

ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

Custom engineering
so your equipment works exactly as you specify.

- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Visit our website - *Click HERE*

Broadmore™ 1750

USER MANUAL



Part Number: 770-0020-DC
Product Release 4.6
January 2008

Copyright© 2008 Carrier Access Corporation. All rights reserved.

The information presented in this manual is subject to change without notice and does not represent a commitment on the part of Carrier Access Corporation. The hardware and software described herein are furnished under a license or non-disclosure agreement. The hardware, software, and manual may be used or copied only in accordance with the terms of this agreement. It is against the law to reproduce, transmit, transcribe, store in a retrieval system, or translate into any medium–electronic, mechanical, magnetic, optical, chemical, manual, or otherwise–any part of this manual or software supplied with the Broadmore 1750 for any purpose other than the purchaser's personal use without the express written permission of Carrier Access Corporation.

Broadmore and the Carrier Access logo are trademarks of Carrier Access Corporation. All other brand or product names are trademarks or registration trademarks of their respective companies or organizations.

Contact Information:

Carrier Access Corporation
5395 Pearl Parkway
Boulder, CO 80301-2490
Corporate Phone: (303) 442-5455
Fax: (303) 443-5908
www.carrieraccess.com

Customer Support Direct: (800) 786-9929
E-mail: tech-support@carrieraccess.com

PREFACE

Compliance

FCC Requirements, Part 15

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the Federal Communications Rules. These limits are designed to provide reasonable protection against harmful interference when equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

WARNING! **TO MEET FCC PART 15 CLASS A RADIATED EMISSIONS REQUIREMENTS, YOU MUST FOLLOW SPECIFIC INSTALLATION REQUIREMENTS GIVEN FOR EACH MODULE USED IN THIS CHASSIS WHICH ARE PROVIDED IN THE MODULE INSTALLATION SECTION. FOR MORE INFORMATION ABOUT INSTALLING CABLES ACCORDING TO FCC PART 15 CLASS A, FOLLOW THE INSTRUCTIONS IN *"Cabling and Compliance Requirements" on page 6-4*.**

Common Criteria Evaluation and Validation Scheme (CCEVS) issued Validation Report number CCEVS-VR-06-0039, 26 June 2006, for EAL 3 Conformance for the Carrier Access Broadmore 500, 1700, and 1750 Release 4.1.1. This report is maintained on the NIAP Validated Products List (VPL) at http://niap.bahialab.com/cc-scheme/.

DISA Validated

Defense Information System Agency, Center for Information Assurance Engineering validated Broadmore Information Assessment, 2 August 2006, contract number SP0700-98-D-1002, TAT 5-15.

FIPS 140-2 Validated

FIPS 140-2 Inside.

National Institute of Technology (NIST) Cryptographic Module Validation Program (CMVP) validated Broadmore to FIPS 140-2, Level 1 overall, Certificate #478, November 2004. Certificate and Security Policy maintained at http://csrc.nist.gov/cryptval/.

JITC Validated

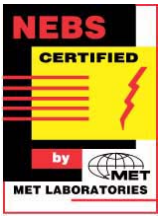
Joint Interoperability Test Certification (JITC) at Ft. Huachuca, 23 June 2006. TSSI Certificate on NIPRNET at http://jitc.fhu.disa.mil/tssi/.

IPv6 Ready

The IPv6 Forum certified the Broadmore as IPv6 ready on 26 January, 2007. The certificate is maintained at http://www.ipv6ready.org/logo_db/logo_search2.php?logoid_number=01-000379&btm=Search

NEBS Validated

Network Equipment Building System (NEBS). The Broadmore 1750 has been validated to Telcordia GR-1089-CORE, Level 3 Requirements, Issue 2, December 1997 Revision 1, February 1999. See MET Labs report ESL-9647 and TEL-9647.2000.



National Electrical Code Requirements

Equipment intended to be electrically connected to a telecommunications network shall be listed for the purpose. The Broadmore 1750 is listed and is in compliance with UL60950 third edition, and CSA-C22.2 NO. 60950-00.

No. 950-95 Standard for Safety for Information Technology Equipment. CSA has certificated to both standards for product safety. The CSA File Number is LR 107313.

Some telecommunications equipment does not provide overvoltage or power-cross protection on DS1 lines. Equipment that does not provide overvoltage or power-cross protection is not compliant with the National Electrical Code for customer premises installation. The Broadmore 1750 provides this protection.

UL60950/CSA-C22.2 NO. 60950-00 compliance is an important requirement for carriers installing equipment within customer buildings and is designed to prevent the product and the telephone wiring from starting building fires.

Safety Information

CAUTION! **ALWAYS USE CAUTION WHEN INSTALLING TELEPHONE LINES. READ THE CAUTIONS BELOW FOR DETAILS ON SAFETY GUIDELINES TO PREVENT INJURY.**

- **Never touch uninsulated telephone wires and terminals** unless the telephone line has been disconnected at the Network Interface (NI) as voltage potentials as high as 300 VAC may be present across the transmit and receive pairs.
- **Only use No. 26 AWG or larger** telecommunication line cord, to reduce the risk of fire.
- Never install telephone wiring during a lightning storm.
- **Never install telephone jacks in wet locations** unless the jack is specifically designed for wet locations.
- Refer to the installation section of this manual for a safe and proper installation procedure. All wiring external to this equipment should follow the current provision of the National Electrical Code.

Notices

This manual contains important information and warnings that must be followed to ensure safe operation of the equipment.

DANGER! **A *DANGER* NOTICE INDICATES THE PRESENCE OF A HAZARD THAT CAN OR WILL CAUSE DEATH OR SEVERE PERSONAL INJURY IF THE HAZARD IS NOT AVOIDED.**

CAUTION! **A *CAUTION* NOTICE INDICATES THE POSSIBILITY OF INTERRUPTING NETWORK SERVICE IF THE HAZARD IS NOT AVOIDED.**

WARNING! **A *WARNING* NOTICE INDICATES THE POSSIBILITY OF EQUIPMENT DAMAGE IF THE HAZARD IS NOT AVOIDED.**

NOTE: **A *NOTE* INDICATES INFORMATION TO HELP YOU UNDERSTAND HOW TO PERFORM A PROCEDURE OR HOW THE SYSTEM WORKS. NOTES SHOULD BE READ BEFORE PERFORMING THE REQUIRED ACTION.**

Electrostatic Discharge (ESD) Precautions

WARNING! **THE BROADMORE CONTAINS CIRCUIT CARDS AND COMPONENTS THAT ARE SUBJECT TO DAMAGE BY ELECTROSTATIC DISCHARGE.**

ESD can damage processors, circuit cards, and other electronic components. Always observe the following precautions before installing a system component.

1. Do not remove a component from its protective packaging until ready to install it.
2. Wear a wrist grounding strap and attach it to an ESD connector or a metal part of the system unit before handling components. If a wrist strap is not available, maintain contact with the system unit throughout any procedure requiring ESD protection.



An ESD warning label appears on packages and storage bags that contain static-sensitive products and components.

Warranty

Carrier Access warrants to BUYER that Product Hardware will be free from substantial defect in material and workmanship under normal use in accordance with its Documentation and given proper installation and maintenance for period of one year from the date of shipment by Carrier Access.

Carrier Access warrants that the Licensed Software, when used as permitted under its License Terms and in accordance with the instructions and configurations described in the Documentation (including use on Carrier Access product or a computer hardware and operating system platform supported by Carrier Access), will operate substantially as described in the Documentation for a period of ninety (90) days after date of shipment of the Licensed Software to BUYER.

This warranty shall not apply to Products or Software that have been either resold or transferred from BUYER to any other party. Any such transfer voids the above warranty and related licenses. Carrier Access offers expanded product care beyond what is covered by the warranty through different support plans. The plans are designed to maximize network availability through advance replacement for defective equipment. Please contact your Carrier Access representative for support program details.

Warranty Procedure

BUYER must promptly notify Carrier Access of any defect in the Product or Software and comply with Carrier Access' return/repair policy and procedures. Carrier Access or its agent will have the right to inspect the Product or workmanship on BUYER's premises. With respect to a warranty defect in Product hardware reported to Carrier Access by BUYER during the warranty period, Carrier Access, as its sole obligation and BUYER's exclusive remedy for any breach of warranty, will use commercially reasonable efforts, at its option, to:

a. repair, replace, or service at its factory or on the BUYER's premises the Product, or component therein, or workmanship found to be defective so that the Product hardware operates substantially in accordance with Carrier Access Documentation; or

b. credit BUYER for the Product in accordance with Carrier Access's depreciation policycredit BUYER for the Product in accordance with Carrier Access's depreciation policy.

With respect to a warranty defect in the Licensed Software reported to Carrier Access by BUYER during the 90-day software warranty period, Carrier Access, at its own expense and as its sole obligation and BUYER's exclusive remedy for any breach of the software warranty, will use commercially reasonable efforts to, at its option,

a. correct any reproducible error in the Licensed Software, or

b. replace the defective Licensed Software, as follows: Should a Severity 1 or 2 warranty defect with the Software occur during the 90-day warranty period, Carrier Access will provide, in its sole determination, either

1. software to resolve the defect to be downloaded into the affected units by the BUYER or
2. a documented workaround to address the issue.

Severity 1 issues are failures of the Licensed Software to comply with the Carrier Access software specifications and that completely or severely affect the Carrier Access Product and its traffic or service capacity, or maintenance or monitoring capabilities.

Severity 2 issues are failures of the Licensed Software to comply with the Carrier Access software specifications and that result in a major degradation of the Carrier Access Product so as to impact its system or service performance, or significant impairments to network operator control or effectiveness. Should a Severity 3 warranty defect with the Licensed Software occur during the 90-day warranty period, Carrier Access will provide assistance to Buyer to determine if a solution or workaround will be provided in a subsequent software release following the reported issue.

Severity 3 issues are defined as failures of the Licensed Software to comply with the Carrier Access software specifications but that do not significantly impair the function or service of the Carrier Access Product or the system.

Determination of Severity 1, 2 or 3 shall be made solely by Carrier Access following receipt of the reported problem. Refurbished material may be used to repair or replace the Product. BUYER shall bear the risk of loss for Products or Software returned to Carrier Access for repair, replacement, or service, and the same must be shipped pre-paid by BUYER.

Requests for warranty services and troubleshooting must be made to, and will be provided by, the Carrier Access Customer Support Center via telephone during the warranty period and during normal business hours. Normal business hours for Carrier Access Customer Support Center are 7:00 a.m. to 6:00 p.m. Mountain Standard Time, Monday through Friday, excluding weekends and standard Carrier Access recognized holidays.

Limitation of Warranty & Limitation of Remedies

Correction of defects by repair, replacement, or service will be at Carrier Access's option and constitute Carrier Access' sole obligation and BUYER's sole and exclusive remedy under the limited warranty. Any such error correction or replacement provided to BUYER does not extend the original warranty period for hardware or software, respectively.

Carrier Access assumes no warranty or other liability with respect to defects in the Product or Software caused by:

a. modification, repair, storage, installation, operation, or maintenance of the Product or Software by anyone other than Carrier Access or its agent, or as authorized and in accordance with the Carrier Access Documentation; or

b. the negligent, unlawful or other improper use or storage of the Product or Software, including its use with incompatible equipment or software; or

c. fire, explosion, power failures, acts of God, or any other cause beyond Carrier Access' reasonable control; or

d. handling or transportation after title of the Product passes to BUYER.

Other manufacturer's equipment or software purchased by Carrier Access and resold to BUYER will be limited to that manufacturer's warranty. Carrier Access assumes no warranty liability for other manufacturer's equipment or software furnished by BUYER.

BUYER UNDERSTANDS AND AGREES AS FOLLOWS: Except for the limited warranty set forth above, the Product, License Software and all services performed by Carrier Access hereunder are provided "as is," without representations or warranties of any kind. Carrier Access does not warrant that the Product, License Software, any hardware or software, or any update, upgrade, fix or workaround furnished to BUYER will meet BUYER's requirements, that the operation thereof, including any maintenance or major releases thereto will be uninterrupted or error-free.

THE WARRANTIES IN THIS AGREEMENT REPLACE ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, AND ALL OTHER OBLIGATIONS OR LIABILITIES OF CARRIER ACCESS, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT AND/OR ANY IMPLIED WARRANTIES ARISING OUT OF COURSE OF PERFORMANCE OR COURSE OF DEALING. ALL OTHER WARRANTIES ARE DISCLAIMED AND EXCLUDED BY CARRIER ACCESS.

THE REMEDIES CONTAINED IN THIS AGREEMENT WILL BE THE SOLE AND EXCLUSIVE REMEDIES WHETHER IN CONTRACT, TORT, OR OTHERWISE, AND CARRIER ACCESS WILL NOT BE LIABLE FOR INJURIES OR DAMAGES TO PERSONS OR PROPERTY RESULTING FROM ANY CAUSE WHATSOEVER, WITH THE EXCEPTION OF INJURIES OR DAMAGES CAUSED BY THE GROSS NEGLIGENCE OF CARRIER ACCESS. THIS LIMITATION APPLIES TO ALL SERVICES, SOFTWARE, AND PRODUCTS DURING AND AFTER THE WARRANTY PERIOD. IN NO EVENT WILL CARRIER ACCESS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, LOSS OF DATA, OR COMMERCIAL LOSSES EVEN IF CARRIER ACCESS HAS BEEN ADVISED THEREOF.

No agent, BUYER, or representative is authorized to make any warranties on behalf of Carrier Access or to assume for Carrier Access any other liability in connection with any of Carrier Access's Products, software, or services.

The foregoing summarizes Carrier Access' entire product and software warranties, which are subject to change without notice.

Warranty Product Returns

Before returning any equipment to Carrier Access Corporation, first contact the distributor or dealer from which you purchased the product.

A Return Material Authorization (RMA) number is required for all equipment returned to Carrier Access Corporation. Call Carrier Access Corporation Customer Support at (800) 786-9929 or (303) 442-5455 for RMA number, repair/warranty information and shipping instructions. Be prepared to provide the following information:

- Carrier Access Corporation serial number(s) from the system chassis or circuit card(s)
- Name of distributor or dealer from which you purchased the product
- Description of defect

TABLE OF CONTENTS

Preface

Compliance iii
Safety Information vi
Notices vii
Electrostatic Discharge (ESD) Precautions viii
Warranty ix

1 Product Description

Purpose 1-2
Applications 1-3
Interfaces 1-4
- ATM Interfaces 1-4
- User Equipment Interfaces 1-4
- Management Interfaces 1-5

System Description 1-7
- Features 1-7
- Chassis 1-8
- Fan Tray 1-9
- Power and Redundancy 1-9
- Grounding 1-9
- Alarms 1-9
- Modules 1-10

Module Descriptions 1-12
- OC-12c/STM-4c NIM 1-13
- NIM IOM 1-14
- Unstructured DS3-3 SAM 1-15
- Unstructured E3-3 SAM 1-16
- Unstructured DS3-3/E3-3 IOM 1-17
- Structured DS3 SAM 1-18

Structured DS3 IOM 1-19
Unstructured DS3-3/E3-3 IOM 1-20
Protection IOM 1-21
CPU 1-22
CPU IOM 1-23
Alarm Power Module (APM) 1-24
Alarm Power Module IOM 1-25

2 Planning and Ordering Guide

Application Planning Guide 2-2
Basic Features 2-2
TDM Circuit Aggregation and Backhaul 2-3
Mission-Critical Circuit Resiliency 2-4
System Planning Factors 2-6
System Architecture 2-6
Cell Bus Configuration 2-8
Unstructured DS3-3/E3-3 Configuration Guidelines 2-9
Structured DS3 Configuration Guidelines 2-10
ATM Bandwidth per Cell Bus 2-11
ATM Bandwidth per Module 2-12
ATM Network Loading 2-12
Installation Planning Factors 2-13
Ordering Guide 2-15
Contact Information 2-15
Broadmore 1750 Chassis 2-15
Broadmore 1750 Options and Spares 2-16
Network Interface Module (NIM) Options 2-17
Service Access Module (SAM) Options 2-18

3 Receipt of Product

Receipt 3-2
Unpacking 3-2
Inspection 3-3
Damage Reporting 3-3

4 Chassis Installation and Grounding

Precautions 4-2
Installation Factors 4-3
Rack Mounting 4-4
Tools 4-4
Mounting Brackets 4-5
Rack Mounting Procedure 4-6
Chassis Grounding 4-7
AC Power Supply Tray 4-8

5 Module and Fan Installation

Precautions 5-2
Module Installation Procedures 5-3
Overview 5-4
Tools 5-5
Remove Chassis Covers 5-5
Module Locations 5-6
Installation Sequence 5-8
NIM Installation 5-9
SAM Installation 5-10
CPU Installation 5-10
APM Installation 5-10
NIM IOM Installation 5-11
SAM IOM Installation 5-11
Protection SAM IOM Installation 5-11
CPU IOM Installation 5-12
APM IOM Installation 5-12
Replace Chassis Covers 5-13
Fan Tray Installation Procedure 5-14
Tools 5-15
Remove Front Chassis Cover 5-15
Fan Tray Installation 5-15
Replace Chassis Cover 5-16

6 Electrical Installation

Precautions 6-2
Electrical Requirements 6-3
Tools. 6-3
Power 6-3
Cable Management 6-3
Cabling and Compliance Requirements 6-4
Alarm Port Connections 6-5
Optical Interface Connections. 6-6
BITS Interface Connections 6-7
NIM/SAM IOM Connections 6-8
General Instructions 6-8
Unstructured DS3-3/E3-3 IOM Connections. 6-9
Structured DS3 IOM Connections 6-10
CPU IOM Connections 6-11
Remote Shutdown Connections 6-11
Serial Port Connections 6-11
Ethernet Connections 6-11
Power Supply Connections 6-12
Optional AC Power Supply Connections. 6-12
Broadmore Power Input Connector 6-14
Connecting –48 VDC Power 6-14
Software 6-15

7 Configuration

Overview 7-2
Power-up 7-3
User Interface Requirements 7-4
Screen Display Annotation 7-5
Key Map. 7-6
CAMMI Access 7-7
System Services Configuration 7-8
CAM Name 7-8
Ethernet IP Configuration 7-9
ATM Address. 7-11

ATM Address List (optional) 7-11
Connection Retry 7-13
Retry Cause Codes 7-13
CIP over ATM (RFC 1577) 7-14
Static Routes 7-16
LANE Configuration 7-17
UNI Version 7-19
General Properties. 7-20
User Security Configuration 7-23
Power Supply Redundancy 7-24
Module Redundancy 7-25
Protection Definitions 7-25
NIM Redundancy 7-26
SAM Redundancy. 7-29
CPU Redundancy 7-33
Module Configuration 7-37
How to Configure Specific Modules 7-38
OC-12c/STM-4c 7-39
OC-12c/STM-4c BITS/Timing Redundancy 7-40
Unstructured DS3 SAM 7-43
Structured DS3 SAM 7-50
Unstructured E3-3 SAM 7-57
PVC Connection 7-63
SVC Connection 7-65
VP Reservation 7-67
System Configuration 7-70
Help 7-73

8 Maintenance and Troubleshooting

Statistics 8-2
Chassis Statistics 8-2
OC-12c/STM-4c NIM Statistics 8-3
Alarm Overview 8-4
Slot Statistics for NIM/SAM Cards 8-4
24-Hour Statistics 8-13
PLOA/AAL5 Statistics 8-14
Troubleshooting 8-15
LED Alerts 8-15
Error Codes 8-16
Redundancy 8-16
CPU Sync 8-17
Problem Isolation 8-18
Port Loopback 8-19
Failure Recovery 8-21
Alarm Response/Reset 8-22
Flowchart 8-22
Repair/Replacement 8-30
Power Supply 8-31
NIM Replacement 8-32
SAM Replacement 8-33
IOM Replacement 8-34
CPU Replacement 8-35
CPU IOM Replacement 8-36
Fan Replacement 8-36
Integrated Fan/Alarm Module Replacement 8-37
General Maintenance 8-39
Fan Filter Cleaning and Replacement 8-39
Maintenance/Diagnostics 8-40
Engineering Analysis 8-42
Summary of Front Panel LEDs 8-44

9 Command Line Interface

CLI Access 9-2
Creating and Running Scripts 9-4
Port Configuration 9-6
Monitor. 9-8
About Command 9-9

10 Security Management

Security Features 10-2
Security Guidance 10-3
Logging In 10-5
Log-in Banner 10-6
System Clock 10-7
Network Time Protocol 10-8
Managing Users and Audit Trails 10-10
User ID Rules 10-10
Change User ID 10-11
User Audit Trails 10-13
IP ICMP Messages. 10-17
SNMP Messages 10-18
Shell Commands (Non-FIPS Mode) 10-19
FIPS Mode 10-19
Authorized Access to Shell Commands 10-19
FTP Login 10-21

11 Security Management (FIPS Mode)

Security Features 11-2
Security Guidance 11-3
Authentication and Identification 11-6
Authorized Services 11-7
Key Management 11-8
- Default DSA Key 11-8
- Generating DSA Key Pairs 11-8
- Installing the DSA Key 11-8

Logging In 11-9
- Logging in with SecurID Disabled 11-9
- Logging in with SecurID Enabled 11-11

Log-in Banner 11-13
System Clock 11-14
Network Time Protocol 11-15
Changing Security Modes 11-17
- Help About Security 11-17
- Enabling FIPS Mode 11-18
- Disabling FIPS Mode 11-20
- Enabling SecurID 11-21
- Disabling SecurID 11-24
- IP ICMP Messages 11-24
- SNMP Messages 11-25

User Administration and Audit Trails 11-26
- User ID Rules 11-26
- Change User ID 11-27
- User Audit Trails 11-30

Shell Commands (FIPS Mode) 11-34
- fipsmode 11-34
- selftest 11-34
- settimeout 11-35
- sshdShow 11-35
- sshdSessionShow 11-37
- scp 11-38
- resetSecurID 11-39

zeroize 11-40
Authorized Access to Shell Commands 11-41
SFTP Login 11-43
Logging in with SecurID Disabled 11-43
Logging in with SecurID Enabled 11-46
SecurID Features 11-49
Residual Data and Memory Volatility 11-50
Non-Volatile Memory 11-50
Network Interfaces 11-51
Sanitation Procedures 11-51

12 SNMP Configuration

SNMP Overview 12-2
SNMP Properties 12-3
USM/VACM Configuration 12-6
Users 12-8
Groups 12-13
Views 12-16
Access 12-19
Communities 12-24
Trap Configuration 12-28
Trap Detection Overview 12-28
Trap Management Overview 12-29
Table Usage 12-32
Targets 12-33
Target Parameters 12-35
Notifications 12-37
Notify Filters 12-40
Notify Profiles 12-42

A Technical Specifications

Broadmore 1750 Platform A-2
System Architecture A-2
Management A-2
Network Standards A-3
Redundancy A-3
Alarms A-3
Testing & Diagnostics A-4
Power A-4
Regulatory Approvals A-4
Physical A-5
Environment A-5
Broadmore Modules A-6
OC-12c Network Interface Modules (NIMs) A-6
DS3 (T3) Structured Circuit Emulation SAM A-6
DS3 Unstructured Circuit Emulation SAM A-7
E3 Unstructured Circuit Emulation SAM A-7

B Spare Parts List

C Software Error Messages

Overview C-2
System Errors C-3
Setup Errors C-4

D Sample Network with RFC 1577 Configuration

E Chassis Differences

Broadmore Chassis Differences E-2
Hardware Differences E-2
Software Differences E-3

F IPv6 Support

Overview F-2
Configuring IPv6 Addresses for Network Interfaces. F-2
Adding an IPv6 Address F-2
Displaying an Address F-2
Deleting an IPv6 Address F-3
Pinging over IPv6. . . . . F-4
Pinging an IPv6 Host F-4
Ping the Loopback Interface Address F-4
Testing route6 Application. F-5
Adding an IPv6 Route. F-5
Adding a Host Route. F-5
Adding a Network Route F-5
Showing all IPv6 routes configured in the Broadmore. F-6
Deleting the Default Route F-7
Deleting a Host Route. F-7
Deleting a Network Route F-7

G Broadmore Command List

Commands Available at the Command Prompt. G-2
Commands Available at the CLI Prompt. G-3

Glossary

Acronyms and Abbreviations. Glossary-1
Glossary of Terms Glossary-6

Index

CHAPTER 1

Product Description

In this Chapter

- Purpose ... *1-2*
- Applications ... *1-3*
- Interfaces ... *1-4*
- System Description ... *1-7*
- Module Descriptions ... *1-12*

Purpose

The Broadmore 1750 is an Asynchronous Transfer Mode (ATM) service multiplexer that enables connection of existing and future services through an ATM network. The Broadmore allows users to implement tailored ATM strategies. This modular system has flexible configurations for service access, network interface, and redundancy.

