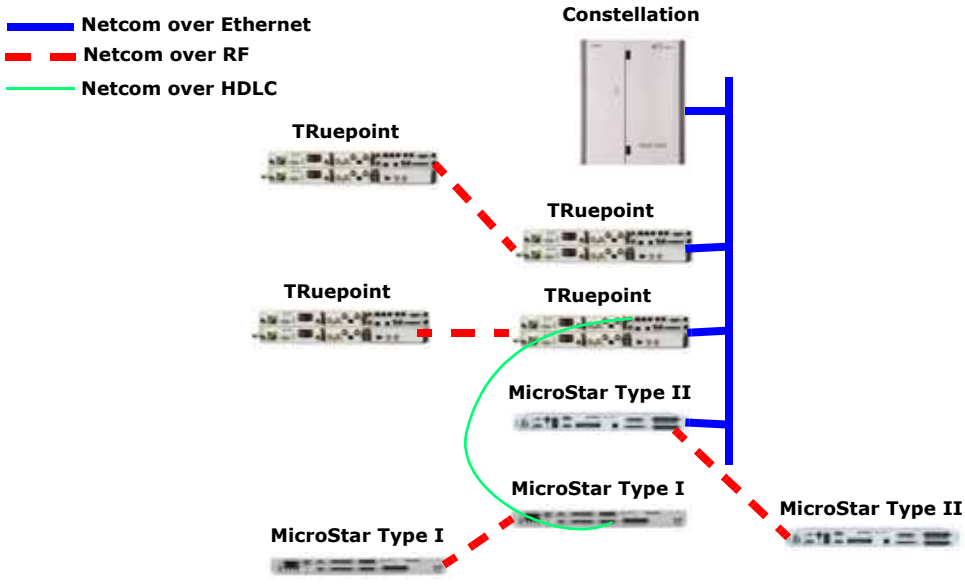
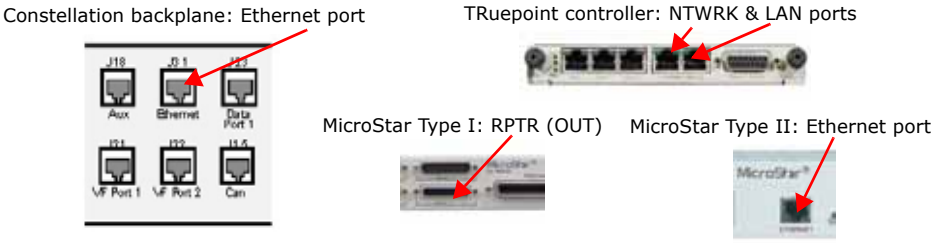


Figure 3-29: Connection Points from Figure 3-17



For an ethernet connection, we recommend that all external device(s) you use support auto-negociation. If the external device does not support auto-negociation, then the external device should be configured as 10 Mbits/s half duplex.

For more information on connecting the TRuepoint radio to other radios, please refer to Appendix B of the ***SPU Installation*** Manual, IMN-903002-Exx.

Network Configuration

The Netcom protocol uses an addressing scheme based upon the NE address. Each radio in the network should have its own NE address and messages can be sent to any node in the network by using that NE address. Each radio also needs an IP address which can be assigned manually or automatically based on the NE address.

Each radio has an Ethernet IP interface as well that has an IP address which can be assigned manually, automatically based on the Netcom NE address, or automatically using a DHCP Server. The Ethernet address is needed for connection to the Web-CIT and other customer equipment.

The NE address must be unique within a Netcom cloud. The Netcom cloud extends from a given radio to all neighbor radios connected to the given radio over air link, by Ethernet, or via a HDLC port. NE addresses can be re-used within different subnet clouds.

In order to break the Netcom cloud between two radios, you must make sure that the radios are not linked by air link nor connected via HDLC or Ethernet. If two radios are connected via Ethernet ports, you can break the Netcom cloud by disabling Netcom over Ethernet. When this is disabled, the two radios cannot talk via Netcom but can talk via IP.

The following information describes how to configure your local radio for networking. To connect to and configure remote radios through the Web-CIT, DHCP must be enabled on the Netcom interfaces, and the Ethernet interface of the remote radio must be configured.

For Network configuration, go to CONFIGURATION > IP ROUTING > NETWORK INTERFACES in the Web-CIT. The NETCOM IP INTERFACE should be set to ENABLE. Under MODE, select **Auto** or **Manual**. Auto is the default and will automatically generate the Netcom IP address and subnet mask for each radio based on the NE address. For example, if the radio's NE address is 333, then the Netcom IP address will be 172.23.33.1. If you select Manual, you will need to enter a Netcom IP address and subnet mask in the appropriate boxes.

Still in CONFIGURATION > IP ROUTING > NETWORK INTERFACES, the ETHERNET INTERFACE should be set to ENABLE as well. Under MODE, select **Auto**, **Manual**, or **DHCP**.

Auto is the default and will automatically generate the Ethernet IP address and subnet mask for each radio based on the NE address. For example, if the radio's NE address is 333, then the Ethernet IP address will be 10.3.33.1. See Figure 3-30.

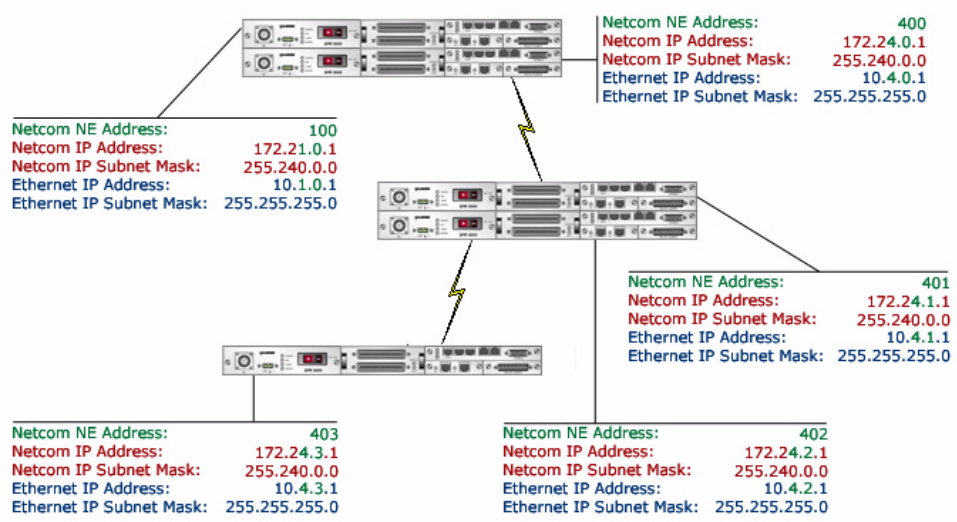
You also can elect to use the DHCP Server in the radio in order to configure other equipment such as a laptop or NMS. The DHCP Server will generate an IP address that in turn will grant a lease to a laptop (or other equipment) plugged into the Ethernet port on the radio. To use this option, select **Auto** for MODE, and then ENABLE the DHCP SERVER.

If you select **Manual**, you will need to enter a Ethernet IP address and subnet mask in the appropriate boxes.

If you select **DHCP**, you will need to have a DHCP server on your network. With this option, the radio becomes a DHCP client on your pre-existing network and the Ethernet IP interface will request an IP address from a DHCP server.

If you reconfigure the IP settings (change from Auto to DHCP for example), it is recommended that you perform a software boot.

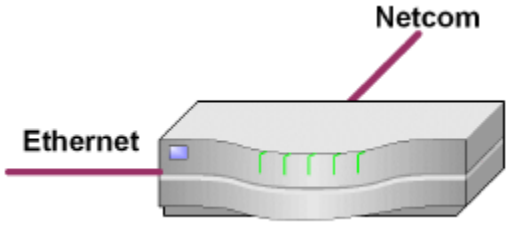
Figure 3-30: Example showing the automatic Netcom and Ethernet IP configuration based on the NE addresses



HHT: CONFIGURATION > NETWORK MANAGEMENT > IP ROUTING.

Routing

Each TRuepoint radio can be viewed as an IP router with two interfaces: Ethernet and Netcom.



In order to configure the router, the user has three options. The first option is to disable routing altogether and use a piece of third party equipment at each site to connect to each radio's Ethernet interface for management.

The second option is to define the network with a user-defined static routing table on each radio. This is applicable to very small networks only since there are 10 maximum static routes that can be defined. To use this option, go to CONFIGURATION > IP ROUTING > STATIC ROUTING. Enter the IP address, mask, and next IP router for each static route that you want to use.

HHT: CONFIGURATION > NETWORK MANAGEMENT > IP ROUTING > STATIC ROUTES.

The third option involves dynamic routing. The TRuepoint radio supports the RIP dynamic routing protocol which is a simple dynamic routing protocol that will broadcast all of its known routes periodically to the rest of the network. Each router receiving these updates can update their own routing tables with this information. The RIP daemon on the TRuepoint radio is configured to supply routes when more than one interface is enabled on the TRuepoint radio. The routes can be selectively broadcast on either or both of the Netcom or Ethernet interfaces. When enabled, routing updates will be sent every 30 seconds. Any received route that is not updated within 180 seconds will expire and be removed from the routing table. The RIP daemon can be configured in three different modes: disabled, Version 2 broadcast, or Version 2 multicast. The disabled mode disables all RIP operations. Version 2 sends and receives only RIPv2 updates which support classless addressing and variable length subnet masks.

HHT: CONFIGURATION > NETWORK MANAGEMENT > IP ROUTING > DYNAMIC ROUTING.

Data Transmission Protocols

The various protocols which can be used for data transmission are described in this subsection along with any limitation of use.

TLS

The TLS protocol is based on the SSL ver. 3.0 specification published by Netscape. The TRuepoint supports TLS version 1.0 per RFC2246 and uses the NE certificate for authentication. The TRuepoint accepts a TLS connection only if the security mode is set to strong.

Telnet and Telnet over SSL/TLS

When a Telnet connection is established, a VT-100 session is automatically started and the user is prompted for the required login. The VT-100 interface accessed by Telnet or by a terminal emulator allows a 20 column x 24 line screen and the ability to enter any alphanumeric character that is available from a keyboard. The type of connection depends on the security mode settings, as follows:

- Basic security mode – can only be used if the connection is not encapsulated
- Strong security mode – the connection must be encapsulated in TLS.

HTTP/HTTPS

The type of connection depends on the security mode settings, as follows:

- Basic security mode – a CIT session is started using HTTP
- Strong security mode – A HTTPS over TLS connection is started which is encapsulated.

FTP/FTPS

The type of connection depends on the security mode settings, as follows:

- Basic security mode – This requires a user name and password before completing the data connection request.
- Strong security mode – This requires a TLS connection with the client and a user name and password is required.

FTP can only be used with the Microwave Software Upgrade Utility (MSUU) and Paperless Chart Recorder (PCR) utility programs which are supplied by Harris.

SNMP

The type of connection depends on the security mode settings, as follows:

- Basic security mode – The SNMPv1 agent will reject all the SNMPv3 PDUs.
- Strong security mode – The SNMPv3 agent will accept and transmit data using the SNMPv1 security model. However, the default values are set so by default it is the SNMPv1 security model that is used to ease transition between the security models in the network.

SCAN

The FarSCAN and the ESCAN protocols are not secure, therefore, the system will not respond to requests unless security is set to basic. The maximum level of access is to access files.

SNMP

Each TRuepoint radio has an embedded SNMP agent on board allowing the user to configure, control and monitor the system using a remote station that supports SNMP Network Management.

To set up SNMP managers or trap destinations, go to SECURITY > SNMP MANAGERS or TRAP DESTINATIONS. You may enter up to 10 SNMP managers and up to 10 trap destinations. To set up trap parameters, go to CONFIGURATION > NETWORK MANAGEMENT > TRAP PARAMETERS. For a complete list of traps, please see page 5-13.

HHT: CONFIGURATION > NETWORK MANAGEMENT > SNMP.

The Get and Set community strings need to be configured as well if you do not want to use the defaults of “public” for Get community and “private” for Set community. Get and Set community can be modified only through a VT-100 terminal. To modify these, go to CONFIGURATION > NETWORK MANAGEMENT > SNMP > COMMUNITY STRINGS. Enter the name you want using the VT-100 terminal.

The SNMP protocol was developed to provide an easy to implement network management tool. The TRuepoint SNMP agent supports SNMPv1, v2c, and v3. The SNMP manager is usually running on a computer at the network operation center. An STNP agent is embedded in the NE.

A terminal that is configured as SNMPv3 (strong security) will reject any unsecured SNMPv1 commands that are addressed to that terminal. However, the terminal will let SNMPv1 commands pass through. Likewise, a SNMPv1 terminal will let SNMPv3 commands pass through but will reject any SNMPv3 commands that are addressed to that terminal.

CHAPTER

4

UPGRADES

Introduction

This chapter is designed to guide you through the options you have when upgrading your software and firmware. Harris provides two utilities that provide many different options of upgrading your system.

The Microwave Software Upgrade Utility (MSUU) offers the following options for upgrading your software and firmware:

- Single-host Upgrade
- Multi-host Upgrade[1]
- Direct Flash Upgrade
- ESCAN Upgrade

In addition, the following tools are also available through the MSUU:

- Configuration Backup/Restore
- Customization
- Software Key

The MSUU is designed to run with Windows 2000®.

The Configuration Transfer Utility (CTU) gives you the ability to upgrade from a V1 to a V2 Controller or downgrade from a V2 to a V1 Controller without losing your configuration files.

If you are upgrading from software version 4.x or lower to 6.x or higher you will need the V2 Controller. You cannot upgrade the software without purchasing a V2 controller because the V1 controller does not support software version 6.x and higher.

1. *Future availability*

Please refer to the ***SPU Installation*** manual, IMN-903002-Exx for information on upgrading the Controller.

It is strongly recommended that you upgrade to the latest TRuepoint software before swapping any spare parts. This will ensure that your system can recognize the latest hardware.

If you want to transfer your configuration data from one flash card to another, and you are not changing the Controller type, you can use the Direct Flash Upgrade tab of the MSUU. See Configuration Data Transfer.

To backup your configuration files from your flash card or from a remote site, use the Configuration Backup/Restore tab of the MSUU.

Upgrade Kits

Upgrade kits are available for MUX capacities and for the software features that require a software key. Contact Harris Customer Service for more information on purchasing an upgrade kit. For information on upgrading your software with a software key, go to Software Key on page 4-20.

MUX Connection

When upgrading from a release earlier than Release 3.x.x of the software to Release 3.x.x software, you may need to change the connection if you have one of the following multiplexers:

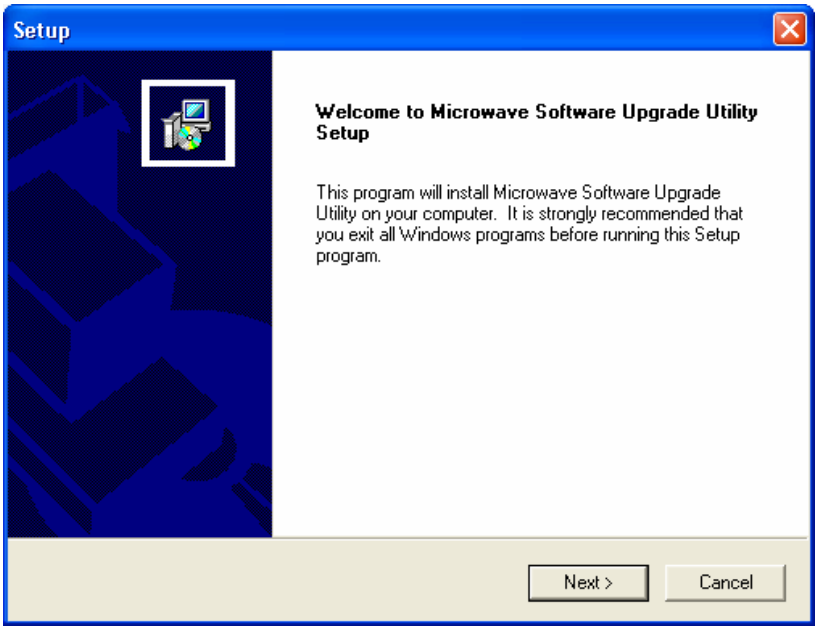
- OC3/STM1
- DS3/E3/100BT

If you have one of these two MUXes, and you have a 2 RMS shelf with a SDM installed, then you will need to reconnect the cables from the MUX face plate to the SDM during the upgrade to Release 3.x.x.

Microwave Software Upgrade Utility

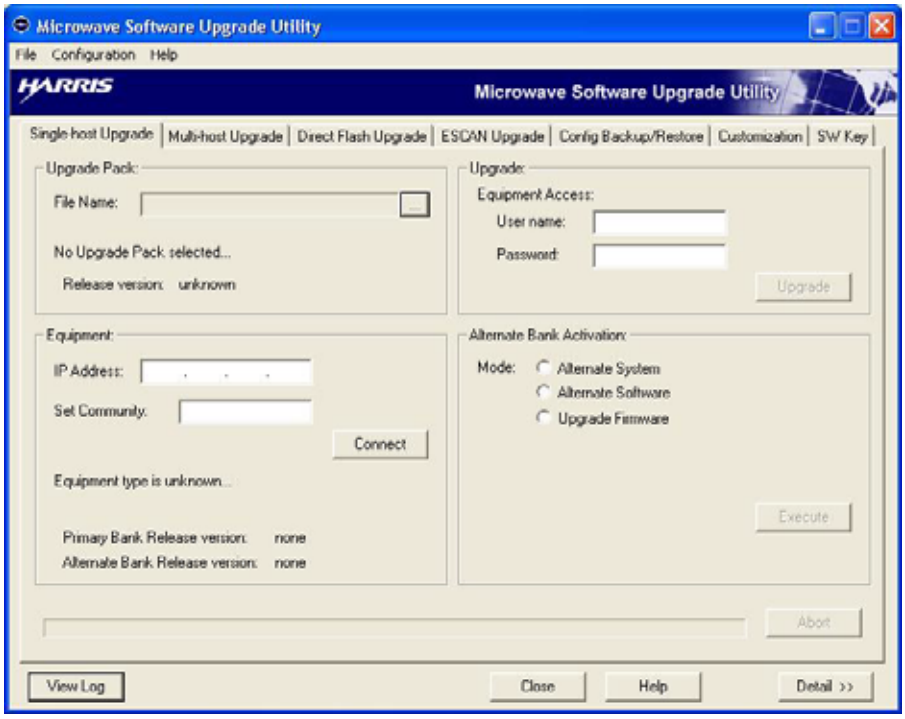
To install the program, extract the files from the MSUU.zip file found on your Harris TRuepoint Software CD. Click on the setup.exe file and Figure 4-1 will appear.

Figure 4-1: MSUU Installation



Once you have installed the MSUU, a shortcut will appear in your Start Menu under Programs > Harris MCD > Microwave Software Upgrade Utility. When you load the MSUU, a screen similar to Figure 4-2 will appear.

Figure 4-2: MSUU

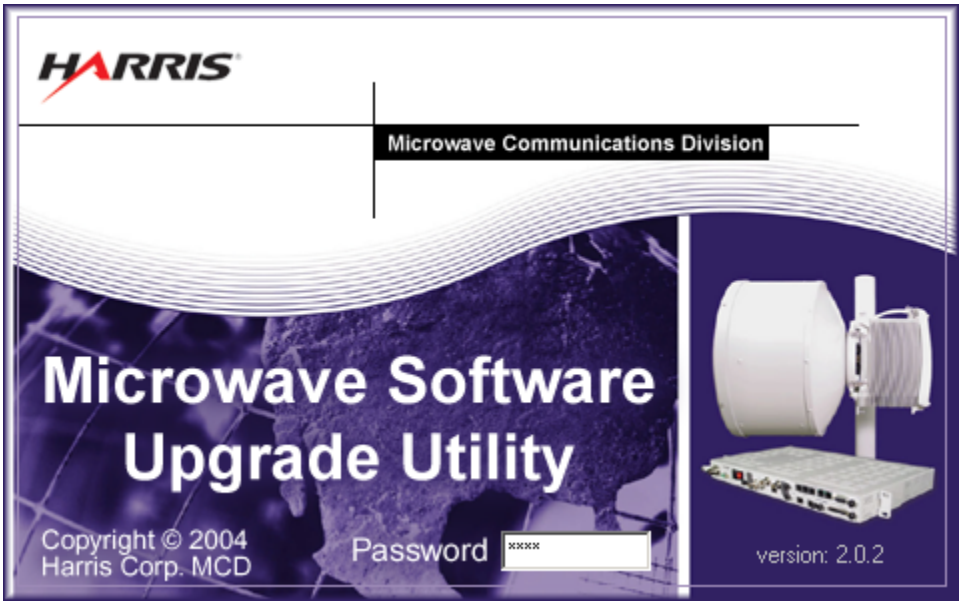


Anytime you switch to new software, the Web-CIT should be closed and reopened to make sure that any new or updated pages are uploaded.

You can password protect the MSUU. If you want to turn password protection on, go to the Configuration Menu and then choose MSUU Access. You will need to enter a password in the New Password and Retype New Password fields and then click the OK button. To change the password at a later date, follow the same steps. Passwords can be up to 15 characters.

Once you have set a password, when the MSUU starts up you will see the screen shown in Figure 4-3. Enter the password in the appropriate spot and then the Enter key.

Figure 4-3: MSUU password screen

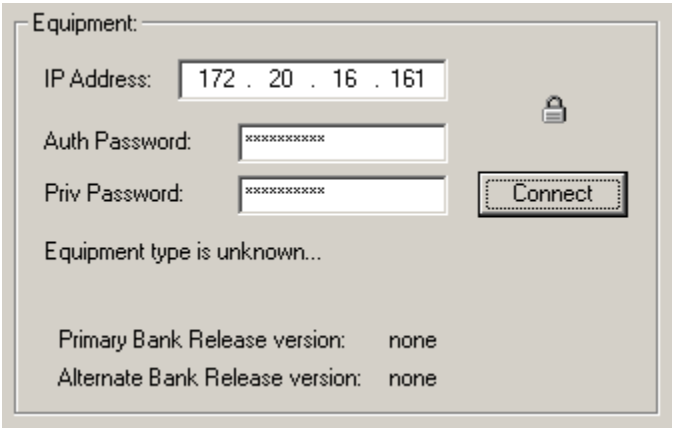


Single-host Upgrade

The Single-host Upgrade allows you to upgrade the software and firmware in a specific Harris radio. See Figure 4-2.

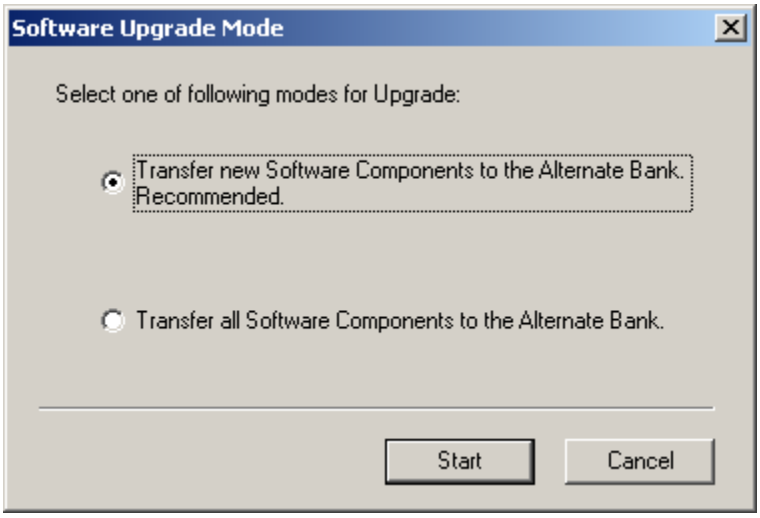
1. Click on the ... button and select the appropriate Upgrade Pack file. This will be a .zip file. Click on the Detail button for the contents of the Upgrade Pack file.
2. Enter the IP Address and SNMP Set Community name of the target radio. If the MSUU is operating in Strong Security mode, you will need to enter the authentication and privacy passwords instead of the community name.

Figure 4-4: Strong Security option



3. Press the Connect button to get a SNMP connection to the target radio. Once the connection is established, the software and firmware information will be retrieved from that radio and the Primary Bank Release version and Alternate Bank Release versions will appear. Click on the Detail button for more information on the Primary Bank content and the Alternate Bank content.
4. Enter your user name and password for the target radio. You must be an authorized user with Software Upgrade permissions. See "Security" on page 3-38 for more information.
5. Click the Upgrade button. If the radio has data already in the Alternate Bank Figure 4-5 will appear. You must choose whether to transfer all components or just those that are new and then click the Start button. If there is no software in the Alternate Bank, the MSUU will automatically transfer all new components. When the process is done a new window should appear stating that the upgrade process was successful.

Figure 4-5: Upgrade Mode: Single Host



6. To switch memory banks (restart the radio with the alternate memory bank) select Alternate System or Alternate Software and then press the Execute button. A warning message will pop up; click Yes to continue the process.

The Alternate System option will download the firmware files as well as switching the Primary and Alternate banks. This option will interrupt traffic. The Alternate Software option only switches the Primary and Alternate banks and thus does not affect traffic.

7. If you only want to download the firmware files to the cards but do not want to switch the software banks, select Upgrade Firmware. This will upgrade the cards from the firmware contained in the Primary Bank.

The Upgrade Firmware option cannot be accessed unless the Alternate Software option has already been executed.

8. Once the restart process has finished, the Equipment, Primary Bank content, and Alternate Bank content boxes under Detail will be updated.

Direct Flash Upgrade

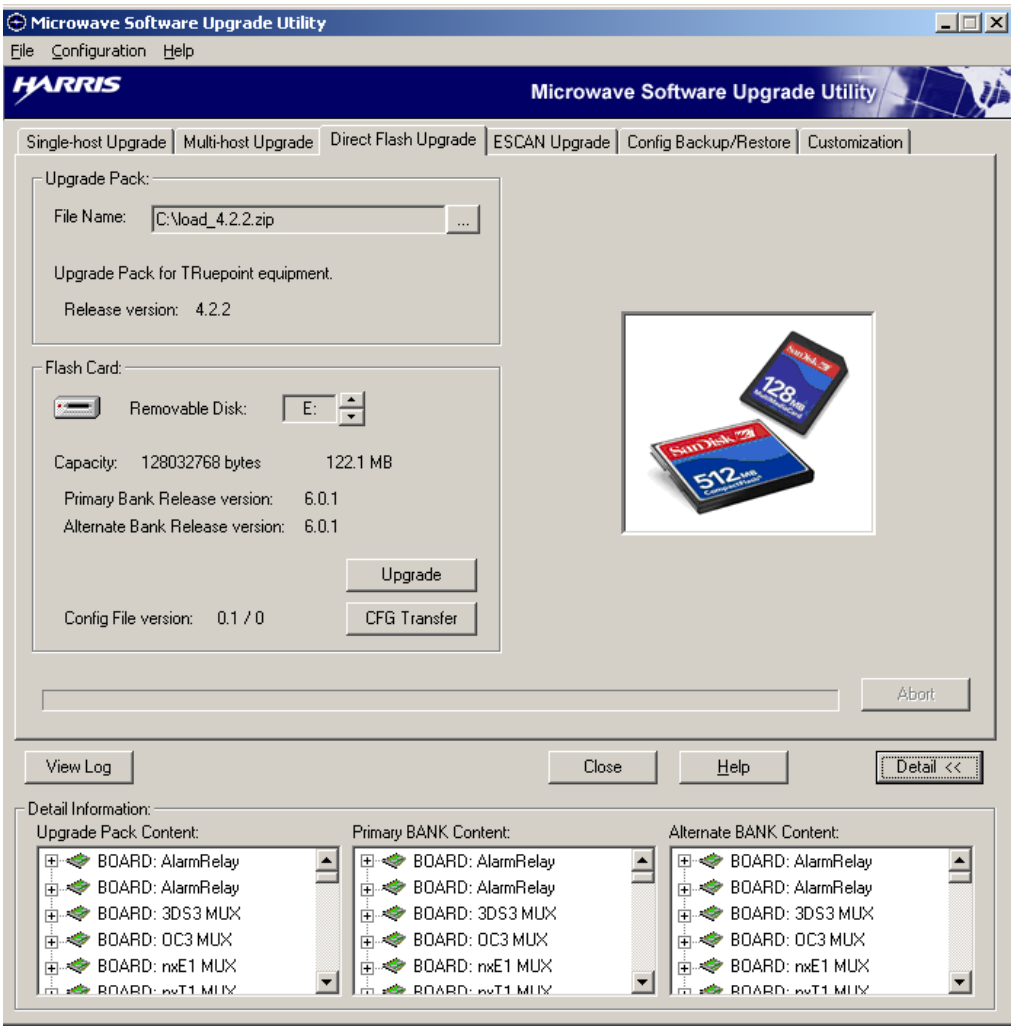
The Direct Flash Upgrade allows you to upgrade the software and firmware in the flash card by using a flash card reader connected to your PC. If you have the V1 Controller you have a MMC type flash card. If you have a V2 Controller you have a compact flash card.