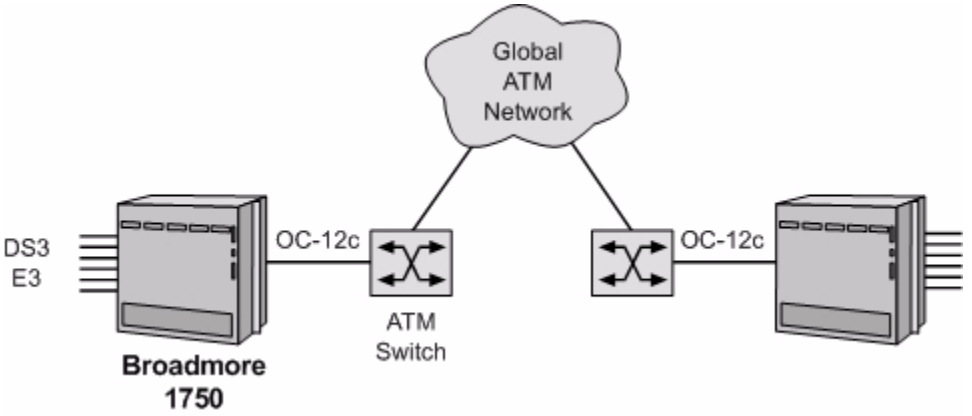
The Broadmore functions as an ATM network service access node that supports the transport of existing broadband services (voice, video, and data) over ATM networks. Typically, it is deployed at the edge of an ATM network as the ATM node element closest to the customer. The Broadmore accepts signals from non-ATM-ready equipment, converts the signals to standard ATM cells, and multiplexes the cells onto a single ATM User Network Interface (UNI) port. The Broadmore accepts constant-bit-rate (CBR) services. Permanent Virtual Circuit (PVC) and Switched Virtual Circuit (SVC) services are available based upon the user-defined module configuration.

The Broadmore now includes FIPS 140-2 validated system management software that meets the security requirements of Federal Information Processing Standard PUB 140-2.



Applications

The Broadmore 1750 is currently deployed in Government and commercial ATM and satellite networks. The Central Office configuration described in this manual has fully redundant network and service interfaces, CPUs, and power supplies. The OC-12c network interface transports a variety of multiplexed TDM services including structured and unstructured DS3, and unstructured E3 services for voice and data communications.



Interfaces

- ATM Interfaces ... *1-4*
- User Equipment Interfaces ... *1-4*
- Management Interfaces ... *1-5*

ATM Interfaces

The Broadmore 1750 supports the following ATM Network Interface Modules (NIMs):

- OC-12c/STM-4c (622 Mbps), singlemode, intermediate reach (IR), SC connectors
- OC-12c/STM-4c (622 Mbps), multimode, premise reach (PR), SC connectors

User Equipment Interfaces

The Broadmore 1750 supports the following network and Service Access Modules (SAMs) to support user data services:

- Unstructured DS3-3 (three ports)
- Unstructured E3-3 (three ports)
- Structured DS3

Management Interfaces

- Security ... *1-5*
- FIPS Interface ... *1-5*
- Physical and Logical Interfaces ... *1-6*
- User Interfaces ... *1-6*
- File Access and Software Upgrades ... *1-6*

Security

The Broadmore is controlled via system management software embedded in the CPU's "flash disk" memory. This software defines the system command structure and provides a user interface for operation and administration. The Broadmore supports multiple user accounts and access levels. There are four levels of user access. Only a network administrator or crypto officer with "SuperUser" access can assign user names, passwords, and access levels.

FIPS Interface

The Broadmore now includes the Broadmore/SSHield Management Module, which is a FIPS 140-2 validated software-only module that meets the security requirements of Federal Information Processing Standard PUB 140-2. The Broadmore can operate in either FIPS mode or non-FIPS mode, depending on the desired level of security. (For a description of the FIPS mode features, see *"Security Management (FIPS Mode)" on page 11-1*.)

NOTE: Enabling FIPS mode security will disable FTP and Telnet access. Users must then log in using secure client replacements such as SecureCRT® and SecureFX®. A secure terminal emulator is required to enter a secure Broadmore system. Although many secure terminal emulators are available, SecureCRT is recommended.

Physical and Logical Interfaces

The CPU is the entry point for both local and remote network management of the Broadmore. The management interface can be reached either in-band or out-of-band via Telnet or SecureCRT. The CPU module provides a serial port (DB9) for local console access and the CPU IOM provides a 10Base-TX Ethernet port for LAN access. Both interfaces provide full support for out-of-band access to all of the Broadmore management interfaces, depending on the user's assigned security level.

The embedded software operating system can be accessed via:

- Craft terminal or PC using the RS-232 serial or modem interface
- IP over ATM protocols: RFC-1577 Classical IP (CLIP) and LAN Emulation Client (LANE) with the Broadmore acting as the LEC
- Telnet or SecureCRT via Ethernet or IP over ATM

User Interfaces

There are two principal user interfaces to the Broadmore system management software:

- Communication Access Multiplexer Management Interface (CAMMI), a quasi-graphical user interface accessible from a serial terminal and by Telnet or SecureCRT over IP.
- Command line interface (CLI) accessible from a serial terminal and by Telnet or SecureCRT over IP.

File Access and Software Upgrades

Data stored on the CPU's flash disk is protected. In FIPS mode, only a SuperUser can access data files or upgrade the system software. In non-FIPS mode, a SuperUser or SysAdmin can transfer files.

System Description

- Features ... *1-7*
- Chassis ... *1-8*
- Fan Tray ... *1-9*
- Power and Redundancy ... *1-9*
- Grounding ... *1-9*
- Alarms ... *1-9*
- Modules ... *1-10*

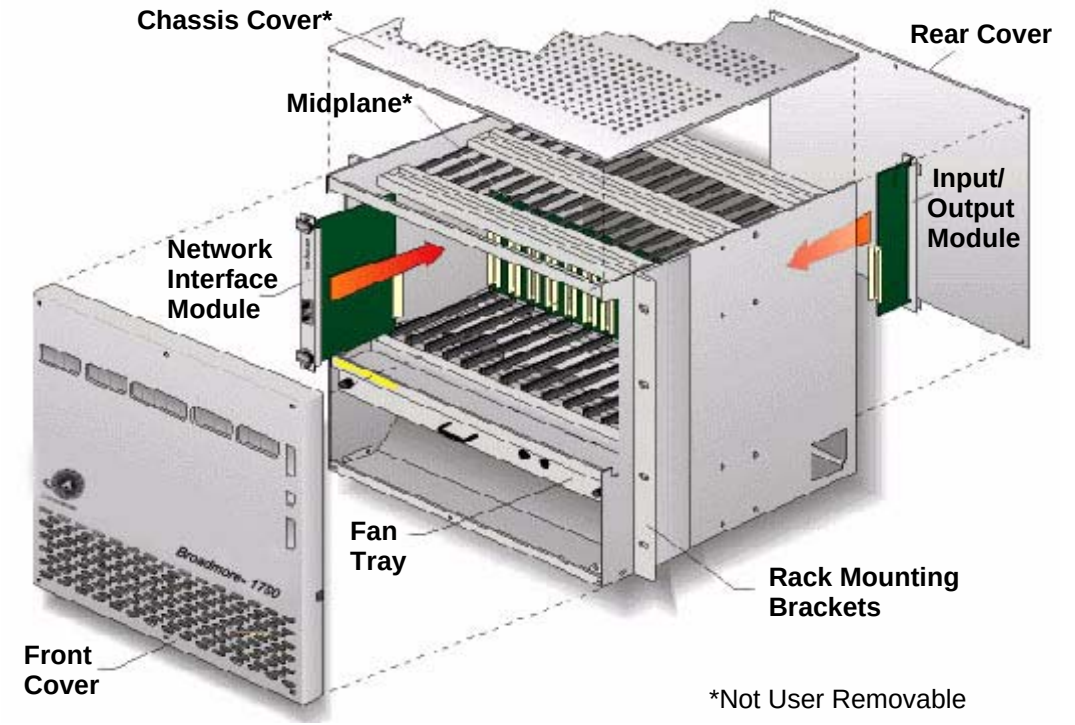
Features

The Broadmore 1750 consists of a chassis and various plug-in modules. This fully integrated system provides the following features:

- Redundant power sources, CPUs, NIMs, and SAMs.
- Front-loadable, hot-swappable modules that allow for single part replacement without affecting other portions of the system.
- Cable separation with user equipment copper/coax interfaces on the chassis rear, and fiber optic ATM interface cables on the chassis front.

Chassis

The Broadmore 1750 chassis can be configured to perform various functions with plug-in modules. The chassis includes a passive midplane, 17 slots for modules, and a fan assembly. The 1750 midplane also supports 1:N SAM redundancy. Attached mounting brackets are configured for standard EIA 19-inch rack installation. These brackets may be rotated 90 degrees for 23-inch relay rack installation. The chassis has removable front and rear covers, which should remain in place during normal operations. These covers should only be removed to provide internal access for installation, maintenance, or system upgrade.



Fan Tray

A removable fan tray, with two fans, is located below the card slots. These fans provide vertical airflow to aid in heat dissipation. The fan tray can be removed for maintenance or replacement without powering down the Broadmore. Empty module slots must be covered by blank panels to maintain proper air flow.

NOTE: Configurations using more than four Structured DS3 SAMs require a high-capacity 3-fan tray for cooling. (Contact factory for details.)

Power and Redundancy

There are two power input connectors, labeled A and B, for receiving –48 VDC at the rear of the chassis. Normally, power is provided directly from the installation facility's –48 VDC source to the connectors at the rear of the chassis. The Broadmore will operate with one power input but connecting an independent power source to the second input will provide redundancy.

A redundant AC power supply tray (P/N 7660-17PS) is available as a separate unit designed to be rack-mounted directly below the Broadmore 1750 chassis. The AC Power Supply supports two non-load-sharing, hot-swappable power supply modules. Each module is capable of supporting a Broadmore 1750 with a fully loaded complement of interface cards. It is recommended that each power supply have its own separate fused outlet for true power redundancy. There is no impact to the Broadmore 1750 as long as one (or both) of the modules is operating normally.

Grounding

Ground lugs at the rear of the chassis allow connection to the building ground system.

A separate ESD ground connection is provided for use with a ground strap when performing maintenance.

Alarms

A four-wire terminal block at the rear of the chassis provides "form C" relay contact closure connections for major and minor alarm signals.

Modules

Broadmore 1750 system architecture is similar to the Broadmore 1700, except that the Broadmore 1750 midplane design also supports 1:N SAM protection using a redundant SAM installed in slot P. Modules are installed from the front and rear of the chassis. There are 17 vertical slots as viewed from the front with the cover removed.

The Broadmore 1750 is generally configured as a fully redundant system with redundant CPUs, redundant OC-12c NIMs, and redundant SAMs, as shown on the next page. Five Unstructured DS3-3 (or E3-3) SAMs provide 1:4 protection for 4 three-modules. Similarly, twelve Structured DS3 SAMs provide 1:11 protection for 11 one-port modules. Other configurations are possible (contact factory for details).

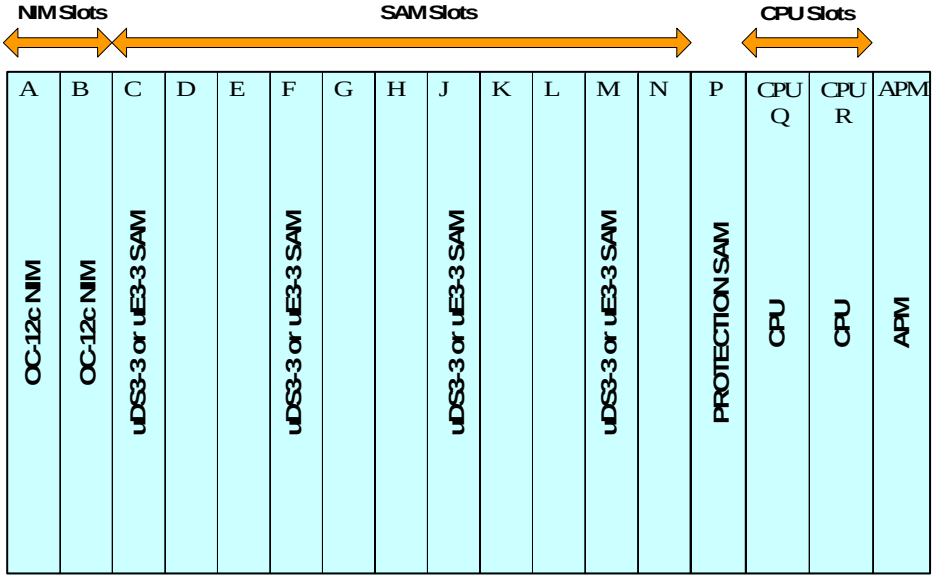
The Broadmore 1750 is shipped in a minimum usable configuration with a factory installed Alarm/Power Module in the right-most slot. Unused slots are covered with blank panels except the slots for a single NIM, SAM, and CPU module.

The Broadmore 1750 chassis can be configured with the following modules.

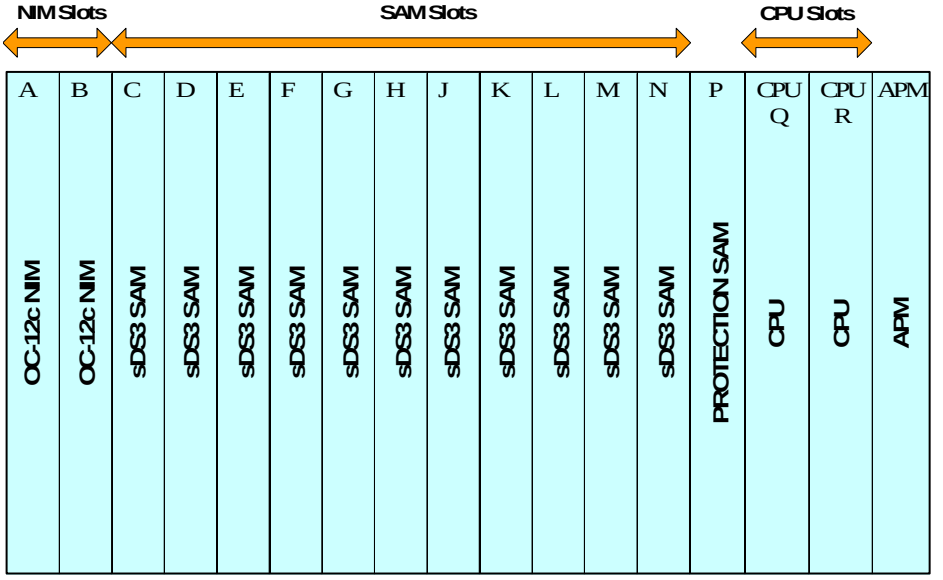
- Network Interface Module (NIM) – 1 or 2 (must be identical)
- Service Access Module (SAM) – 1 to 4 Unstructured DS3-3 or E3-3 SAMs in slots C, F, J, and M; or 1 to 11 Structured DS3 SAMs in slots C to N. (All protected SAMs must be identical.) See figures on next page.
- Protection SAM – 1 SAM in slot P (must be identical to one of the above SAMs)
- Central Processing Unit (CPU) – 1 or 2 (must be identical)
- Alarm/Power Module (APM) – 1 (factory installed)
- Input/Output Module (IOM) – 1 for each NIM, SAM, and CPU (installed in rear panel immediately behind corresponding module in front panel)
- Protection IOM – 1 (installed in rear panel immediately behind Protection SAM)

NOTE: Configurations using more than four Structured DS3 SAMs require a high-capacity 3-fan tray for cooling. (Contact factory for details.)

Example of Fully Redundant Configuration with Unstructured DS3-3 or E3-3 SAMs



Example of Fully Redundant Configuration with Structured DS3 SAMs



Module Descriptions

Network Interface Modules

- OC-12c/STM-4c NIM ... *1-13*
- NIM IOM ... *1-14*

Service Access Modules

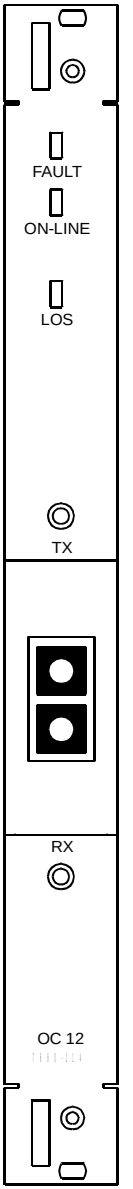
- Unstructured DS3-3 SAM ... *1-15*
- Unstructured E3-3 SAM ... *1-16*
- Unstructured DS3-3/E3-3 IOM ... *1-17*
- Structured DS3 SAM ... *1-18*
- Structured DS3 IOM ... *1-19*
- Protection IOM ... *1-21*

System Modules

- CPU ... *1-22*
- CPU IOM ... *1-23*
- Alarm Power Module (APM) ... *1-24*
- Alarm Power Module IOM ... *1-25*

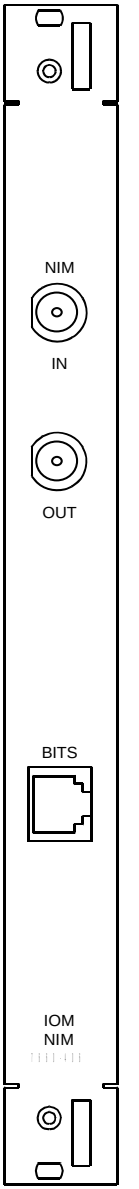
OC-12c/STM-4c NIM

Module Type	NIM
Part Number	7660-113 (Premise Reach, Multi Mode fiber) 7660-114 (Intermediate Reach, Single Mode fiber)
Slot Number	A (Protection), B (Working)
Features	OC-12 (622.080 Mbps) SC fiber optic connectors
Description	The OC-12c/STM-4c NIM is available with either Intermediate Reach or Premise Reach fiber optic terminations. It is compatible with any combination of SAMs installed in the Broadmore 1750 chassis, up to the available bandwidth. Interface from the SAMs to the NIM is accomplished via the chassis midplane. An OC-12c/STM-4c, single mode, Intermediate Reach (IR) module supports ATM physical (PHY) data rates up to OC-12 (622.080 Mbps).
Indicators	FAULT – normal (no fault), major alarm, or minor alarm ON-LINE – normal, standby, or not ready LOS – good RX power, or loss of signal
Connectors	TX and RX fiber interfaces to the ATM network are made via the SC connectors on the NIM, accessed from the front of the chassis.



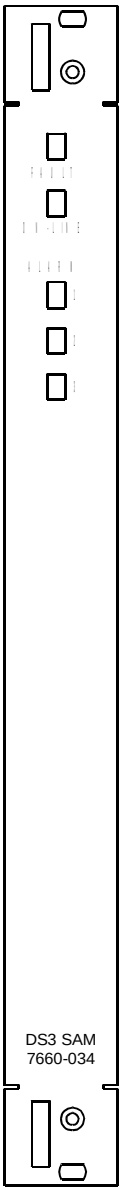
NIM IOM

Module Type	NIM IOM
Part Number	7660-406
Slot Number	Mounts in rear behind corresponding OC-12c/STM-4c NIM
Features	BITS clock input Jumper selectable BITS clock termination impedance
Description	The NIM IOM provides a physical interface to an external clock, giving the option of synchronizing the Broadmore 1750 master clock to an external source. BITS timing is provided to the Broadmore 1750 via the NIM IOM. In a redundant system, BITS clock may be provided to each NIM IOM.
Connectors	NIM IN – BNC connector reserved for future use. NIM OUT – BNC connector reserved for future use. BITS – RJ48C connector for BITS input clock.
Jumpers	BITS impedance matching jumpers located on the component side of the circuit board provide selection of 100 ohms, 75 ohms, or no termination.

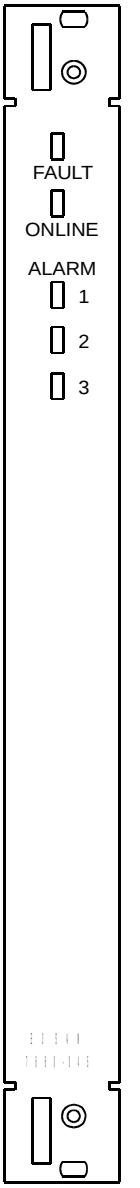


Unstructured DS3-3 SAM

Module Type	SAM
Part Number	7660-034
Slot Number	Working: C, F, J, M Protection: P
Features	Three DS3 port (44.736 Mbps) 622.080 Mbps total ATM bandwidth
Description	The Unstructured DS3 SAM provides three bi-directional ports, each at 44.736 Mbps. Input and output coax connectors are provided for each port on the DS3 IOM. Both PVC and SVC services are provided. Either may be chosen through appropriate module configuration. The Broadmore 1750 supports 11 DS3 ports within the available OC-12 ATM bandwidth of 622.080 Mbps.
Indicators	FAULT – normal (no fault), major alarm, minor alarm, or no connection ONLINE – normal, standby, or not ready ALARM (one LED per port) – normal (enabled), major alarm, minor alarm, or no connection



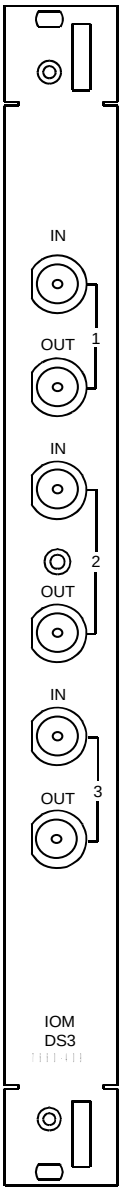
Unstructured E3-3 SAM



Module Type	SAM
Part Number	7660-045
Slot Number	Working: C, F, J, M Protection: P
Features	Three E3 ports (34.368 Mbps)
Description	The Unstructured E3-3 SAM provides three bi-directional ports, each at 34.368 Mbps. Input and output coax connectors are provided for each port on the IOM. Both PVC and SVC services are provided. Either may be chosen through appropriate module configuration. The Broadmore 1750 supports 12 Unstructured E3 ports within the available OC-12 ATM bandwidth of 622.080 Mbps.
Controls	FAULT – normal (no fault), major alarm, minor alarm, or no connection ONLINE – normal, standby, or not ready ALARM (one LED per port) – normal (enabled), major alarm, minor alarm, or no connection

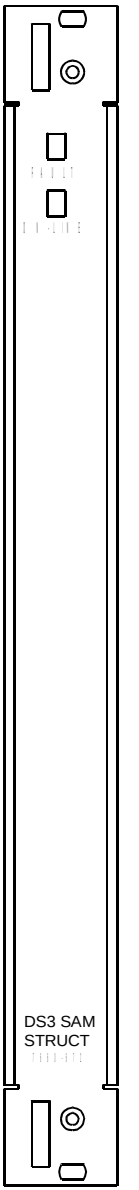
Unstructured DS3-3/E3-3 IOM

Module Type	IOM
Part Number	7660-409
Slot Number	Mounts in chassis rear behind corresponding SAM
Description	Each Unstructured DS3/E3 IOM provides three ports. When used with a DS3 SAM, each port operates at 44.736 Mbps. When used with an E3 SAM, each port operates at 34.368 Mbps.
Connectors	Three pairs of BNC coaxial connectors for RG-59, 75 ohm cable. IN – port receiver RX input OUT – port transmitter TX output



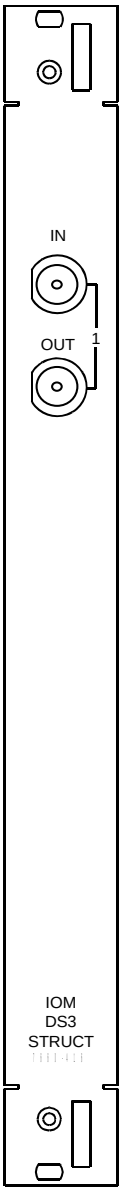
Structured DS3 SAM

Module Type	SAM
Part Number	7660-672
Slot Number	Working: C to N Protection: P
Features	One DS3 port (44.736 Mbps) Logical connections directly to DS1 or DS0
Description	The Structured DS3 SAM provides one bi-directional port at 44.736 Mbps. Input and output coax connectors are provided for the port on the IOM. Both PVC and SVC services are provided. Either may be chosen through appropriate module configuration. The Broadmore 1750 supports a maximum of four Structured DS3 modules with the standard fan tray. Configurations using more than four Structured DS3 SAMs require a high-capacity 3-fan tray for cooling. (Contact factory for details.)
Indicators	FAULT – normal (no fault), major alarm, minor alarm, or no connection ONLINE – normal, standby, or not ready ALARM (one LED per port) – normal (enabled), major alarm, minor alarm, or no connection



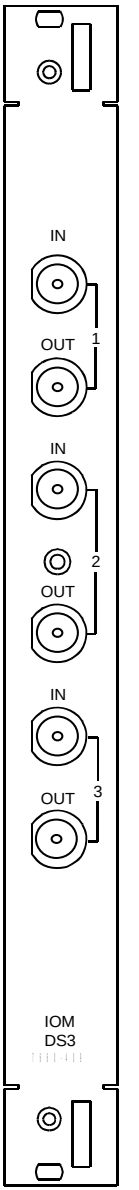
Structured DS3 IOM

Module Type	IOM
Part Number	7660-416
Slot Number	Mounts in chassis rear behind corresponding SAM
Description	One structured DS3 port at 44.736 Mbps.
Connectors	One pair of BNC coaxial connectors. IN – receiver input OUT – transmitter output



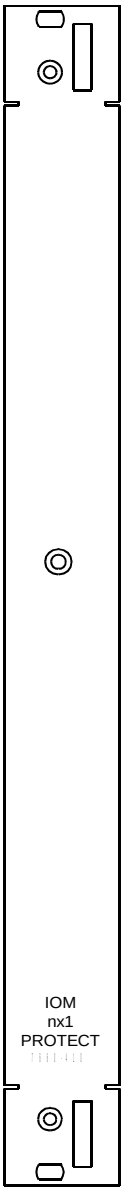
Unstructured DS3-3/E3-3 IOM

Module Type	IOM
Part Number	7660-409
Slot Number	Mounts in chassis rear behind corresponding SAM
Description	Each Unstructured DS3/E3 IOM provides three ports. When used with a DS3 SAM, each port operates at 44.736 Mbps. When used with an E3 SAM, each port operates at 34.368 Mbps.
Connectors	Three pairs of BNC coaxial connectors for RG-59, 75 ohm cable. IN – port receiver RX input OUT – port transmitter TX output



Protection IOM

Module Type	IOM
Part Number	7660-410
Slot Number	Mounts in Broadmore 1750 chassis rear behind corresponding protection SAM in slot P.
Description	Provides n×1 circuit switching for the protection SAM in slot P.
Connectors	None. Inputs and Outputs continue to be provided by the connectors on the failed SAM's IOM.

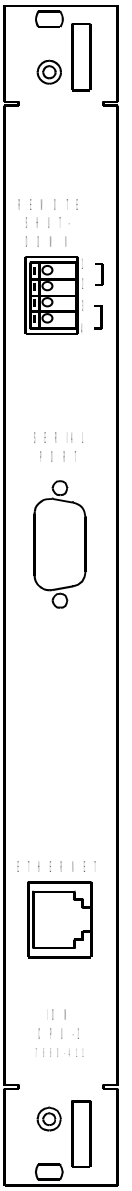


CPU

Module Type	CPU
Part Number	7660-204
Slot Number	CPU Q (primary), CPU R (redundant)
Description	The CPU module provides the facilities for all system monitoring, reporting, logging, and management. The CPU also performs Segmentation and Reassembly (SAR) for all in-band network management over the ATM network. The CPU stores the FIPS-2 validated Broadmore/SSHield management software on a “flash disk” system. The operating system is pSOS version 2.2.7.
Controls	Toggle switch ON – normal operation OFF – turns CPU off RESET – resets the CPU
Indicators	MASTER – lights green when operating as master; lights amber when operating as standby. (Normally, the CPU that comes online first will be the master.) ON-LINE ACTIVITY – blinks amber to indicate CPU activity including master/standby mirroring.
Connectors	SERIAL – DB9 RS-232 DTE serial management port (Ethernet management port is on CPU IOM)



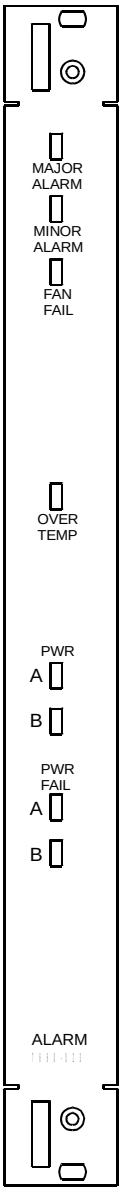
CPU IOM



Module Type	IOM
Part Number	7660-411
Slot Number	Mounts in chassis rear behind corresponding CPU
Description	The CPU IOM provides physical access to the system for Ethernet and also provides the remote shutdown interface as explained below.
Controls	REMOTE SHUT-DOWN – Spring terminal block for installing cables for remote CPU shut-down. A remote contact closure is used to short pins 1-2 or pins 3-4. Jumpers control how these contact closures work.
Jumpers	REMOTE SHUT-DOWN – Two user-installed jumpers on the component side of the module control how the remote contact closures work. As shipped, the jumpers connect pins 1-2 to pins 3-4 so that shorting either pair will reboot both CPUs. With the jumpers removed, shorting pins 1-2 will reboot the other-slot CPU; shorting pins 3-4 will reboot the same-slot CPU. It is recommended that the jumpers be removed.
Connectors	SERIAL – reserved for future use. ETHERNET – RJ48 modular connector.

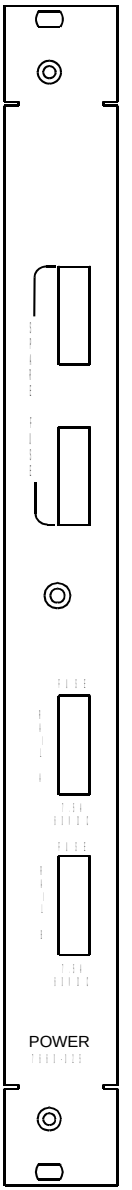
Alarm Power Module (APM)

Module Type	APM
Part Number	7660-023
Slot Number	APM
Description	An APM is factory-installed in the right-most card slot as viewed from the front. The APM provides EMI power conditioning and over-current protection for each of the two –48 VDC power sources. Two 7.5 amp, 60 VDC fuses are located on the bottom of the module. A green LED is provided for each power source to indicate power is present. Major and minor alarms are displayed via LEDs, which are visible with the front panel installed. An over-temperature indicator on the front of this module is reserved for future use. The APM is user-replaceable.
Indicators	MAJOR ALARM – lights red for major alarm MINOR ALARM – lights amber for minor alarm FAN FAIL – lights red when fan tray fails OVER TEMP – (reserved for future use) PWR A/B – lights green when power is applied to the A or B inputs PWR FAIL A/B – lights red when power supply A or B fails



Alarm Power Module IOM

Module Type	IOM
Part Number	7660-025
Slot Number	Mounts in chassis rear behind APM
Description	The Alarm Power IOM comes with four Bussman GMT 7.5A, 60V fuses. Two of the fuses are used to protect the redundant DC power inputs (A and B) and the other two fuses are provided as spares. The chassis will operate with only one power source but two independent sources are recommended to provide power supply redundancy. Power, alarm, and grounding connections are made to the connector panel at the bottom rear of the chassis.
Fuses	RAIL A – protection fuse for –48VDC power input A RAIL B – protection fuse for –48VDC power input B SPARE FUSES – two spare fuses in holders



CHAPTER 2

Planning and Ordering Guide

In this Chapter

- Application Planning Guide ... *2-2*
- System Planning Factors ... *2-6*
- Installation Planning Factors ... *2-13*
- Ordering Guide ... *2-15*

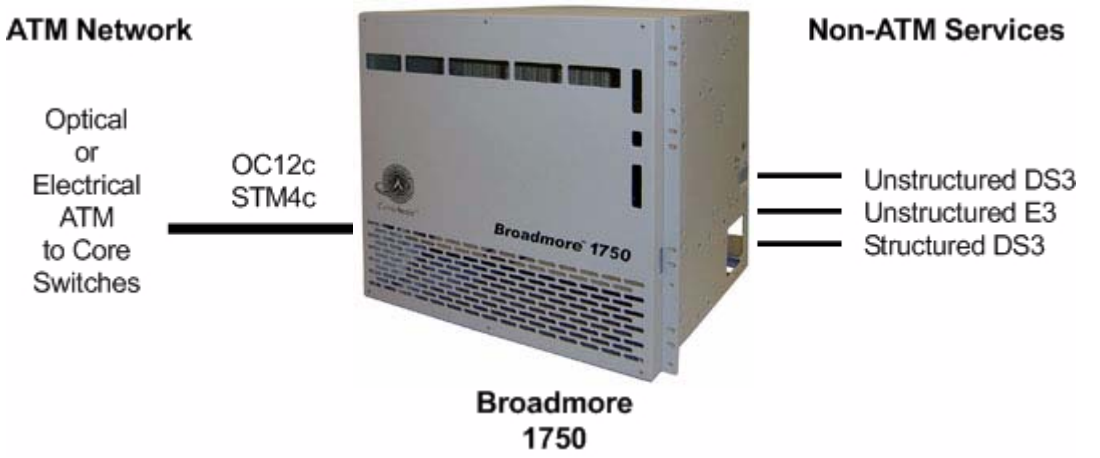
Application Planning Guide

- Basic Features ... *2-2*
- TDM Circuit Aggregation and Backhaul ... *2-3*
- Mission-Critical Circuit Resiliency ... *2-4*

Basic Features

The Broadmore is designed as an ATM network service access node that supports the transport of existing broadband services (voice, video, and data) over ATM networks. The Broadmore accepts signals from non-ATM-ready equipment, converts the signals to standard ATM cells, and multiplexes the cells onto a single ATM User Network Interface (UNI) port. Permanent Virtual Circuit (PVC) and Switched Virtual Circuit (SVC) services are available based upon the user-defined module configuration.

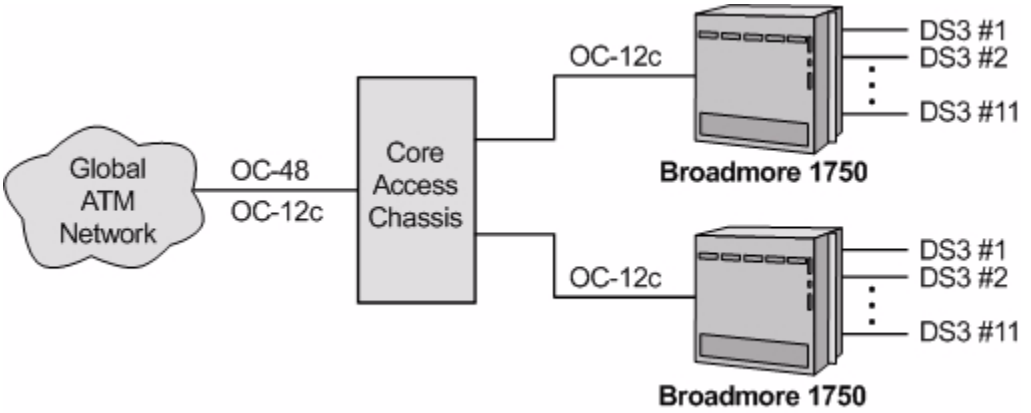
The Broadmore accepts a variety of constant bit rate (CBR) services including structured DS3 and unstructured DS3 and E3.



TDM Circuit Aggregation and Backhaul

The Broadmore 1750 provides:

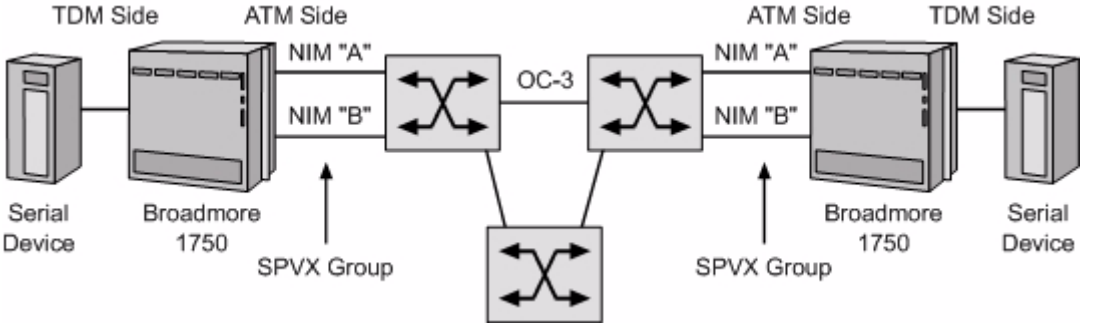
- Massive DS3 trunking
  - – Remote shelf extension to the ATM network
- Reduced costs, increased access
  - – Up to 11 DS3s per ATM Switch interface (versus the usual 4)
- Edge cross-connect capability
  - – User connections switched directly
  - – Central terminations are not required (as with DACS)



Mission-Critical Circuit Resiliency

The Broadmore 1750 provides:

- Carrier-class equipment features including fully redundant, hot-swappable components
- Automatic Protection Switching (APS)
  – Circuit, source, and destination device protection
- Distributed Protection Switching (DPS)
  – Circuit, source, destination device, edge node, and CPE protection
  – Logical and physical redundancy between the switch and access shelf
  – Unprecedented SLA delivery for TDM and Serial link
  – Maximum network availability
  – APS functionality through ATM technology
  – Guaranteed interoperability
  – Simple configuration



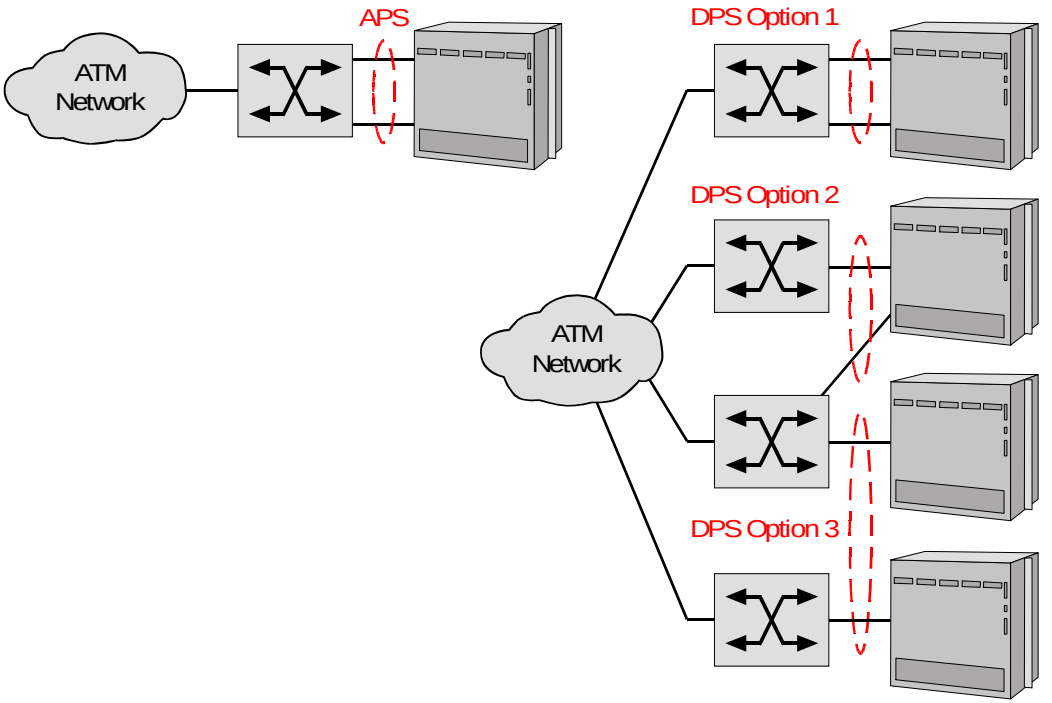
APS Features and Benefits

- Two ports are grouped as primary and secondary SPVC ports (see figure below). Provides access link, core, and port redundancy for source and/or destination devices.

DPS Features and Benefits

- SPVx Redundancy Group (Option 1) – Two ports are grouped as primary and secondary SPVC ports. Provides access link, core, and port redundancy for source and/or destination devices.
- SPVx Source Resiliency (Option 2) – SPVC connection between source switches monitors status of active switch. Once failure is identified, initiates fail-over to backup.
- SPVx Destination Resiliency (Option 3) – Full redundancy for the destination device, port, destination switch, access link, and core. Primary and backup destinations can be geographically separate.

APS and DPS Features



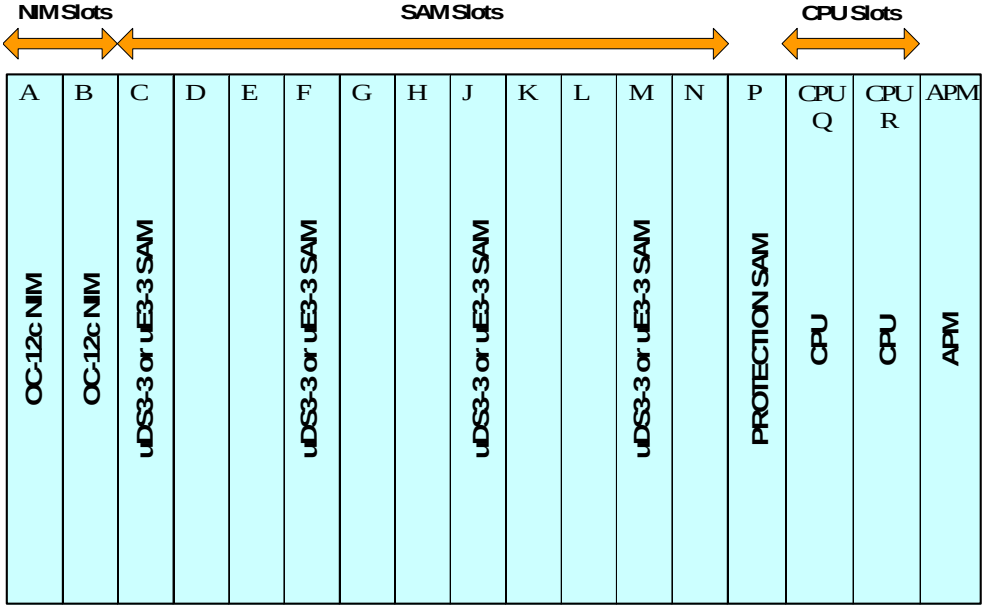
System Planning Factors

- System Architecture ... *2-6*
- Cell Bus Configuration ... *2-8*
- Unstructured DS3-3/E3-3 Configuration Guidelines ... *2-9*
- ATM Bandwidth per Cell Bus ... *2-11*
- ATM Bandwidth per Module ... *2-12*
- ATM Network Loading ... *2-12*

The Broadmore 1750 is a customizable system. The following factors should be considered when planning and configuring a system to meet customer requirements.

System Architecture

The Broadmore 1750 system architecture is based upon a midplane design allowing modules to be installed from the front and rear of the chassis. There are 17 vertical slots as viewed from the front with the cover removed. The figure shown below shows a fully redundant system configured with OC-12c NIMs and Unstructured DS3 SAMs.



The Broadmore 1750 is shipped in a minimum usable configuration with a factory installed Alarm/Power Module in the right-most slot. Unused slots are covered with blank panels except the slots for installing a single NIM, SAM, and CPU module.

The Broadmore 1750 chassis can be configured with the following modules:

- Network Interface Module (NIM) – 1 or 2 (must be identical)
- Service Access Module (SAM) – 1 or more
- Central Processing Unit (CPU) – 1 or 2 (must be identical)
- Alarm/Power Module (APM) – 1 (factory installed)
- Input/Output Module (IOM) – 1 for each NIM, SAM, and CPU (installed in rear panel immediately behind corresponding module in front panel)

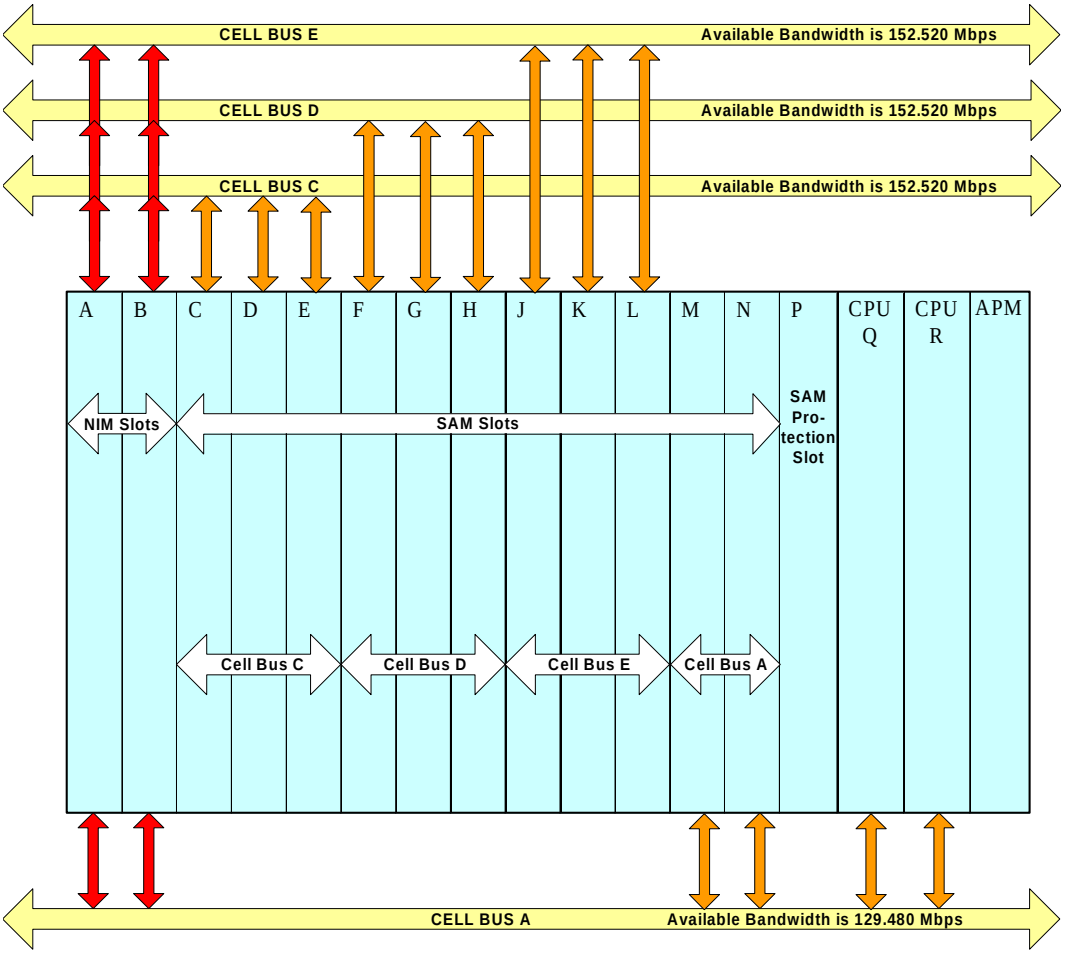
Module slots are populated as follows:

- The right-most slot, labeled “APM”, is for the Alarm/Power Module.
- The two left-most slots, labeled “A” and “B”, support Network Interface Modules (NIMs). The protection NIM goes in slot “A” and the working protection NIM in slot “B”. If the system is not configured for NIM redundancy, the single NIM should be inserted in slot “B”.
- The two slots closest to the APM slot, labeled “CPU Q” and “CPU R”, support the CPU modules. Either CPU can operate as the master or redundant protection unit. If the system is not configured for CPU redundancy, the single CPU can be inserted in either slot.
- Slots “C” through “N” are for Service Access Modules (SAMs). SAMs should be installed from left to right, so that they will be close to the NIMs.
- Slots “P” if for the Protection SAM.
- Input/Output Modules (IOMs) install from the rear of the chassis, directly behind the corresponding front panel modules.

NOTE: For recommended SAM locations, see the following configuration guidelines.

Cell Bus Configuration

The Broadmore multiplexes user data onto ATM cell buses. Depending on the installed NIM and SAMs, there can be up to four cell buses, designated A, C, D, and E. Each cell bus is associated with specific module slots, as shown below.