You may use any type of reader as long as it supports the type of flash card you have. For MMC cards, Harris recommends a SanDisk MMC reader.

WARNING!!!
The software files from one flash card should never be copied to a PC and then to another flash card. Use the MSUU to transfer the configuration data from one flash card to another (see "Configuration Data Transfer"). The MSUU validates the files and sets a hidden attribute which is required for the software to work properly.

The only file that can be copied is a configuration file - _CONFIG.DAT file located in the CONFIG folder. If you want to archive the configuration you should copy only this file to a PC which can be used to restore the configuration. This can be accomplished by copying the archived _CONFIG.DAT file into the card which is initialized during the software file installation process.

Figure 4-6: MSUU: Direct Flash Upgrade

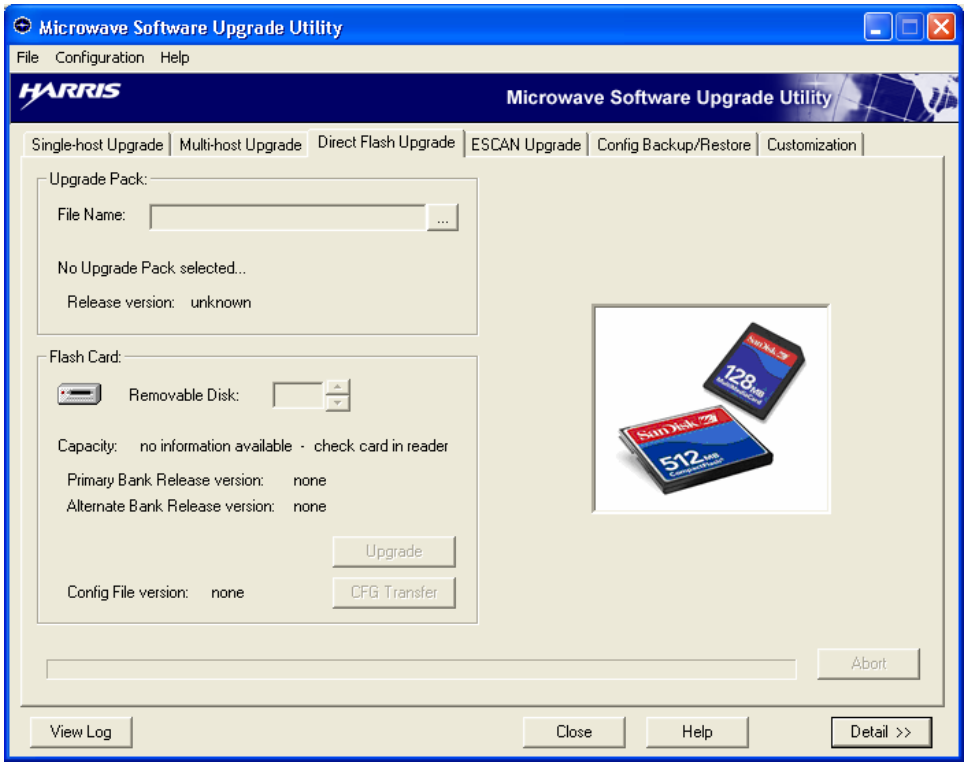


1. Click on the ... button and select the appropriate Upgrade Pack file. This will be a .zip file. Click on the Detail button for the contents of the Upgrade Pack file.
2. Insert the flash card into the flash card reader. The MSUU will automatically find the flash card and display the card capacity in the Capacity field as well as the primary and alternate bank versions. If the flash card has software already, the primary and alternate bank information will display in the Detail area. See Figure 4-6.

If you have two or more card readers on your computer, the removable disk (mapping the card reader) should be selected using the arrow buttons. The current card reader disk is shown in the Removable Disk field.

If for some reason the reader does not recognize the flash card, the boxes under Capacity will stay shaded. See Figure 4-7.

Figure 4-7: Direct Flash Upgrade: card not recognized



If this happens you have the following two options.
Option 1: From the Task bar, double-click the reader icon and STOP the USB Mass storage device. Figure 4-8 should appear. Now unplug the reader and then plug it back in.

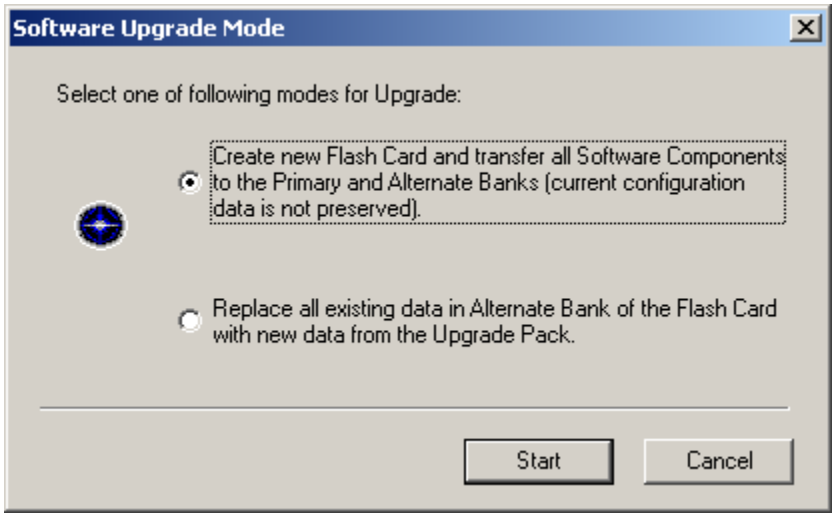
Figure 4-8: Stopping the USB Mass Storage Device

Never unplug the reader from a PC or remove the MMC card from the reader without stopping the USB Mass storage device.

Option 2: Highlight the removable disk in the "My Computer" window. In the File menu, select Eject. Now remove the flash card and then reinsert it.

3. Click the Upgrade button. If the radio has data already in the Alternate Bank Figure 4-9 will appear. You must choose whether to create a new flash card or just to replace the data in the alternate bank and then click the Start button. If there is no software in the Alternate Bank, the MSUU will automatically create a new flash card.

Figure 4-9: Upgrade Mode: Direct Flash



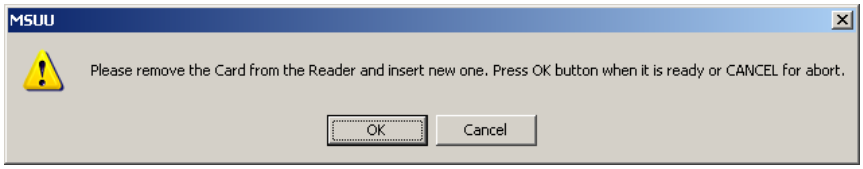
4. After the upgrade process is finished, a new window will appear asking you to eject the flash card from the reader.

Configuration Data Transfer

You can use the Direct Flash Upgrade screen as well to transfer configuration data from one flash card to another flash card.

1. Insert the flash card into the flash card reader. The MSUU will automatically find the flash card and display the card capacity in the Capacity field as well as the primary and alternate bank versions. If the flash card has software already, the primary and alternate bank information will display in the Detail area. See Figure 4-6. If no configuration data is found on the flash card then the CFG Transfer button will be disabled.
2. Click the CFG Transfer button to start the configuration data transfer. The MSUU will read the data from the flash card and ask you to insert a new card.

Figure 4-10: Data Transfer



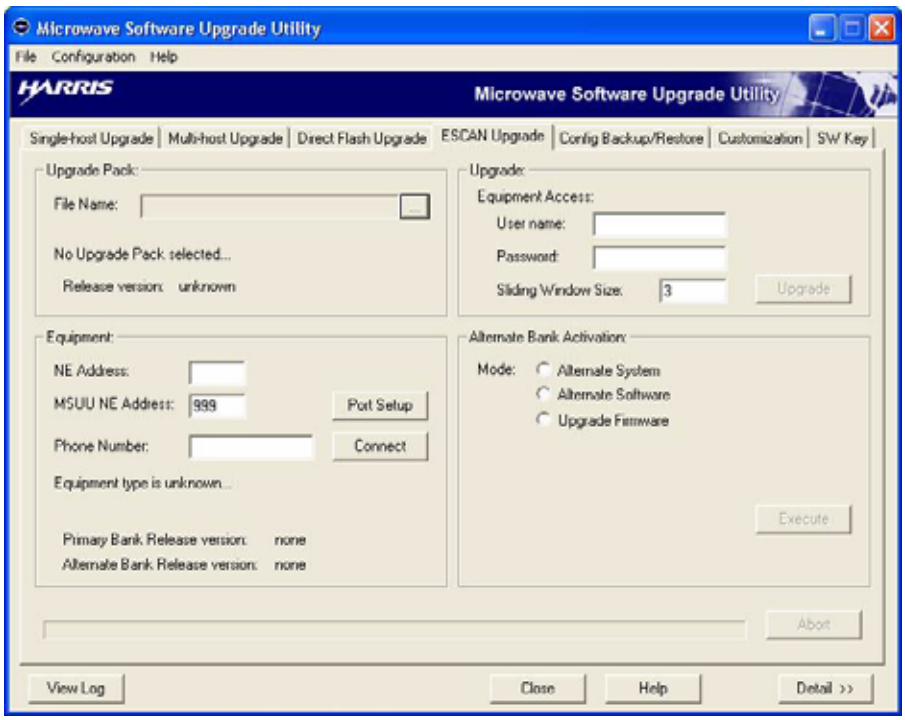
3. When the transfer process is done, a new window will appear asking you to eject the flash card from the reader.

Only the configuration data that can be changed with the Web-CIT or the HHT will be transferred. Any history data or the event log will not be transferred.

ESCAN Upgrade

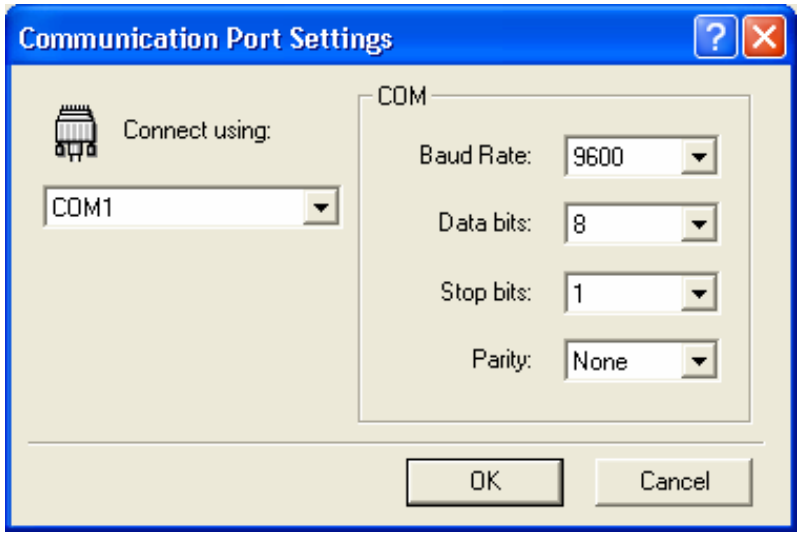
The ESCAN Upgrade allows you to upgrade the software and firmware utilizing the radio's ESCAN interface.

Figure 4-11: MSUU: ESCAN Upgrade



1. Click on the ... button and select the appropriate Upgrade Pack file. This will be a .zip file. Click on the Detail button for the contents of the Upgrade Pack file.
2. Enter the NE Address for the equipment. Make sure that the MSUU NE Address is filled in as well; the default for the MSUU NE Address is 999.
3. Click on Port Setup. Figure 4-12 will appear.

Figure 4-12: Port Setup



4. Enter the appropriate settings. The settings you enter should match the COM port settings in the Harris Keypad. If you selected a modem for connection, enter the phone number. Click OK when you are finished.
5. Click Connect. Once you are connected to the equipment, the current software (primary bank release), the software in the alternative bank, and a description of the equipment should appear.
6. Enter your user name and password for the target radio in the "Upgrade" box at the top right of the screen. You must be an authorized user with the appropriate security access. See "Security" on page 3-38 for more information.
7. Enter the sliding window size; the default is 3 and the maximum is 7. If you are upgrading a radio that is some distance from the current site then you may want to increase the sliding window size to facilitate a faster download.
8. Click Upgrade. If the equipment already has data in the Alternate Bank, you will need to select an Upgrade Mode (see Figure 4-5) and then click Start.
9. Once the download process has finished, a new window should appear stating that the download/upgrade process was successful and the Alternate Bank Release version will be updated.
10. To switch memory banks (restart the radio with the alternate memory bank) select Alternate System or Alternate Software and then press the Execute button. A warning message will pop up; click Yes to continue the process.

The Alternate System option will download the firmware files as well as switching the Primary and Alternate banks. This option will interrupt traffic. The Alternate Software option only switches the Primary and Alternate banks and thus does not affect traffic.

11. If the firmware components in the cards are different than the firmware components in the Primary Bank, you can select Upgrade Firmware. This will upgrade the cards from the firmware contained in the Primary Bank.

The Upgrade Firmware option cannot be accessed unless the Alternate Software option has already been executed.

12. Once the restart process has finished, the Equipment, Primary Bank content, and Alternate Bank content boxes under Detail will be updated.

13. When you are done, click Close to exit the program.

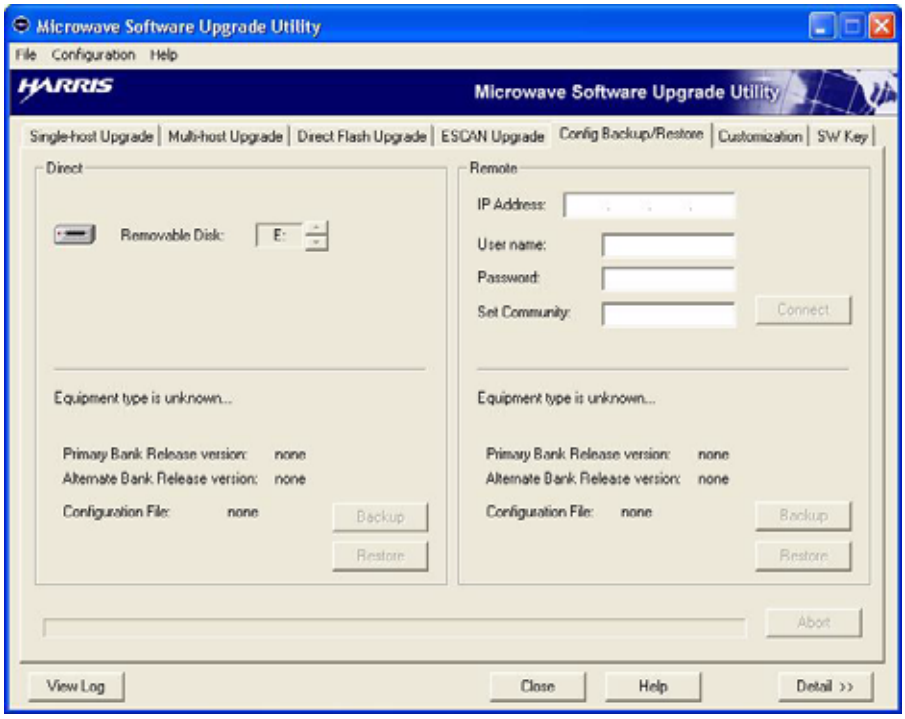
Configuration Backup/Restore

To back up the configuration data contained on the radio, select the Config Backup/Restore tab. This allows you to upload the config. dat file from the radio remotely or the radio's flash card using a reader, put it on a local drive, and then restore the file.

This is a traffic affecting action as it reboots the Controller.

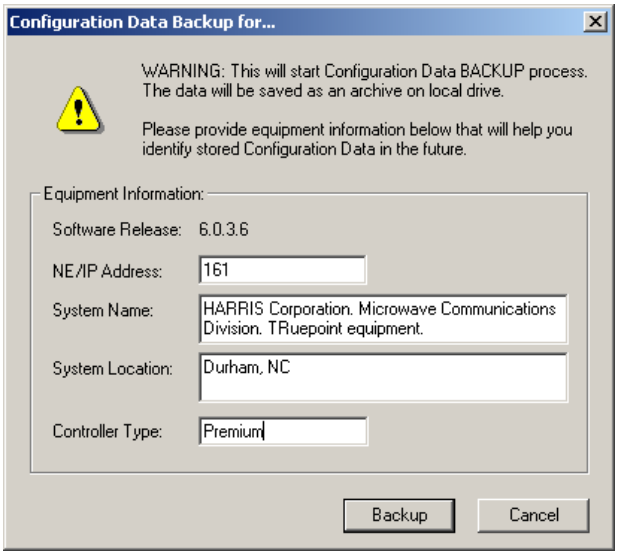
1. Insert the flash card into a appropriate reader and then select the removable disk. If you want to get a remote radio's config.dat file, enter the appropriate information under the "Remote" section and press the Connect button.

Figure 4-13: Config Backup/Restore



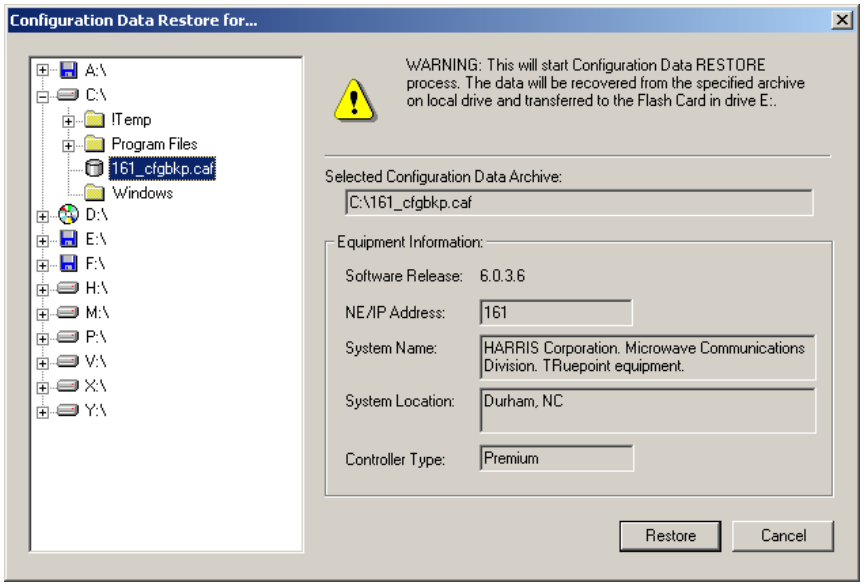
2. Once you have chosen the flash card or connected to the remote site, the Primary and Alternate Bank versions should appear. Click on the Backup button to upload the information from the radio. You will be asked for information that will aid in the restore process; see Figure 4-14.

Figure 4-14: Backup/Restore Information



3. Once you have filled out this information, press the Backup button to continue the process. You will then be asked for a password (8-32 characters) that will be used to access the configuration data that will be stored on the local drive. Press the OK button to continue.
4. You will be prompted to enter a file name; this file will have a .caf extension. The MSUU will decrypt the file and then re-encrypt it to put on the local drive.
5. To restore the file, insert a flash card into a reader or connect to a remote radio as you did for the Backup process. Click on the Restore button.
6. Select the backup file as shown in Figure 4-15 and click the Restore button to continue. You will then be prompted to enter the password that you specified in the Backup process. If you enter the wrong password 3 times then the restore process will be cancelled.

Figure 4-15: Select a Backup File



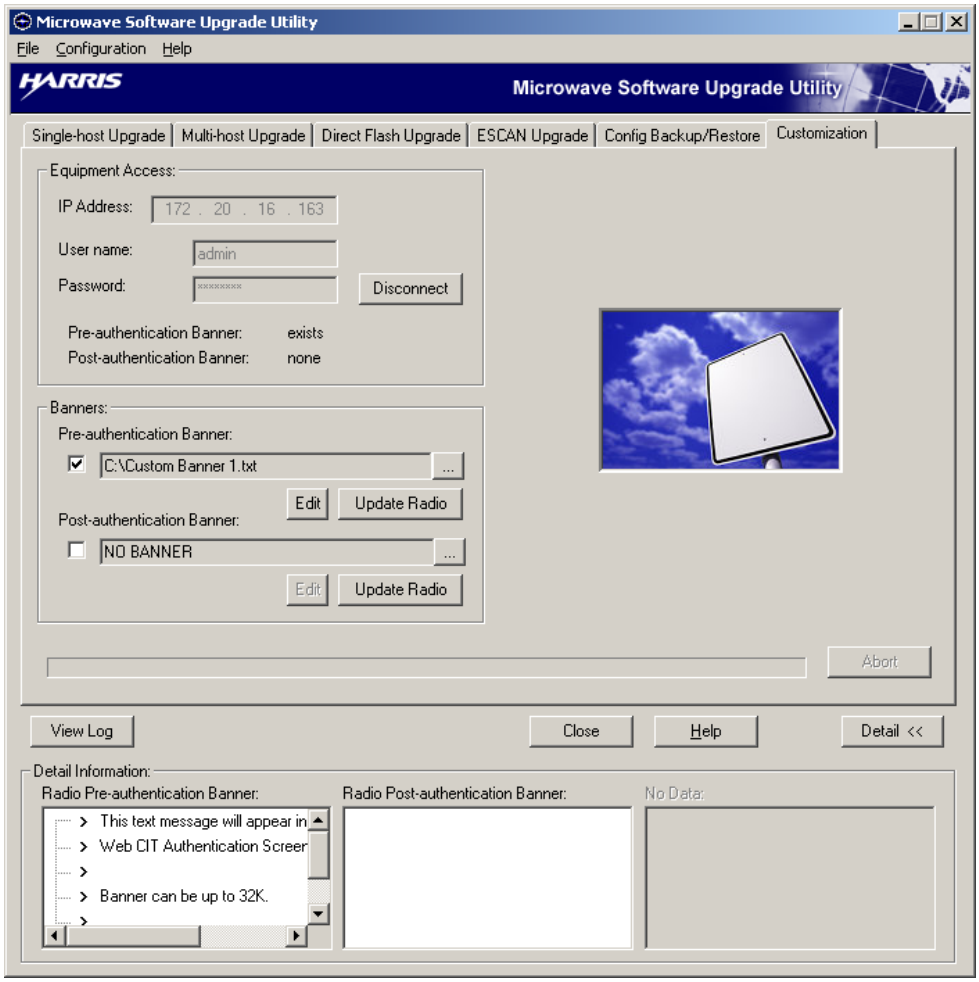
7. Once you have entered your password, click OK to continue. The MSUU will then save the file back to the radio.

Customization

The Customization tab in the MSUU allows you to update custom defined data in the radio. There are two type of customization data:

- Pre-authentication Banner: This is a text message that appears on your web browser as soon as a HTTP connection is made with the radio, before the Web-CIT login prompt.
- Post-authentication Banner: This is a text message that appears on your web browser after a user has been authorized to access the radio.

Figure 4-16: Customization

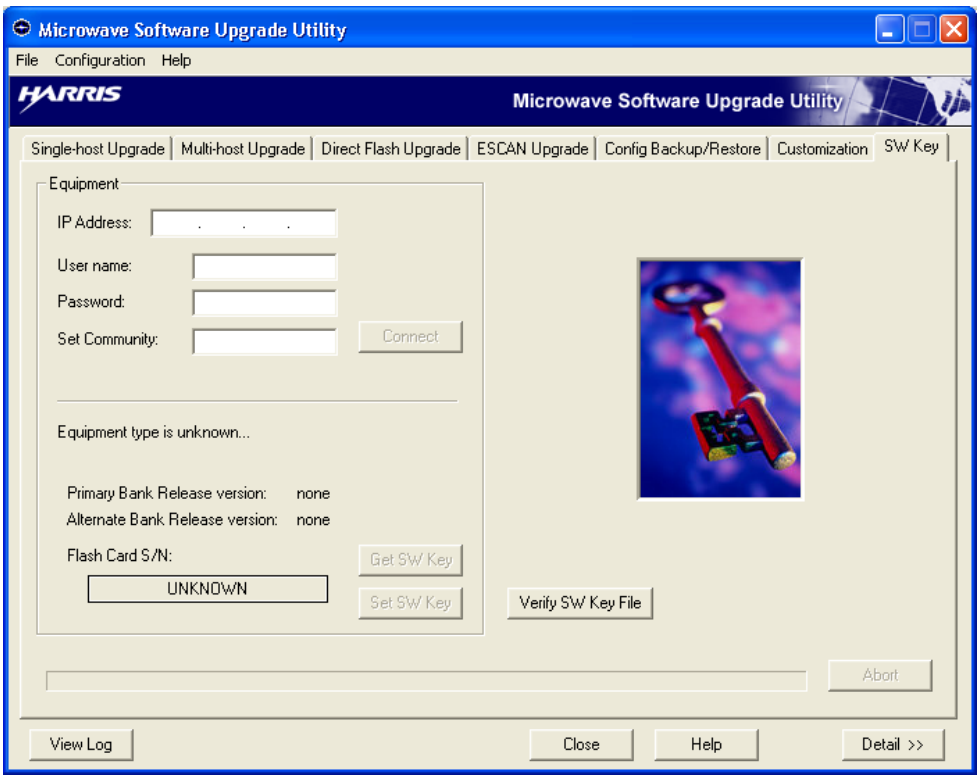


1. Connect to the radio by entering the IP address, user name, and password and then clicking the Connect button.
2. If there are any banners present already, these will shown in the appropriate boxes under Detail. See Figure 4-16.
3. To specify a file that contains the banner text, click on the ... button and select the appropriate text file. Once you select a file, the checkbox next to the file name will be automatically checked. If you want to remove an existing banner, uncheck the check box.
4. To edit the banner text, click the Edit button. Make your changes and save.
5. Click on the Update Radio button to upload the information to the radio. As long as the checkbox is checked, the MSUU will transfer the data to the radio and set it as a banner. When the process is complete the Detail boxes will be updated.