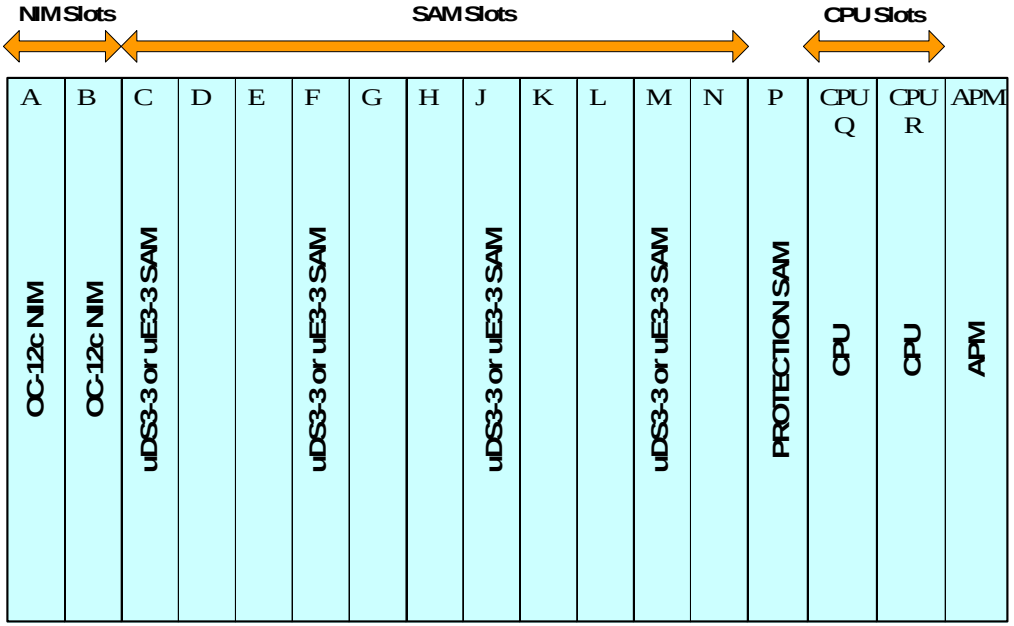


Unstructured DS3-3/E3-3 Configuration Guidelines

A Broadmore 1750 with OC-12c NIM can utilize Cell Buses A, C, D, and E and support up to 11 unstructured DS3 or 12 unstructured E3 ports within the available OC-12 ATM bandwidth of 622.080 Mbps.

Because each unstructured DS3-3 and E3-3 SAM has three ports, only one SAM is needed for each cell bus. However, to utilize the 1:N SAM protection feature, all SAMs must be identical and be installed in specific slots.

- For NIM redundancy, install OC-12c NIMs in slots A and B
- If a single OC-12c NIM is used, it should be installed in slot B
- Working SAMs must be installed in slots C, F, J, and M, corresponding to cell buses C, D, E, and A, respectively
- The Protection SAM is installed in slot P

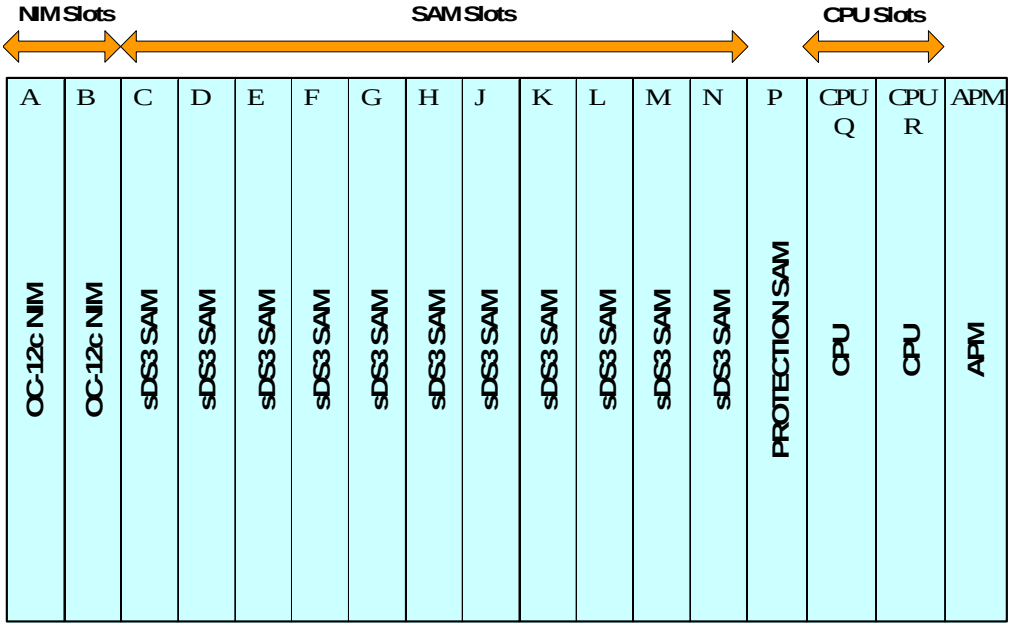


Structured DS3 Configuration Guidelines

A Broadmore 1750 with OC-12c NIM can utilize Cell Buses A, C, D, and E and support up to 11 Structured DS3 ports within the available OC-12 ATM bandwidth of 622.080 Mbps.

- For NIM redundancy, install OC-12c NIMs in slots A and B
- If a single OC-12c NIM is used, it should be installed in slot B
- To utilize the 1:N SAM protection feature, working SAMs are installed in slots C to N and the protection SAM is installed in slot P

NOTE: Configurations using more than four Structured DS3 SAMs require a high-capacity 3-fan tray for cooling. (Contact factory for details.)



ATM Bandwidth per Cell Bus

Depending on the SAMs being used, a Broadmore 1750 chassis with an OC-12c NIM can multiplex data onto all four ATM cell buses, providing a maximum ATM bandwidth of up to 599.04 Mbps.

The maximum ATM bandwidth for each cell bus is shown below.

Cell Bus	Service Slots	ATM Bandwidth Available to SAMs
A	C thru N (used by SAMs) Q, R (used by CPUs for AAL5 management traffic)	< 129.48 Mbps
C	C, D, E	< 155.52 Mbps
D	F, G, H	< 155.52 Mbps
E	J, K, L	< 155.52 Mbps
Total	All service slots	< 599.04 Mbps

ATM Bandwidth per Module

The CPU and each SAM uses a specific amount of ATM bandwidth, as shown below.

Module P/N	Module Description	ATM Bandwidth Required (Mbps)
7660-206	CPU, FIPS, 10Base-T, AAL5	Average: < 2.5 Mbps Maximum: 4.0 Mbps
7660-034	DS3, Unstructured, 3 port	Whole DS3: 50.45 Mbps Maximum: 151.35 Mbps (all ports in service)
7660-045	E3, Unstructured, 3 port	Each port: 39.21 Mbps Maximum: 117.62 Mbps (all ports in service)
7660-672	DS3, Structured, 1 port	Whole DS3: 50.45 Mbps

ATM Network Loading

The Broadmore 1750 multiplexes cells from various input SAMs into a single ATM UNI signal that is delivered to the ATM network. There is overhead associated with this process that reduces the total bandwidth available to the connected service equipment. The Broadmore 1750 can load the network UNI to 95% capacity without dropping cells. Service capacities are shown in the following table.

ATM Service Capacity

Module	Cell Bus	ATM Network Rate (Mbps)	ATM Service Capacity (Mbps)
OC-12c/STM-1c	A C D E Total	155.520 155.520 155.520 155.520 622.080	149.760 149.760 149.760 149.760 599.040

Installation Planning Factors

The Broadmore 1750 is designed and delivered ready for installation in a standard 19" or 23" relay or EIA equipment rack. Several factors should be considered and some decisions made to ensure a smooth installation that meets all requirements. Installation factors and system specifications are shown in the following tables.

Factor	Consideration
Access Clearance	Broadmore 1750 requires the following access clearances for service and maintenance: • Front: 24″ • Rear: 4″ • Top: 1.75″ (Broadmore 1750 units may be stacked without this clearance.)
Power Source	DC Power: –48 VDC at 5 amperes is connected to the rear of the Broadmore chassis. A second –48 VDC source may be connected for redundancy. Optional AC Power Supply Tray: Converts 110/240 VAC (50-60 Hz) to –48 VDC. Rack mounted tray (3.5″ high) installs immediately below Broadmore chassis and can hold two power supplies. Unit comes with one power supply and cables. A second power supply with cables can be added to provide redundant DC power to the Broadmore. AC and DC power connections are at the rear of the unit. The DC cable is approximately 3.5 ft. long.

Cable Management	Overall cable lengths can be optimized by equipment placement. • User equipment interface cable connections are made to the input/output modules at the rear of Broadmore chassis. • ATM interface connections is via fiber cable to the network interface modules at the front of Broadmore chassis. • Access and cable strain-relief tie-down points are provided. • Chassis front and rear cover removal is required.

Ordering Guide

- Contact Information ... *2-15*
- Broadmore 1750 Chassis ... *2-15*
- Broadmore 1750 Options and Spares ... *2-16*
- Network Interface Module (NIM) Options ... *2-17*
- Service Access Module (SAM) Options ... *2-18*

Contact Information

Inside Sales Direct: 800-365-2593
Fax: 303-218-5680
E-mail: inside-sales@carrieraccess.com
Products and Solutions: www.carrieraccess.com

Broadmore 1750 Chassis

Each Broadmore 1750 chassis comes equipped with one CPU and IOM, one APM and IOM, Dual –48VDC Power Inputs, and a Fan Tray. The following items are also included: CD-ROM with Users Guide and Software, Grounding Strap, Console Cable, Combination 19”/23” Rack Mount, and one year warranty.

Item	Part No.
Broadmore 1750 Chassis, –48 VDC	7665-1750

Broadmore 1750 Options and Spares

The following items are optional and are not required for basic operation. They can be included to enhance network availability or utilized as spares.

Item	Part No.
Broadmore 1750 –48 VDC Chassis (with APM and IOM only)	7665-17B
Broadmore 1700/1750 AC Power Tray Converts voltage from 110/220 VAC (50-60 Hz) to –48 VDC. Includes one 240W AC Power Supply, one additional slot for a Redundant 240W AC Power Supply, one 48 VDC Inverter, and one Cable to connect to the Broadmore's –48 VDC Power Input.	7665-17PS
Broadmore 1700/1750 AC Power Supply This is the 240W AC Power Supply used for redundancy in the Broadmore 1700/1750 AC Power Tray.	7660-115
Alarm & Power Module (APM)	7660-023
Alarm & Power I/O Module (APM IOM)	7660-025
Bussman 7.5 Amp Fuse	GMT7.5
Bussman Fuse Cover	GMT-X
Broadmore 1700/1750 Fan Tray	7660-024
Globe Motors Fan Filter	FFM745
Broadmore CPU Module with FIPS 140-2 validated Operating Software	7660-206
Broadmore CPU I/O Module (CPU IOM)	7660-411
CPU Disk-On-Chip Flash Module	750-0044
CPU-2 replacement battery. Panasonic VL1220-1HF, or equivalent	034-0016
LapLink Cable, PC to Broadmore 1700 serial port cable with DB9-F and DB25-F connectors on both ends	51670066-01

Network Interface Module (NIM) Options

- NIM Sets ... *2-17*
- Individual Modules ... *2-17*

The Broadmore 1750 chassis has two NIM slots available for redundancy. Both NIMs must be identical in redundant installations.

NIM Sets

Each set includes the NIM, IOM, and cable option where applicable.

Optical Service Sets	Part No.
OC-12c/STM-4c Single Mode Intermediate Reach Optics (SC) Module Set	7660-314
OC-12c/STM-4c Multi-Mode Optics (SC) Module Set	7660-313

Individual Modules

Each NIM and corresponding IOM is offered separately for sparing purposes.

Optical Service Modules	Part No.
OC-12c/STM-4c NIM, Single Mode Intermediate Reach Optics (SC)	7660-114
OC-12c/STM-4c NIM, Multi-Mode Optics (SC)	7660-113

Service Access Module (SAM) Options

- SAM Sets ... *2-18*
- Individual Modules ... *2-18*

The Broadmore 1750 chassis has 12 SAM slots available for user connectivity.

SAM Sets

Each set includes the SAM and corresponding IOM.

TDM Service Sets	Part No.
DS3 Structured Single Port Module Set	7660-372
DS3 Unstructured Three Port Module Set	7660-334
E3 Unstructured Three Port Module Set	7660-345

Individual Modules

Each SAM and IOM is offered separately for sparing purposes.

TDM Service Modules	Part No.
DS3 Structured Single Port SAM	7660-672
DS3 Structured Single Port IOM	7660-416
DS3 Unstructured Three Port SAM	7660-034
E3 Unstructured Three Port SAM	7660-045
DS3/E3 Unstructured Three Port IOM	7660-409
Protection IOM, 1:N	7660-410

CHAPTER 3

Receipt of Product

In this Chapter

- Receipt ... *3-2*
- Unpacking ... *3-2*
- Inspection ... *3-3*

Receipt

All Broadmore components with FIPS 140-2 validated software are packaged and sealed at the factory with tamper-proof security tape.

Upon receipt, carefully examine the security sealing tapes on the shipping containers for any signs of tampering.

NOTE: Report any tampering to your security officer.

Inventory all material upon receipt to ensure that a complete shipment was received in accordance with the packing list.

NOTE: Report any damage sustained during shipment of equipment to the transporter immediately upon receipt.

Unpacking

The Broadmore 1750 chassis is shipped with the Alarm/Power module and fan tray installed. Additional modules ordered by the customer will normally be installed in the chassis prior to shipping. When requested, modules can be individually boxed, identified, and shipped separately in a second container.

WARNING! THE BROADMORE 1750 CHASSIS WEIGHS APPROXIMATELY 31 POUNDS WITHOUT MODULES INSTALLED. USE CARE IN REMOVING AND LIFTING THE CHASSIS FROM THE SHIPPING CONTAINER TO AVOID EQUIPMENT DAMAGE.

The chassis container will include an accessory kit with the following materials:

- users documentation on CD
- ground strap
- accessory cables
- miscellaneous hardware

Inspection

Perform a visual inspection of all components for obvious damage or irregularities. Pay special attention to the connectors, indicators, and switches on the individual circuit cards. Follow ESD procedures when removing cards from protective bags for this inspection. Carefully return the cards to their bags for storage until installation.

WARNING! SOME BROADMORE 1750 CIRCUIT BOARDS ARE ESD-SENSITIVE. THESE ASSEMBLIES ARE IN INDIVIDUAL STATIC DISSIPATIVE BAGS WITH AN ESD CAUTION LABEL ATTACHED. EMPLOY STANDARD ESD HANDLING PROCEDURES, INCLUDING USE OF A PROPERLY GROUNDED ESD WRIST STRAP BEFORE OPENING OR HANDLING THESE ITEMS. ONLY OPEN THESE BAGS AT AN APPROVED ESD WORKSTATION. CAREFULLY RETURN THE CARDS TO THEIR BAGS FOR STORAGE UNTIL INSTALLATION. FAILURE TO FOLLOW THESE PROCEDURES WILL VOID THE WARRANTY AND MAY RESULT IN COMPONENT DAMAGE.

Damage Reporting

Compare the contents of the shipping containers with the packing list provided. Immediately report any inconsistencies to Carrier Access at (800) 786-9929. The Customer Support Center will provide detailed instructions to resolve any issue or concern.

CHAPTER 4

Chassis Installation and Grounding

In this Chapter

- Precautions ... *4-2*
- Installation Factors ... *4-3*
- Rack Mounting ... *4-4*
- Chassis Grounding ... *4-7*
- AC Power Supply Tray ... *4-8*

Precautions

DANGER! EXERCISE NORMAL PRECAUTIONS FOR LIFTING HEAVY OBJECTS. USE TWO PEOPLE TO LIFT THE BROADMORE 1750. WHEN LIFTING, SUPPORT IT FROM THE BOTTOM AND TAKE CARE TO AVOID SHARP EDGES OR CORNERS.

WARNING! THE FRONT AND REAR COVERS OF THE CHASSIS MUST REMAIN IN PLACE DURING RACK-MOUNTING. THESE COVERS SHOULD ONLY BE REMOVED FOR MODULE INSTALLATION AND MAINTENANCE AS REQUIRED. THE COVERS SHOULD BE REPLACED AS SOON AS POSSIBLE AFTER SUCH TASKS ARE COMPLETED.

WARNING! THE BROADMORE 1750 MOUNTING BRACKETS SHALL BE CONNECTED TO THE CHASSIS USING ONLY THE SCREWS PROVIDED FOR INITIAL BRACKET INSTALLATION. THE INSTALLER SHALL BE RESPONSIBLE FOR PROVIDING A STABLE RACK THAT SUPPORTS THE WEIGHT OF THE BROADMORE 1750 AS INSTALLED.

WARNING! THE INSTALLER SHALL BE RESPONSIBLE FOR PROVIDING A PROPER CHASSIS GROUND CONNECTION.

Installation Factors

The Broadmore 1750 is designed and delivered ready for installation in a standard EIA 19" equipment rack. The mounting brackets can be repositioned for installation in a 23" rack. To ensure a smooth installation that meets all requirements, the following installation factors should be considered.

Factor	Consideration
Access Clearance	Broadmore 1750 requires the following access clearances for service and maintenance: • Front: 24″ • Rear: 4″ • Top: 1.75″ (Broadmore 1750 units may be stacked without this clearance.)
Power Source	DC Power: –48 VDC at 5 amperes is connected to the rear of the Broadmore chassis. A second –48 VDC source may be connected for redundancy. Optional AC Power Supply Tray: Converts 110/240 VAC (50-60 Hz) to –48 VDC. Rack mounted tray (3.5″ high) can hold two power supplies. Unit comes with one power supply and DC cable. A second power supply with cable can be added to provide redundant DC power to the Broadmore. AC and DC power connections are at the rear of the unit. The DC cable is approximately 3.5 ft. long.
Cable Management	Overall cable lengths can be optimized by equipment placement. • User equipment interface cable connections are made to the input/output modules at the rear of Broadmore chassis. • ATM interface connections is via fiber cable to the network interface modules at the front of Broadmore chassis. • Access and cable strain-relief tie-down points are provided. • Chassis front and rear cover removal is required.

Rack Mounting

- Tools ... *4-4*
- Mounting Brackets ... *4-5*
- Rack Mounting Procedure ... *4-6*

Tools

The following tools are recommended to install, configure, operate, and maintain the Broadmore 1750:

- #1 flathead screwdriver (for cover removal/installation)
- ¼-inch hex driver
- Rack-mounting hardware with compatible tools
- Other standard electronic installation tools as preferred

Mounting Brackets

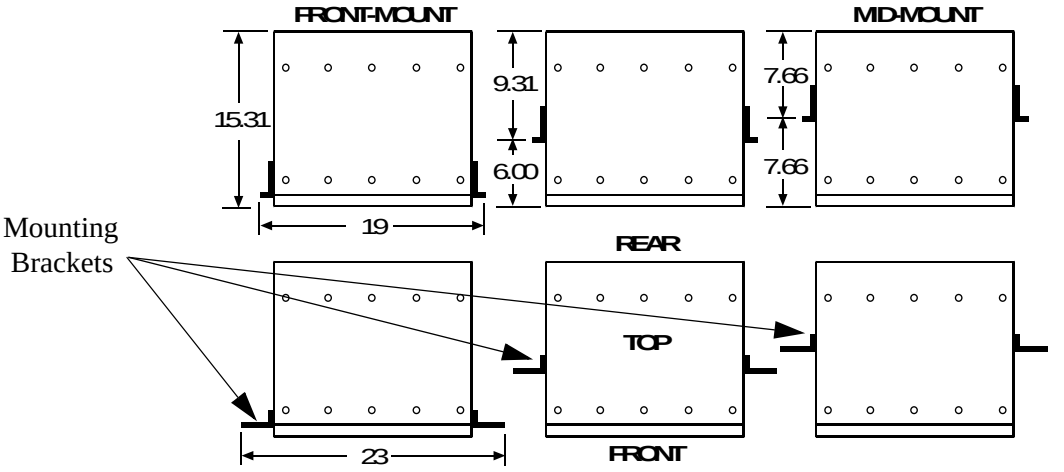
The Broadmore 1750 chassis 17.5" high and is shipped from the factory assembled for front-mounting in a standard 19" EIA or relay rack.

WARNING! THE BROADMORE 1750 MOUNTING BRACKETS SHALL BE CONNECTED TO THE CHASSIS USING ONLY THE SCREWS PROVIDED FOR INITIAL BRACKET INSTALLATION. THE INSTALLER SHALL BE RESPONSIBLE FOR PROVIDING A STABLE RACK THAT SUPPORTS THE WEIGHT OF THE BROADMORE 1750 AS INSTALLED.

The mounting brackets can be moved to accommodate 23" racks and other mounting positions. To install the chassis in 23" racks, remove the mounting brackets, rotate them 90 degrees, and reattach them to the chassis.

If desired, alternate mounting holes are provided for moving the mounting brackets forward or backward for other mounting configurations.

The six possible rack-mounting bracket configurations are shown below.



Rack Mounting Procedure

Rack-mounting the Broadmore 1750 chassis requires:

- two technicians
- clear access to front and rear of rack
- user-provided rack mounting hardware (screws)

DANGER! **EXERCISE NORMAL PRECAUTIONS FOR LIFTING HEAVY OBJECTS. USE TWO PEOPLE TO LIFT THE BROADMORE 1750. WHEN LIFTING, SUPPORT IT FROM THE BOTTOM AND TAKE CARE TO AVOID SHARP EDGES OR CORNERS.**

WARNING! **THE FRONT AND REAR COVERS OF THE CHASSIS MUST REMAIN ATTACHED TO PREVENT THE CHASSIS FROM BENDING DURING THE RACK-MOUNTING PROCEDURE.**

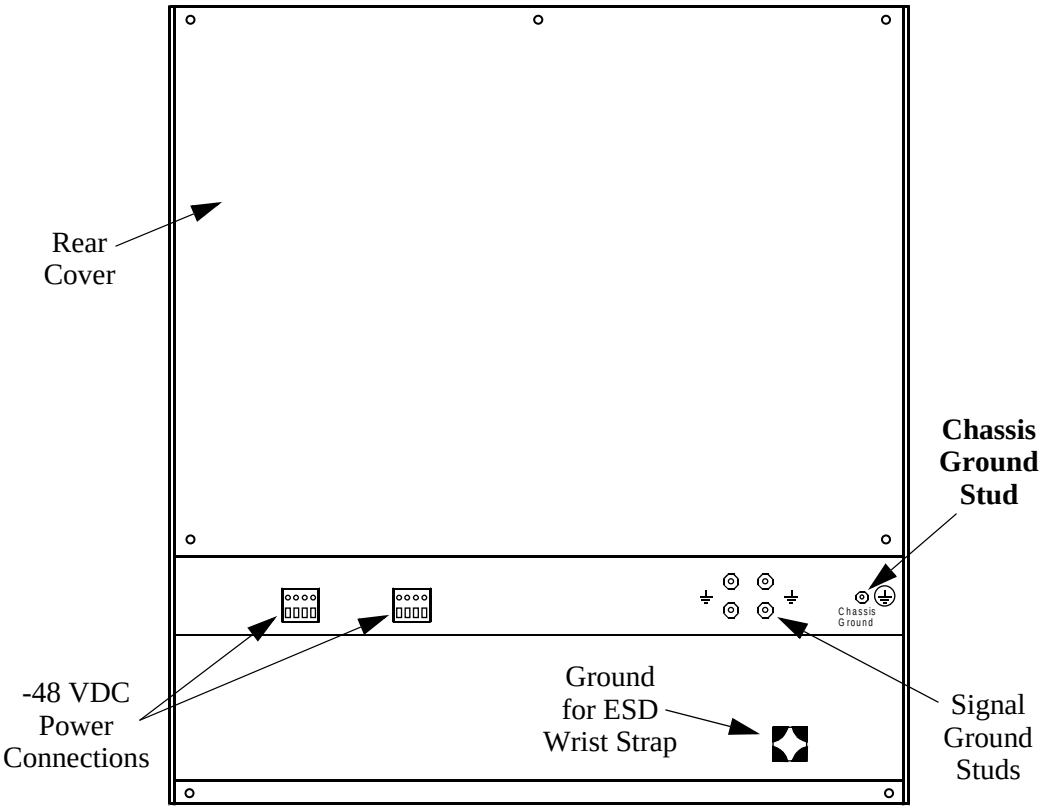
Perform the following steps:

1. Ensure that the front and rear chassis covers are firmly attached to provide mechanical support and prevent accidental damage.
2. Carefully lift the Broadmore 1750 and position it in the desired rack location. One technician should support the rear and the second should support the front.
3. Ensure that there is a 1.75 inch space above the chassis for adequate air flow.
4. Insert screws through the chassis and rack mounting holes. Every bracket hole must have a screw securely installed to ensure proper weight distribution and support.

Chassis Grounding

The Broadmore 1750 chassis has a chassis ground stud on the rear panel for connecting a ground wire to the equipment rack building ground.

WARNING! **THE INSTALLER SHALL BE RESPONSIBLE FOR PROVIDING A PROPER CHASSIS GROUND CONNECTION. CONNECT BUILDING GROUND TO THE CHASSIS GROUND STUD. DO NOT USE THE SIGNAL GROUNDING STUDS FOR THE BUILDING GROUND CONNECTION.**

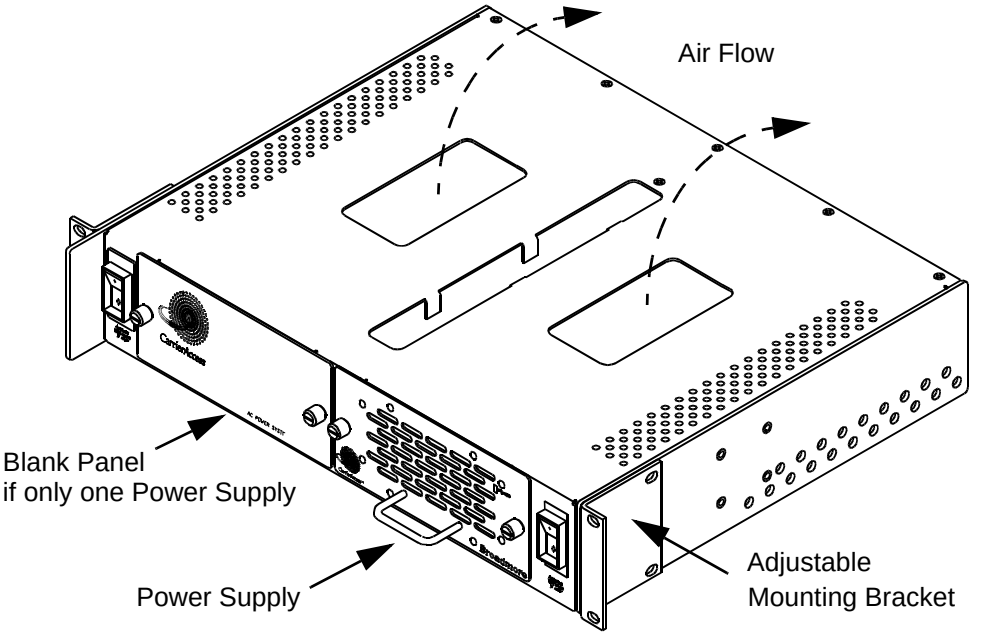


Perform the following steps:

1. Attach the ground wire supplied with the Broadmore chassis to the 6-32 chassis grounding stud located on the right rear of the chassis below the rear cover.
2. Attach the other end of the ground wire to the equipment rack building ground.

AC Power Supply Tray

The optional AC Power Supply Tray (7665-17PS) is a 3.5-inch high rack mounted unit that converts voltage from 110/220 VAC (50-60 Hz) to –48 VDC. The unit comes with one 240W AC Power Supply (7660-115), one AC power cord, and one 3.5 ft. DC cable for connecting to the Broadmore's –48 VDC power input. A second power supply with cables can be used to provide redundant DC power to the Broadmore chassis.



Rack-mounting the AC Power Supply Tray requires:

- clear access to front of rack
- user-provided rack mounting hardware (screws)

NOTE: No additional air space is needed above the AC Power Supply Tray when it is mounted directly below the Broadmore 1750 fan tray, which has a sloped bottom that does not interfere with air flow. Otherwise, provide at least 1.75 inch (1 RU) of free air space above the AC Power Supply Tray to ensure proper ventilation.

Perform the following steps:

1. Unpack and visually inspect the AC Power Supply Tray assembly.
2. For ease of rack installation, you can remove the power supply module(s) from the tray to make it lighter.
3. Adjust the rack mounting brackets for desired for a 19 or 23 inch rack and for front/rear mounting configuration. As shipped, the brackets will fit a 19” rack with front-mount configuration. The brackets can be removed and rotated 90 degrees to fit a 23” rack.
4. Rack mount the tray directly below the Broadmore 1750 using facility-provided mounting hardware.
5. Replace the power supply module(s) after rack-mounting the tray and tighten the module’s front panel screws.
6. If the tray came with only one power supply module and a redundant power supply is to be installed, remove the blank cover on the front of the tray, insert the second power supply, and tighten the front panel screws.

CHAPTER 5

Module and Fan Installation

In this Chapter

- Precautions ... *5-2*
- Module Installation Procedures ... *5-3*
- Fan Tray Installation Procedure ... *5-14*

Precautions

The Broadmore 1750 chassis is normally shipped with modules and fan tray installed at the factory. If they have been shipped separately, observe the following precautions when unpacking, handling, and installing these assemblies.

WARNING! **THE FRONT AND REAR COVERS OF THE CHASSIS SHOULD ONLY BE REMOVED FOR MODULE INSTALLATION AND MAINTENANCE AS REQUIRED. THE COVERS SHOULD BE REPLACED AS SOON AS POSSIBLE AFTER SUCH TASKS ARE COMPLETED.**

WARNING! **THE BROADMORE CONTAINS CIRCUIT CARDS AND COMPONENTS THAT ARE SUBJECT TO DAMAGE BY ELECTROSTATIC DISCHARGE (ESD). DO NOT REMOVE A COMPONENT FROM ITS PROTECTIVE PACKAGING UNTIL READY TO INSTALL IT. WEAR A WRIST GROUNDING STRAP AND ATTACH IT TO AN ESD CONNECTOR OR A METAL PART OF THE SYSTEM UNIT BEFORE HANDLING COMPONENTS. IF A WRIST STRAP IS NOT AVAILABLE, MAINTAIN CONTACT WITH THE SYSTEM UNIT THROUGHOUT ANY PROCEDURE REQUIRING ESD PROTECTION.**

NOTE: After installation is complete, ensure that blank panels cover all empty module slots to provide proper cooling when the fan is turned on.

Module Installation Procedures

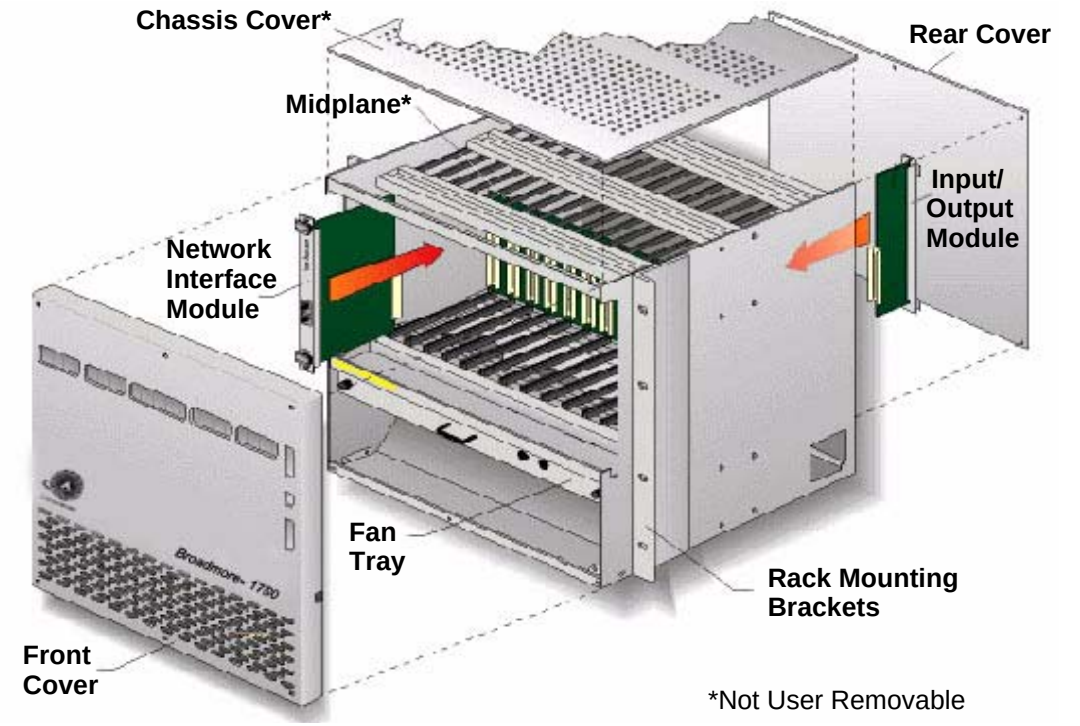
- Overview ... *5-4*
- Tools ... *5-5*
- Remove Chassis Covers ... *5-5*
- Module Locations ... *5-6*
- Installation Sequence ... *5-8*
- NIM Installation ... *5-9*
- SAM Installation ... *5-10*
- CPU Installation ... *5-10*
- APM Installation ... *5-10*
- NIM IOM Installation ... *5-11*
- SAM IOM Installation ... *5-11*
- CPU IOM Installation ... *5-12*
- APM IOM Installation ... *5-12*
- Replace Chassis Covers ... *5-13*

Overview

The Broadmore 1750 chassis is normally shipped with modules installed at the factory. If they have been shipped separately, perform the following procedures to configure and install the modules.

NOTE: Modules with jumpers are normally configured during installation to meet user requirements. If the chassis is shipped with modules installed, the modules may need to be removed, configured, and reinstalled.

The Broadmore 1750 system architecture is based upon a midplane design allowing modules to be installed from the front and rear of the chassis, as shown below.



Tools

The following tools are recommended to install, configure, operate, and maintain the Broadmore 1750:

- #1 flathead screwdriver (for cover removal/installation)
- Dual jeweler's flathead/Phillips screwdriver
- ESD wrist strap
- Other standard installation tools as desired.

Remove Chassis Covers

1. Loosen captive screws securing the front and rear covers and set the covers aside.
2. Connect an ESD wrist strap to the front or rear ESD connector and follow standard ESD procedures while handling unit components.

WARNING! USE ESD PRECAUTIONS: WEAR AN ESD GROUNDING STRAP WHILE HANDLING ANY MODULES OR ACCESSING THE INSIDE OF THE BROADMORE 1750. FAILURE TO FOLLOW ESD PROCEDURES MAY DAMAGE SENSITIVE COMPONENTS AND VOID THE WARRANTY.

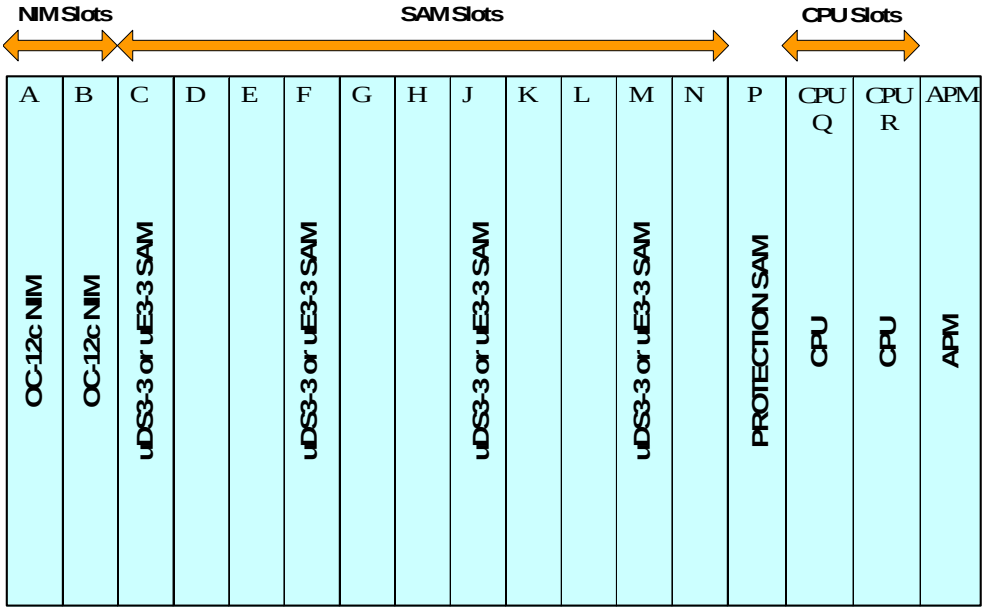
Module Locations

Obtain the office records showing the module slot installation locations for this chassis. The network design engineer will assign module slots to ensure proper system operation. (For detailed system design and configuration information, see *"System Planning Factors" on page 2-6*.)

The Broadmore 1750 chassis is designed for modules to go into specific slots to support various user requirements and cell bus bandwidths. As a minimum requirement, the module slot installations must conform to the guidelines on the following page.

The Broadmore 1750 is normally configured with redundant CPUs, redundant OC-12c NIMs, and five Unstructured DS3 SAMs providing 1:4 protection, as shown in the figure below. Other configurations are possible (contact factory for details).

The Broadmore 1750 system architecture is based upon a midplane design allowing modules to be installed from the front and rear of the chassis. There are 17 vertical slots as viewed from the front with the cover removed, as shown below. Input/Output Module (IOM) slots on the rear panel are numbered in the reverse order, so that they align with the module slots on the front panel. Each NIM, SAM, CPU, and APM requires a matching IOM installed in the rear.



CAUTION! **WHEN USING REDUNDANT OPTICAL NIMS, BOTH NIMS MUST BE IDENTICAL.**

Module Type	Description	Available Slot(s)
CPU	CPU	Q
	Redundant CPU	R
NIM	OC-12c/STM-4c	B
	Redundant NIM (OC-12c)	A
SAM	Unstructured DS3	C, F, J, M
	Unstructured E3	C, F, J, M
	Protection Unstructured DS3/E3	P
	Structured DS3 (up to 10 modules)	C-N
	Protection Structured DS3	P

NOTE: The Broadmore 1750 chassis will only support five Structured DS3 modules with the standard 2-fan cooling tray. For applications needing more than five Structured DS3 modules, a 3-fan cooling tray is required (contact factory for details).

Installation Sequence

The Broadmore 1750 is shipped in a minimum usable configuration. Unused slots are covered with blank panels except the slots for a single NIM, SAM, or CPU.

NOTE: After installation is complete, ensure that blank panels cover all empty module slots to provide proper cooling when the fan is turned on.

NIM, SAM, APM, and CPU cards are inserted from the front. IOM cards are inserted from the rear. All cards align in card guides for ease of installation and removal. Each card will have two retaining screws to hold it in place, one at the top and one at the bottom. These screws must not be used for seating or unseating the cards. Each card also has a set of ejectors, one on top and one at the bottom. These ejectors are used to unseat the card from the midplane connector for card removal.

NOTE: Modules with jumpers are normally configured before installing the modules in the chassis. However, modules are hot-swappable and may be removed at any time to verify or reconfigure the jumpers, then reinstalled. The following procedures include instructions for setting the jumpers.

Install modules in the following order:

- NIM (1 or 2)
- SAM (1 or more)
- CPU (1 or 2)
- NIM IOM (1 for each NIM)
- SAM IOM (1 for each SAM)
- Protection SAM IOM (1 in slot P)
- CPU IOM (1 for each CPU)

NOTE: The APM and APM IOM are factory installed at the factory.

NIM Installation

1. If a Building Integrated Timing Supply (BITS) clock will be used, an impedance matching adjustment may be required before installing an OC-12 NIMs. BITS impedance matching jumpers are located on the NIM component side below the midplane connectors. They are labeled **JMP1**, **JMP2**, **JMP3**, and **JMP4**. The following settings are available.

JMP3, JMP4 in (default)	100 ohms
JMP1, JMP2, JMP3, JMP4 in	75 ohms
All jumpers out	No termination

   BITS input is provided to the RJ48C BITS connector on the corresponding NIM IOM (see *"BITS Interface Connections" on page 6-7*).

NOTE: OC-12 NIMs go in slots A and B. (Both optical NIMs must be identical.) The NIM in slot B is the Working unit and the NIM in slot A is the Protection unit.

2. Place the Working NIM in slot B from the front so that it slides smoothly in the top and bottom card guides and the card connector aligns with the midplane connector.
3. Firmly press the NIM into the chassis until the connectors seat against each other completely. Use pressure simultaneously at the top and bottom of the NIM to ensure a proper fit to the midplane.
4. Secure the screws on the top and bottom of the module, being careful not to over-tighten.
5. For redundant NIMs, repeat this process to install the Protection NIM in slot A.

SAM Installation

1. Unstructured DS3-3 and E3-3 SAMs are installed in slots C, F, J, and M. Structured DS3 SAMs are installed in slots C thru N. The protection SAM is installed in slot P. All SAMs must be of the same type.
2. Place a SAM in the desired slot. so that it slides smoothly in the top and bottom card guides and the card connector aligns with the midplane connector.
3. Firmly press the SAM into the chassis until the connectors seat against each other completely. Use pressure simultaneously at the top and bottom of the SAM to ensure a proper fit to the midplane.
4. Secure the screws on the top and bottom of the module, being careful not to over-tighten.
5. Repeat this process to install the other SAMs as desired.

CPU Installation

1. Place the CPU card in slot Q from the front of the chassis so that it slides smoothly in the top and bottom card guides and the card connector aligns with the midplane connector.
2. Firmly press the CPU card into the chassis until the connectors seat against each other completely. Use pressure simultaneously at the top and bottom of the CPU to ensure a proper fit to the midplane.
3. Secure the screws on the top and bottom of the card, being careful not to over-tighten.
4. In a similar fashion, install the second CPU in slot R

APM Installation

The APM is shipped factory installed in the right-most slot, labeled APM, which is to the right of slot S.

NIM IOM Installation

1. From the chassis rear, place the NIM IOM in slot B so that it slides easily in the top and bottom card guides with the connector aligned to the midplane connector.
2. Visually verify that the NIM IOM physically aligns with the NIM installed above.
3. Firmly press the NIM IOM into the chassis until the connectors completely seat.
4. Secure the retaining screws on the top and bottom of the module, being careful not to over-tighten.
5. Repeat this process for the NIM IOM in slot A.

SAM IOM Installation

1. From the chassis rear, place each SAM IOM so that it slides easily in the top and bottom card guides with the connector aligned to the midplane connector for the slot matching the corresponding SAM.
2. Visually verify that the SAM IOM physically aligns with the SAM installed above.
3. Firmly press the SAM IOM into the chassis until the connectors completely seat.
4. Secure the retaining screws on the top and bottom of the module, being careful not to over-tighten.
5. Repeat this process for each slot with a corresponding SAM installed.

Protection SAM IOM Installation

1. From the chassis rear, place the Protection SAM IOM so that it slides easily in the top and bottom card guides with the connector aligned to the midplane connector for the slot matching the corresponding SAM in slot P.
2. Visually verify that the Protection SAM IOM physically aligns with the SAM installed above.

3. Firmly press the Protection SAM IOM into the chassis until the connectors completely seat.
4. Secure the retaining screws on the top and bottom of the module, being careful not to over-tighten.

CPU IOM Installation

1. Before installing the CPU IOM, an adjustment may be needed to configure the remote shutdown operation. There are two jumpers on each CPU IOM module labeled JMP1 and JMP2. These jumpers control how the remote shutdown contacts work. As installed at the factory, jumpers JMP1 and JMP2 connect pins 1-2 to pins 3-4 so that shorting either pair will reboot both CPUs. With both jumpers removed, shorting pins 1-2 will reboot the other-slot CPU; shorting pins 3-4 will reboot the same-slot CPU. For a redundant unit with two CPUs, it is recommended that both jumpers be removed so that the CPUs can be rebooted individually without disrupting system operation.
2. Visually verify that each CPU IOM physically aligns with its respective CPU installed above, slots Q and R respectfully.
3. Firmly press each CPU IOM into the chassis until the connectors completely seat.
4. Secure the retaining screws on the top and bottom of each module, being careful not to over-tighten

APM IOM Installation

The APM IOM is installed at the factory. This power module has fuses for each power source, as well as fuse holders for two spares.

Replace Chassis Covers

WARNING! **THE FRONT AND REAR COVERS OF THE CHASSIS SHOULD ONLY BE REMOVED FOR MODULE INSTALLATION AND MAINTENANCE AS REQUIRED. THE COVERS SHOULD BE REPLACED AS SOON AS POSSIBLE AFTER SUCH TASKS ARE COMPLETED.**

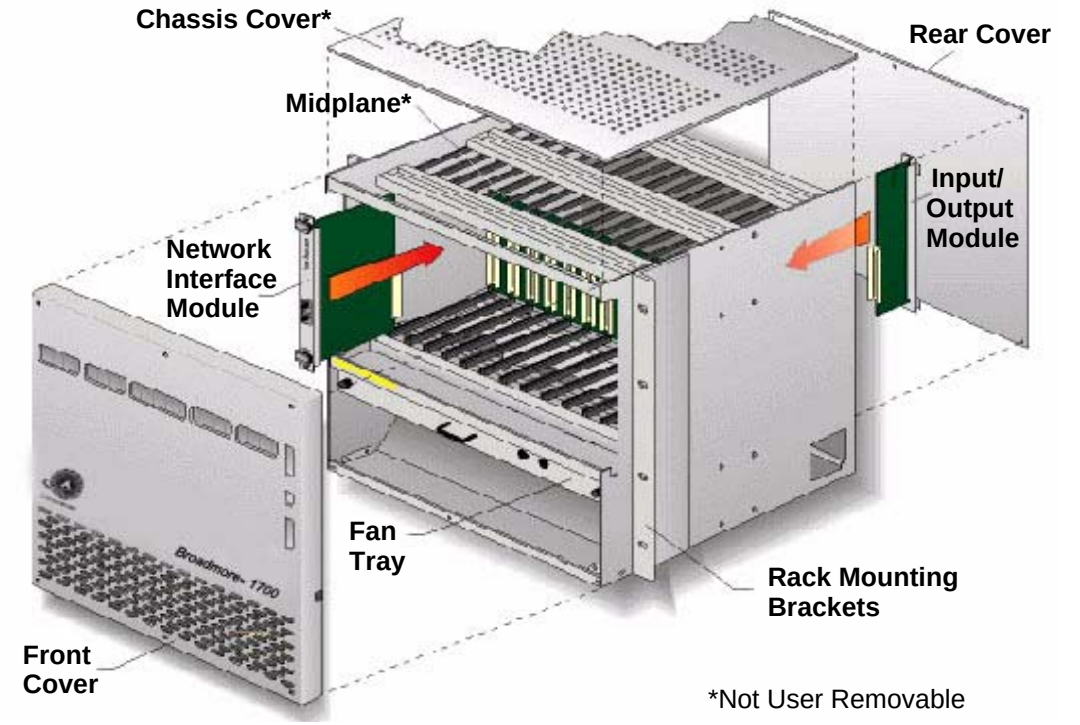
NOTE: After installation is complete, ensure that blank panels cover all empty module slots to provide proper cooling when the fan is turned on.

This completes module installation. Replace the front and rear covers unless additional installation or maintenance procedures are to be performed at this time.

Fan Tray Installation Procedure

- Tools ... *5-15*
- Remove Front Chassis Cover ... *5-15*
- Fan Tray Installation ... *5-15*
- Replace Chassis Cover ... *5-16*

The fan tray is normally shipped installed in the front of the chassis below the modules, as shown below. If it is not installed, follow the procedure below to install it.



Tools

The following tools are recommended to install, configure, operate, and maintain the Broadmore 1750:

- #1 flathead screwdriver (for cover and fan tray removal/installation)
- Dual jeweler's flathead/Phillips screwdriver
- ESD wrist strap
- Other standard installation tools as desired.

Remove Front Chassis Cover

Only the front cover must be removed to install the fan tray.

1. Loosen captive screws securing the front cover and set the cover aside.
2. Connect an ESD wrist strap to the front or rear ESD connector and follow standard ESD procedures while handling unit components.

WARNING! **USE ESD PRECAUTIONS: WEAR AN ESD GROUNDING STRAP WHILE HANDLING ANY MODULES OR ACCESSING THE INSIDE OF THE BROADMORE 1750. FAILURE TO FOLLOW ESD PROCEDURES MAY DAMAGE SENSITIVE COMPONENTS AND VOID THE WARRANTY.**

Fan Tray Installation

1. The fan tray installs from the front, directly below the modules. Fan tray guides are provided on each side of the chassis. Slide the fan tray into the guides and firmly push it into place so that connectors totally seat with the midplane.
2. Tighten the two front panel retaining screws using a flathead screw driver.