Software Key

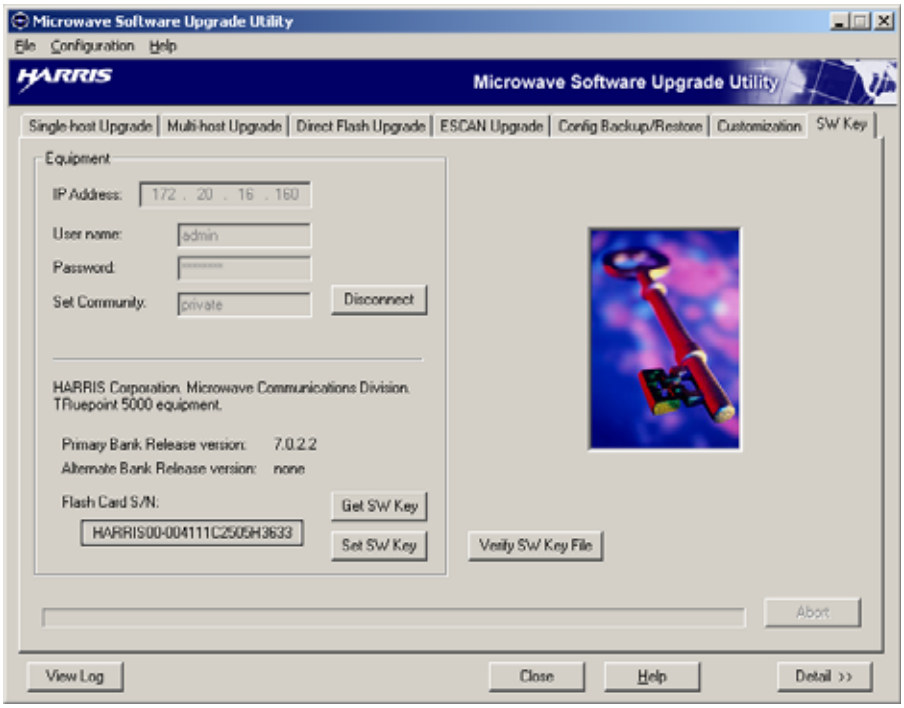
Once you have purchased a software key you will need to upload it to your radio using the MSUU. Select the SW Key tab.

Figure 4-17: Software Key Tab



1. Enter the IP Address, User name, Password, and Set Community to connect to the radio that is going to be upgraded. If you are in Strong security mode, you will need to enter the Auth and Priv passwords instead of the Set Community. Click Connect to connect to the radio.
2. Once you are connected, the Primary and Alternate Bank versions will appear as well as the Flash Card serial number of the radio (see Figure 4-18). This serial number is a unique number for the specific flash card. If you click on the number, it will automatically copy to the clipboard.

Figure 4-18: SW Key screen: Connected to radio



3. If you do not already have your software key file, you will need to email this serial number to Harris Customer Service who will then generate a software key file for you and email it back. If you do have a software key file, and you want to verify it, click on the Verify SW Key File button.
4. Click on the Set SW Key button. Select the software key file that you received from Harris Customer Service. The software key will install on your radio and then the radio will reboot.
5. If you already have a software key and you want to upgrade it, you can use the Get SW Key button to get the software key file off of the flash card, save it, and then email it to Harris Customer Service. They will upgrade it and send it back to be uploaded using the Set SW Key button.

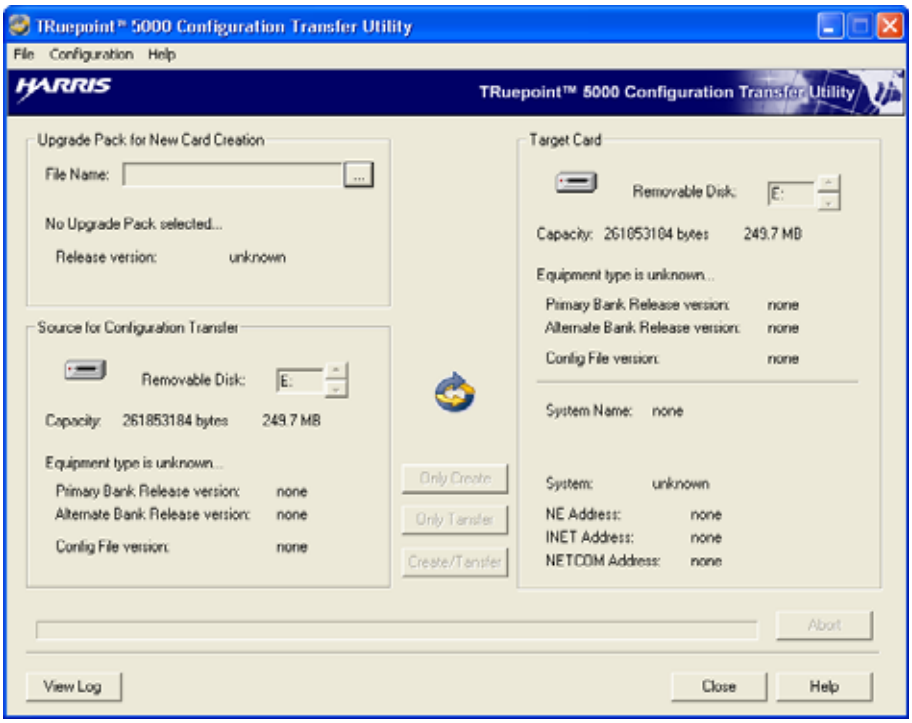
You CANNOT upload the software key directly on to the flash card using a flash card reader. The software key will not work.

If the software key file does not match the serial number of your flash card, you will get an error message and the software key will not work.

Configuration Transfer Utility

The Configuration Transfer Utility (CTU) is designed to transfer configuration files from one type of Controller (V1 or V2) to a different type of Controller. To install the program, extract the files from the CTU.zip file found on your Harris TRuepoint Software CD. Once you have installed the CTU, a shortcut will appear in your Start Menu under Programs > Harris MCD > Configuration Transfer Utility. When you load the CTU, a screen similar to Figure 4-19 will appear.

Figure 4-19: CTU



There are three possible actions: Create a new Flash Card, transfer configuration data from one flash card to another, or do both of these actions as one step.

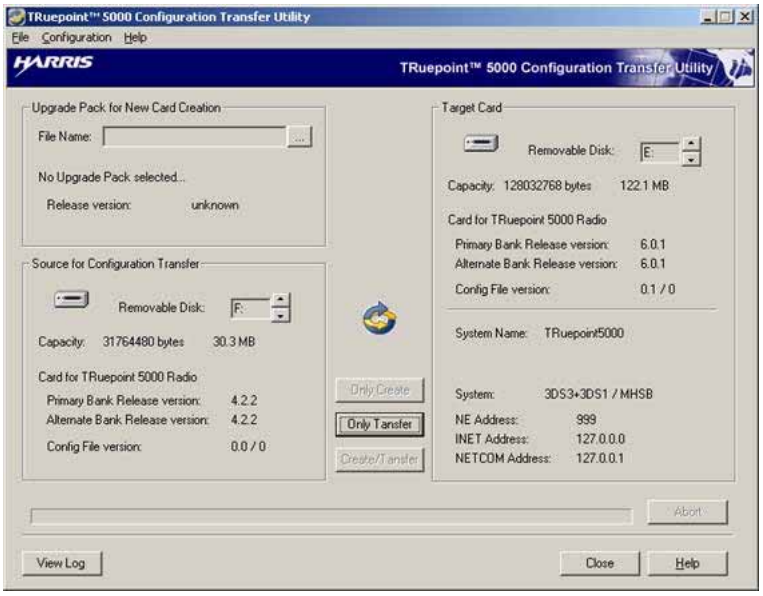
Create a new Flash Card

1. Click on the ... button and select the appropriate Upgrade Pack file. This will be a .zip file. See Figure 4-19. Once you have done this, the type of radio and software version number will appear.
2. Insert a flash card into your card reader and select the appropriate drive using the "Removable Disk" scroll buttons under "Target Card". If the card is empty, only the card capacity will appear. If the card contains TRuepoint software, the radio type information and Primary and Alternate bank software versions will appear. If the card has configuration data, the Configuration File version will appear.
3. Once you have an Upgrade Pack and a Target Card selected, the "Only Create" button will be active. Press this button to create a new flash card.
4. The flash card you specified will be formatted and the data from the upgrade pack will be transferred to the Primary and Alternate banks. You can stop this process at any time by selecting the "Abort" button. If you Abort, the data on the flash card will be corrupted.
5. After the upgrade process is finished, a new window will appear asking you to eject the flash card from the reader.

Transferring Configuration Data

1. Insert the flash card with the configuration data you want to transfer into your card reader and select the appropriate drive using the "Removable Disk" scroll buttons under "Source Card". The Primary and Alternate bank software versions and the Configuration File version will appear.
2. Insert the target flash card into a second card reader and select the appropriate drive using the "Removable Disk" scroll buttons under "Target Card". If the card contains TRuepoint software, the radio type information and Primary and Alternate bank software versions will appear. If the card has configuration data, the Configuration File version will appear.
3. Once both cards are selected, and the Target card has valid software, the "Only Transfer" button will be available. Press this button to transfer the configuration data from the source flash card to the target flash card.
4. After the transfer process is finished, a new window will appear asking you to eject the flash card from the reader. If you keep the card in the reader, the CTU will automatically update information about the data on the Target Card.

Figure 4-20: Transferring Data



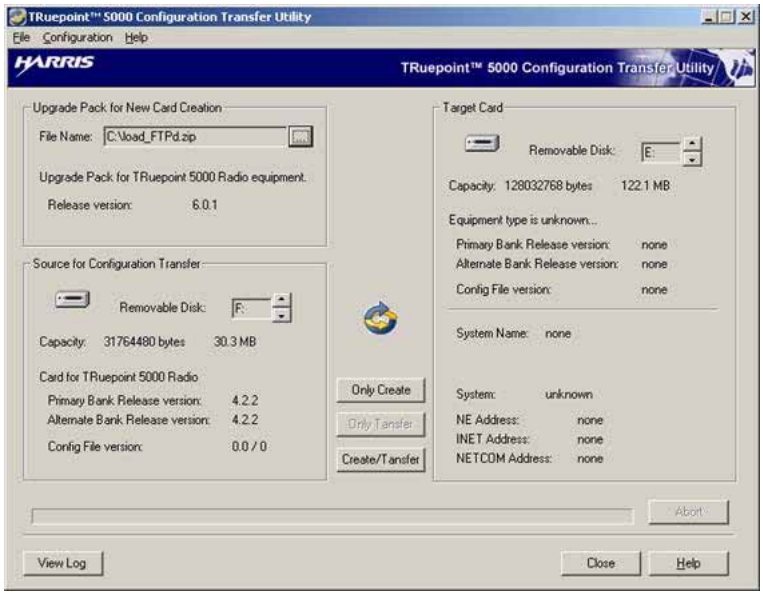
Using the same card reader for Source and Target Cards

1. If you want to use the same card reader for the Source and Target cards, select the same “Removable Disk” letter for both. The Source card should be in the slot before you start the process.
2. Once the process has started and the CTU has read the configuration data from the source card, you will be asked to remove it from the card reader and insert the Target card.
3. After the transfer process is finished, a new window will appear asking you to eject the flash card from the reader.

Creating & Transferring at the same time

1. If you want to create a new flash card and transfer configuration data at the same time, you must have an Upgrade Pack selected as well as Source and Target cards selected. Once these are selected, the "Create/Transfer" button will be available. See Figure 4-21.

Figure 4-21: Create/Transfer



2. Press the "Create/Transfer" button to start the process. The CTU will format the flash card you specified, transfer the data from the upgrade pack to the primary and alternate banks, and then transfer the configuration data from the source card to the target card. Any previous data on the target card will be lost.

3. You can stop the process at any time by pressing "Abort." If you do so, data on the Target card will be corrupted. After the transfer process is finished, a new window will appear asking you to eject the flash card from the reader.

CHAPTER

5

TROUBLESHOOTING

LEDs

Table 5-1: Indicator Light Display Description

Module	Label	Color	Meaning
MODEM 	TRAFFIC	Green	The module is on-line (see Note below)
		Off	No traffic passing
	RFU	Green	The RFU is operating properly
		Red	The RFU has failed (Refer to Manual IMN-903001-Exx)
	CABLE	Green	The cable connecting the IDU to the RFU is working properly
		Red	The cable connecting the SPU to the RFU has failed.
	MODEM	Green	The modem is operating properly
		Red	The modem has failed
MUX 	TRAFFIC	Green	The module is on-line
		Off	No traffic passing
	MUX	Green	The MUX is operating properly
		Red	The MUX has failed

Module	Label	Color	Meaning
Controller 	RMT	Off	The remote site is operating properly
		Yellow	The remote site is in alarm
	MIN	Off	The System is operating properly
		Yellow	Traffic has been manually forced to one of the two channels, or other minor alarms
	MAJ	Green	The System is operating properly
		Red	Major Alarm; traffic-affecting problem (outage)

In a protected system, the receive protection switching is typically achieved through the RFU receive Decoder switch (Modem **B**) and the receive DADE demux switch (Modem **A**). For this reason, "Traffic" LEDs on **both** Modems will be lit and path STATUS > ONLINE EQUIPMENT will display "ONLINE" for **both** MDM A RX and MDM B RX.

Mixed Mode MUX

The following table describes the behavior of the different mixed mode Muxes when you have a protected system and only one modem is powered up. This information is provided to clear up any confusion over how the different mixed mode Muxes operate.

Type of Mux	Modem A on	Modem B on
Mixed Mode Mux on Side A & B	Online Mux is on; Offline Mux is off	Online Mux is on; Offline Mux is off
Dual Mode Mixed Mode Mux on Side A & B	Both Muxes are on	Both Muxes are on
Mixed Mode Mux on Side A & Dual Mixed Mode Mux on Side B	Provides power to Mux B	Does not provide power to Mux A
Dual Mixed Mode Mux on Side A & Mixed Mode Mux on Side B	Does not provide power to Mux B	Provides power to Mux A

Loopback Testing

The following loopback tests can be performed through the HHT or Web-CIT.

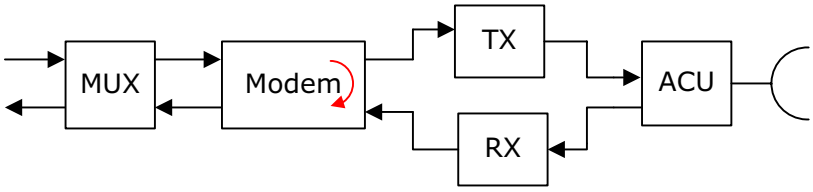
- Modem IF loopback (local only)
- High level Mux loopback
- Tributary or STM1/OC3 Input or Radio loopback
- Wayside Input or Radio loopback

Modem IF Loopback Test

From the Web-CIT, select ADMINISTRATION > LOOPBACK. Select the appropriate loopback from the drop-down menu.

From the HHT, select CONTROL > LOOPBACK > HIGH LVL LPBK > MDM IF LPBK.

Figure 5-1: Modem IF loopback test



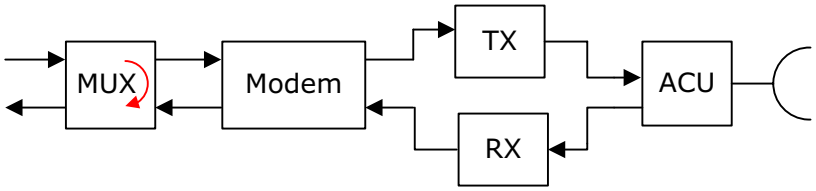
The traffic on a 10/100BASE-T tributary may not be looped back when the high level loopback is set.

High Level Mux Local Loopback Test

From the Web-CIT, select ADMINISTRATION > LOOPBACK. Select the appropriate loopback from the drop-down menu.

From the HHT, select CONTROL > LOOPBACK > HIGH LVL LPBK > MUX LPBK.

Figure 5-2: High Level MUX local loopback test



The traffic on a 10/100BASE-T tributary may not be looped back when the high level loopback is set.

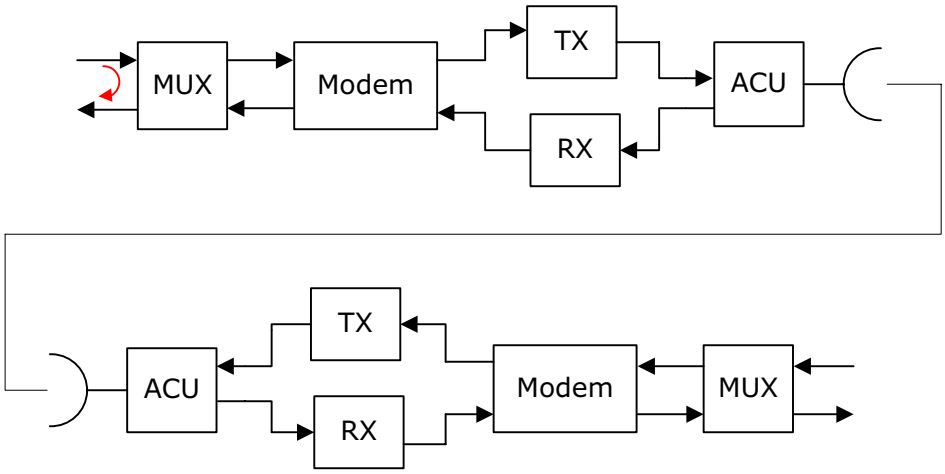
Tributary or STM1/OC3 Loopback Tests

Local Tributary or STM1/OC3 Input Loopback

From the Web-CIT, select ADMINISTRATION > LOOPBACK. Select the appropriate loopback from the drop-down menu.

From the HHT, if you have DS1/DS3 or E1, select CONTROL > LOOPBACK > LOCAL LPBK > TRIB N LOC LPBK. If you have STM1/OC3, select CONTROL > LOOPBACK > LOCAL LPBK > MUX LOC LPBK.Then select INPUT under new value for either.

Figure 5-3: Local Tributary or STM1/OC3 Input Loopback

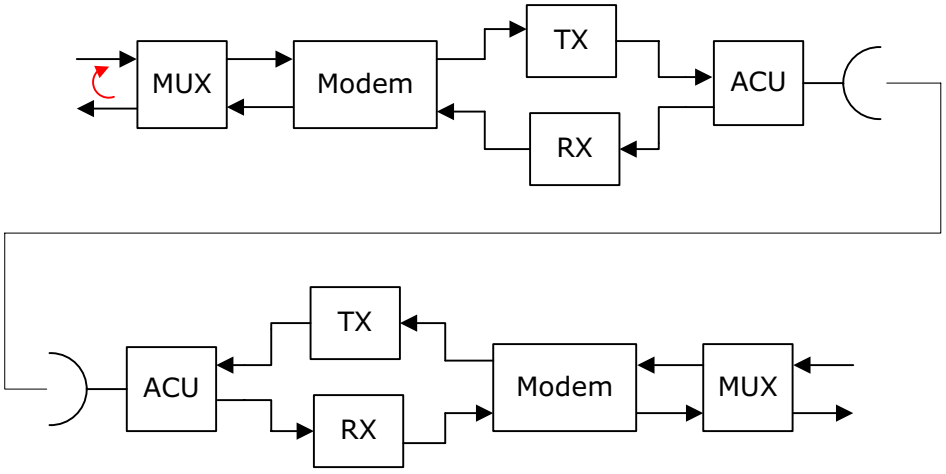


Local Tributary or STM1/OC3 Radio Loopback

From the Web-CIT, select ADMINISTRATION > LOOPBACK. Select the appropriate loopback from the drop-down menu.

From the HHT, if you have DS1/DS3 or E1, select CONTROL > LOOPBACK > LOCAL LPBK > TRIB N LOC LPBK. If you have STM1/OC3, select CONTROL > LOOPBACK > LOCAL LPBK > MUX LOC LPBK. Then select RADIO under new value for either.

Figure 5-4: Local Tributary or STM1/OC3 Radio Loopback



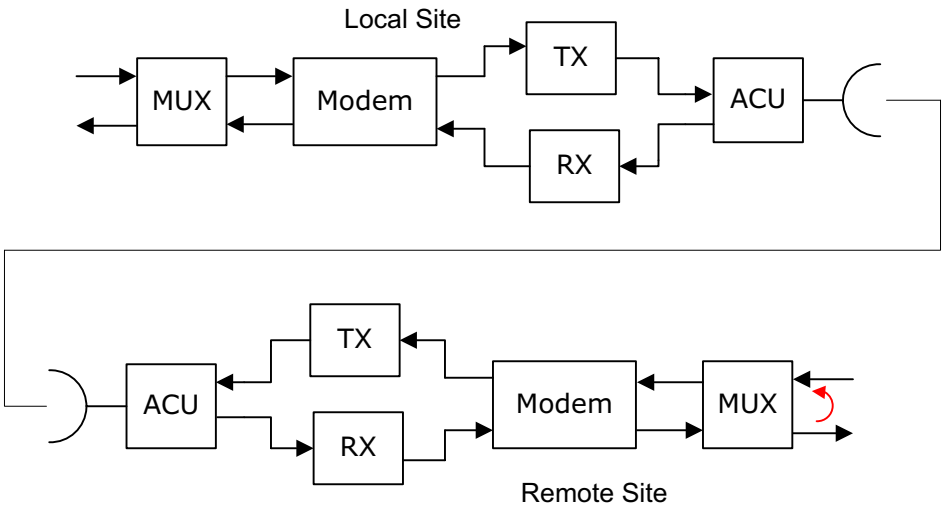
TROUBLESHOOTING

Remote Tributary or STM1/OC3 Radio Loopback

From the Web-CIT, select ADMINISTRATION > LOOPBACK. Select the appropriate loopback from the drop-down menu.

From the HHT, if you have DS1/DS3 or E1, select CONTROL > LOOPBACK > RMT RADIO LPBK > TRIB N RMT LPBK. If you have STM1/OC3, select CONTROL > LOOPBACK > RMT RADIO LPBK > MUX RMT LPBK.

Figure 5-5: Remote Tributary or STM1/OC3 Input Loopback



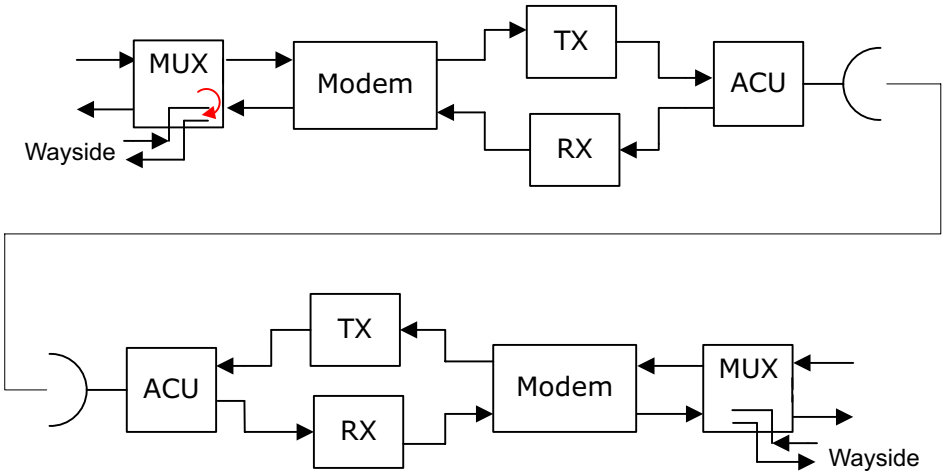
Wayside Loopback Tests

Local Wayside Input Loopback

From the Web-CIT, select ADMINISTRATION > LOOPBACK. Select the appropriate loopback from the drop-down menu.

From the HHT, select CONTROL > LOOPBACK > WS 1 LPBK > LOCAL LPBK. Then select INPUT under new value.

Figure 5-6: Local Wayside Input Loopback

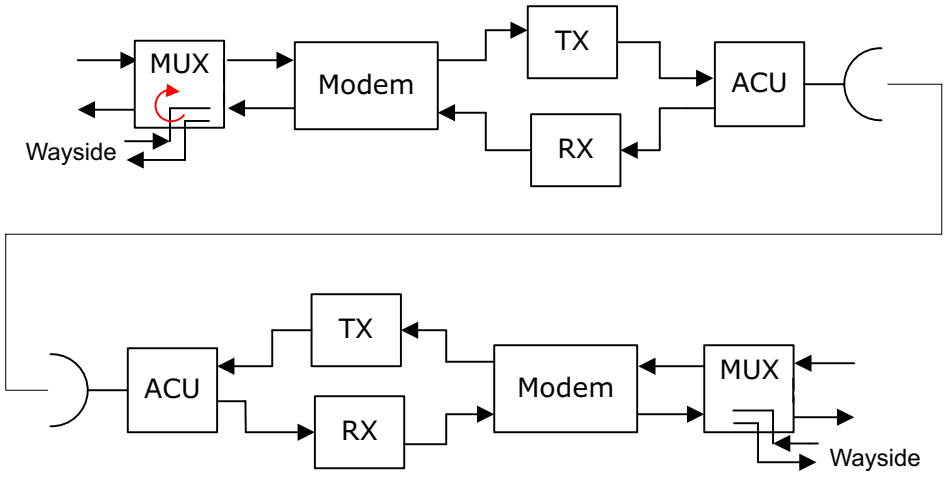


Local Wayside Radio Loopback

From the Web-CIT, select ADMINISTRATION > LOOPBACK. Select the appropriate loopback from the drop-down menu.

From the HHT, select CONTROL > LOOPBACK > WS 1 LPBK > LOCAL LPBK. Then select RADIO under new value.

Figure 5-7: Local Wayside Radio Loopback

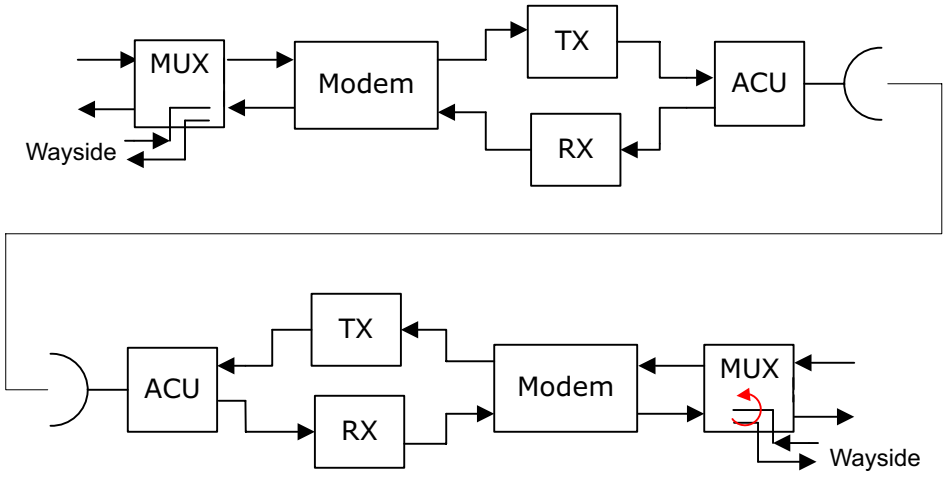


Remote Wayside Radio Loopback

From the Web-CIT, select ADMINISTRATION > LOOPBACK. Select the appropriate loopback from the drop-down menu.

From the HHT, select CONTROL > LOOPBACK > WS 1 LPBK > RMT LPBK.