Replace Chassis Cover

WARNING! THE FRONT AND REAR COVERS OF THE CHASSIS SHOULD ONLY BE REMOVED FOR MODULE INSTALLATION AND MAINTENANCE AS REQUIRED. THE COVERS SHOULD BE REPLACED AS SOON AS POSSIBLE AFTER SUCH TASKS ARE COMPLETED.

This completes fan tray installation. Replace the front and rear covers unless additional installation or maintenance procedures are to be performed at this time.

CHAPTER 6

Electrical Installation

In this Chapter

- Precautions ... *6-2*
- Electrical Requirements ... *6-3*
- Cabling and Compliance Requirements ... *6-4*
- Alarm Port Connections ... *6-5*
- Optical Interface Connections ... *6-6*
- BITS Interface Connections ... *6-7*
- NIM/SAM IOM Connections ... *6-8*
- CPU IOM Connections ... *6-11*
- Power Supply Connections ... *6-12*
- Software ... *6-15*

Precautions

WARNING! THE BROADMORE 1750 IS INTENDED FOR INDOOR INSTALLATION ONLY. A PROPER CHASSIS GROUND CONNECTION IS REQUIRED. ITS ELECTRICAL COMMUNICATIONS INTERFACES SHALL NOT BE CONNECTED TO WIRING SYSTEMS THAT LEAVE THE BUILDING UNLESS APPROPRIATE INTERFACE DEVICES ARE USED. THE INSTALLER SHALL BE RESPONSIBLE FOR PROVIDING ADEQUATE LIGHTNING OR SURGE PROTECTION FOR WIRING THAT LEAVES THE BUILDING. THE INSTALLER SHALL BE RESPONSIBLE FOR PROVIDING APPROVED INTERFACE DEVICES IF CONNECTIONS ARE MADE TO PUBLIC COMMUNICATIONS NETWORKS.

WARNING! THE FRONT AND REAR COVERS OF THE CHASSIS SHOULD ONLY BE REMOVED FOR MODULE INSTALLATION AND MAINTENANCE AS REQUIRED. THE COVERS SHOULD BE REPLACED AS SOON AS POSSIBLE AFTER SUCH TASKS ARE COMPLETED.

WARNING! THE BROADMORE CONTAINS CIRCUIT CARDS AND COMPONENTS THAT ARE SUBJECT TO DAMAGE BY ELECTROSTATIC DISCHARGE (ESD). WEAR A WRIST GROUNDING STRAP AND ATTACH IT TO AN ESD CONNECTOR OR A METAL PART OF THE SYSTEM UNIT BEFORE HANDLING COMPONENTS. IF A WRIST STRAP IS NOT AVAILABLE, MAINTAIN CONTACT WITH THE SYSTEM UNIT THROUGHOUT ANY PROCEDURE REQUIRING ESD PROTECTION.

NOTE: After installation is complete, ensure that blank panels cover all empty module slots to provide proper cooling when the fan is turned on.

Electrical Requirements

- Tools ... *6-3*
- Power ... *6-3*
- Cable Management ... *6-3*

Tools

The following tools are recommended to install, configure, operate, and maintain the Broadmore 1750:

- #1 flathead screwdriver (for cover removal/installation)
- ¼-inch hex driver
- Dual jeweler's flathead/Phillips screwdriver
- PC with VT100 Emulation software program
- DC Volt-Ohm Meter (VOM)
- ESD wrist strap
- Other standard electronic installation tools as preferred

Power

DC power connections are made at the rear of the Broadmore chassis. The primary DC power source is –48 volts at 5 amperes and is connected to the "A" inputs. For redundancy, a second –48 VDC source may be connected to the "B" inputs.

For AC power applications, the optional dual AC redundant power supply tray is usually mounted below the Broadmore and requires 110/240 VAC, 50/60 Hz. AC power is connected at the rear of the power supply tray, and the two –48 VDC outputs are then wired to the DC power inputs on the Broadmore chassis.

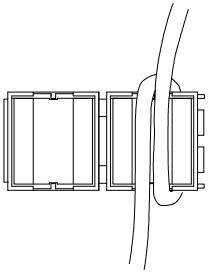
Cable Management

Overall cable lengths can be optimized through equipment location. Access and cable strain-relief tie-down points are provided.

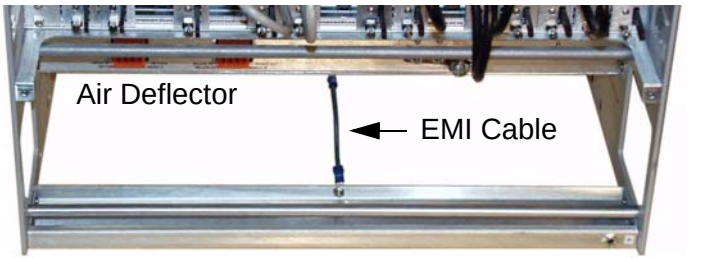
Cabling and Compliance Requirements

For FCC Part 15 Class A compliance for EMI/RFI suppression, the Broadmore 1750 requires that a ferrite bead (P/N 010-0051) must be attached to each DC power cable, Ethernet cable, and alarm cable. FCC compliance also requires that an EMI cable be attached between the chassis and air deflector. Accessory kits are included with the Broadmore chassis. Use the following guidelines for FCC compliance.

- DC power, one or two cables. Attach one ferrite bead to each cable, using a single wrap so that the cable passes through the bead twice (see figure below left).
- Ethernet, one or two cables. Attach one ferrite bead to each cable, using a single wrap so that the cable passes through the bead twice.
- Alarm cable. Attach one ferrite bead to the cable, using a single wrap so that the cable passes through the bead twice.
- EMI cable. The EMI cable must be attached vertically across the bottom rear opening (see figure below right). Remove the existing screw at the top center of the air deflector at the rear of the unit. Discard the existing flat washer. Using the existing screw, attach the ring terminal of the EMI cable to the air deflector. Attach the ground clip to the other end of the EMI cable. Attach the ground clip with the EMI cable to the top center of the rear cable tray support channel.



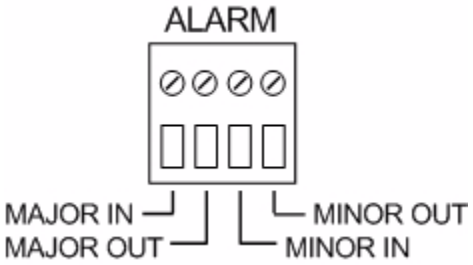
Ferrite Bead



Cable Tray

Alarm Port Connections

Alarms are sent to the control console and the system log. LEDs display alarm conditions. Additionally, the Broadmore 1750 has an alarm port on the chassis rear for connection to the user's remote indicators. The alarm port is a four-wire terminal block providing form "C" relay contact closure signals. Two wires are labeled "Major" (in and out) and two are labeled "Minor" (in and out) as shown below. The alarm connector on the lower back of the chassis is shown below. The connector is a compression type in which the wire is inserted in the lower opening and the compression screw above is tightened to secure the wire. A small flathead screwdriver is required to secure the wires.



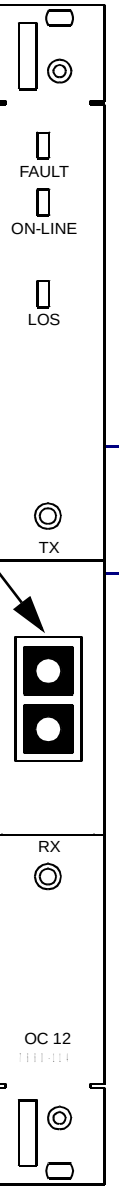
1. Run the alarm cables to the connection point on the chassis rear as shown above.
2. Insert the cable wires and tighten the compression screws to secure the wires.

Optical Interface Connections

The Broadmore 1750 interfaces to an ATM network via fiber optic cable using SC connectors on the front panel of the OC-12c NIMs.

1. Route the cable to the front of the chassis.
2. Route the cable into the chassis via the small square opening on the lower-right, front cover of the chassis.
3. Connect the cables to the labeled TX and RX connectors on the front of the NIM. (See example at right.)
4. Use the plastic cable guides and cable protector shipped with the Broadmore 1750 to secure the cable.

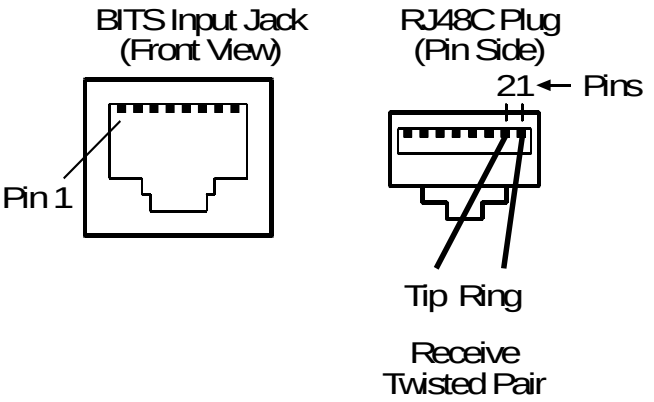
WARNING! UNTERMINATED OPTICAL CONNECTIONS MAY EMIT LASER RADIATION. DO NOT VIEW BEAM WITH OPTICAL INSTRUMENT.

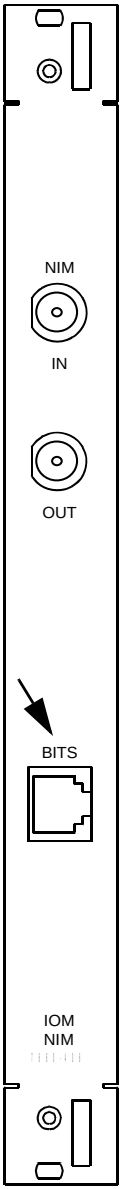


BITS Interface Connections

NIM IOMs include a Building Integrated Timing Supply (BITS) input connector for network timing. If required, the BITS impedance jumpers on the OC-12 NIMs are normally adjusted during *"NIM Installation" on page 5-9*.)

1. Use cable rated for Category 3 (CAT3) or better.
2. Route the cable to the lower-left, rear of the chassis.
3. Connect the cable to the RJ48C BITS connector on the rear of the chassis. (See example at right.)
4. Use the plastic cable guides and cable protector shipped with the Broadmore 1750 to secure the cable.





NIM/SAM IOM Connections

- General Instructions ... *6-8*
- Unstructured DS3-3/E3-3 IOM Connections ... *6-9*
- Structured DS3 IOM Connections ... *6-10*

General Instructions

Network equipment (excluding fiber optic) and user equipment connect to the Broadmore 1750 via cables routed to connectors on the back of each IOM. The physical interface varies by type of IOM (see *"Module Descriptions" on page 1-12*). Adapter cables are available for most serial interface SAMs (see *"Cable Specifications" on page E-1*).

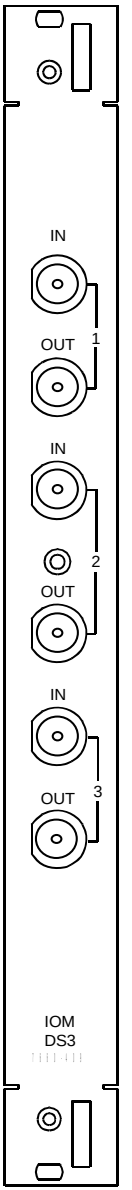
1. Route the equipment cables to the chassis rear.
2. Install the plastic edge protector around both rear access square openings. Note the chassis internal cable tray. Two bars are provided as anchor points for cable ties. This will serve as cable strain relief.
3. Route the cables into the chassis via the square openings on either side of the rear cable tray.
4. Connect the cables to the IOM connectors as labeled for each port and dress out the cables. Use the tray and bars to secure the cable.

NOTE: After completing the hardware installation, visually inspect all modules and connectors. Replace the front and rear covers, if not already in place.

Unstructured DS3-3/E3-3 IOM Connections

Each Unstructured DS3 IOM provides three pairs of BNC coaxial connectors (labeled 1 to 3) for RG-59, 75 ohm cable.

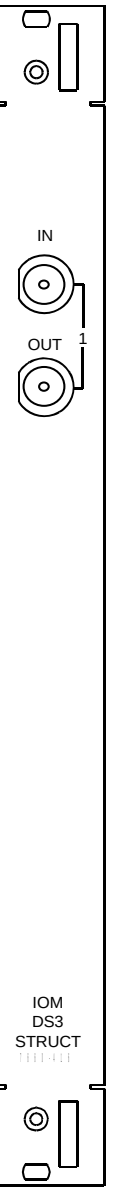
1. Connect receiver RX inputs to the IN ports.
2. Connect transmitter TX outputs to the OUT ports.



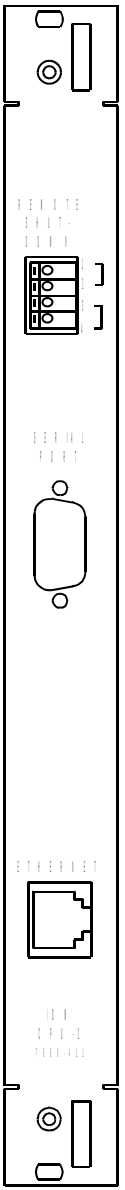
Structured DS3 IOM Connections

Each Structured DS3 IOM provides one pair of BNC coaxial connectors for RG-59, 75 ohm cable.

1. Connect receiver RX input to the IN port.
2. Connect transmitter TX output to the OUT port.



CPU IOM Connections



Remote Shutdown Connections

The CPU Remote Shutdown feature allows a connection to be made across one of the contact pairs to remotely close the contacts, which forces a reset of the CPU in the event that the CPU cannot be reset through software.

The behavior of these terminals are set by jumpers on the card (see *"CPU IOM Installation" on page 5-12*).

To use this feature, connect a cable to terminals 1-2 and/or 3-4 on the CPU IOM. (See example at right.) The spring terminal block accepts 26 to 18 AWG wire.

Serial Port Connections

This is a standard DB9 RS-232 DTE serial management port that can be connected to a serial terminal or PC running a terminal emulation program. Access to this port is determined by the security settings.

Ethernet Connections

This is a standard ethernet DTE management port that can be connected to an IP network. Access to this port is determined by the security settings.

Power Supply Connections

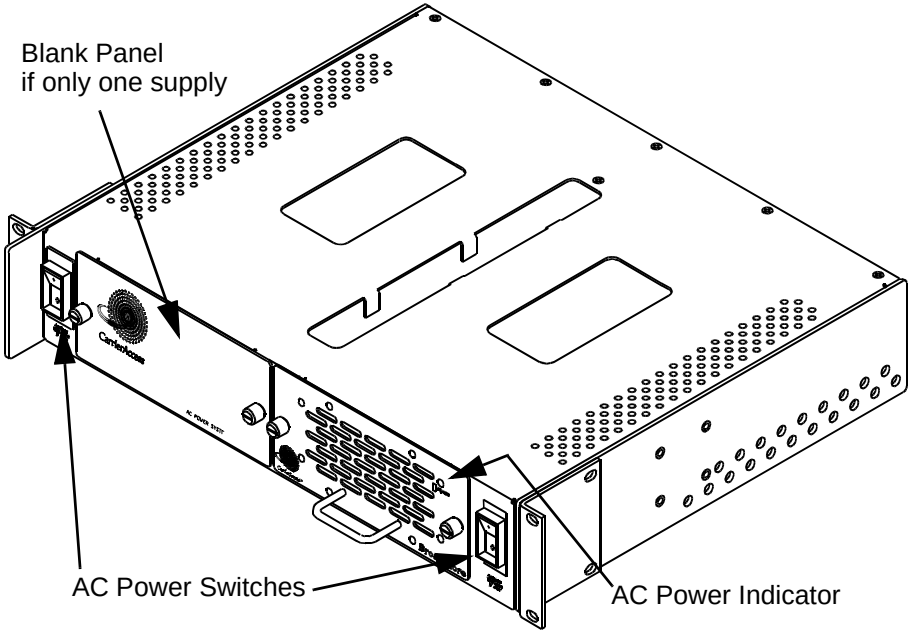
- Optional AC Power Supply Connections ... *6-12*
- Broadmore Power Input Connector ... *6-14*
- Connecting –48 VDC Power ... *6-14*

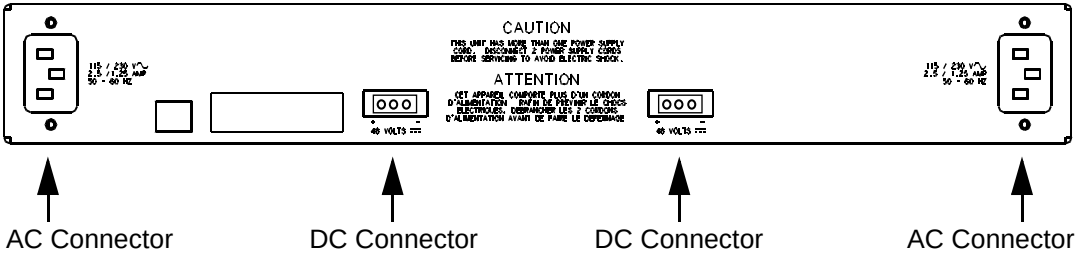
WARNING! **THE INSTALLER SHALL ENSURE THAT ALL POWER CONNECTIONS TO THE BROADMORE 1750 HAVE AN APPROVED SERVICE DISRUPTION FEATURE EXTERNAL TO THE BROADMORE 1750 FOR EMERGENCY USE. THIS MAY BE A FUSE, CIRCUIT BREAKER, CORRECTLY LABELED SWITCH, OR OTHER APPROPRIATE DEVICE.**

Optional AC Power Supply Connections

The optional redundant AC Power Supply Tray mounts in the rack directly below the Broadmore 1750 chassis (see *"AC Power Supply Tray" on page 4-8*). Each 40W power supply module in the tray converts voltage from 110/220 VAC (50-60 Hz) to –48 VDC. Each DC cable has pigtail wires for connecting –48 VDC power to the Broadmore chassis.

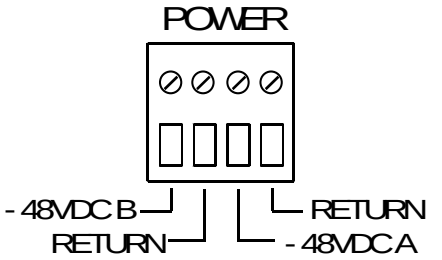
1. Locate the AC power cord provided with each power supply module and connect one end to the AC connector on the rear of each module.
2. Ensure the power switch on the front of each module is turned OFF and that the AC power indicator (LED) does not light.
3. Connect each AC power cord to a facility 110 VAC power receptacle. Cords may be connected to different AC sources for additional redundancy if desired.
4. Turn each power switch to the ON position. The green AC power indicator (LED) should illuminate beside each switch to indicate normal operation.
5. Turn each module power switch to the OFF position and verify that the power indicator is off.
6. Locate the DC power cord provided with each power supply module and connect the plug to the DC connector on the rear of each module.


Blank Panel
if only one supply
AC Power Switches
AC Power Indicator


CAUTION
ATTENTION
AC Connector
DC Connector
DC Connector
AC Connector

Broadmore Power Input Connector

Power is provided as –48 VDC to the connection points in the rear of the chassis. Voltage may be provided directly from the user's power source. Optionally, the Broadmore 1750 comes with a redundant AC power supply. The power connector on the lower back of the chassis is shown below. The connector is a compression type in which the wire is inserted in the lower opening and the compression screw above is tightened to secure the wire. A small flathead screwdriver is required to secure the wires.



Connecting –48 VDC Power

1. Identify the power cables and secure their power.
2. Use a Volt-Ohm Meter (VOM) to verify the voltage and polarity of the cable wires.
3. Turn off power to the cables and use a VOM to verify there is no voltage present.
4. Run the power cables to the connection point on the chassis rear as shown above. Note there are two power rail inputs, A and B, as labeled.
5. Insert the cable wires and tighten the compression screws to secure the wires.
6. Restore power to the cables. Use the VOM to verify voltage is present at the chassis connection points.
7. Turn off power to the cables until ready for the power-up sequence.

Software

The Broadmore 1750 is delivered with operating software pre-installed. The FIPS 140-2 validated Broadmore/SSHield Management software is installed on each CPU's disk-on-chip memory. DSP software code also exists on each NIM and SAM and is unique for each type of module.

Two programs may be used to communicate with the CPU operating system. These are the Communication Access Multiplexer Management Interface (CAMMI) and Command Line Interface (CLI). This manual is based upon CAMMI. For information on the CLI, see *Command Line Interface on page 9-1*.

CHAPTER 7

Configuration

In this Chapter:

- Overview ... *7-2*
- Power Supply Redundancy ... *7-24*
- Module Redundancy ... *7-25*
- Module Configuration ... *7-37*
- PVC Connection ... *7-63*
- SVC Connection ... *7-65*
- VP Reservation ... *7-67*
- System Configuration ... *7-70*
- Help ... *7-73*

Overview

- Power-up ... *7-3*
- User Interface Requirements ... *7-4*
- Screen Display Annotation ... *7-5*
- Key Map ... *7-6*
- CAMMI Access ... *7-7*
- System Services Configuration ... *7-8*
- CAM Name ... *7-8*
- Ethernet IP Configuration ... *7-9*
- ATM Address ... *7-11*
- ATM Address List (optional) ... *7-11*
- Connection Retry ... *7-13*
- Retry Cause Codes ... *7-13*
- CIP over ATM (RFC 1577) ... *7-14*
- Static Routes ... *7-16*
- LANE Configuration ... *7-17*
- UNI Version ... *7-19*
- General Properties ... *7-20*
- User Security Configuration ... *7-23*

CAUTION! **FOR SECURE OPERATION, A SUPERUSER (CRYPTO OFFICER) SHOULD PERFORM THE INITIAL CONFIGURATION AND CREATE USER ACCOUNTS, AS DESCRIBED IN CHAPTERS 10 AND 11.**

The Broadmore 1750 must be correctly configured, using CAMMI, before ATM network communications can be established. This section provides background information, equipment requirements, and other prerequisites for accomplishing the actual system configuration.

Configuration information is retained in three subdirectories collectively referred to as the configuration database. Access to this database is to set variables to acceptable values for successful operation. The three subdirectories are:

- CAM\CONFIG\CURRENT – contains the complete set of startup configuration data for all modules. This data is saved when **Save Config. For PowerUp** is selected from the user interface.
- CAM\CONFIG\DEFAULTS – contains the defaults to be used for new cards and ports. Default values for new modules are automatically loaded if a startup configuration for that module does not exist.
- CAM\CONFIG***user-name*** – contains a snapshot of the system and module configuration data as of the time the SAVE CONFIGURATION command was issued. Data is stored in a subdirectory with user-supplied ***user name***.

Power-up

1. Power-up the chassis. The Broadmore 1750 is designed for continuous service. There is no on/off power switch since the system is designed to remain on at all times. Simply apply power.
2. Observe the LED indicators to ensure that the system is operating properly. See *"Summary of Front Panel LEDs" on page 8-44*.

Power-on diagnostics take approximately 30 seconds, after which the LEDs indicate the operational condition. Refer to Chapter 5, *Maintenance and Troubleshooting* if any problems arise. The rest of this chapter assumes normal operation

User Interface Requirements

Communicate with the CPU to complete configuration actions in one of several ways. An RS-232 serial connection is provided on the front of the CPU card (via the CPU IOM card will be a future release). This serial connection requires a VT100 compatible emulating software package running on the PC.

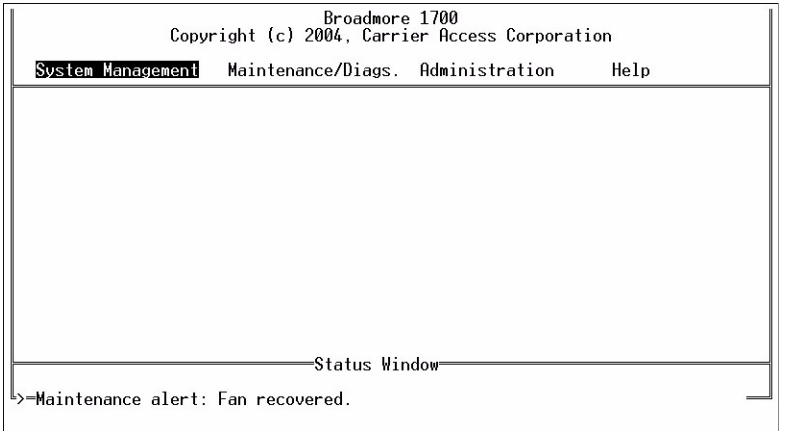
NOTE: We do not recommend using Microsoft Hyperterm due to unsatisfactory terminal emulation.