Figure 5-8: Remote Wayside Radio Loopback



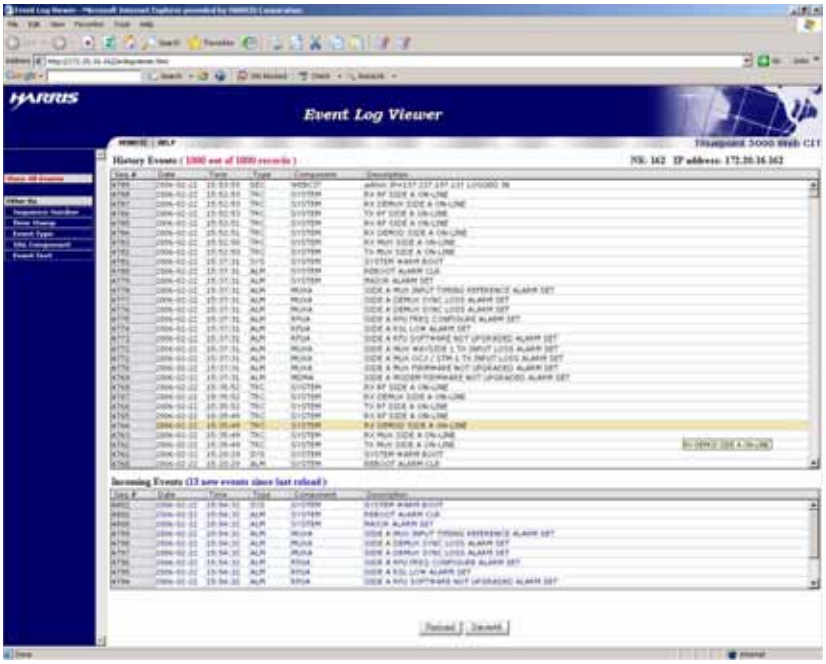
BER Testing

The BER value is measured over the duration of the system BER Performance Measurement test. To run this test, go to PERFORMANCE in the Web-CIT or PERFORMANCE > SYS BER > MEASUREMENT in the HHT. When the BER measurement is set to STOP, the BER elapsed time counter will not count and N_{parity} will not be cumulated. Any BER value accumulated before the BER measurement was stopped will remain available. When the BER measurement is set to RUN, the BER statistic will be reset, the BER elapsed counter will start incrementing once a second, and the BER will be calculated.

Event Log Viewer

The Event Log Viewer is launched from the Web-CIT. Go to ADMINISTRATION > EVENT LOG VIEWER. The Event Log Viewer will pop up as a new window (if you have pop-ups disabled in your internet browser, make sure you enable them).

Figure 5-9: Event Log Viewer

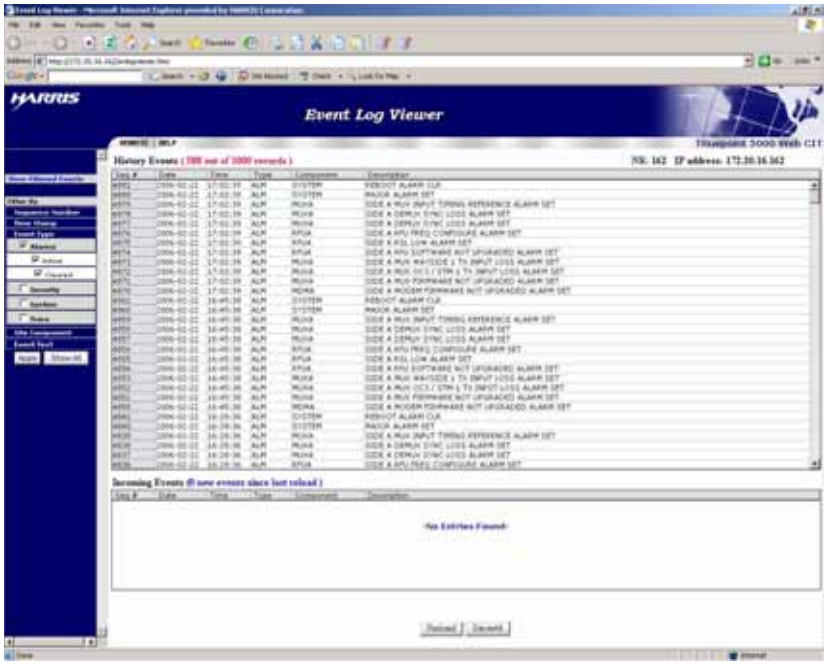


The following key events that occur on the radio are captured in Event Log Viewer:

- Security events (for example, attempted logins)
- Trace events (for example, a configuration change)
- Alarm events (for example, the setting or clearing of an alarm)

Events can then be filtered and/or sorted for further diagnosis. To sort events, click on the top of the column you want to sort by to sort the list in ascending or descending order. To filter, click on the filter choices on the left-hand side of the screen and select your filter options. In the example shown in Figure 5-10, the total list of events (138) has been filtered down to 18 events by selecting **Trace** and **Web-CIT**. Once Apply has been entered, a list returns of only the events that are the type TRC and the component WEBCIT.

Figure 5-10: Filtered History Events



Clicking on the SAVE button will save the whole list as a comma delimited text file which can then be opened and manipulated in Microsoft Excel.

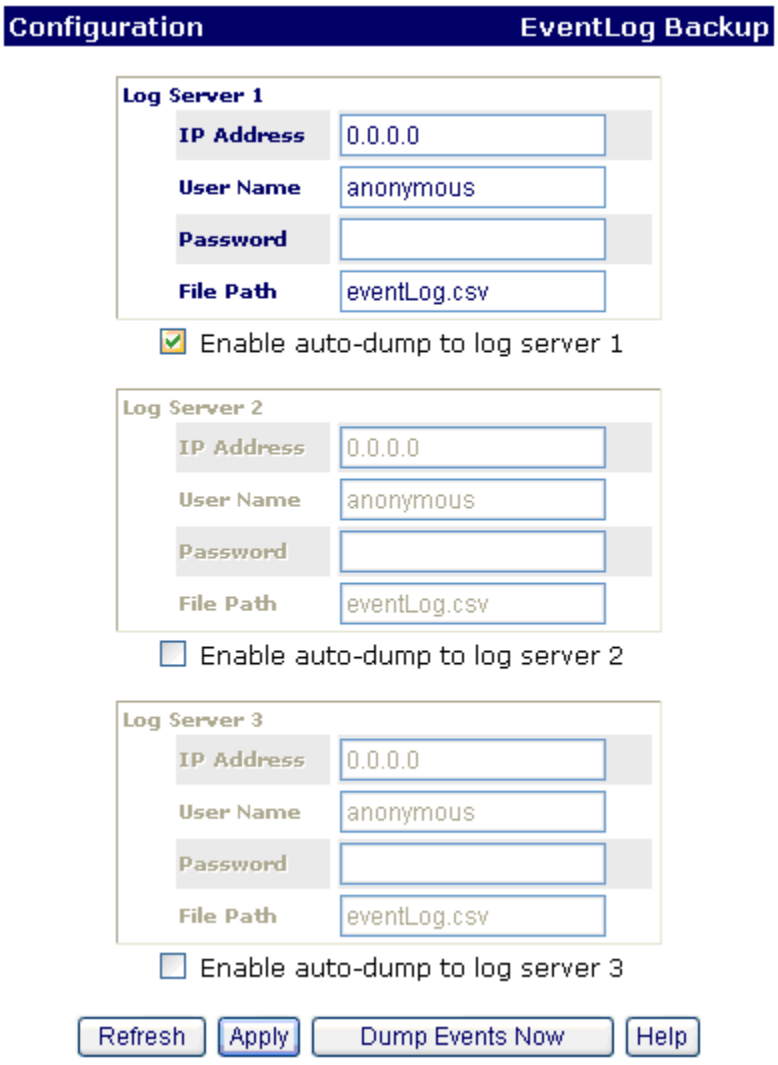
For more information on Alarms recorded in the Event Log Viewer, please refer to the "Glossary of Alarms" on page 5-14.

Event Log Viewer will hold up to 3000 events at a time. Each event is numbered sequentially and goes from 1 to 99,999. When the radio reaches event number 3000, the next event that comes in will be numbered 3001 and event number 1 will no longer appear in the log. This pattern will continue until the number of events reaches 99,999 at which point the numbering will restart at 1.

You can configure the radio to auto-dump the events once you have reached the threshold to up to three external FTP servers. Every time you do a new auto-dump, the new information will be appended to the existing file.

Go to CONFIGURATION > EVENTLOG BACKUP to set up the FTP servers.

Figure 5-11: EventLog Backup



Locks & Switches

In a protected system, the operator has the ability to lock or switch traffic to a selected side which can be useful for isolating problems.

A lock switches traffic to a selected side and locks it there regardless of the alarm condition. There are four lock controls:

- Lock TX Out
- Lock TX MUX
- Lock RxRFU/Decoder
- Lock RxDADE/Demux

A switch switches traffic only if it is safe to do so (no alarms are present). Traffic is not locked on a selected side and switching is allowed. Traffic will switch back automatically if any problem occurs. There are four manual switch controls:

- Switch TX Modem/RF
- Switch TX MUX
- Switch RxRFU/Decoder
- Switch RxDADE/Demux

Relays & External Alarms

The SPU controller provides four relay contacts. In addition, an Orderwire card or an AlarmRelay card can be placed in the option slots. The optional AlarmRelay card provides either 6 or 12 additional relay contacts. These relays can be programmed to indicate an alarm status or to control local site equipment.

These relay outputs are available: RFU ALARM, SPU ALARM, OPT 1 OW RING[1], OPT 2 OW RING, DEMUX A/B SYNC LOSS, RSL A/B LOW, RA A/B SIG DEGRAD, MUX A/B ERR SEC ALM, BER A/B ALARM, TX A/B PWR ALM, TX A/B PWR EXCEED, MDM A/B ONLINE, SYS MUX A/B ONLINE, MUX A/B TX ONLINE, MDM A/B TX ONLINE, MDM A/B RX ONLINE, MUX A/B RX ONLINE, MANU CTL, MAJOR ALARM, MINOR ALARM, CONTROL ACTIVE, MUX INPUT LOS, and CABLE ALARM.

1. *If you assign OPT 1 OW RING as an alarm relay, this alarm will appear when the phone set at the site is ringing. Please note that this alarm does not mean a hardware failure, but indicates that the technician's attention to the ringing phone is requested.*

The SPU controller also provides two digital inputs for local site alarm monitoring. These alarms are reported in the Web-CIT or HHT the same way that the radio alarms are reported. The optional AlarmRelay card provides either 12 or 30 digital inputs.

If you have a V1 Controller, and you do a soft-boot (re-inserting the controller or selecting "Software reboot" in the Web-CIT), the relays will go into alarm for a few seconds before returning to their initial condition.

Trap Customization

The following SNMP traps are available: REMOTE ALM, NO ETHER ADDR, CFG IN PROGRESS, SPI COMM ALM, MODEM CABLE, REBOOT ALM, SIGNAL DEGRADED, RFU COMM, SVC CHAN COMM, FLASH FILE SYS, CONFIG FILE, ATPC FAIL, EXTERNAL ALM, ALIGN ALM, BER ALM, RSL ODU, INPUT LOS, INPUT OOF, OUT_FAIL ALM, CODE ERROR, INPUT AIS, LOCK, INPUT LPBK, RADIO LPBK, HIGH LPBK, RFU MUTE, CW TONE, CARD MISMATCH, CARD ABSENT, CARD DWNLD, CARD ABSENT LEVEL, UNKNOWN_CARD, CARD_NOT ACTIVE, FW NOT UPGRADED, CARD CONFIG, REPLACE ME, TX LEVEL MOD, RX LEVEL MOD, MOD SYNC LOSS, FEC SYNC MOD, DADE MOD, TX MOD CLOCK, RX SYNC MUX, TX LOS MUX, MUX INP LOS, MUX CODE ERROR, MUX OUTPUT FAIL, RFU TX RF LOCK, RFU RX RF LOCK, SILENT FAIL, RFU TX IF LOCK, RFU RX IF LOCK, RFU LPA, RFU IN UC, RFU EEPROM, MALFUNC, TX TO MOD MUX, CALIBRATION TABLE MISM, RX OUT-OF-RANGE, LOGIN ATTACK ALM, SNMP AUTH FAIL, LINKID MISMATCH.

Web-CIT

If the pages in the Web-CIT do not look correct, or pages are partially loaded only, you should clear your internet cache and reboot.

You also may need to clear your internet cache after a software upgrade.

Glossary of Alarms

Message	Explanation	Action
MAJOR ALARM	Indicates the presence of a major alarm on the system.	Check the alarms on the local NE.
MINOR ALARM	Indicates the presence of a minor alarm on the system.	Check the alarms on the local NE.
REMOTE ALARM	Indicates the presence of an alarm on the remote site.	Check the alarms on the remote NE.
CARD ABSENT MENU		
MDM A ABSENT	Indicates that a modem is not inserted and powered in the MDM A slot.	Put the missing modem in the shelf.
MDM B ABSENT	Indicates that a modem is not inserted and powered in the MDM B slot.	Put the missing modem in the shelf or modify the system protection configuration.
MUX A ABSENT	Indicates that a module is not inserted and powered in the MUX A slot.	Put the missing MUX in the shelf.
MUX B ABSENT	Indicates that a module is not inserted and powered in the MUX B slot.	Put the missing MUX in the shelf or modify the MUX protection configuration.
OPT 1 ABSENT	Indicates that a module is not inserted and powered in the OPT 1 slot.	Put the missing optional card in the shelf or modify the option card configuration.
OPT 2 ABSENT	Indicates that a module is not inserted and powered in the OPT 2 slot.	Put the missing optional card in the shelf or modify the option card configuration.
RFU A ABSENT	The RFU is not responding to the controller card.	Check for the presence of an installed RFU. If it is installed, check the cable alarm LED. If the IF cable is correct, reboot the controller. If this does not fix the problem, turn the modem off, wait a few seconds, and then turn the modem on again. If this does not work, replace the controller, modem, RFU, or SPU shelf.
RFU B ABSENT	The RFU is not responding to the controller card.	See RFU A ABSENT.
SDM ABSENT	Indicates that a module is not inserted and powered in the SDM slot.	Insert the SDM card or change the MUX protection or tributary configuration if applicable.

Message	Explanation	Action
CONTROL ACTIVE MENU		
155MB LOCAL INPUT LOOPBACK	OC-3/STS-3 input loopback is set.	Clear the loopback control.
155MB LOCAL RADIO LOOPBACK	OC-3/STS-3 radio loopback is set.	Clear the loopback control.
155 MB REMOTE RADIO LOOPBACK	OC-3/STS-3 remote radio loopback is set.	Clear the loopback control.
155 MB REMOTE RADIO LOOPBACK REQUEST	The request for an OC-3/STS-3 remote radio loopback is received from the remote site.	Clear the loopback control.
LOCK RX DADE DEMUX A	Rx Modem DADE and Demux is manually switched and locked on side A.	
LOCK RX DADE DEMUX B	Rx Modem DADE and Demux is manually switched and locked on side B.	
LOCK RX RFU DECODER A	Rx RFU and Modem Decoder is manually switched and locked on side A.	
LOCK RX RFU DECODER B	Rx RFU and Modem Decoder is manually switched and locked on side B.	
MODEM IF LOOPBACK	Modem IF loopback is set.	Clear the loopback control.
MUX HIGH LEVEL LOOPBACK	Mux High level loopback is set.	Clear the loopback control.
RFU A MUTED	RFU A is manually muted.	
RFU B MUTED	RFU B is manually muted.	
TRIB DS3 X LOCAL INPUT LOOPBACK	DS3 Tributary x input loopback is set.	Clear the loopback control.
TRIB DS3 X LOCAL RADIO LOOPBACK	DS3 Tributary x radio loopback is set.	Clear the loopback control.
TRIB DS3 X REMOTE RADIO LOOPBACK	DS3 Tributary x remote radio loopback is set.	Clear the loopback control.
TRIB DS3 X REMOTE RADIO LOOPBACK REQUEST	The request for a DS3 Tributary x remote radio loopback is received from the remote site.	Clear the loopback control.
TRIB X LOCAL INPUT LOOPBACK	DS1/E1 Tributary x input loopback is set.	Clear the loopback control.
TRIB X LOCAL RADIO LOOPBACK	DS1/E1 Tributary x radio loopback is set.	Clear the loopback control.

Message	Explanation	Action
TRIB X REMOTE RADIO LOOPBACK	DS1/E1 Tributary x remote radio loopback is set.	Clear the loopback control.
TRIB X REMOTE RADIO LOOPBACK REQUEST	The request for a DS1/E1 Tributary x remote radio loopback is received from the remote site.	Clear the loopback control.
TX A CW TONE	CW-tone mode is set on Tx A.	
TX B CW TONE	CW-tone mode is set on Tx B.	
TX A LOCK	Transmitter is manually switched and locked on side A.	
TX B LOCK	Transmitter is manually switched and locked on side B.	
WAYSIDE Y LOCAL INPUT LOOPBACK	Wayside y input loopback is set.	Clear the loopback control.
WAYSIDE Y LOCAL RADIO LOOPBACK	Wayside y radio loopback is set.	Clear the loopback control.
WAYSIDE Y REMOTE RADIO LOOPBACK	Wayside y remote radio loopback is set.	Clear the loopback control.
WAYSIDE Y REMOTE RADIO LOOPBACK REQUEST	The request for a Wayside y remote radio loopback is received from the remote site.	Clear the loopback control.
EXTERNAL ALARMS MENU		
CONTROLLER EXTERNAL INPUT 1	Reports an alarm on the external inputs of the controller card. This string is configurable.	Check the equipment reporting an alarm.
CONTROLLER EXTERNAL INPUT 2	Reports an alarm on the external inputs of the controller card. This string is configurable.	Check the equipment reporting an alarm.
OPTIONAL 1 EXTERNAL INPUT	Reports an alarm on the external inputs of Option Card 1.	Check the equipment reporting an alarm.
OPTIONAL 2 EXTERNAL INPUT	Reports an alarm on the external inputs of Option Card 2.	Check the equipment reporting an alarm.
MODEM A, B MENU		
MDM A/B BATTERY	The battery in the Modem has died or is not functioning.	Check the modem and replace if necessary.
MDM A FPGA DOWNLOAD	There is a firmware initialization failure on MDM A.	Update the firmware with the latest version. If the problem persists, replace the card.
MDM B FPGA DOWNLOAD	There is a firmware initialization failure on MDM B.	Update the firmware with the latest version. If the problem persists, replace the card.
MDM A/MDM B FPGA SETTING	The controller failed to find or download the modem parameters.	Download the latest software version.

Message	Explanation	Action
MDM A NOT UPGRADED	MDM A is currently running firmware that is different than what is in the SPU's active software bank.	Upgrade the firmware of the card.
MDM B NOT UPGRADED	MDM B is currently running firmware that is different than what is in the SPU's active software bank.	Upgrade the firmware of the card.
MDM A/MDM B REPLACE ME	Modem equipment failure.	Replace the modem.
MDM A/MDM B SYNTHESIZER	The modem Tx synthesizer is unlocked.	This alarm may cause a temporary loss of traffic. If the problem occurs frequently, replace the modem.
MDM A/MDM B UNKNOWN	The software does not support the modem model in slot A.	Upgrade the software with the latest version.
MDM A/MDM B WRONG OPTION	The modem does not support the currently configured bandwidth.	Replace the modem with a wideband modem or change the system configuration to use a smaller bandwidth.
MUX A, B MENU		
INTERM LVL TX OOF	There is a framing loss of an intermediate signal in the multiplexed signal of a tributary from the user equipment.	
MUX A FPGA DOWNLOAD	There is a firmware initialization failure on MUX A.	Update the firmware with the latest version. If the problem persists, replace the card.
MUX B FPGA DOWNLOAD	There is a firmware initialization failure on MUX B.	Update the firmware with the latest version. If the problem persists, replace the card.
MUX A/MUX B FPGA SETTING	The controller failed to find or download the MUX parameters.	Download the latest software version.
MUX A/MUX B INTERM LVL RX OOF	There is a framing loss of an intermediate signal in the multiplexed signal from the air interface	
MUX A NOT UPGRADED	MUX A is currently running firmware that is different than what is in the SPU's active software bank.	Upgrade the firmware of the card.
MUX B NOT UPGRADED	MUX B is currently running firmware that is different than what is in the SPU's active software bank.	Upgrade the firmware of the card.

Message	Explanation	Action
MUX A/MUX B REPLACE ME	MUX equipment failure.	Replace the MUX.
MUX A/MUX B TX CLOCK INPUT LOSS	No external clock input from the customer.	
MUX A/MUX B UNKNOWN	The software does not support the model of the MUX.	Upgrade the software with the latest version.
RDI IN ALM	OC-3/STS3 or DS1/E1 tributary x or DS3 tributary x or Wayside y: remote defect indication. AIS from the SPU received from the customer.	If there is no Rx path problem and there is no MUX Replace Me LED alarm, check the connection between the user equipment and the SPU.
RX OUTPUT FAILED	DS1/E1 tributary x or DS3 tributary x or Wayside y: output to the customer failed.	Check the MUX Replace Me LED. If the MUX is okay, check the user equipment or the connection.
TX INPUT AIS	OC-3/STS3 or DS1/E1 tributary x or DS3 tributary x or Wayside y: AIS input received from the customer.	Check the MUX Replace Me LED. If the MUX is okay, check the user equipment.
TX INPUT CODE ERROR	DS1/E1 tributary x or DS3 tributary x or Wayside y: code errors or bipolar violations on the tributary.	Check the MUX Replace Me LED. If the MUX is okay, check the user equipment or the connection.
TX INPUT DEGRADED	OC-3/STS-3: Indicates a BER higher than 10E-6 on the tributary.	Check the connection between the user equipment and the SPM.
TX INPUT LOS	OC-3/STS-3 or DS1/E1 tributary x or DS3 tributary x or Wayside y: No input signal from the customer.	Check the MUX Replace Me LED. If the MUX is okay, check the user equipment or the connection.
TX INPUT OOF	DS3 tributary y: No DS3 frame in input data from customer.	Check the MUX Replace Me LED. If the MUX is okay, check the user equipment or the connection.
OPT 1,2 MENU		
OPT 1/OPT 2 10BT COMM	Loss of communication between both ends of the Ethernet over 64kbits/s tunnel.	Check for the presence and configuration of the ethernet over 64kbit/s cards at both ends of the tunnel. If the cards and the configuration are correct, check for loss of communication between both NEs. If communication is okay, it is also possible that the path of the 64kbits/s tunnel traverses a NE that does not have enough resources to carry the data in the tunnel. If this is the case, consider a change in the network topology.

Message	Explanation	Action
OPT 1 FPGA DOWNLOAD	There is a firmware initialization failure on Optional Card 1.	Update the firmware with the latest version. If the problem persists, replace the card.
OPT 2 FPGA DOWNLOAD	There is a firmware initialization failure on Optional Card 2.	Update the firmware with the latest version. If the problem persists, replace the card.
OPT 1/OPT 2 FPGA SETTING	The controller failed to find or download the optional card parameters.	Download the latest software version.
OPT 1/OPT 2 NOT SUPPORTED IN SIMPLEX	The optional card is not supported in the current network configuration.	Configure the system in duplex mode or connect system to another NE through a local link.
OPT 1 NOT UPGRADED	OPT 1 is currently running firmware that is different than what is in the SPU's active software bank.	Upgrade the firmware of the card.
OPT 2 NOT UPGRADED	OPT 2 is currently running firmware that is different than what is in the SPU's active software bank.	Upgrade the firmware of the card.
OPT 1/OPT 2 REPLACE ME	The optional card failed.	Replace the optional card.
OPT 1/OPT 2 UNKNOWN	The software does not support the model of the optional card.	Upgrade the software with the latest version.
PATH MENU		
ALIGNMENT	The difference between path A and path B in space diversity is too large.	Reduce the space between the antennas so the difference between the antenna to SPU on side A and the antenna to SPU on side B is less than 75m.
DEMUX A SYNC LOSS	Sync loss due to a path problem.	This is a temporary problem due to air conditions. If the problem persists, check for the output power on the remote site or antenna alignment.
DEMUX A WAYSIDE SYNC LOSS	Sync loss due to a path problem affecting only the wayside.	The wayside may be more sensitive to sync losses than the main tributary. This is a temporary problem. If it persists, consider revising the output power of the remote site.
DEMUX B SYNC LOSS	Sync loss due to a path problem.	See DEMUX A SYNC LOSS
DEMUX B WAYSIDE SYNC LOSS	Sync loss due to a path problem affecting only the wayside.	See DEMUX A WAYSIDE SYNC LOSS

Message	Explanation	Action
MUX RMT LOF	The remote site reports a sync loss from the local site.	This may be caused by a path problem towards the remote site. If the problem persists, check for a local transmitter failure, a remote receiver equipment failure or antenna alignment.
REMOTE SYNC LOSS	The Rx remote online demux cannot synchronize on main traffic.	See DEMUX A SYNC LOSS
RSL A LOW	The RSL of RFU A is below the system threshold.	This is a temporary path problem due to air condition. If the problem persists, check for the output power on the remote site or antenna alignment.
RSL B LOW	The RSL of RFU B is below the system threshold.	See RSL A LOW
SIGNAL DEGRADED A	The signal quality on side A is degrading.	Indicates a path problem. Check for a RSL alarm. If this alarm persists check for antenna alignment or for the RFU Replace Me LED, the modem Replace Me LED, or a modem cable alarm.
SIGNAL DEGRADED B	The signal quality on side B is degrading.	See SIGNAL DEGRADED A
RFU A, B MENU		
RFU A/RFU B CALIBRATION TABLE MISMATCH	At least one of the modules (IF/RPC, Tx, Rx) has a wrong version of the calibration table.	
RFU A/RFU B EEPROM	The RFU's EEPROM is not functional.	Replace the RFU.
RFU A/RFU B FAILED	The RFU initialization failed.	Upgrade the RFU with the latest software. If the problem persists, replace the RFU.
RFU A/RFU B FREQUENCY CONFIGURATION	The TX or RX frequency is incorrect.	Check the TX and RX frequencies.
RFU A/RFU B MUTE FOR TELEMETRY	The RFU is muting because it cannot communicate with the installed controller.	Check first for the modem cable alarm LED. If the IF cable is correct, then reboot the controller. If this does not solve the problem, turn the modem off, wait a few seconds, and then turn the modem on again. If the problem is still not solved, try replacing the controller, the modem, the RFU or finally, the SPU shelf.

Message	Explanation	Action
RFU A NOT UPGRADED	RFU A is currently running software that is different than what is in the SPU's active software bank.	Upgrade the RFU software.
RFU B NOT UPGRADED	RFU B is currently running software that is different than what is in the SPU's active software bank.	Upgrade the RFU software.
RFU A/RFU B PA LOW	The PA output is low (more than 3 dB below the set value).	
RFU A/RFU B PA OUTPUT OUT OF RANGE	The PA output power is out of range. When this occurs, an Out of Range value will appear in the OUTPUT POWER menu.	
RFU A/RFU B REPLACE ME	There is a RFU equipment failure.	Replace the RFU.
RFU A/RFU B RX EQUIPMENT	There is a RFU equipment failure in the Rx direction.	Replace the appropriate RFU.
RFU A/RFU B SETTING	The controller failed to find or download the RFU parameters.	Download the latest software version.
RFU A/RFU B SOFTWARE DOWNLOAD	The RFU software is corrupted.	This alarm should disappear by itself after a few moments. If the alarm persists, upgrade the system with the latest software version.
RFU A/RFU B SYNTHESIZER	Indicates a hardware failure of a synthesizer on the RFU.	Replace the RFU.
RFU A/RFU B TX EQUIPMENT	There is a RFU equipment failure in the Tx direction.	Replace the appropriate RFU.
RFU A/RFU B TX SILENT FAILURE	Indicates a silent failure of the PA of the RFU.	Replace the RFU.
SDM MENU		
INTERM LVL TX OOF	There is a framing loss of an intermediate signal in the multiplexed signal of a tributary from the user equipment.	
RX OUTPUT FAILED	Tributary on the SDM: output to customer failed.	Check the MUX Replace Me LED. If the MUXes are okay, check for a short circuit in the cable or the user equipment. Also check the clock signal. If all of this is okay, replace the MUXes and the SDM.
SDM UNKNOWN	The software does not support the model of the SDM.	Upgrade the software with the latest version.

Message	Explanation	Action
TX INPUT AIS	Tributary on the SDM: AIS received from the customer.	Check the MUX Replace Me LED. If the MUXes are okay, check the user equipment.
TX INPUT CODE ERROR	Tributary on the SDM: code errors or bipolar violation.	Check the MUX Replace Me LED. If the MUXes are okay, check the user equipment.
TX INPUT LOS	Tributary on the SDM: loss of input from the customer.	Check the MUX Replace Me LED. If the MUXes are okay, check the user equipment.
TX INPUT OOF	Tributary on the SDM: loss of framing from the customer.	Check the MUX Replace Me LED. If the MUXes are okay, check the user equipment.
SYSTEM MENU		
ATPC TX A/B HIGH POWER	Tx power is above the coordinated Tx power on side x.	Indicates a probable fading condition at the remote site. Traffic is not necessarily affected. If this alarm is frequent, review the coordinated Tx power.
BANDWIDTH UNKNOWN	The configured capacity is not supported in the current frequency band.	Download the latest software version. If this does not solve the problem, either configure another capacity or replace the RFU with a RFU that has a different frequency band option.
BER	This indicates that the BER is above the threshold (10E-6) in 1+1 and 1+0 systems.	Indicates a path problem. Check for a RSL alarm. If this alarm persists, check for antenna alignment or for the RFU Replace Me LED, modem Replace Me LED or modem cable alarm.
BER A & B	This indicates that the BER is above the threshold for Channel A and/or Channel B in 2+0 systems.	See BER.
CABLE A	There is a cable problem between the SPU and RFU A.	Check the modem Cable Alarm LED.
CABLE B	There is a cable problem between the SPU and RFU B.	Check the modem Cable Alarm LED.
CNTLR REPLACE ME	Indicates local controller EEPROM corruption.	Replace the controller card.
CONFIG FILE	The system could not restore the configuration from the config files; the default values were used.	Review all the configuration values and correct them as needed.

Message	Explanation	Action
DHCP CLIENT FAILED	Indicates communication failure with a DHCP server.	Check for connectivity with a DHCP server on the LAN. If no DHCP server is available, change the configuration.
EVENT LOG UPDATE FAILED	The previous attempt to update the Event Log sink has failed.	
FLASH FILE SYSTEM	Failed write attempts to the MMC card.	If this alarm persists or is frequent, replace the MMC card on the controller board. If this does not solve the problem, report it to Harris.
INVALID SW KEY	The existing software key could not be validated.	Check your software key settings and then contact Harris customer service.
LINK ID	The remote radio has an unexpected link ID.	
LOAD CORRUPTED	The current software load has missing or corrupted components.	Upgrade the software with the latest version.
LOGIN ATTACK	There has been an unauthorized login attempt(s) that exceeds the threshold.	
MDM A SPI COMMUNICATION	Communication between the Controller and Modem A is broken.	If the problem persists or is too frequent, replace the controller first. If this does not solve the issue, replace the modem. Lastly, replace the SPU enclosure.
MDM B SPI COMMUNICATION	Communication between the Control and Modem B is broken.	See MDM A SPI COMMUNICATION
MUX A SPI COMMUNICATION	Communication between the Controller and MUX A is broken.	If the problem persists or is too frequent, replace the controller first. If this does not solve the issue, replace the MUX. Lastly, replace the SPU enclosure.
MUX B SPI COMMUNICATION	Communication between the Controller and MUX B is broken.	See MUX A SPI COMMUNICATION
MUX B REMOVAL REQD	MUX B must be removed.	Remove MUX B.
MUX CARD MISMATCH	The MUX options are incompatible, or the MUX hardware keys do not match or the SDM does not match the MUXes.	Check the MUX options, the SDM and the MUX hardware keys and replace the inappropriate cards or keys.
NO ETHERNET ADDRESS	No Ethernet (MAC) address is specified.	Enter an address.

Message	Explanation	Action
NO RF NEIGHBOR	There is no service channel communication with the remote radio over the RF link.	
OPT 1 SPI COMMUNICATION	Communication between the Controller and the Option 1 card is broken.	If the problem persists or is too frequent, replace the controller first. If this does not solve the issue, replace the optional card. Lastly, replace the SPU enclosure.
OPT 2 SPI COMMUNICATION	Communication between the Controller and the Option 2 card is broken.	See OPT 1 SPI COMMUNICATION
RADIUS SERVER ACCESS FAILED	The radius server could not be accessed for authentication.	
REBOOT	System is rebooting.	
RF LINK SVC FAIL	Indicates the loss of the service channel with the remote site.	This problem may be caused by a path problem, an equipment failure on the local receiver or the remote transmitter, or removal or rebooting of the controller card at the remote site. If the problem persists for more than 5 minutes and the tributary traffic is not affected, it is likely that the remote controller failed or was removed.
RFU A COMMUNICATION	Communication between the SPU and RFU A is broken.	Reboot the controller. If this does not solve the problem, turn off the modem, wait and a few seconds and then turn the modem on again. If the problem is still not solved, try replacing the controller, the modem, the RFU, or finally the SPU enclosure.
RFU B COMMUNICATION	Communication between the SPU and RFU B is broken.	See RFU A COMMUNICATION
RFU MISMATCH	RFU A does not match the frequency band of RFU B.	Replace one of the RFUs with a RFU that has the frequency option of the other.
SDM MISMATCH	The SDM card does not match the system capability (MUX).	Check the MUX options, the SDM and the MUX hardware keys and replace the inappropriate cards or keys.
SDM REMOVAL REQD	The SDM must be removed.	Remove the SDM.

Message	Explanation	Action
TPC TIME LIMIT	Tx power is above the coordinated Tx power longer than the time limitation allows.	Review the coordinated Tx power or the configured maximum time period.
TPC A/B TIME LIMIT	Tx power is above the coordinated Tx power longer than the time limitation allows.	Review the coordinated Tx power or the configured maximum time period.

CHAPTER

6

SOFTWARE MENU TREE

The following figures display the items in the radio software menus when using the hand-held terminal or a PC running VT-100 terminal emulation.

Menus are dependent on your system configuration and thus vary from system to system. This menu tree covers multiple possibilities and should not be viewed as an exact replica of your system.

Figure 6-1: Main Menu

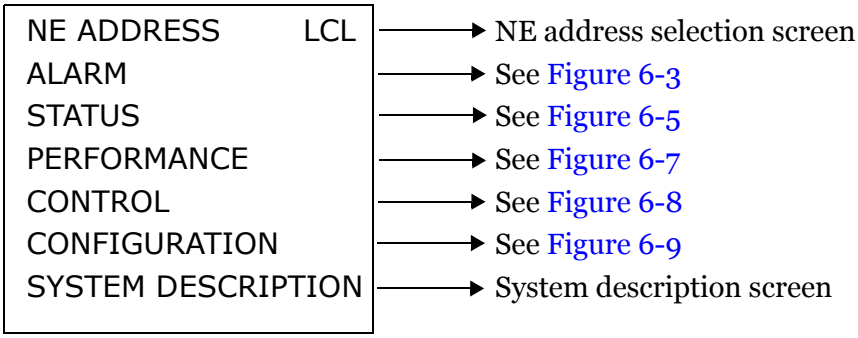


Figure 6-2: Some Alternate Displays

The displays below are not on the menu tree, but appear under certain circumstances, replacing the current display from the menu tree.

ABSENT	Appears when items in a particular menu are not installed.
S/W CORRUPTED	Appears if the software in the RFU is corrupted.
FORGOT PASSWORD?	Appears in the main menu when a user has logged in as a guest.

Figure 6-3: The Alarm Branch

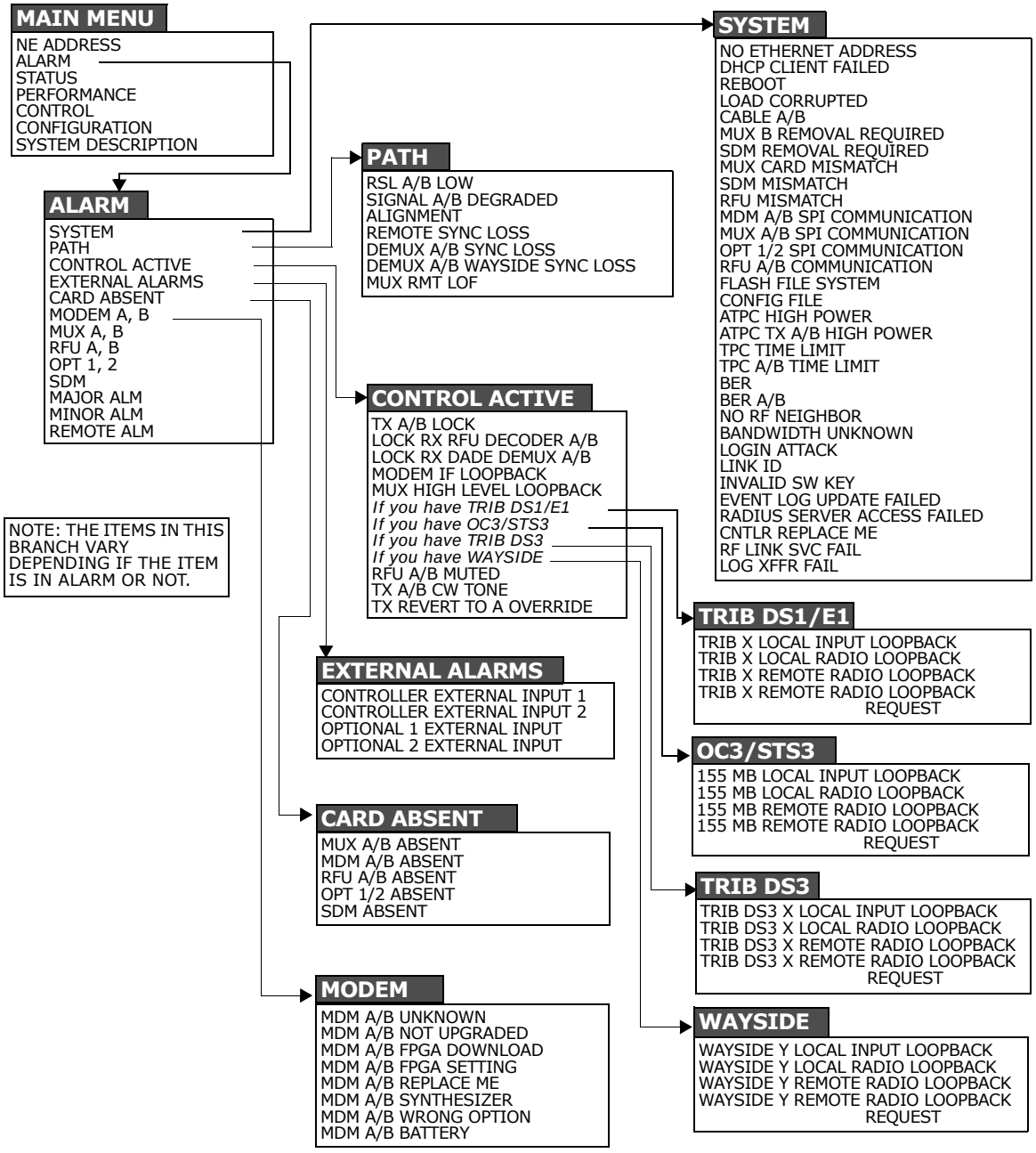


Figure 6-4: The Alarm Branch continued

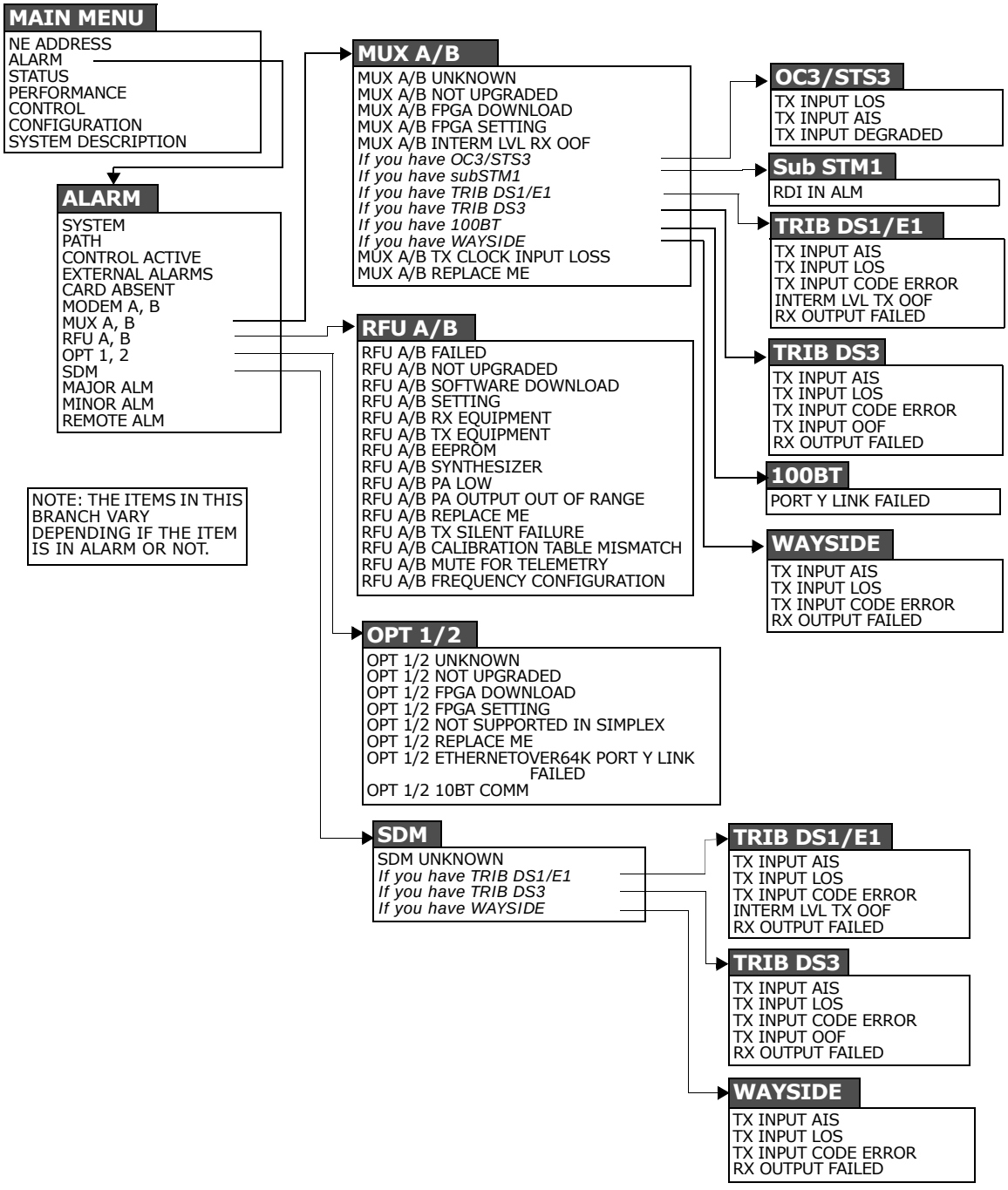


Figure 6-5: The Status Branch

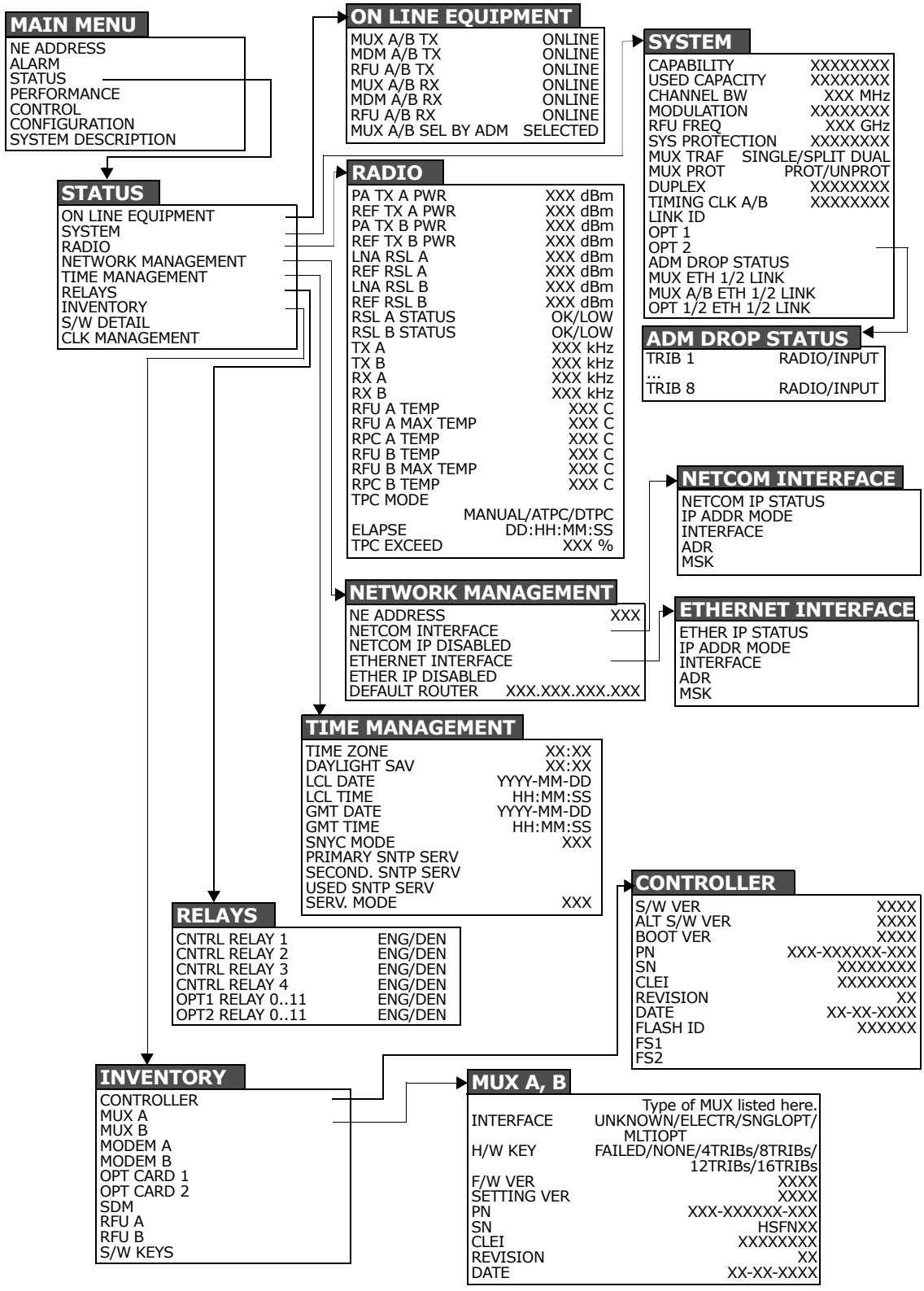


Figure 6-6: The Status Branch continued

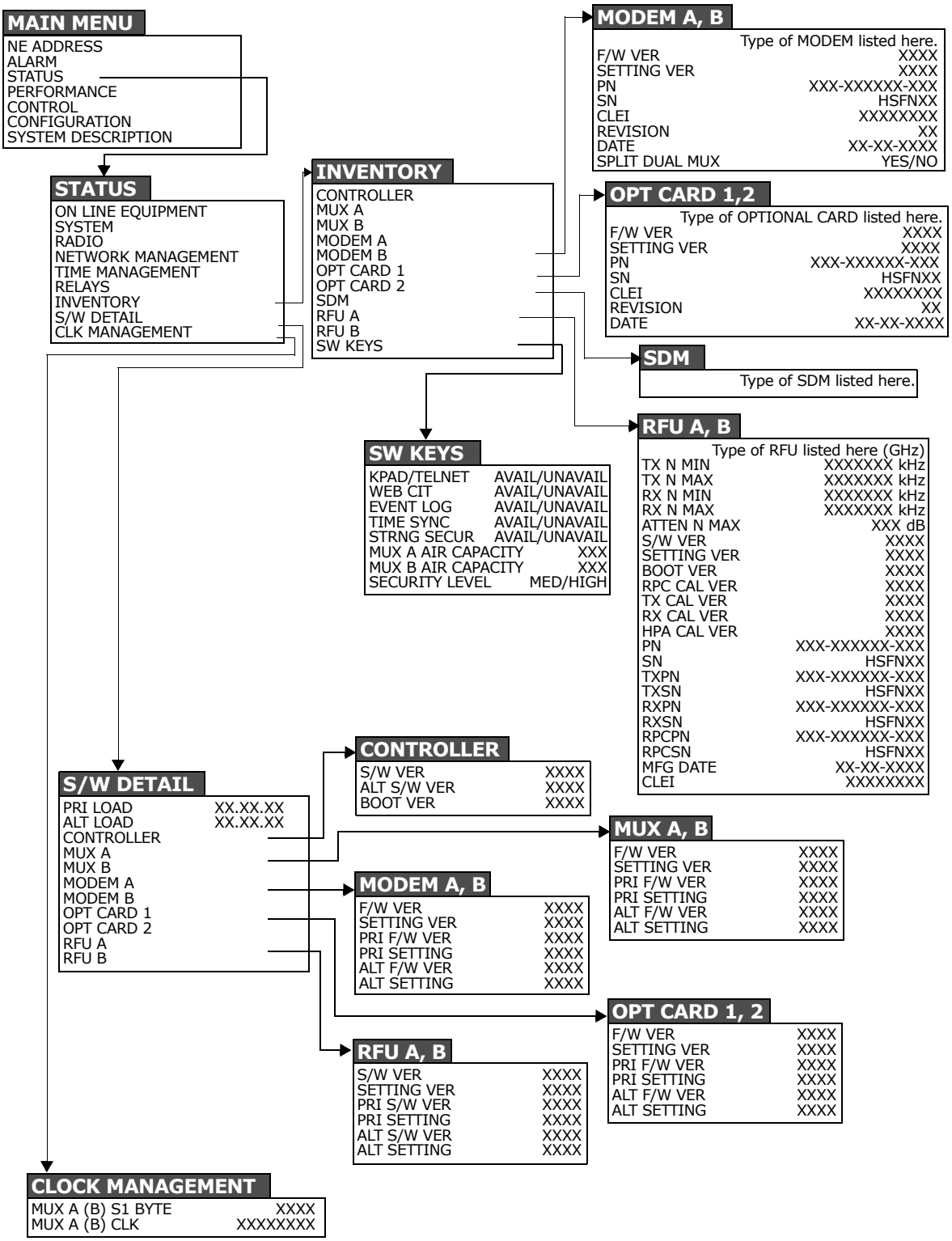
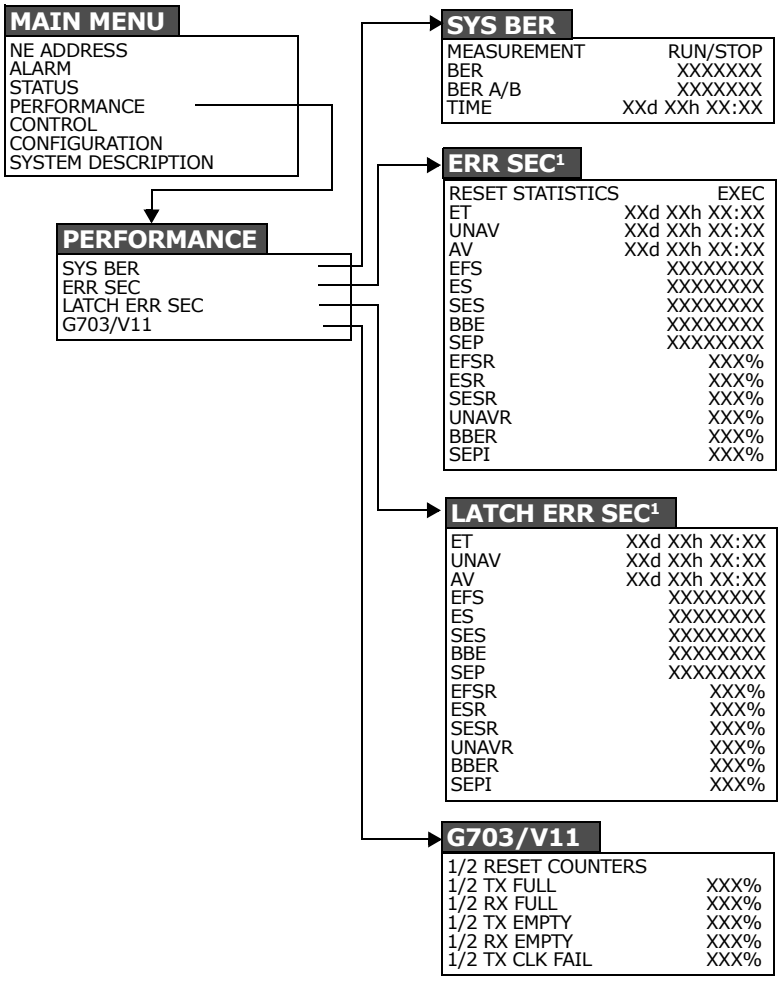


Figure 6-7: The Performance Branch



1. *If you have a 2+0 system, them ERR SEC and LATCH ERR SEC will be available for both MUX A and MUX B.*