Remote execution can be accomplished via a Telnet client application configured as a VT100 terminal. An SNMP connection can be established via Ethernet to the CPU IOM, via CIP (RFC 1577), or via LANE.

NOTE: In a Broadmore system with redundant CPUs, the primary IP address is used to log into the online CPU and the secondary IP address is used to log into the standby CPU.

CAMMI is used throughout this manual. The CLI (Chapter 9) supports the same command set as CAMMI, however the CLI is a pure text interface.

Reset the terminal preference font if the borders are not solid lines. Depending on the terminal emulation application, ANSI BBS may also be more satisfactory.



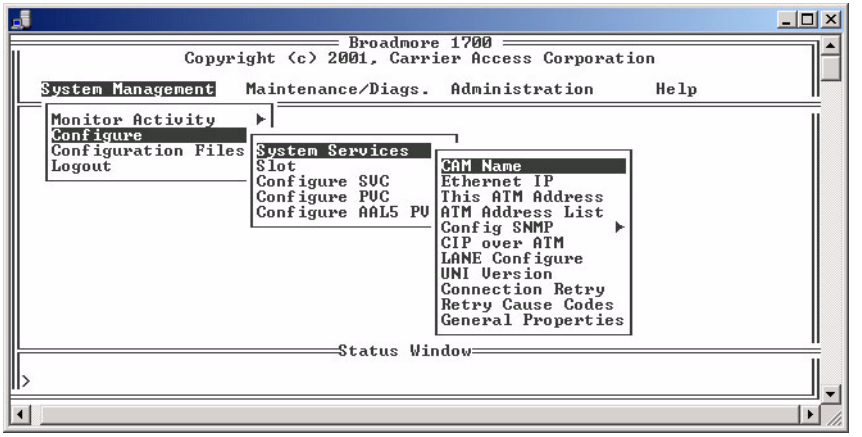
Screen Display Annotation

The symbol ↵ (**Enter** key) will be used throughout this manual to indicate selection. Typically the selection is from a list of choices on a drop-down menu. Often, there is a sequence of multiple drop-down menus where the selection process will be displayed as a series of ↵ symbols. For example, the CAMMI main menu is shown below.

Highlight **System Management** and ***press*** **Enter** to display the first submenu. ***Highlight*** **Configure** on the drop-down menu and ***press*** **Enter** to display the second drop-down menu. ***Highlight*** **System Services** on this menu and again ***press*** **Enter** to display the third drop-down menu. This type of sequence will be annotated as follows throughout this manual:

> *Select* **System Management** ↵
> *Select* **Configure** ↵
> *Select* **System Services** ↵

This example sequence displays the screen on the next page. Each item in the final window is followed by a " ▸ " to indicate that an additional entry screen follows.



Choose the second item, **Ethernet IP**, to display a screen for entering six lines of IP address information (not shown).

This method of annotating screen displays will make the text and logic easier to follow and less prone to error. Specific steps will be clear and easy to follow, leading to more efficient system operation.

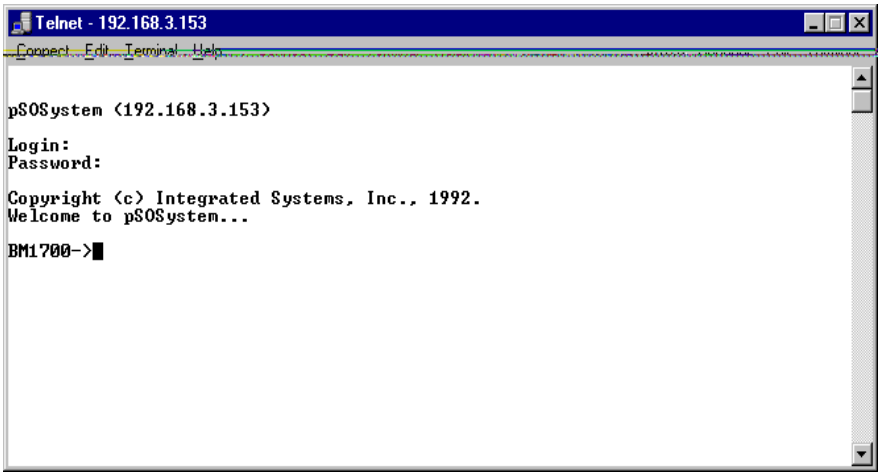
Key Map

The following key map correlation is provided to assist in navigating through the various menus. This may be required since some terminal emulation packages do not recognize the full keyboard character set.

Up	[
Down	]
Page Up	{
Page Down	}
Home	(
End	)
Insert	:
Delete	@
Help (cli only)	?

CAMMI Access

To access the CAMMI main menu, log into the system with a valid user identification (**SYSADMIN**) and password (**INITIAL**). This default user ID/password is delivered with the system with supervisor access as explained in *"General Properties" on page 7-20*. User ID and password are case-sensitive when entered.



At this point, you may change the terminal interface baud rate. The default is 9600 baud and the system reverts to this at every reboot. The command to change the rate is setbaud <rate> where a valid <rate> is 300, 600, 1200, 2400, 4800, 9600, 19200,38400, 57600, or 115200.

NOTE: The baud rate default is 9600. The terminal will return to 9600 baud *on each system boot or reboot*. Operation above 19200 is not recommended.

Upon successful entry, you are asked to change the terminal baud rate to match the new setting. The system will then change its baud rate. You will not be able to communicate with the system until your terminal baud rate is changed to match.

System Services Configuration

Configure System Services to communicate with the ATM switch and set up parameters for Broadmore 1750 control. The data entry screens are accessed as shown.

Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Configure each item as explained below

CAM Name

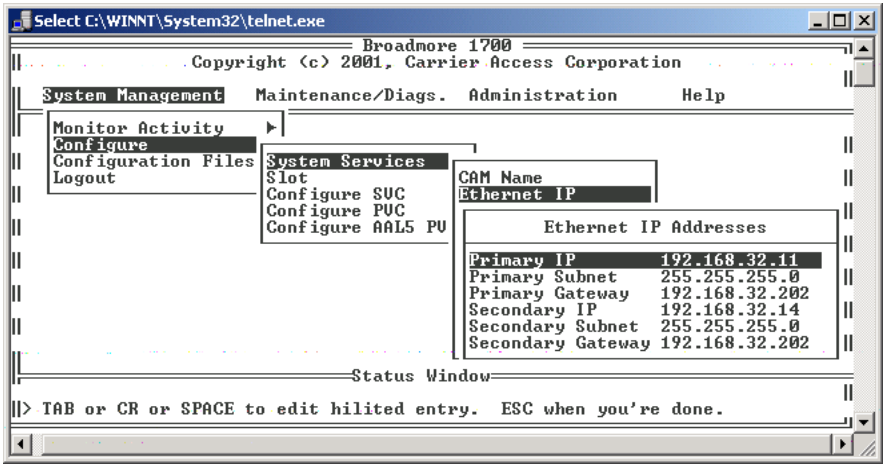
Each Broadmore 1750 can be named locally. A short (10-character) name and a long (64-character) name are available. These two names are independent as chosen by the operator. The long name appears at the top of CAMMI screens to provide on-screen identification. The short name appears as a shell prompt. The default long name is a null field and the default short name is **Broadmore>.**

From CAMMI, follow the sequence below to enter names.

Select **System Management** ↵
Select **Configure** ↵
Select **System Services** ↵
Select **CAM Name** ↵
Enter the desired long and short names ↵

Ethernet IP Configuration

Select Ethernet IP and the screen below appears. On initial boot-up, enter the IP address, which will not go into effect until the system is rebooted. Use the reset toggle switch on the front of the CPU to reboot the system.



Follow the pull-down menu selections to enter the Broadmore 1750's IP address. This address is then used for Telnet access to the CAMMI program.

NOTE: In a Broadmore system with redundant CPUs, the primary IP address is used to log into the online CPU and the secondary IP address is used to log into the standby CPU.

NOTE: Changes to the following settings only take effect upon system reboot:

- IP Configuration
- CIP Configuration
- LANE Configuration
- Redundancy (APS) Configuration
- UNI Version Configuration
- Cause Code changes
- ATM Address Changes

On initial setup, configure all of these items before doing a system reboot.

Subnet is the mask for the network. Subnet and Gateway are assigned by your facility's network administrator. Reboot the Broadmore 1750 to have this IP address take effect. The entire Broadmore 1750 will reboot with the new IP address. Log into the system with a valid user ID and password (ID ***SYSADMIN***, password ***INITIAL***).

1. Enter the IP, subnet, and gateway addresses (obtained from the network administrator). These settings take effect when the Broadmore 1750 is rebooted.
2. Follow the sequence below to reboot on a single CPU system.

   Select **Maintenance/Diags.** ↵
   Select **Reboot System** ↵

3. Log into the system, and return to the system services configuration screen to continue the process.

ATM Address

Follow the sequence below and choose **Change** on the user-defined ATM address screen.

CAUTION! AN ADDRESS CHANGE WILL CAUSE SERVICE DISRUPTION.

Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **This ATM Address** ↵

A screen displays to enter the ATM address.

The Media Access Control (MAC) address is the initial default ATM address. Save the new ATM address after entry to update ATM access information. This newly saved address will not take effect until the system is rebooted. With signaling turned off, the ATM address will be displayed as all zeroes.

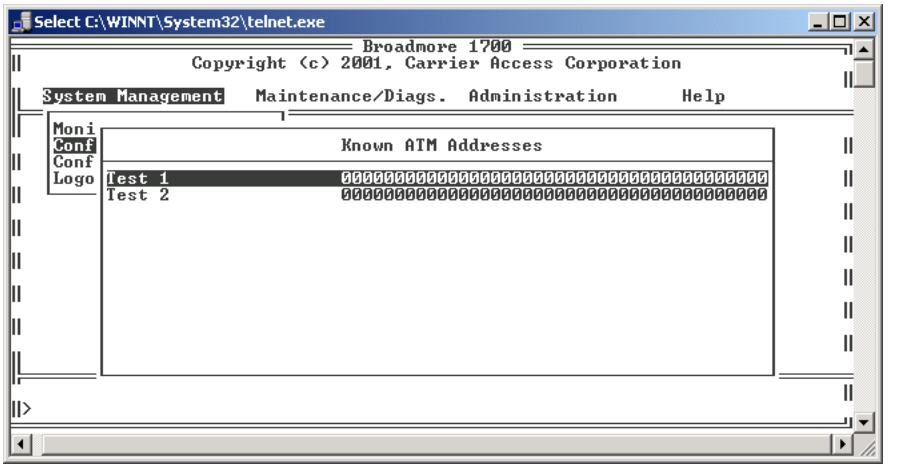
For dual CPU systems, define the ATM address to keep the same address during a CPU switchover. Otherwise, an address change will cause service disruption.

ATM Address List (optional)

The following steps are optional for SVC services and are not used for PVCs. The ATM address list provides a convenient way to store frequently called SVC addresses, instead of having to enter each address manually when needed. To use this optional feature, follow the sequence below to display user-defined ATM addresses.

Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **ATM Address List** ↵

This displays the Known ATM Addresses.



Follow the sequence below to Edit, Copy, Delete, or add a New user to the ATM list.

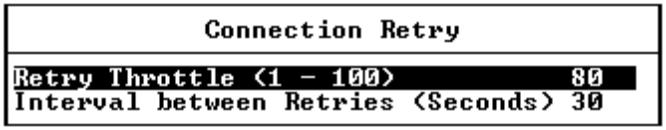
Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **ATM Address List** ↵ ↵
Select one of the following:

* **Edit** ↵, edit the description and/or ATM address
* **Copy** ↵, (to put a copy of the ATM address into the list)
* **Delete** ↵
* **New** ↵, enter the description and/or ATM address

With each selection, confirm your changes and press *Esc* to exit.

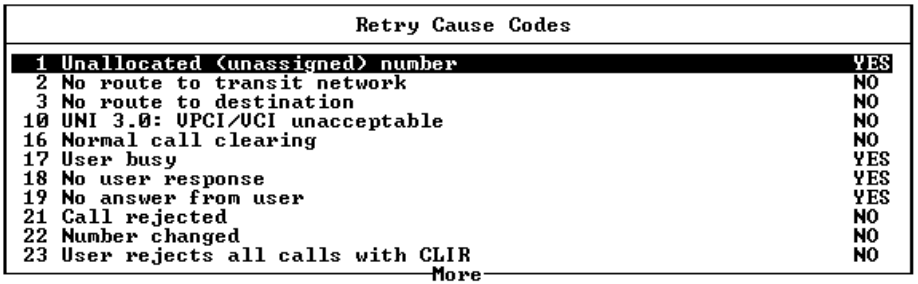
Connection Retry

Applicable to SVCs only, the retry throttle value is the number of SVC call setups/ teardowns that the Broadmore 1750 works on at one time. An initial throttle value of 80 and interval of 30 seconds are recommended. These values can then be adjusted to meet local requirements.



Retry Cause Codes

Applicable to SVCs only, each item in this list can be set to yes or no, based upon local requirements. These codes are set as factory defaults to the most common values. Changing them will overwrite the defaults. Only the “yes” values are retried.



CIP over ATM (RFC 1577)

RFC 1577 support is also known as Classical IP (CIP) over ATM. CIP is provided as a path for controlling multiple Broadmore 1750s when IP connectivity over Ethernet is not available to all of the installed Broadmore 1750s. Control signals are sent to a Broadmore 1750 over the ATM if the Broadmore 1750 is not on the Ethernet with the control station. As a prerequisite, the configuration process must be completed.

Configuration forms the Broadmore 1750s into a subnetwork, with either an ATM switch or workstation designated the server and others designated as clients. The server maintains a Logical IP Subnetwork (LIS), which cross-references logical IP addresses to ATM addresses. When the control station sends IP traffic (e.g., control signals) via the subnetwork IP address to a Broadmore 1750, the server uses LIS data to tell the sender an equivalent ATM address to use in place of the IP address. The IP datagrams are then sent over the ATM network to the desired Broadmore 1750, which takes appropriate action and responds. The control station has full communications with the Broadmore 1750 over ATM/Ethernet. Control is identical to control over Ethernet, and the ATM control path is essentially transparent to the user.

Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **CIP over ATM** ↵

Follow the path shown to reach the CIP over ATM configuration items. These items are listed in the following table.

Item	Description
ATM IP Address	Enter the IP address within the subnet. Set to all zeros to disable CIP.
ATM Subnet Mask	The mask is the same for all Broadmore 1750s on the network.
Server Address	The address of the server containing the LIS. This may be a workstation on the ATM network or ATM switch. Set to zero if you want to use AAL5 PVCs for CIP instead of SVCs.
Peak Cell Rate	This controls the bandwidth allocation to RFC 1577 support.
Enable RIP	Normally disabled. Only set to Yes for router operation as the CIP subnet server.

This configures the Broadmore 1750. Some Broadmore 1750s may need routing table additions to recognize and respond to the control station via the ATM subnetwork.

These Broadmore 1750s will be configured individually, based upon network topology. Each unit may or may not have an Ethernet connection.

In the case of no Ethernet connection, the unit routes Ethernet traffic to the ATM by default. The Ethernet gateway setting is a null field. Follow the sequence on the next page to verify that no gateway is defined. Do this for each applicable Broadmore 1750 without an Ethernet connection.

Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **Configure IP** ↵
Select **Gateway 0.0.0.0** (correct if necessary)

Static Routes

Each Broadmore 1750 has an additional Ethernet route to support RFC 1577 unless it is on the same Ethernet network as the master control station. Follow the steps below to add this routing. For sample configuration with static routes, see *"Sample Network with RFC 1577 Configuration" on page D-1*.

1. Connect to the Broadmore 1750 via the serial port and log-in using the default user ID and password, ***SYSADMIN*** and ***INITIAL***.
2. This will give you the prompt: **Broadmore>**
   Enter **route –a** ↵ to display the current routing table.
3. Add a routing entry in the format
   route add xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy ↵
   where xxx.xxx.xxx.xxx is the destination IP address (control station)
   yyy.yyy.yyy.yyy is the ATM subnet IP address of the Broadmore 1750 on the Ethernet segment serving as the control station.
4. Enter **savert** ↵ to save this entry. The new routing entry is immediately active.
5. Enter **route –a** ↵ to observe that the route has been added to the table.

NOTE: You may enter **route delete xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy** to remove the entry from the routing table.

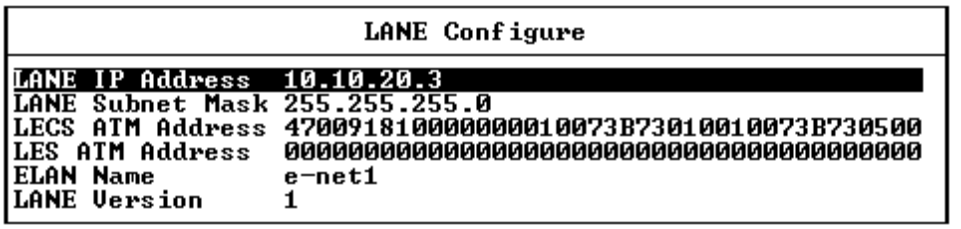
6. Enter **cammi** ↵ to return to CAMMI.

Repeat this procedure for each Broadmore 1750.

LANE Configuration

The Broadmore 1750 supports LANE version 1 and 2 acting as LAN Emulation Client, LEC. Follow the sequence below to display the LANE configuration screen shown. Six fields appear for data entry.

Select **System Management** ↵
Select **Configure** ↵
Select **System Services** ↵
Select **LANE Configure** ↵



Explanations are provided for each in the table below.

Item	Description
LANE IP Address	This is the IP Address for the Broadmore 1750. To get onto the ELAN, the address must be on a different logical subnet than the OSC's Ethernet IP Address. This address must be different than the ATM CIP Address subnet.
Subnet Mask	This is the subnet mask to be used in conjunction with the Broadmore 1750's LANE IP Address.
LECS ATM Address	This address is optional. This is the ATM Address of the LAN Emulation Configuration Server, LECS. If the ATM Address of the LAN Emulation Server, LES, is known and is entered below, this LECS value may be left blank. If the LECS is needed and no address is entered here, then the "well known" ATM Address (as defined by ATM Forum's LANE standard) will be used by default. The "well known" default address is 4700 7900 0000 0000 0000 0000 0000 A03E 0000 0100.
LES ATM Address	This field is optional. The ATM Address of the LAN Emulation Server is entered here. If data is entered here, the ELAN name and the LECS ATM address will not be needed and will not be used by the system if they are entered below.
ELAN Name	This field is optional. If a name is entered, it will be sent to the LECS to locate the LES for this ELAN. If the ELAN Name is not specified, and no LES is specified, then, the default ELAN, as entered in the LECS, will be used. The Broadmore 1750 is never an LECS.
LANE Version	This value will be either **1** or **2**. Use the LANE version supported and active in the segment's LECS and in the other LE clients.

Using LANE may require static routes in a manner similar to CIP. Refer to the Static Routes section above and the example in Appendix D.

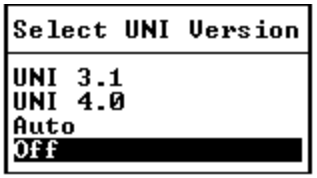
UNI Version

The signaling options are UNI 3.1, UNI 4.0, Auto, and Off. Follow the sequence below and make the appropriate choice from the screen shown.

Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **UNI Version** ↵

NOTE: You must select the UNI Version before configuring any SVCs. If there are active SVCs, the UNI Version will not appear in the menu until you release all the SVCs. This is done to prevent interrupting service on those circuits.

The UNI Version selection screen appears as shown below with the current selection highlighted.



CAUTION! **UNI VERSION SHOULD BE OFF WHENEVER THE NIMS ARE NOT CONNECTED TO AN ATM SWITCH INTERFACE CONFIGURED FOR UNI SUPPORT.**

General Properties

- Max VP/VC ... *7-20*
- Bandwidth Meter ... *7-22*

Max VP/VC

The Max VP/VC option allows you to set the maximum number of Virtual Paths (VPs) and corresponding Virtual Channels (VCs). The maximum number of VCs allowed per VP is based on the number of VPs set. Table 7-1 shows the Max VP/VC settings and the valid values for VP and VC numbering.

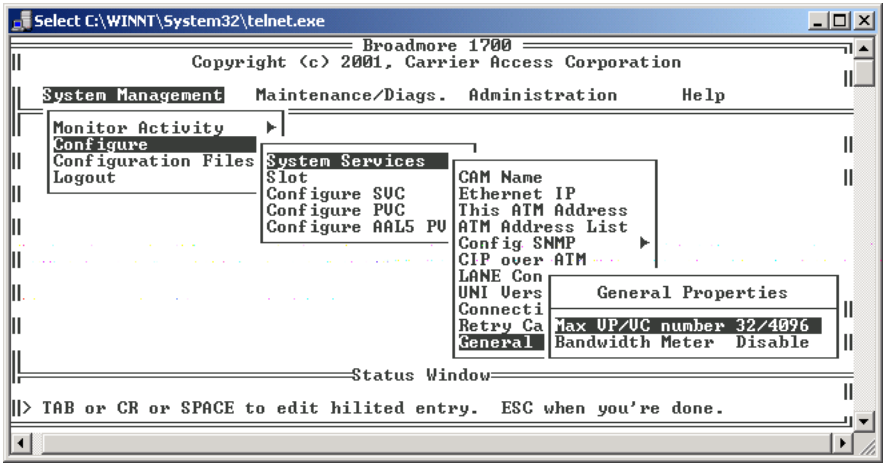
Table 7-1: Settings for Max VP/VC and Valid Values for VP/VC Numbering

Max VP/VC Setting	Maximum Number of VPs Allowed	Valid Values for VP Numbering	Maximum Number of VCs Allowed	Valid Values for VC Numbering*
2/65536	1	0 or 1**	65,535	1 - 65535
4/32768	4	0 - 3	32,767	1 - 32767
8/16384	8	0 - 7	16,383	1 - 16383
16/8192	16	0 - 15	8,191	1 - 8191
32/4096 (default)	32	0 - 31	4,095	1 - 4095
64/2048	64	0 - 63	2,047	1 - 2047
128/1024	128	0 - 127	1,023	1 - 1023
256/512	256	0 - 255	511	1 - 511

*VC numbering must start at 32 if the VP number is 0.
**For the ATM DS3, CBI, and HSSI-CBI modules, the VP number must be 0; 1 is invalid.

To set Max VP/VC, follow the sequence below and make the appropriate choice from the screen shown.

Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **General Properties** ↵
Select **Max VP/VC** ↵



Bandwidth Meter

The Bandwidth meter allows you to track the amount of bandwidth in use. Follow the sequence below and make the appropriate choice from the screen shown.

Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **General Properties** ↵
Select **Bandwidth Meter** ↵

NOTE: The Bandwidth meter uses the clock rate of the HSSI NIM as the bus rate. If the HSSI NIM is set for received timing, the bandwidth meter will not be using the correct bus rate because the clock is supplied by the HSSI at the other end. Be sure to check how the HSSI's clock is set before using the Bandwidth meter.

User Security Configuration

The Broadmore 1750 system has a user identification procedure for security. Each user has a unique password. Users are divided into four privilege levels providing access to selected command functions.

Browser – Limited to viewing current configurations, statistics, and logs.

Operator – Can perform all normal operations such as configuring modules, establishing connections and removing connections.

Sys_Admin – Can perform all operator functions plus FTP, diagnostics and test functions.

Super_User – Can perform all operator and maintenance technician functions plus add/delete/modify user access. A Super_User can add, delete, or change user access privileges (user ID, password, and level of access) from the Administration main menu drop-down.

Select **Administration** ↵
Select **Change User ID** ↵

Each user can change his/her personal password from the Administration main menu drop-down item **Change Password** (below). Follow the on-screen directions and enter the new password twice. Change the password for user ID SYSADMIN to something other than **INITIAL**.

Select **Administration** ↵
Select **Change Password** ↵

NOTE: For more information about Security features and privilege levels, see *"Security Management" on page 10-1* and *"Security Management (FIPS Mode)" on page 11-1*.

Power Supply Redundancy

The Broadmore 1750 has two power input connectors for receiving –48 VDC. The user may provide power to these connectors from different sources as one form of redundancy. Carrier Access offers an optional dual AC power supply with 110 VAC, and provides two sources of –48 VDC to the Broadmore 1750. This is power supply contains two independent modules, each sufficient to operate the Broadmore 1750. These modules are hot-swappable, and they may be connected to different sources for an additional degree of redundancy. There is no impact to the Broadmore 1750 as long as one (or both) of the modules is operating normally.