Figure 6-8: The Control Branch

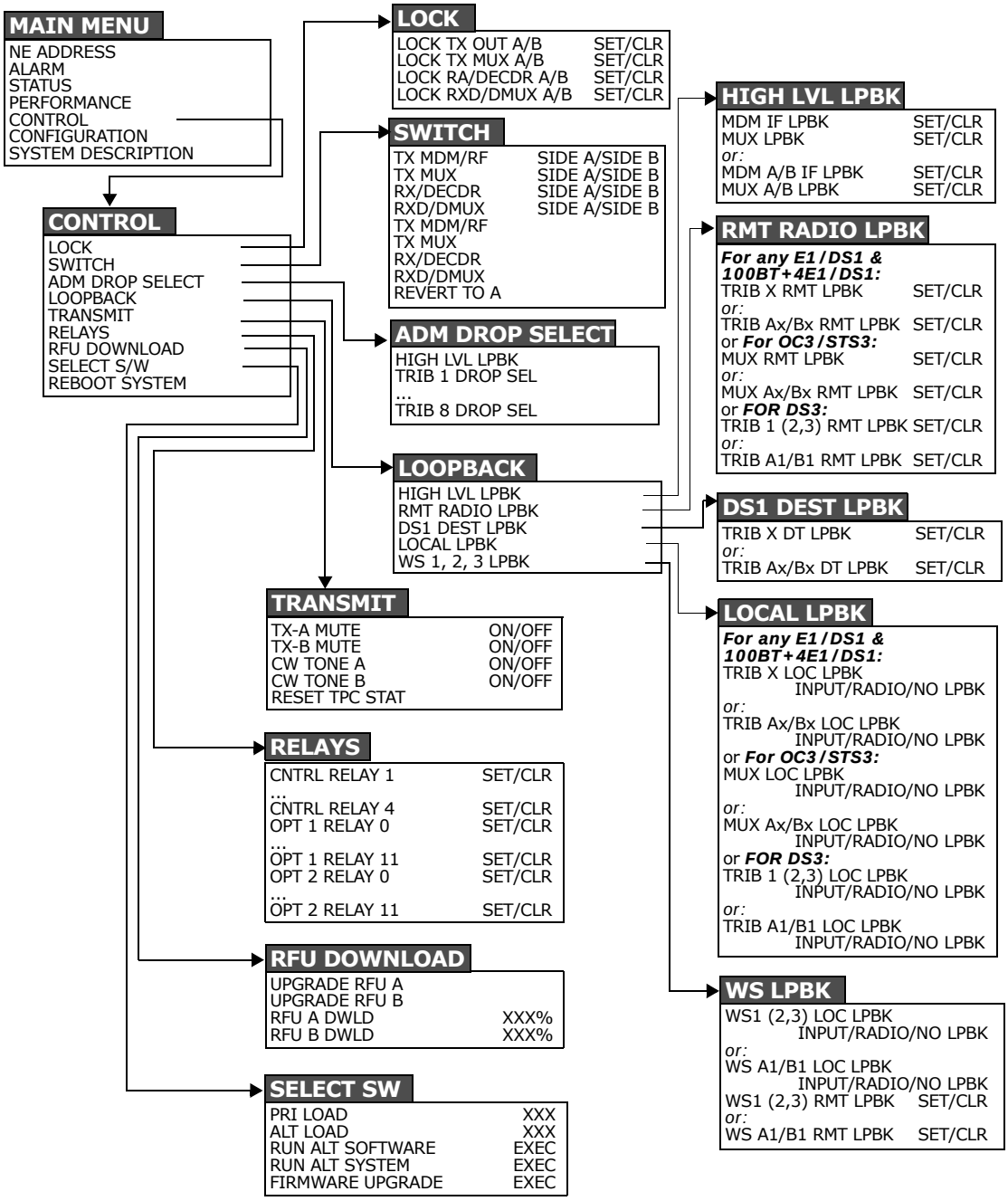
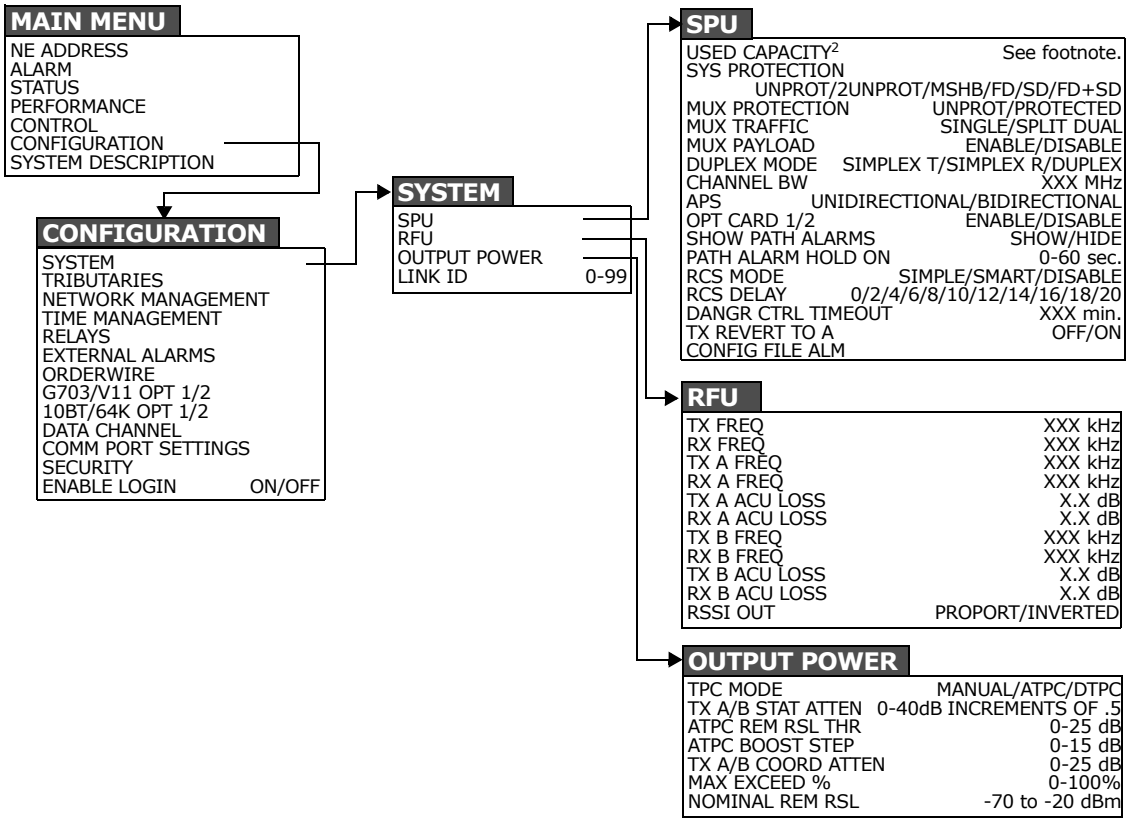


Figure 6-9: The Configuration Branch



2. See the following table for available values.

Max. System Capability	Available values
NxE1	2E1, 4E1, 8E1, 16E1
NxDS1	4DS1, 8DS1, 12DS1, 16DS1
OC3/STM1	OC3-STS3, STM1
Sub STM1	Sub STM1
21E1	21E1
28DS1+WS	28DS1, 28DS1+WS
3DS3+WS	3DS3, 3DS3+WS
DS3+DS1	DS3, DS3+DS1, E3+E1
100BT+DS1	DS3, DS3+DS1, E3+E1, 100BT, 100BT+E1, 100BT+DS1
mix100BT+100DS1	mix4DS1, mix8DS1, mix12DS1, mix16DS1, mix29DS1, mix58DS1, mix87DS1, mix100DS1, 100BT+4DS1, mix100BTANSI
mix100BT+STM1	mix2E1, mix4E1, mix8E1, mix16E1, mix35E1, mix50E1, mix75E1, mix100BT+4E1, mix 100BTCEPT, mix32E1-dm
ADM8DS1/DS3+DS1	8DS1ADM (DS3), 8DS1ADMws (DS3+DS1)

Figure 6-10: The Configuration Branch continued

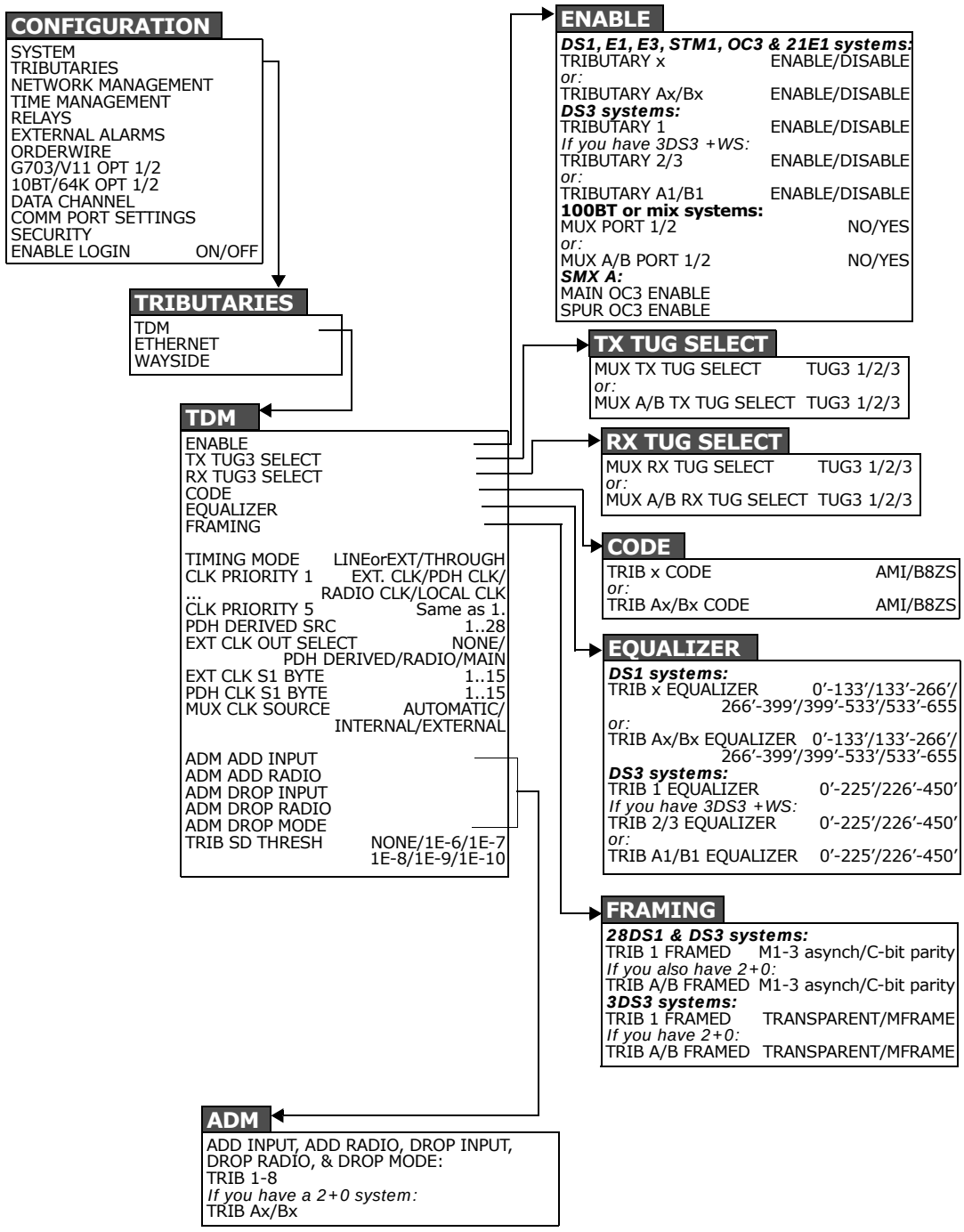


Figure 6-11: The Configuration Branch continued

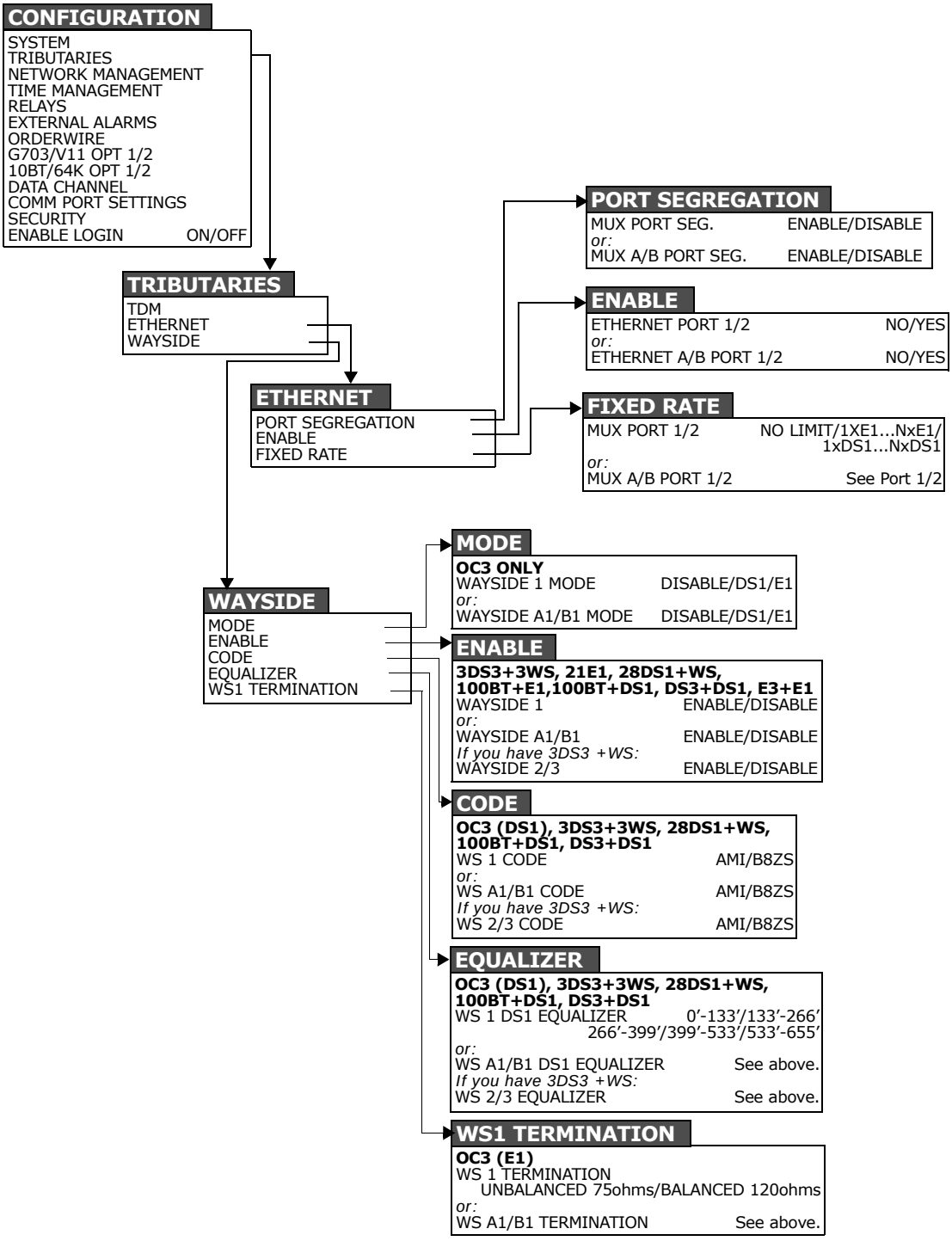
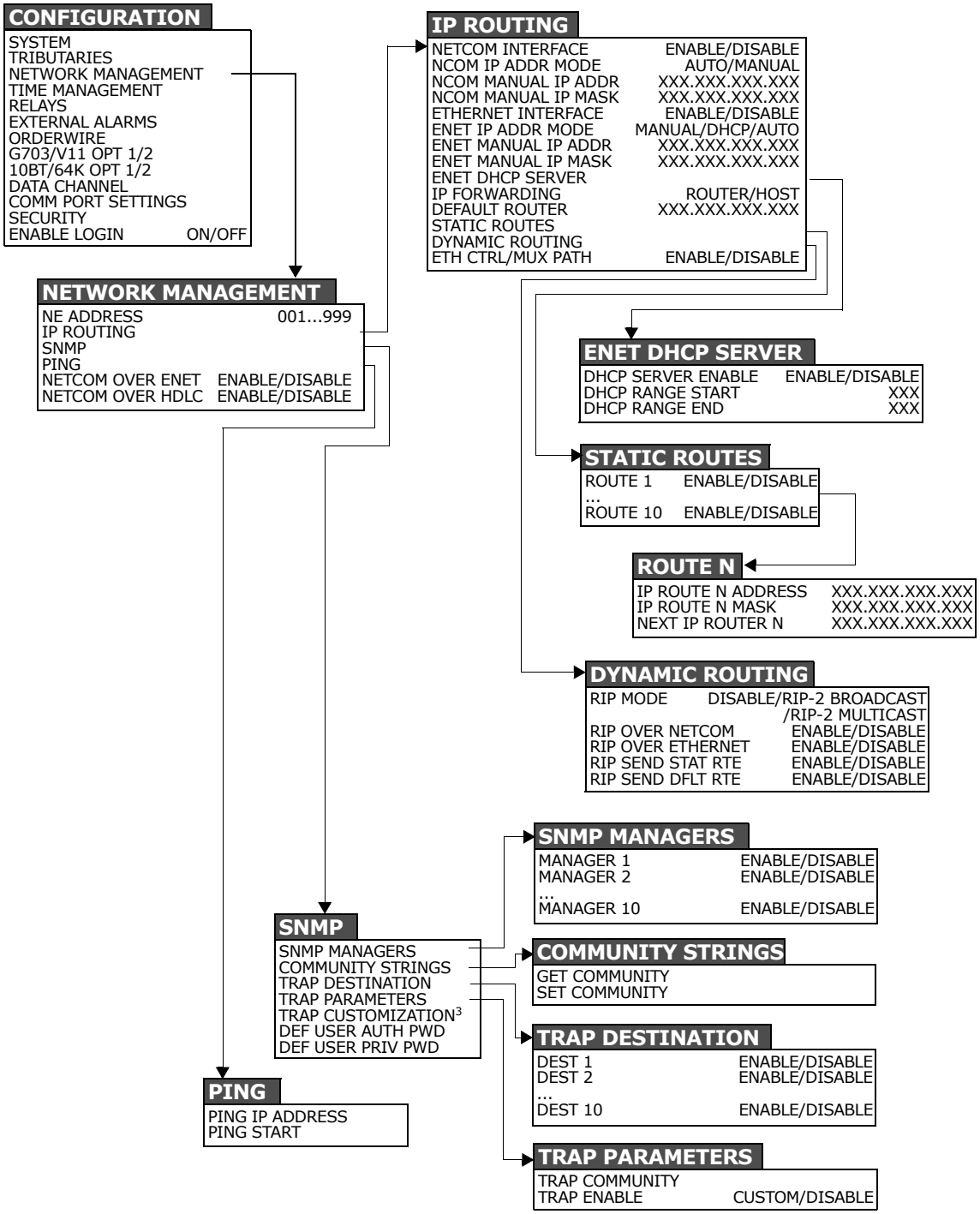
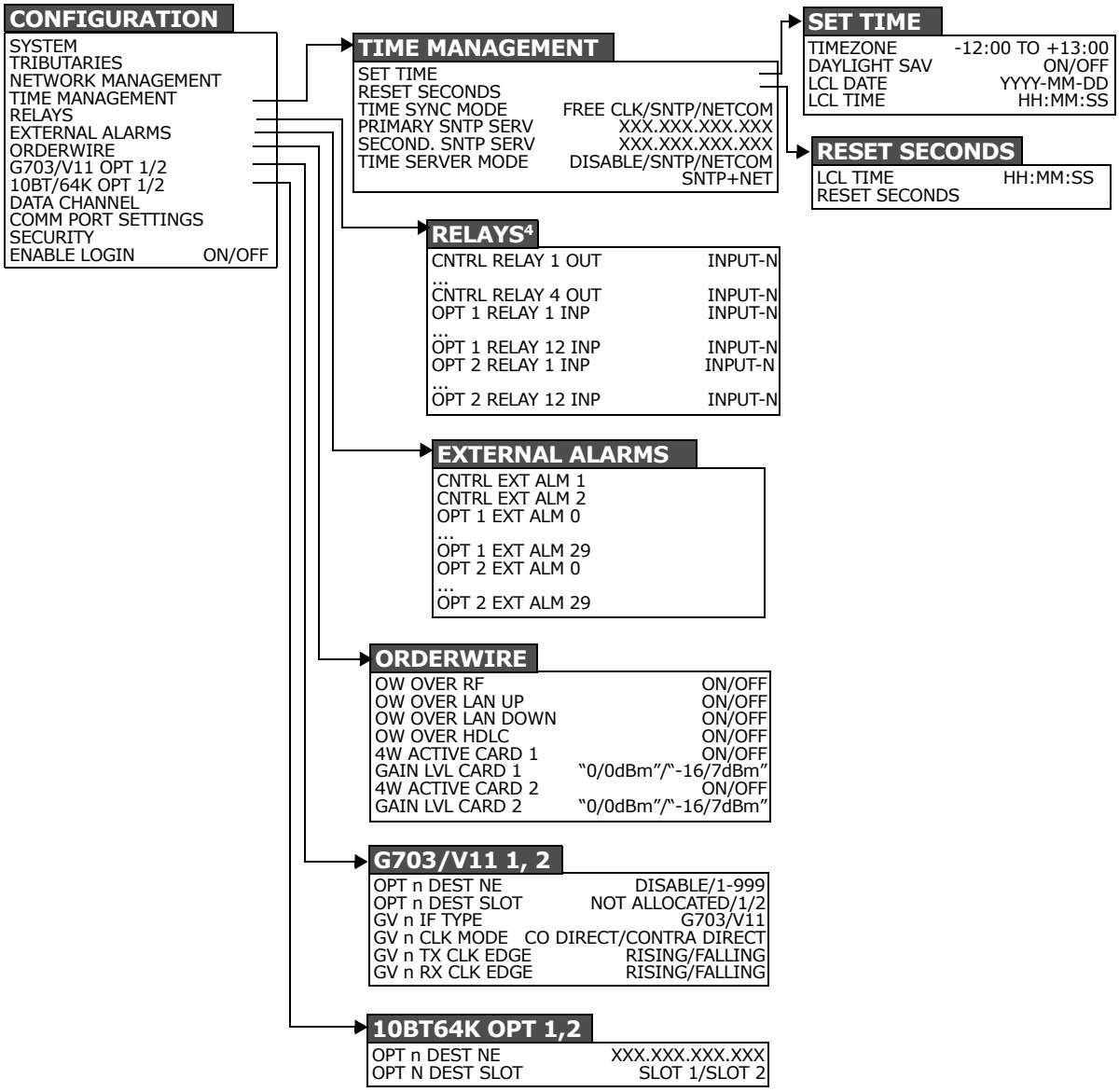


Figure 6-12: The Configuration Branch continued



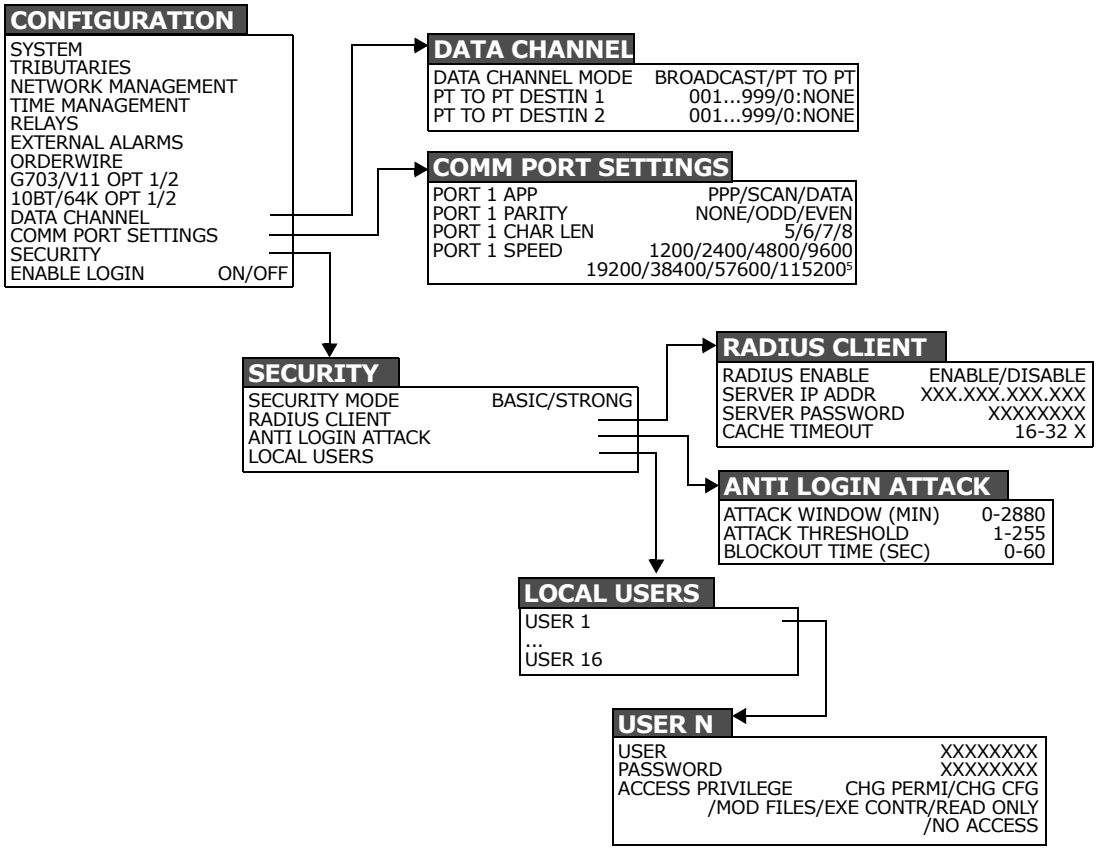
3. See "Trap Customization" on page 5-13 for a list of available traps.

Figure 6-13: The Configuration Branch continued



4. See *"Relays & External Alarms" on page 5-12* for a list of available relay inputs.

Figure 6-14: The Configuration Branch continued



5. *If SCAN application, Port 1 char length is not displayed. Port 1 baud rate: DATA CHANNEL 1200...19200, SCAN 1200...57600*

CHAPTER

7

MENU ITEM GLOSSARY

The following menu item glossary lists many of the terms used in the Web-CIT and/or the hand held terminal.

For definitions of alarms, please refer to the Glossary of Alarms in Chapter 5.

ATPC BOOST STEP	Allows for entering the number of dB that the transmitter will increase the TX output power by when allowed.
ATPC REMOTE RSL THRESHOLD	Defines the remote end's receiver ATPC low threshold. The default value is 5 dB. (5 dB above the system threshold.)
AV	Displays the amount of time that the signal was available over the elapsed time (ET) period.
BANK LOAD VERSION	Specifies the version of the software load in a particular software bank.
BANK SOFTWARE VERSION	Specifies the Software/Firmware version number of the cards.
BBE	Displays the number of Background Block Errors over the elapsed time (ET) period.
BBER	Displays the percentage of Background Block Errors Ratio over the elapsed time (ET) period.
BER	Displays the Bit Error Rate over the elapsed time (ET) period.
CHANNEL BANDWIDTH	Allows for entering the channel bandwidth of the system in MHz. When changing the USED CAPACITY, the CHANNEL BW may be modified automatically if the current value becomes invalid.

CLK PRIORITY/ MUX CLK SOURCE	Allows you to set clock priorities for the MUX when you have a 21E1 MUX.
CW TONE	Allows you to turn the Continuous Wave tone mode ON or OFF.
DANGEROUS CONTROL TIMEOUT	Sets a timeout period for certain commands. Some commands, such as a loopback from the remote site, will disrupt the system. This setting sets the time at which the system will re-establish the link.
DATA CHANNEL DESTINATION/PT TO PT DESTIN	If point to point was selected for data channel mode, then this sets the point to point destinations.
DATA CHANNEL MODE	Allows the user to select between broadcast or point to point.
DAYLIGHT SAV (ADJUST)	Turn on to adjust the local clock setting by one hour if the radio is installed in a country where daylight savings time is observed.
DHCP RANGE	Allows you to enter the start and end of the server address range when DHCP is enabled.
DUPLEX MODE	Available for non 10/100BT capacities. Allows the user to define the system operation mode. If the DS3 duplex configuration is set to SIMPLEX TX on one end of a hop, it must be set to SIMPLEX RX at the other end of the hop.
EFS	Displays the number of error free seconds over the elapsed time (ET) period.
EFSR	Displays the percentage of error free seconds over the elapsed time (ET) period.
ELAPSE (TIME)	Displays the elapsed time when using ATPC or DTPC mode.
ELAPSED TIME	Displays the elapsed time over which the BER measurement is computed.
ENABLE LOGIN	Allows for turning login capabilities ON or OFF.
ES	Displays the number of errored seconds over the elapsed time (ET) period.
ESR	Displays the percentage of errored seconds over the elapsed time (ET) period.
ET	Displays the time elapsed since the BER calculator was last reset (in ERR SEC) or between last two resets (in LATCH ERR SEC).
ETHERNET IP ADDR MODE	Allows for selecting Auto, DHCP, or manual for the ethernet IP addressing mode. In Auto mode, the IP address of the ethernet interface is derived from the NE ADDRESS.
EXTERNAL CLOCK S1 BYTE	Allows you to specify a synchronization quality level for the timing reference of the external clock input 1.
FIRMWARE UPGRADE	Executes the command to upgrade the firmware with the new software load.
GET COMMUNITY	Sets the SNMP Get Community name. The SNMP Manager needs to use the same name to read information from the radio.
H/W KEY	Displays the type of hardware key attached to the MUX.

LINK ID	Allows you to set the link ID as a value from 0 to 99. When the link ID received from a remote station is different from the local link ID, the link ID alarm is set and MUX A and MUX B will insert AIS at the tributary output to lock up the unwanted transmitter.
LNA RSL	Displays the RSL in dBm measured at the input of the low noise amplifier.
LOCK RX DADE/DEMUX	Allows you to SET or CLEAR the lock on the RXD/DMUX.
LOCK RX DECODER	Allows you to SET or CLEAR the lock on the RA/DECDR
LOCK TX MUX	Allows you to SET or CLEAR the lock on the TX MUX.
LOCK TX OUT	Allows you to SET or CLEAR the lock on the TX's output power.
MAX EXCEED %	Allows for entering the maximum exceeding time percentage that the output power is above the TX coordinated attenuation. This is available only if the TPC mode is set to ATPC or DTPC.
MEASUREMENT/ RUN	Allows you to RUN a new BER calculation and to STOP it.
MUX PAYLOAD SCRAMBLING	Allows you to enable or disable scrambling for OC-3/STM1 MUXes. SONET optical interface signals use binary line coding and therefore must be scrambled to assure an adequate number of transitions (0s to 1s and 1s to 0s) for such purposes as line rate clock recovery at the receiver.
MUX RX TUG3 SELECT	Allows you to decide which TUG-3 (55 Mb/s) from the STM1 signal (155 Mb/s) is selected to be transmitted in the air.
MUX TX TUG3 SELECT	Allows you to decide which TUG-3 (55 Mb/s) should be used in the STM1 signal (155 Mb/s) to transmit the signal received from the air.
MUX TRAFFIC MODE	Select SPLIT DUAL MUX for 32E1. When you change the traffic mode from Single Mux to Split Dual Mux or vice versa, you should always reboot the Controller software.
NETCOM IP ADDR MODE	Allows for selecting Auto or Manual for the Netcom IP addressing mode. In Auto mode, the IP address of the Netcom interface is derived from the NE ADDRESS.
NETCOM OVER ETHERNET	Allows for enabling or disabling the Netcom IP traffic to run over the Ethernet.
NETCOM OVER HDLC	Allows for enabling or disabling the Netcom IP traffic to run over the HDLC link.
NOMINAL REMOTE RSL	Available in DTPC mode only. Allows for setting the nominal remote RSL which the transmitter then compares to received remote RSL.
OW OVER HDLC	Allows for enabling or disabling the orderwire traffic to run over the HDLC link.
OW OVER LAN DOWN	Allows for enabling or disabling the orderwire traffic to run over the local LAN in the direction of the next lowest address.
OW OVER LAN UP	Allows for enabling or disabling the orderwire traffic to run over the local LAN in the direction of the next highest address.
OW OVER RF	Allows for enabling or disabling the orderwire traffic to run over the RF link.

OPT N DEST NE	Allows you to set the destination for the data being sent through the circuit emulation tunnel to a specific NE.
OPT N DEST SLOT	Allows you to allocate a slot for the data being sent through the circuit emulation tunnel.
PA TX POWER	Displays the transmit signal's power at the power amplifier.
PDH CLOCK S1 BYTE	Allows you to specify a synchronization quality level for the timing reference derived from PDH (E1) incoming signal.
PORT 1 APPLICATION	Sets the application (PPP, SCAN, or DATA) for Port 1.
PORT 1 BAUD RATE/SPEED	Sets the baud rate (1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200) for Port 1.
PORT 1 CHAR LENGTH	Sets the character length for Port 1 at 5, 6, 7, or 8.
PORT 1 PARITY	Sets the parity mode for Port 1 at None, Odd, or Even.
PORT SEGREGATION	Allows you to ENABLE or DISABLE the ability to segregate the Ethernet traffic from different ports on to different time slots.
RCS DELAY	Allows for selecting how fast the Reverse Channel Switching action will start after receiving a Remote Sync Loss alarm. This feature is available only with a MHSB or Space Diversity protected system.
RCS MODE	Allows for selecting the Reverse Channel Switching mode; choices are Smart, Simple, or Disabled. This feature is available only with a MHSB or Space Diversity protected system.
REF RSL	Displays the RSL in dBm at the specified reference point.
REF TX POWER	Displays the reference point's transmit signal power.
RESET STATISTICS	Allows you to reset the system error performance numbers. The numbers present in the ERR SEC menu are copied in the LATCH ERR SEC menu.
RESET TPC STATISTIC	Allows you to reset the TPC statistics.
RFU DOWNLOAD	Displays the percentage complete of a RFU download.
RIP MODE	Indicates the RIP mode, which may be DISABLED or RIP-2 BROADCAST or RIP-2 MULTICAST.
RIP OVER ETHERNET	Indicates whether RIP is enabled or disabled over the Ethernet interface.
RIP OVER NETCOM	Indicates whether RIP is enabled or disabled over the Netcomm interface.
RSL STATUS	Displays whether the RSL is OK or LOW. This status is available when the "RSL Low Severity" configuration is set to "Status."
RSSI OUTPUT POLARITY[a]	Allows for setting the RSSI output polarity as proportional to RSL or inversely proportional to RSL.
RX ACU LOSS	Allows for entering, in tenth of a dB, the total loss of extra components that are installed on the received signal path between the LNA port and the reference point at which the user would like to see the RSL value.

SECURITY LEVEL	Displays the level of encryption used by the software as either Medium or High.
SEP	Displays the number of severely errored periods over the elapsed time (ET) period.
SEPI	Displays the severely errored period intensity over the elapsed time (ET) period.
SES	Displays the number of severely errored seconds over the elapsed time (ET) period.
SESR	Displays the percentage of severely errored seconds over the elapsed time (ET) period.
SET COMMUNITY	Sets the SNMP Set Community name. The SNMP manager needs to use the same name to change the information on the radio.
SOFTWARE FEATURE/SW KEYS	Displays the types of software keys and if a particular software key is available or unavailable.
SOFTWARE REBOOT (IMMEDIATE)	Immediately reboots the system. It's a cold reboot of the system which will affect traffic. The software loaded upon reboot will come from the primary software bank.
SOFTWARE UPGRADE/RUN ALT SOFTWARE	Reboots the controller card and forces the execution of the software version stored in the alternate bank. The RFU software and SPU firmware are not reloaded.
SYS PROTECTION	Configures the radio for the following operations: Unprotected, Monitored Hot Standby, Frequency Diversity, Space Diversity, or Frequency Diversity with Space Diversity.
SYSTEM CAPABILITY	Displays the maximum capacity of the system. See Capacity.
SYSTEM UPGRADE/RUN ALT SYSTEM	Reboots the system and forces the usage of the load stored in the alternate bank. The SPU software, RFU software, and the SPU firmware are all affected.
TIME SERVER MODE/ENABLE RADIO AS TIME SERVER	Allows you to select which time server you want to use: Disable (none), SNTP, Netcom, or SNTP and Netcom.
TIME SYNC MODE	Allows you to select the time synchronization mode: SNTP, Netcom, or a free running clock.
TIME ZONE	Allows you to set the difference between the local radio's time and GMT.
TIMING CLOCK	Displays the type of timing clock as one of the following: THROUGH/ LOCAL/EXTINP1/EXTINP2/PDH/SPUR/EAST/WEST.
TPC EXCEED	Displays the percentage of time the radio was operating above the coordinated TX output power level.
TPC MODE[b]	Allows for setting the TPC mode to Manual, ATPC, or DTPC.
TRAP COMMUNITY	Allows for entering the SNMP trap community name up to 20 characters.
TRIBUTARY CODE	Allows the operator to set the code for a given tributary. Appears in NxDS1, 28DS1 or 28DS1+WS capacity systems.

TRIBUTARY EQUALIZER	Allows the operator to set the equalizer value for a given tributary. Appears in NxDS1, 28DS1, 28DS1+WS, DS3, or 3DS3+3WS capacity systems.
TRIBUTARY FRAMING	Allows you to set framing at M1-3 asynchronous or C-bit parity. Available for 28DS1, 28DS1+WS, or DS3 capacities.
TRIBUTARY MODE	Allows the operator to set the mode for a given tributary.
TX ACU LOSS[c]	Allows for entering, in tenth of a dB, the total loss of extra components that are installed on the transmitting signal path between the PA port and the reference point at which the user would like to see the TX output power value.
TX COORD ATTEN	Allows the operator to set the coordinated attenuation anywhere from 0-25 dB. The TPC mode must be ATPC or DTPC for this feature. Some countries require the radio to stay below this level the majority of the time.
TX MUTE	Allows you to mute the RFU using ON or OFF. The default is OFF.
TX REVERT TO A	Available when RCS mode is disabled. See "Transmitter Switching" on page 3-43.
TX STAT ATTEN	Allows the operator to set the static attenuation anywhere from 0-30 dB in 0.5 increments.
UNAV	Displays the amount of time that the signal was unavailable over the elapsed time (ET) period.
UNAVR	Displays the percentage of time that the signal was unavailable over the elapsed time (ET) period.
UPGRADE RFU	Executes the command to upgrade the RFU software to the version compatible with the current SPU software version.
USED CAPACITY	Allows you to change your system's capacity to use all or part of the maximum system capability. See "Capacity" on page 3-18.
WAYSIDE CODE	Available if system capability is OC3 (DS1), 3DS3+3WS, 28DS1+WS, 100BT+DS1, DS3+DS1, or E3+E1. Allows for setting the wayside code as either AMI or B8ZS.
WAYSIDE EQUALIZER	Available if system capability is OC3 (DS1), 3DS3+3WS, 28DS1+WS, 100BT+DS1, or DS3+DS1. Allows the operator to set the equalizer value for the wayside channel.
WAYSIDE MODE	Available if system capability is OC3 only. Allows for setting the mode of the wayside channel.
WAYSIDE TERMINATION	Available only when the maximum capacity of the system is OC3 and the Wayside mode is E1. Select E1 unbalanced (75 ohms) if using a BNC cable or E1 balanced (120 ohms) if using a RJ-45 cable.

*a. For more information, please refer to "Fine align the antenna" in the **SPU Installation** manual, IMN-903003-Exx.*

b. When the Transmit Power Control is set as ATPC, and there is fading of the receive signal of the online channel, software version 1.1.x and 2.0.x always boosts output power of BOTH transmitters. Manual mode and DTPC mode allow each transmitter to be adjusted independently.

c. Losses include RF branching, coupling, filters, or diplexer losses in the transmit and receive directions, between the radio antenna port and the transceiver. The measured transmitter power minus the supplied ACU loss value give the best indication of the power into the transmit antenna.

CHAPTER

8

GLOSSARY

This chapter provides an expanded description (as appropriate) of most of the acronyms used in this manual.

ACU	*Antenna Coupling Unit*
ADM	*Add/Drop Multiplexer* — A Digital multiplexing equipment that adds/removes individual signals to/from a collection of multiplexed signals in a network.
AGC	*Automatic Gain Control*
AIS	*Alarm Indication Signal*
AIS-L	*Line Alarm Indication Signal*
AMI	*Alternate Mark Inversion*
ARP	*Address Resolution Protocol*
ATM	*Asynchronous Transfer Mode* — A dedicated connection switching technology that organizes digital data into 53-byte cell units and transmits them over a physical medium using digital signal technology. Relative to other related cells, each cell is processed asynchronously and queued before being multiplexed over the transmission path.
ATPC	*Automatic Transmit Power Control* — A feature of digital microwave radio equipment that adjusts the transmitter output power based on path fading detected at the receiver.
B1	*Bit Interleaved Parity-8 (BIP-8)* — An RSOH byte for error checking the complete STM-1 signal at the end of a regenerator section.
B2	*Bit Interleaved Parity-24 (BIP-24)* — MSOH bytes for error checking an STM-1 signal (minus the RSOH) at the end of the multiplexer section.
B8ZS	*Bipolar 8 Zero Substitution*

CLEC	*Competitive Local Exchange Carrier* — A service provider that builds and operates communication networks in metropolitan areas, thus providing customers with an alternative to local telephone companies.
Compact Flash®	A compact, removable standard for storing and retrieving digital information in small, low-power devices. Such cards use flash technology for reusable recording, and ROM technology for read-only applications. Replaces the MMC (Multi Media Card), as of Product Release 6.0
CTU	*Configuration Transfer Utility* — A Harris' proprietary software utility for transferring the configuration data of the radio from a Version 1 Controller to a Version 2 Controller or vice versa.
DADE	*Differential Absolute Delay Equalization* — An adjustment to render a protected system hitless.
DHCP	*Dynamic Host Configuration Protocol*
DTPC	*Dynamic Transmit Power Control* — A feature enabling the regulation of a target receive signal level by remotely and proportionally controlling the corresponding transmitter output power level.
ESCAN	*Extended SCAN Protocol* — A Harris proprietary protocol that is more efficient and allows for faster communications than the SCAN protocol, also from Harris.
FD	*Frequency Diversity*
FEC	*Forward Error Correction* — A communication technique that compensates for a noisy transmission channel by sending, along with the primary data payload, additional information to correct for errors that occur in transmission.
FIR	*Finite Impulse Response* filter — Designates one of two primary types of digital filters used in Digital Signal Processing applications.
FTP	*File Transfer Protocol*
HDB3	*High Density Bipolar order 3*
HDLC	*High-level Data Link Control* — A bit-oriented synchronous data link layer protocol developed by ISO. HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.
HHT	*Handheld terminal* — A Harris' user interface device (also known as a display keypad). It allows the user to configure and monitor the radio when not using CIT or Web-CIT.
IDU	*Indoor Unit* — Apiece of equipment located inside the user's location.
IF	*Intermediate Frequency*
IP	*Internet Protocol* — A method or protocol by which data is sent from one computer to another on the Internet.
K1 and K2	In an SDH system, K1 and K2 are MSOH bytes used for • controlling the multiplexer section protection switching, • signalling Alarm Indication Signal (AIS), Far End Remote Failure (FERF), and • signalling Automatic Protection Switching (APS) alarms, when implemented.
LAN	*Local-area Network* — A data network located on a user's premises within a limited geographical area. Widely used technology standards in LANs are Ethernet, FDDI, and Token Ring.

LOH	*Line Overhead* — Contains the media's framing, routing protocol, and network-layer protocol overhead.
MHSB	*Monitored Hot Standby*
MMC	*MultiMediaCard* — A compact, removable standard for storing and retrieving digital information in small, low-power devices. MultiMediaCards use flash technology for reusable recording, and ROM technology for read-only applications.
MSOH	*Multiplexer Section Overhead* — As part of an SDH frame (multiplexer), refers to the processing time required by codes for error checking and control of transmissions.
MSUU	*Microwave Software Upgrade Utility* — A Harris' proprietary software utility for upgrading the software and firmware of the TRuepoint™ radios. Uses Microsoft Windows 2000® Service Pack 4 or later.
MTBF	*Mean Time Between Failures* — The average time (usually expressed in hours) in which a component operates without failure. It is calculated by dividing the total number of failures into the total number of operating hours observed.
MTBO	*Mean TIme Between Outages* — A function of MTBF, MTTR and the probability that the monitoring circuits detect a failure. The only circuits considered in the MTBO calculations are the ones that impact traffic.
MTR	*Mean Time To Restore*
MTTR	*Mean Time To Recovery* — The average time (usually expressed in minutes) that a device will take to recover from a non-terminal failure.
MUX	*Multiplexer* — A circuitry that combines two or more information-carrying channels for transmission over one channel, by using frequency division or time division techniques
NMS	*Network Management System* — such as Harris' FarScan™.
OC-*n*	*Optical Carrier Level n* — The optical signal that results from an optical conversion of a synchronous transport signal *n* (STS-n). This is the signal that will form the basis of the interface.
ODU	*Outdoor Unit* — Refer to RFU, described below.
OMM	*Optical Multimode*
OSM	*Optical Single Mode*
PCR	*Paperless Chart Recorder* — A software based diagnostic tool that stores operational data from a remote radio and provides view capability to the user.
PDH	*Plesiosynchronous Digital Hierarchy* — A complex multiplexing scheme of bit stuffing and byte interleaving. It multiplexes the lower level 64 kbit/s circuits into a successively higher order 2 Mbit/s, 34 Mbit/s, 140 Mbit/s and 565 Mbit/s aggregate rates.
PPP	*Point-to-Point Protocol* — A TCP/IP routing protocol that allows communications over serial communications lines without the use of other adapters, such as modems.
QAM	*Quadrature Amplitude Modulation* — A method of combining two amplitude-modulated signals into a single channel, thereby doubling the effective bandwidth.

QPSK	*Quadrature Phase Shift Keying* — A digital frequency modulation technique used for sending data over coaxial cable networks.
RDI-L	*Remote Defect Indication - Line*
RCS	*Reverse Channel Switching* — A rich feature set that provides protection against potential far-end transmitter silent failure.
Restricted Area	A location qualified in accordance with IEC Standard 60950-1 as providing an • access that can only be gained by Skilled Persons or users who have been instructed about the reasons for the restriction applied to the location and about any precautions to be taken; and • access achieved through the use of a Tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.
RFCOH	*Radio Frame Complementary Overhead* — Refers to data that is added to a data transmission unit, (such as Netcom data packets).
RFU	*Radio Frequency Unit* — The radio unit that is installed mainly outdoors.
RIP	*Routing Information Protocol*
RMS	*Rack Mounting Space*
RPC	*Radio Processing Card*
RS	*Revertive Switching* — A process that sends traffic back to the original working card after the card returns online.
RSL	*Received Signal Level*
RSOH	*Regenerator Section Overhead* — As part of an SDH frame (regenerator), refers to the processing time required by codes for error checking and control of transmissions.
RSSI	*Received Signal Strength Indicator* — A parameter returned from a transceiver that gives a measure of the RF signal strength, either uplink or downlink.
SD	Space Diversity
SDH	*Synchronous Digital Hierarchy* — An international standard for synchronous data transmission on optical media. SDH uses a multiplexing structure that enables direct access to individual 2 Mbit/s data streams from within the higher order aggregate line signals, which lays the foundation for benefits of distributed traffic switching and protection.
SDLC	*Synchronous Data Link Control* — A bit-oriented, full-duplex serial protocol that has spawned numerous similar protocols, including HDLC and LAPB.
SDM	*Signal Distribution Module* — An optional module used in conjunction with a redundant multiplexer, as part of the protection unit that is integrated with the SPU.

Skilled Person	A ***skilled person*** is considered to have the necessary knowledge and practical experience of electrical and radio engineering to appreciate the various hazards that can arise from working on radio transceivers, and takes appropriate precautions to ensure the safety of personnel. This individual is considered to be a ***skilled person*** only if he/she is competent to take responsibility for both his/her safety and for that of unskilled personnel under his/her immediate supervision, when working on the transceiver. Training requirements for a ***skilled person*** should not only be confined to technical matters and, preferably, should include first-aid treatment, especially methods of artificial resuscitation: respiration and cardiac compression (heart massage).
SNCP	*Subnetwork Connection Protection* — Designates path-switched SDH rings that employ redundant, fiber-optic transmission facilities. Organized in pairs, one fiber transmits in one direction while the backup fiber transmits in the other. If the primary ring fails, the backup takes over.
SNMP	*Simple Network Management Protocol* — Protocol used to facilitate network management by exchanging information between equipment on a network.
SONET	*Synchronous Optical Network* — An ANSI standard for synchronous data transmission on optical media that is the equivalent of SDH, described above.
SPU	*Signal Processing Unit* (Also referred to as IDU) — The indoor rack-mounted unit that contains plug-in modules for handling and processing the signal received from the RFU.
STM-*n*	*Synchronous Transport Module* — A data unit transmitted within a fixed time slot of 125 μs, also known as frame. SDH transport defines a range of frames, STM-1...STM-64, each corresponding to a particular transmission rate, such as STM-1 (155 Mbit/s), STM-4 (622 Mbit/s), STM-16 (2.5 Gbit/s), and STM-64 (10 Gbit/s).
STS-*n*	*Synchronous Transport Signal, Level* n— The basic logical building block signal of a SONET. The STS-1 (level 1) signal has a rate of 51.840 Mbit/s. The international equivalent of this rate is the STM.
TCM	*Trellis-Coded Modulation* — A bandwidth-efficient scheme that combines error-correction coding with modulation. The redundancy thus introduced by the coding does not expand the bandwidth, since the parity bits are absorbed by the extended signal constellation. Two-dimensional (2D) TCM uses dependency between in-phase and quadrature symbols, while four-dimensional (4D) TCM introduces dependency between symbols of two successive intervals.
TCP/IP	*Transmission Control Protocol/Internet Protocol* — A standard that provides connectivity across computer platforms ranging from mainframes to Macintoshes. These computers can exchange data when connected over a compatible network scheme, such as Ethernet or X.25. Originally developed by the Department of Defense in the 70's, these protocols are now a de facto industry standard.
UDP	*User Datagram Protocol* — A TCP/IP protocol that describes how messages reach application programs within a destination computer.

WAN — *Wide-area Network* — A network that provides telecommunication services to a geographic area larger than that served by a local area network or a metropolitan area network.

***Web*-CIT** — *Web-Craft Interface Tool* — A Harris' proprietary software utility for monitoring and controlling the operation and configuration of the TRuepoint™ radios. Located on the TRuepoint™ Controller, any of the two **RPTR/NMS** ports allows for connecting a PC running the *Web*-CIT server that is embedded in the radio. This web server stores HTML pages and applets that provide a user interface for monitoring and controlling any TRuepoint™ Network Element, using the Microsoft® Internet Explorer, version 5.5 and later.

APPENDIX

A

ETHERNET THROUGHPUT MEASUREMENT PROCEDURE

Introduction

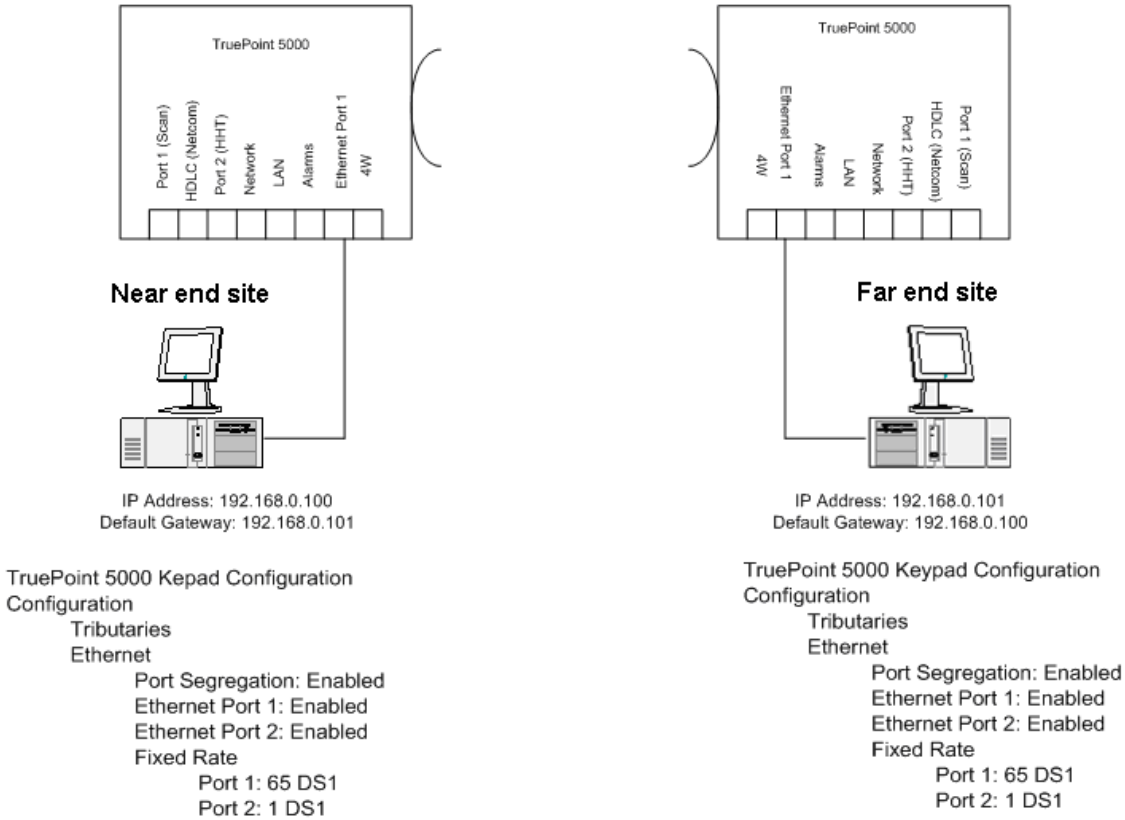
The following test procedure describes how to measure the layer 3 throughput over a single hop of TRuepoint 5000 using the NetPerf application. This procedure is intended for a field technician that does not have the recommended Smart Bit test set to properly measure the layer 2 throughputs. It is important to note that only layer 2 throughput measurements will provide accurate measurement since a receiver is not required to generate data acknowledgement at this layer.

The NetPerf measurement set up is described below. Only one PC is required at each end of the hop. To simplify the number of PC configuration changes Windows XP has to be used.

Pre-requisites: 2 PC's with Windows XP.

The recommended software for TRuepoint is 4.6.3 or higher.

Figure A-1: Set-up



Netperf is a benchmark application that can be used to measure various aspects of networking performance. The primary focus is bulk (unidirectional) data transfer and request/response performance using either TCP or UDP. The available tests described in this procedure include:

- TCP and UDP unidirectional transfer and request/response over IPv4 and IPv6 using the Sockets interface.

Netperf is designed around a basic client-server model. There are two executables: netperf and netserver. With this procedure, only the netperf program will be executed while the netserver program is invoked by the remote system's end. Executing netperf corresponds to the establishment of a control connection to the remote system.

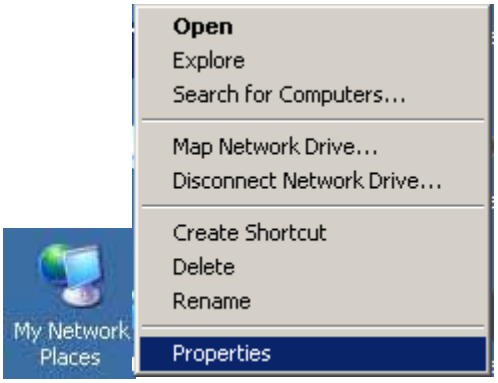
The download location for Netperf is http://www.netperf.org/netperf/DownloadNetperf.html.

Configuring IP addressing and flow control on PC's

Procedure to set an IP address

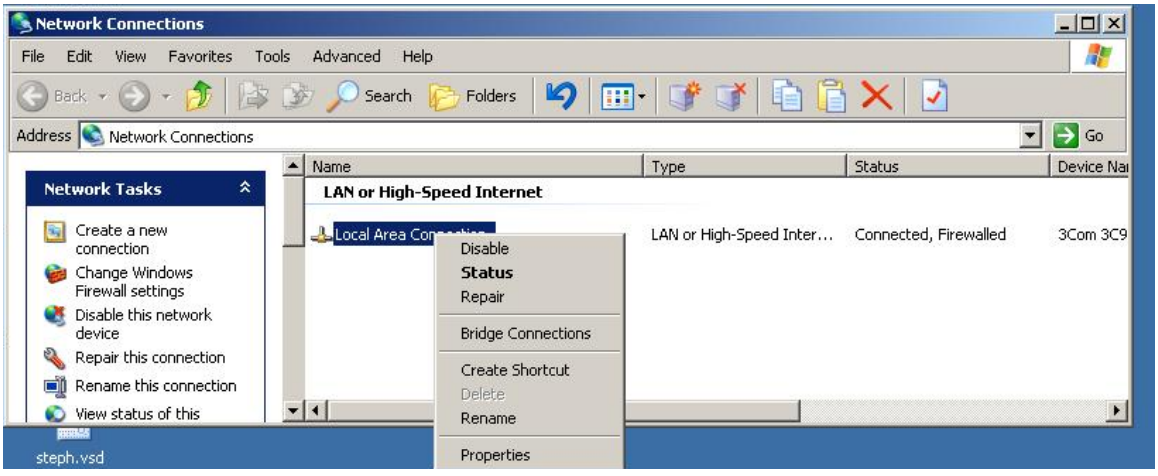
1. On the near end PC Desktop right click on the "My Network Places" icon. You should see a window similar to Figure A-2.

Figure A-2: My Network Places



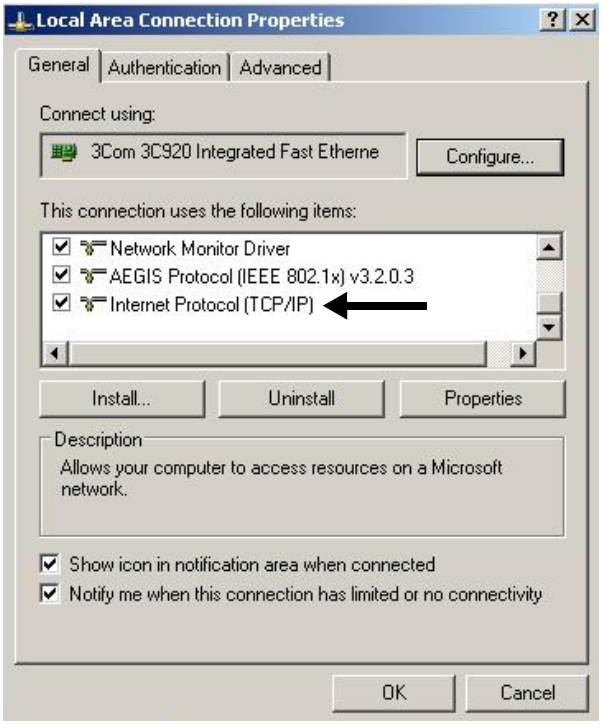
2. Select Properties. The following window should appear as shown in Figure A-3. Select Local Area Connection and right click on it.

Figure A-3: Local Area Connection



3. Select Properties and the window shown in Figure A-4 should appear.

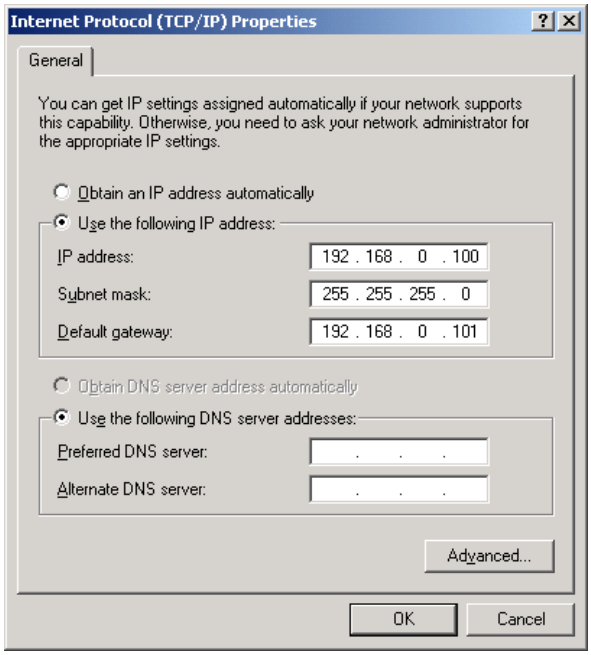
Figure A-4: Local Area Connection Properties



4. Select Internet Protocol and click on Properties. Figure A-5 should appear.

5. Configure a manual IP address as shown in Figure A-5 and press OK.

Figure A-5: Internet Protocol Properties

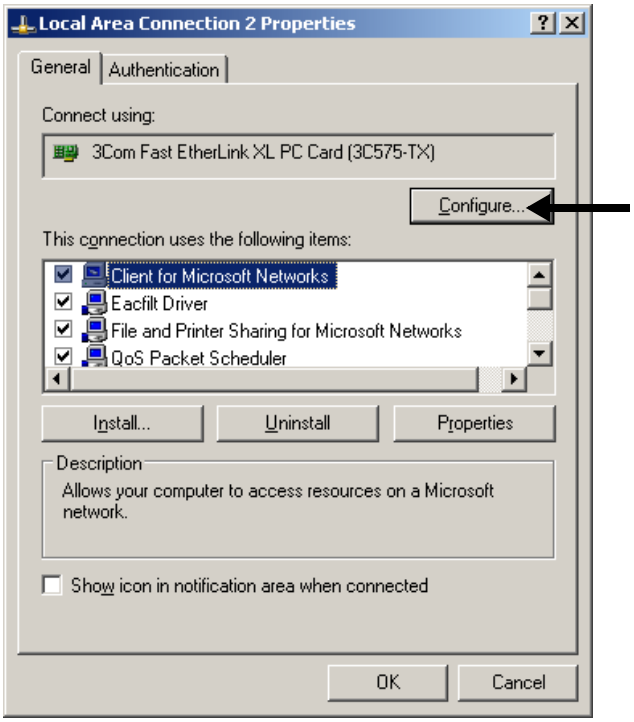


No DNS server IP addresses are required for NetPerf testing.

Procedure to set the flow control

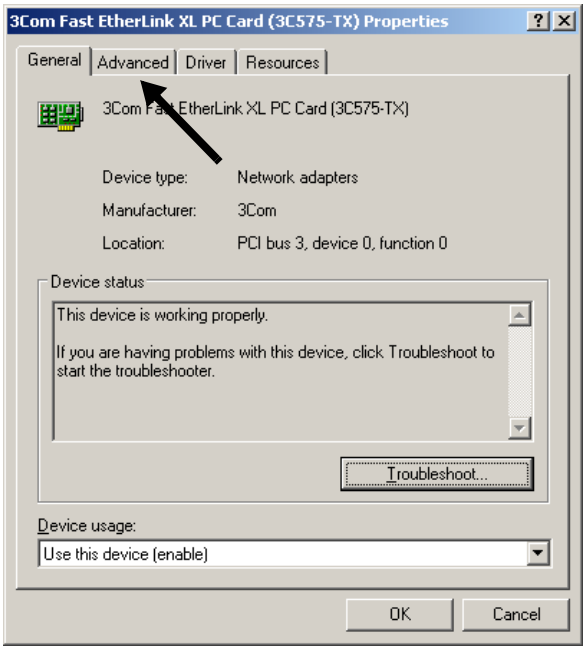
1. Go back to the General tab and select Configure.

Figure A-6: Local Area Connection Properties Example 2



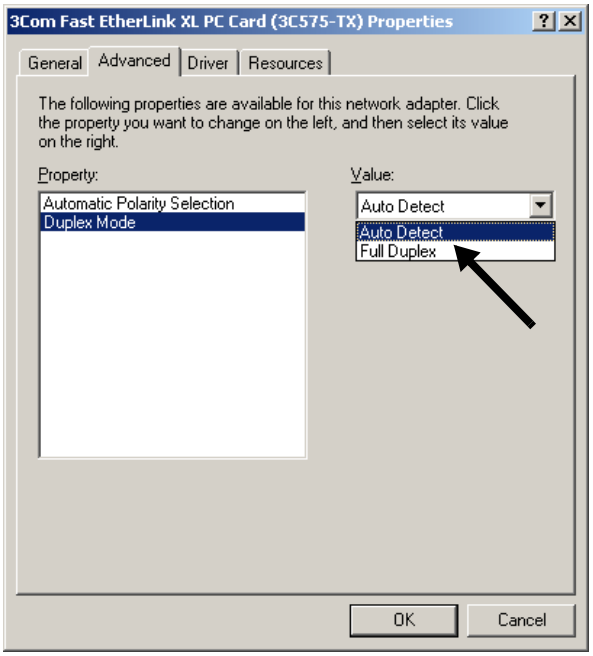
2. Select the Advanced tab as shown in Figure A-7.

Figure A-7: Ethernet Properties



3. Make sure that Auto Detect (XP) or Auto Mode (2000) is selected for the Duplex Mode.

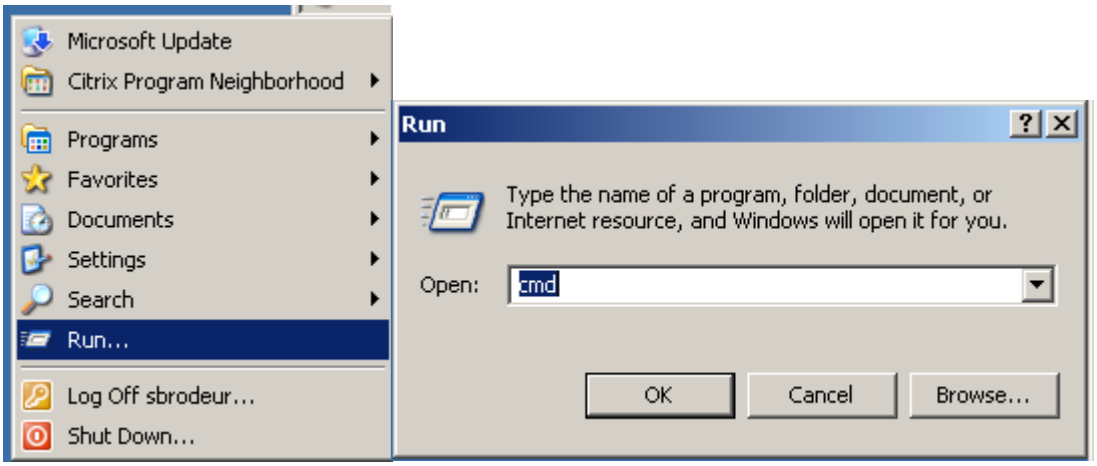
Figure A-8: Ethernet Properties Advanced Tab



4. Click on OK to configure the IP address. This address corresponds to the PC attached to the near end TRuepoint 5000.

5. Verify if this IP address is correctly set by clicking the Windows Start Button (Windows flag) and by clicking Run as shown in Figure A-9. Type cmd in the box and then press OK.

Figure A-9: Run

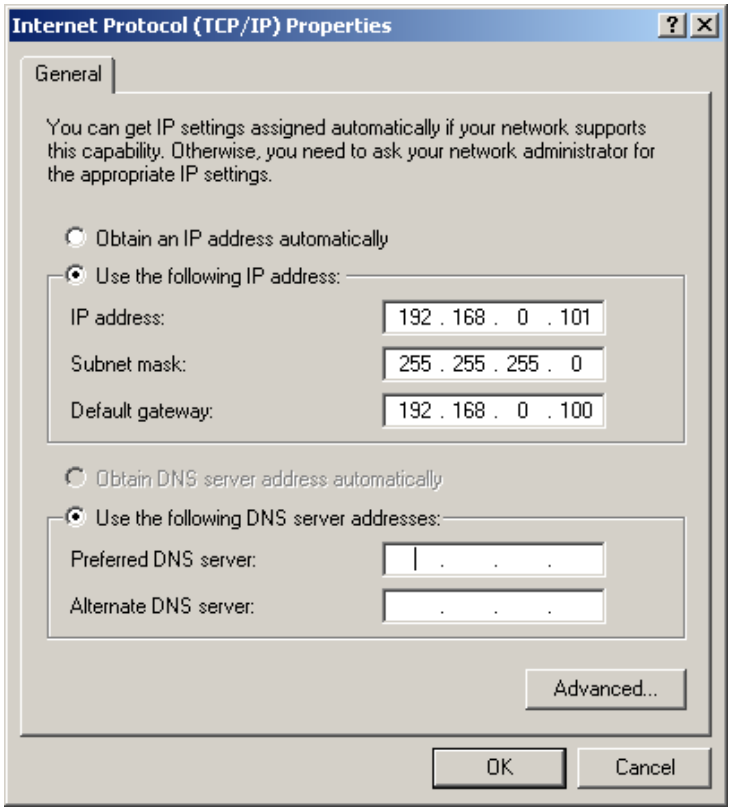


6. A DOS Windows should appear on the screen. Type the **ipconfig/all** command in the DOS windows and the configured IP address should appear.

   Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix.:
   Description.....: 3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible)
   Physical Address.....: 00-0B-DB-D8-2F-1C
   Dhcp Enabled.....: No
   Autoconfiguration Enabled....: No
   IP Address.....: 192.168.0.100
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.0.101

   The IP address and flow control of the near end PC are now set. The same steps must be taken to set the IP address of the far end TRuepoint 5000 as described here.

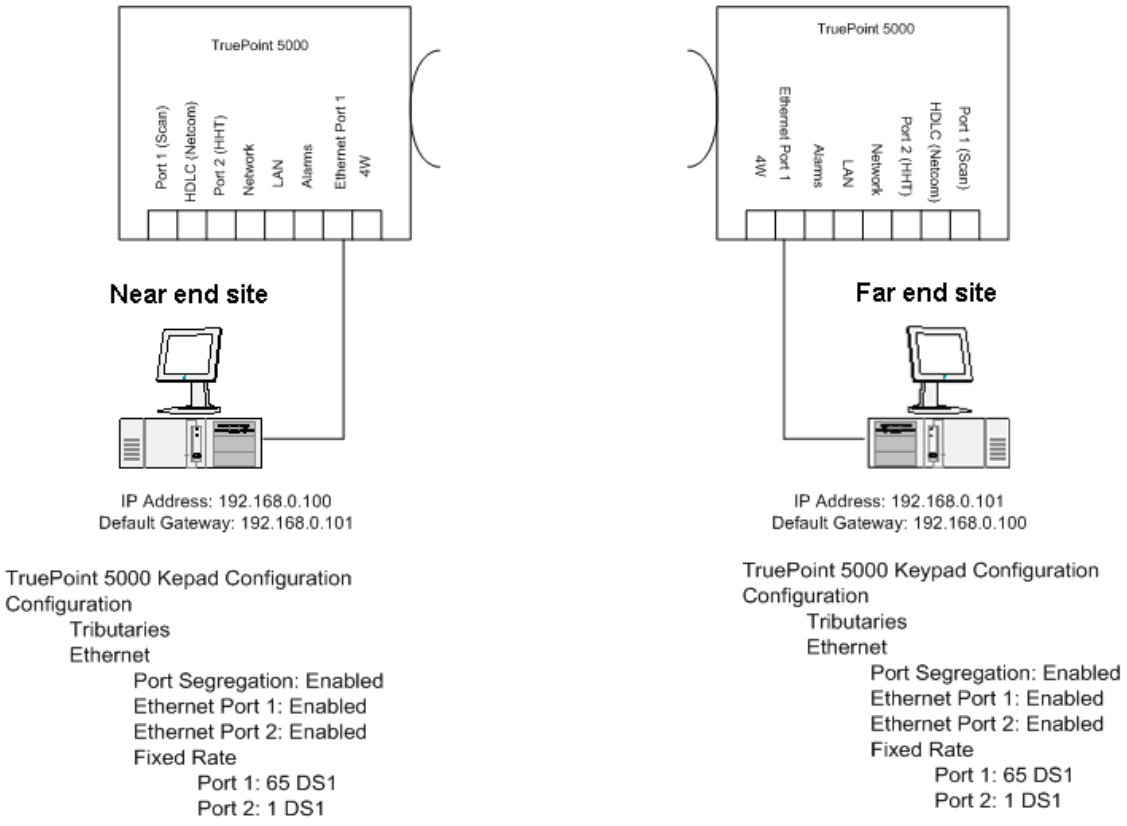
Figure A-10: Far End Internet Protocol Properties



Ping remote PC

The second step consists in connecting a PC at each end of the hop.

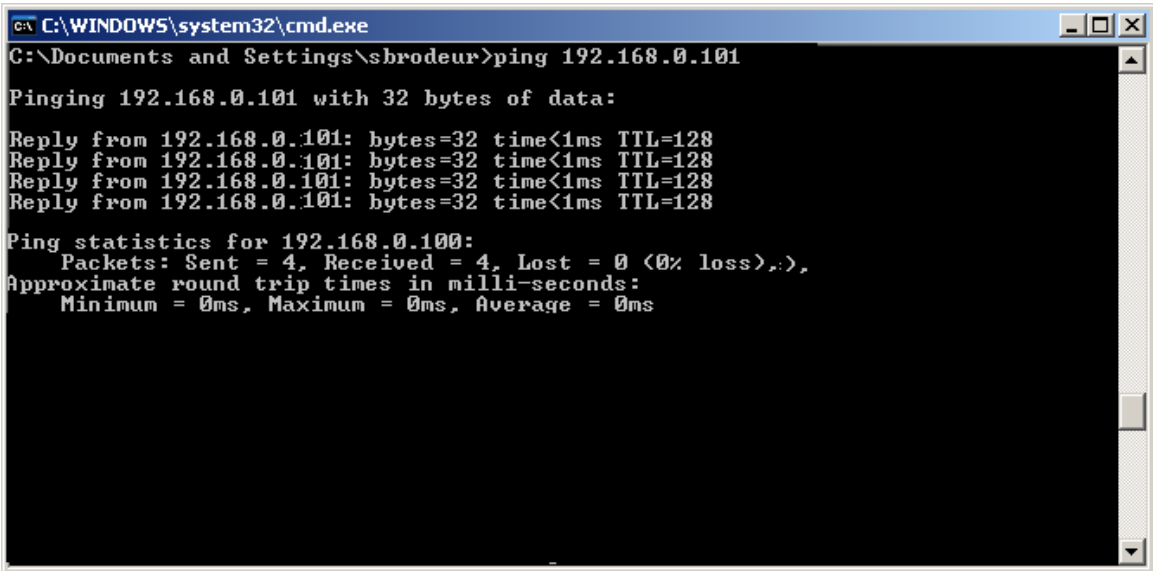
Figure A-11: Connecting a PC at each hop



The TRuepoint 5000 Ethernet port 1 LED should flash green. The connectivity between the near end's PC and the far end's PC must now be tested. This can be done by pinging the far end PC.

1. Click the Windows Start Button (Windows flag) and then on Run. See Figure A-9. Type cmd in the box and then press OK.
2. At the near end site type the following command in the DOS window (see Figure A-12). **A reply from the far end site should be received if the set up is correct.**

Figure A-12: DOS window command



Measuring throughput with the Netperf utility

No other application should be running on both PC's during a Netperf test.

1. On the far end PC that is running the netperf server, start the server by this Netperf command line:
   C:\netperf > netserver-a4.exe

Figure A-13: Netperf Command Line Example

2. On the near end PC that will run the netperf client, start the client by one of the following:

Netperf command line:
C:\NetPerf1>netperf-a4.exe -H 192.168.0.101 -v 2 -t TCP_STREAM -l 60 -- -s 17520 -S 17520
where

- H is the target machine IP address
- -v 2 specifies a high level of verbose
- -t specifies the test name (TCP_STREAM or UDP_STREAM)
- -s is the local socket (send/receive) buffer size. Often, this will affect the advertised and/or effective TCP or other window, but on some platforms it may not. This explains why it is important to set the proper TCP/IP window register. By default, Netperf use the system's default socket buffer sizes.
- -S is the remote socket (send/receive) buffer size. Often, this will affect the advertised and/or effective TCP or other window, but on some platforms it may not. While the historic expectation is that setting the socket buffer size has a direct effect on say the TCP window, today that may not hold true for all stacks. Further, while the historic expectation is that the value specified in a setsockopt() call will be the value returned via a getsockopt() call, at least one stack is known to deliberately ignore history. This explains why it is important to set the proper TCP/IP window register. By default, Netperf uses the system's default socket buffer sizes.

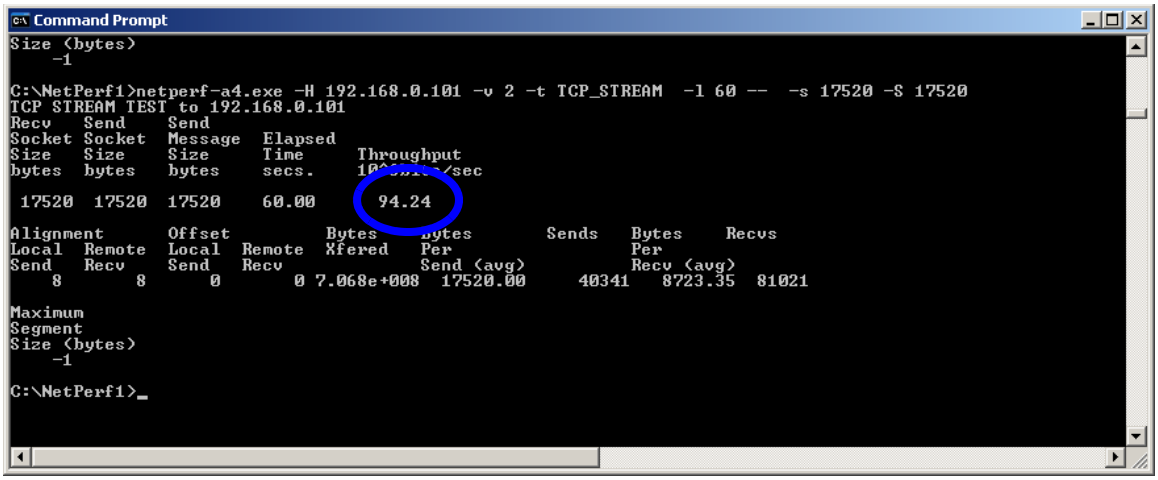
The suggested syntax omits the following flags that should be at least known by the user.

- -m specifies the size of the buffer passed-in to the “send” calls of a TCP or UDP_STREAM test. Note that this may have only an indirect effect on the size of the packets sent over the network, and certain Layer 4 protocols do not preserve or enforce message boundaries, so setting -m for the send size does not necessarily mean the receiver will receive that many bytes at any one time. This flag will indicate how many bytes will be transmitted before NetPerf sends the same byte pattern again. The default local send socket buffer size for the connection is either the system's default or the value set via the -s option.
- -M is the size of the buffer passed-in to the “recv” calls of a _STREAM test. This will be an upper bound on the number of bytes received per receive call.

The remote receive socket buffer size for the data connection is either the system's default or the value set via the -S option

- `-l The testlen` option controls the length of any iteration of the requested test. A positive value for *testlen* will run an iteration of the test for at least *testlen* seconds. A negative value for *testlen* will run an iteration for the absolute value of *testlen* transactions for a UDP or TCP _STREAM test. Default value for the recommended Netperf syntax is 10 sec.
- -w `The <sizespec>` option controls the number of buffers in the send (first or only value) and or receive (second or only value) buffer rings, Netperf does not continuously send or receive from a single buffer. Instead it rotates through a ring of buffers. [Default: One more than the size of the send or receive socket buffer sizes (-s and/or -S options) divided by the send -m or receive -M buffer size respectively].

Example:



To have the real throughput the following formula must be apply (see Netperf throughput VS Ethernet throughput).

Real_Throughput = Netperf_Throughput * 1538 Bytes/1460 Bytes
= 94.24 bits/sec * 1.0534
= 99.27 Mbits/sec 100Mbits/sec

Netperf throughput VS Ethernet throughput

This is the representation of an Ethernet frame (802.3):

Figure A-14: Ethernet Frame

The maximum Ethernet frame is 1518 bytes. This is when the User Data field is used to its fullest capacity (1460 bytes).

During transmission, a preamble of 8 bytes is added by the NIC card for synchronization reasons, and an IPG – Interpacket Gap – of 12 bytes is also added to the Ethernet frame. The IPG allows many users or applications to send traffic on a network at approximately the same time.

Extra BitsTable A-1 presents these extra bits added to an Ethernet packet and compares the time it takes to transmit these bits depending on whether you are using Fast Ethernet or Ethernet:

Table A-1: Extra Bits

Rate	Preamble			Minimum Gap between two packets			Total		
	(us)	(Byte)	(Bit)	(us)	(Byte)	(Bit)	(us)	(Byte)	(Bit)
100 Mb/s	0.64	8	64	0.96	12	96	1.6	20	160
10 Mb/s	6.4	8	64	9.6	12	96	16	20	160

When measuring throughput, this information needs to be considered.

The table below presents results measured by SmartBits 2000 on a TRuepoint 5000 hop with 16DS1 + 2x10/100BT module cards, and demonstrates why measuring 100Mbps is nearly impossible.

The port segregation feature is enabled. This feature requires a 4 byte tag to indicate which port is being used to send the data. This tag does not imply interoperability issues with external equipment, since it will be disregarded if not recognized.

Table A-2: SmartBits 2000 Example

A	B	C	D	E	F
Ethernet Standard Frame Packet Length	**Transmitted Standard Frame** Includes 8 bytes - Preamble 12 bytes - IPG	**Transmitted TRuepoint Frame** Includes 4 bytes - Segregation	**TRuepoint Maximum Throughput** 100 MB/s	**Theoretical Calculated Maximum Throughput**	**SmartBits Measured Throughput**
Byte	*Byte*	*Byte*	*Pkt/sec*	*Mb/s*	*Mb/s*
64	84	88	142045	95.45	95.45
128	148	152	82236	97.36	97.37
256	276	280	44642	98.56	98.57
512	532	536	23320	99.24	99.26
1024	1044	1048	11927	99.61	99.67
1280	1300	1304	9585	99.68	99.70
1518	1538	1542	8106	**99.73 (max)**	99.72

Column Description:

A - Ethernet frame size

B - Ethernet Frame size with preamble of 8 bytes and IPG of 12 bytes

C - Frame size including 4 byte tag for the Port Segregation feature

D - On a 100Mbps line, the maximum amount of packets that can be transmitted is:

$$100\ Mbp/sec = \text{Frame } bytes/Packet \times 8\ bits/byte \times \text{N } Packets/sec$$

$$\Rightarrow \text{N} = \frac{100 \times 10^6}{Frame \times 8}$$

Example => We need to consider the actual **frame** size being transmitted; this will correspond to **column C**. Let's calculate using the largest possible frame size:

$$\Rightarrow \text{N} = \frac{100 \times 10^6}{1542 \times 8} = 8106 \text{ Packets}$$

E – The theoretical throughput corresponds to:

$$Throughput = N\ Packets / \sec \times Frame\ byte / Packet \times 8\ bit / byte$$

Example => Let's calculate using the largest possible frame size:

$$Throughput = 8106\ Packets / \sec \times 1538\ bytes \times 8\ bit / byte$$

$$= 99.73 \text{ Mbps}$$

F – Measured Data
The values in column F will differ if the method of test is different. If using an application tool such as Netperf, the measured throughput will be lower. Figure A-14 clearly segments the different fields. An application tool measures the effective throughput of the User Data field, or in other words the payload.

The TCP/IP Maximum Segment Size (MSS) is the largest amount of data, specified in bytes, that a computer or communications device can handle in a single, un-fragmented piece. The default MSS is 1460 byte.

In conclusion the maximum TCP/IP throughput achievable with any benchmark tool (ex: Netperf) is:
1460 byte/1538 byte * 99.73 Mb/s= 94.62 Mb/s

Since this value depends on many parameters like the processing power of the CPU, the Ethernet line Interface card, etc., the Netperf test objective should be around 90 Mb/s.

INDEX

S

T

U

V

W