Module Redundancy

- Protection Definitions ... *7-25*
- NIM Redundancy ... *7-26*
- SAM Redundancy ... *7-29*
- CPU Redundancy ... *7-33*

Protection Definitions

Automatic protection switching (APS) is performed in accordance with specifications except as noted. The following definitions are provided to clarify the terms used in NIM redundancy.

Item	Definition
APS	Automatic Protection Switching
Reverting	After redundancy switching, the system will switch back to the original primary NIM when repairs are completed.
Non-reverting	After redundancy switching, the protection NIM will remain the system primary NIM after repairs are completed. In this case, the repaired NIM becomes the protection NIM. This only applies to manual switching.
1+1 Protection	The signal is continuously bridged to the working and protection equipment so payloads are transmitted identically over both paths. The receiving equipment chooses either path. The user must set their equipment to bi-directional. The Broadmore 1750 supports bi-directional 1+1 APS for the NIM. The Broadmore 1750 does not support uni-directional 1+1 APS for the NIM.
1:*n* Protection	There is one backup for *n* critical components. Any of the *n* working channels can be bridged to a single protection line.

Item	Definition
1:1 Protection	A special case of 1:*n* protection where *n*=1. Each critical component has a dedicated backup, which assumes operation if the primary unit fails, so that connectivity is not adversely impacted.

NIM Redundancy

ATM redundancy is provided by installation of a second NIM. The Broadmore 1750 can then be configured to provide 1+1 or 1:1 NIM protection in accordance with the SONET-GR-253-CORE specification. The APS is per the SONET-GR-253-CORE specification. The user may select either reverting or non-reverting APS modes as explained in the configuration below.

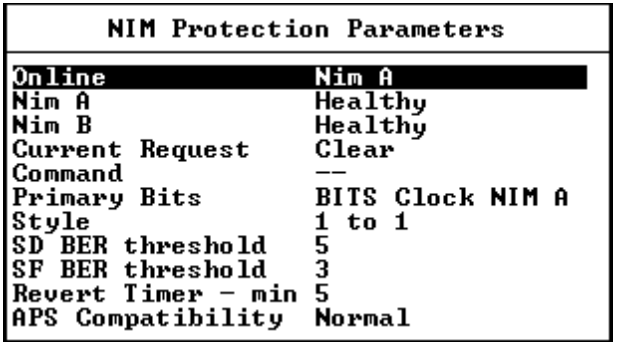
NOTE: The Broadmore will display only those features supported by the installed NIM. Consequently, some of the features described below may not apply to the NIMs you are configuring.

Configure redundancy following steps on the next page.

1. Review the hardware configuration. The Broadmore 1750 must have two NIMs installed to support redundancy, the master NIM in slot "B" and the APS NIM in slot "A". If installing 1:1 protection, reverting or non-reverting, **contact the ATM switch vendor to ensure that 1:1 protection is supported.**

Select **Maintenance/Diagnostics** ↵
Select **Redundancy** ↵
Select **NIM** ↵
Select **APS Parms** ↵

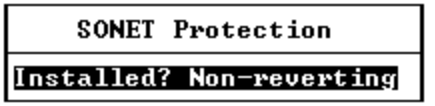
2. From the CAMMI main screen, follow the selection sequence above to display the redundancy screen.



3. Following the instructions on the bottom of the screen and toggle through available choices for each item.

Select **Maintenance/Diagnostics** ↵
Select **Redundancy** ↵
Select **APS Install** ↵

4. Follow the sequence above to display the SONET screen below and make choices to meet your specific configuration. Use the space bar to toggle between **reverting** and **non-reverting**. The third choice, **Single NIM**, is used when only one NIM is installed.



5. In the redundancy configuration on the Protection Parameters shown above, the Command field choices are prioritized per the SONET GR-253-CORE specification. The available choices in priority order top-to-bottom are:

   Lockout
   Force A
   Force B
   Switch to A
   Switch to B
   Clear

The Command Request field indicates the current request status and cannot be changed. The command "Clear" is not prioritized but it acts to remove the last request from its control station. This means that a command (i.e., choice) will not be activated if there is a higher priority current request shown in the Command Request status portion of the display. Broadmore generated requests such as "SD- Signal Degradation" are not shown on the screen but they fall in the priority list between "Force B" and "Switch to A". In other words, a command "Force B" will switch the Broadmore to NIM B regardless of signal degradation, while a command "Switch to B" will be ignored in the same circumstance if there is a current SD request. A Command Request can be received from any user interface.

6. Set the Parameters for Bit Error Rate (BER) Thresholds in the right part of the display. Enter a desired number "x" for each threshold, remembering that the degrade threshold (SD) should be a larger "x" than the failure threshold (SF) and thus a smaller number. The parameter entered is defined by the equation

   $$\text{Threshold} = 10^{-x}$$

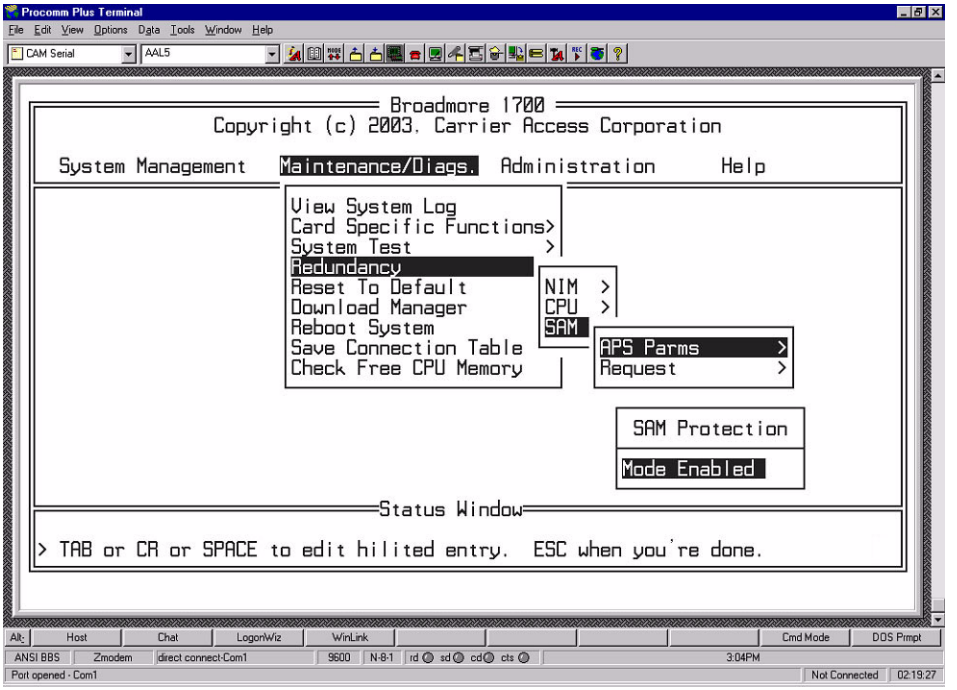
   where "x" is the user-entered number. If the redundancy chosen is revert, then the parameter "Revert Time" will be active and the number of minutes before the system automatically reverts to the original primary NIM may be entered.

7. Switching the protection installation changes module and call configurations. **Follow any change to redundant configuration by immediately rebooting the system.**

SAM Redundancy

In the Broadmore 1750, installing an Unstructured DS3 SAM in slot P provides 1:N SAM redundancy. A special Protection IOM with no user interface is used, since input/output will continue to be provided via the cables attached to the slot of the failed SAM. The Unstructured DS3 in slot P is called the protection SAM, or P-SAM. The working SAMs, called W-SAMs, are installed in slot C, slot F, slot J, and slot M.

Follow the sequence below to enable and configure SAM redundancy.



Select **Maintenance/Diags** ↵
Select **Redundancy** ↵
Select **SAM** ↵
Select **APS Parms** ↵

Slot M has the highest priority, followed in order by slot J, slot F, and slot C. The P-SAM provides redundancy according to the following:

- Only a single W-SAM is protected
- In the case of more than one request for the P-SAM, only the highest priority W-SAM is protected
- If the P-SAM is protecting a W-SAM, then a request from a *lower* priority W-SAM is ignored until the higher priority clears
- If the P-SAM is protecting a W-SAM, then a request from a *higher* priority W-SAM is honored (and the protection for the first-protected W-SAM is lost)
- P-SAM is invoked for removal of a W-SAM, or by user command
- Redundancy is not reverting. After correction of a W-SAM problem, switch back manually
- Wait at least 15 seconds between removal and insertion of SAMs to ensure system stabilization.

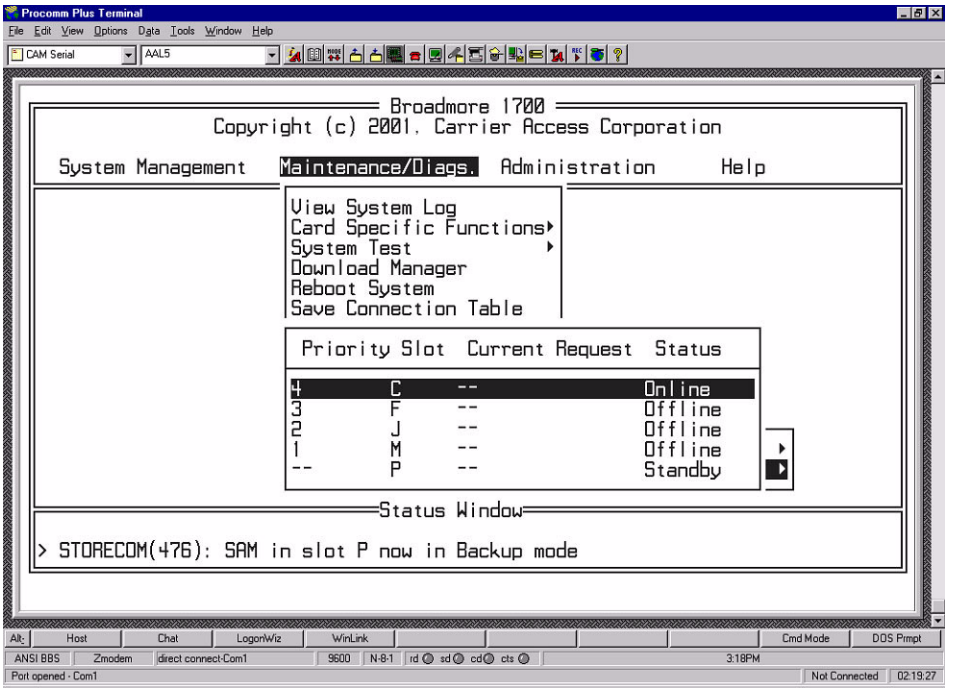
CAUTION! FAILURE TO WAIT 15 SECONDS BETWEEN EVENTS MAY LEAD TO A CONDITION WHERE A W-SAM DOES NOT RETURN TO FULL OPERATION. IN THIS CASE, FOLLOW THE STEPS BELOW TO CORRECT THE PROBLEM.

Perform the following steps to enable SAM Protection:

1. Go to **APS Parms** and select **Mode Enabled**.

Select **Maintenance/Diags** ↵
Select **Redundancy** ↵
Select **SAM** ↵
Select **APS Parms** ↵
***Change* Mode Enabled** ↵

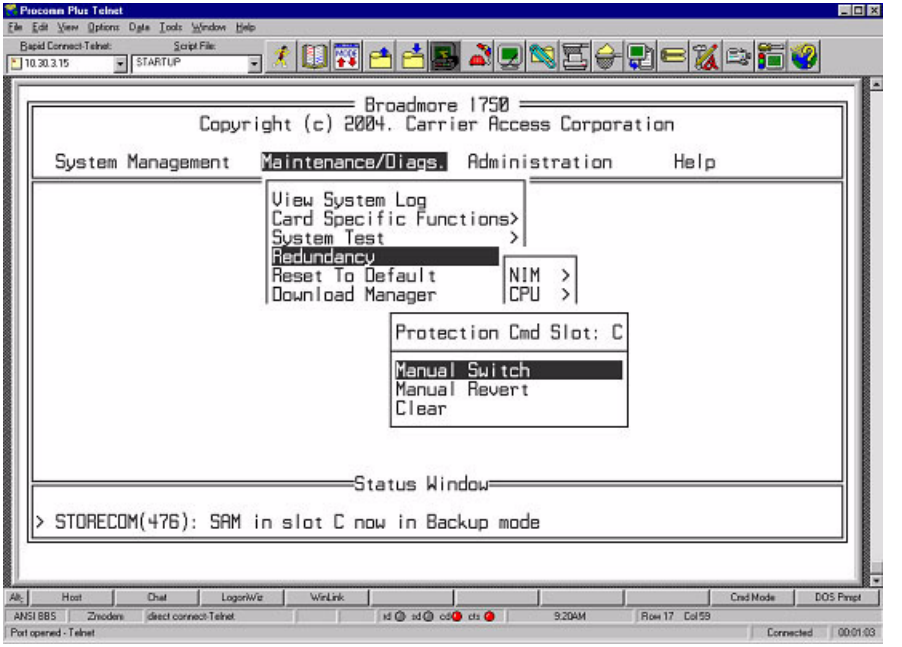
2. Go to **SAM Request** and manually set each W-SAM to **Online**.



Select **Maintenance/Diags** ↵
Select **Redundancy** ↵
Select **SAM** ↵
Select **Request** ↵
Change **Online** ↵

NOTE: Protection switching is non-revertive. After correcting the fault problem, the Offline W-SAM must be manaully set back to Online if it is to be protected.

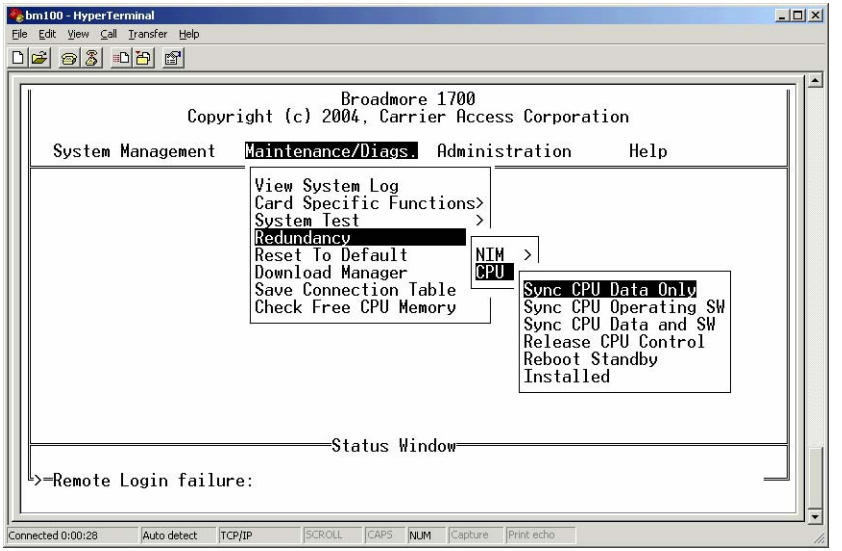
3. After setting a W-SAM to **Online**, you can test the protection feature by performing a **Manual Switch** to divert traffic through the P-SAM and a **Manual Revert** to return traffic back to the W-SAM.



CPU Redundancy

CPU redundancy is automatically activated when a second CPU is detected in the system. If two CPUs are detected at initial boot, the first to boot becomes “online” and the other goes into the standby mode.

CPU redundancy allows the standby CPU to take control if the online CPU experiences a failure. Data files on the two CPUs are synchronized automatically when the standby CPU is powered up. This synchronization process occurs automatically when the standby CPU is powered up. Once both CPUs are functioning (one online and the other in standby) any subsequent changes to the system are mirrored (recorded in the online CPU and sent to the standby CPU). This process keeps the standby CPU up to date.



Select **Maintenance/Diagnostics** ↵
Select **Redundancy** ↵
Select **CPU** ↵

System Log

The system log is unique to each CPU. Entries are sent from each CPU and copied to the partner CPU. Each entry has a time stamp followed by an upper-case or lower-case slot letter. An upper-case letter (Q or R) indicates that the message originated from the current CPU. A lower-case letter (q or r) indicates that the message originated from the partner CPU. Thus, an entry in one log with an upper-case slot letter will have a similar entry in the other log with a lower-case slot letter.

Select **Maintenance/Diagnostics** ↵
Select **View System Log** ↵

IP Addresses

A Broadmore 1750 chassis may have one or two IP addresses (see *"Ethernet IP Configuration" on page 7-9*). The online CPU will have the primary address as configured in the **Config IP** menu. The standby CPU will have the secondary address as configured in the **Config IP** menu. If a CPU switchover occurs, the newly online CPU will change its IP address to the primary IP.

The Broadmore 1750 may also be configured with an IP address for CIP over ATM. This address is only valid for the online CPU.

If used, a LANE address is configured via the **LANE Configure** menu. LANE is only valid for the online CPU.

Select **System Management** ↵
Select **Configure** ↵
Select **System Services** ↵

Synchronizing CPU

CAUTION! MODULE REMOVAL AND INSERTION – ON A POWERED-UP SYSTEM, WAIT AT LEAST 15 SECONDS AFTER ANY MODULE REMOVAL OR INSERTION TO ALLOW THE SYSTEM TO STABILIZE. FAILURE TO FOLLOW THIS PROCEDURE MAY RESULT IN SYSTEM ERRORS REQUIRING TOTAL SYSTEM REBOOT. WHEN INSTALLING A REPLACEMENT CPU IN A REDUNDANT CPU SYSTEM, DO NOT REBOOT OR POWER DOWN THE SYSTEM BEFORE CPU SYNCHRONIZATION IS COMPLETE AS INDICATED BY A SOLID STATUS LIGHT.

CPU data sync occurs automatically and should not require user intervention (see *"CPU Sync" on page 8-17*). If there is a CPU sync problem, follow the steps below to synchronize data and operating software (SW) between the two CPUs. This should only be done when there is file manipulation unknown to the system, such as FTP of new files to the online CPU.

Three options are available for synchronizing CPU: **Sync CPU Data Only**, **Sync Operating SW**, and **Sync CPU Data and SW**. Synchronizing the operating software is very time-consuming and should only be done as a last resort when the standby CPU has no Ethernet connection to update the software by FTP.

Select **Maintenance/Diags** ↵
Select **Redundancy** ↵
Select **CPU** ↵
Select **Sync CPU Data Only** ↵

Release CPU Control

If desired, the online CPU can be made to release control (switch) to the standby CPU by performing the following steps. The online CPU will then become the standby CPU, and vice versa. This command may be used during maintenance procedures.

Select **Maintenance/Diags** ↵
Select **Redundancy** ↵
Select **CPU** ↵
Select **Release CPU Control** ↵

Reboot Standby CPU

If desired, the standby CPU can be rebooted by performing the following steps. This command may be used during maintenance procedures.

Select **Maintenance/Diags** ↵
Select **Redundancy** ↵
Select **CPU** ↵
Select **Reboot Standby** ↵

Install Single or Dual CPU

This configuration item only activates detection of the SNMP trap **Standby CPU missing**. If only one CPU is present, select **Single CPU**. If two CPUs are installed, select **Dual CPU**.

Select **Maintenance/Diags** ↵
Select **Redundancy** ↵
Select **CPU** ↵
Select **Installed** ↵

Module Configuration

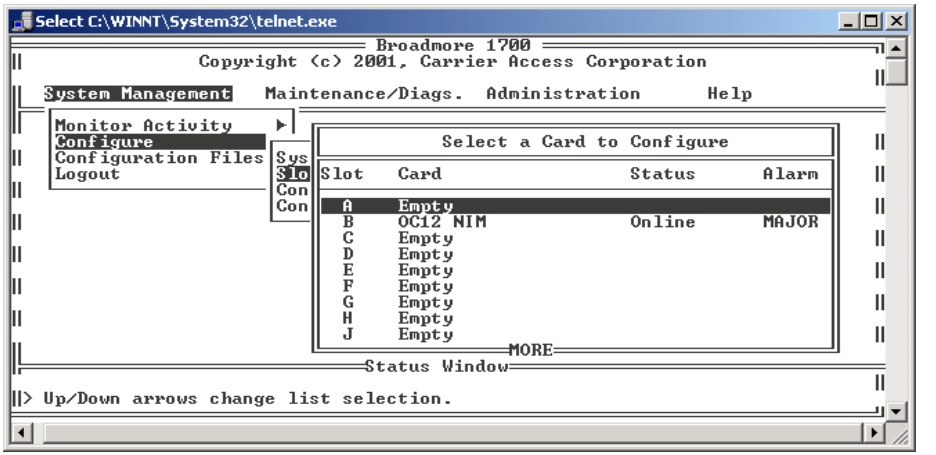
- How to Configure Specific Modules ... *7-38*
- OC-12c/STM-4c ... *7-39*
- OC-12c/STM-4c BITS/Timing Redundancy ... *7-40*
- Unstructured DS3 SAM ... *7-43*
- Structured DS3 SAM ... *7-50*
- Unstructured E3-3 SAM ... *7-57*

How to Configure Specific Modules

The NIM and SAM configuration process applies to each module installed in the system. The parameters vary by module as delineated below. For each module, start the procedure by following the pull-down sequence shown.

Select **System Management** ↵
Select **Configure** ↵
Select **Slot** ↵
Select the slot with the module to be configured ↵

The slot selection screen, as shown below, also displays the current alarm condition of the module in each slot.



NOTE: The list above displays only a portion of the available Retry Cause Codes. Scroll down to view additional codes.

OC-12c/STM-4c

Choose the slot (A or B) containing the OC-12c/STM-4c to be configured and a parameter input screen appears. The table below is a guide to parameter configuration.

Item	Options	Comment
Port Mode	**On-line** **Off-line** **Test Download Standby** **Configuration Request** **Broken**	This field is a status indicator and the items displayed are the result of configuration (or other) actions.
Framing Type	**SONET** **SDH**	SDH is for International ITU applications. SONET is for US applications.
Transmit Timing	**Recovered** **BITS** **Local**	Recovered means from SONET. BITS impedance matching is a hardware function; see NIM Installation, Chapter 3. BITS is tied to the local in-house timing source. Local is on-board Stratum 3 timing source.
SONET Tx	**Enable** **Disable**	If SONET Tx is enabled, framing is enabled; if SONET Tx is disabled, framing is removed (i.e., SONET Tx is all zeroes).
Loopback Mode	**Normal** **Terminal** **Local** **Remote**	Normal is no loopback. Terminal is a loopback from the ATM interface to the user equipment. Local is a loopback before NIM processing to the fiber link. Remote is a loopback from the receive fiber to the ATM before local processing.
ATM Payload Scramble Mode	**Both Scrambled** **Transmit Scrambled** **Receive Scrambled** **No Scramble**	A technique used to prevent a long string of zeros. Both ends of a connection must be configured the same for operation.
BITS Clock Alarm Loss	**Enable** **Disable**	Provides an alarm indication of loss of BITS clock at the NIM IOM when enabled. A corresponding BITS LOS SNMP trap is generated if SNMP is configured properly.

If a second OC-12c/STM-4c is installed, repeat this process for the configuration. Follow the module-specific information above, as appropriate.

OC-12c/STM-4c BITS/Timing Redundancy

Configuration of the timing options on a redundant OC-12c/STM-4c system requires correct settings on both NIMs, the DS3 port, and the NIM redundancy screen. Either of the Broadmore 1750 BITS inputs on NIM IOMs, in slots A and B, can be selected as the primary clock reference. Each BITS input has an enable/disable menu option on the coinciding OC-12c/STM-4c interface. When a condition exists that the primary reference source is not detected, the unit will switch to the other BITS input, if a signal is detected on that input. If a signal is not detected on the opposite BITS, the source clock will be derived from an alternate source propagated from the NIM to the cell bus. The source of the cell bus clock depends on the setting of the OC-12c/STM-4c transmit timing option. Two options are available, ***Local/BITS*** and ***Received***. The Local/BITS option derives clock from the on-board internal oscillator. The received option derives clock from the received SONET stream.

1. Follow the sequence below to set the redundancy primary BITS clock to either A or B.

Select **Maintenance/Diags** ↵
Select **Redundancy** ↵
Select **NIM** ↵
Select **Primary BITS** ↵
Choose **A** or **B**
In the case of a single BITS clock, select it as the primary source (NIM A or NIM B).

2. Follow the sequence below to set the clock mode configuration on the port of interest.

Select **System Management** ↵
Select **Configure** ↵
Select **Slot** with DS3 ↵
Select **Port** of interest ↵
Select **Operational Configuration** ↵
Select **Clock Mode** ↵
Choose the BITS option to allow the DS3 port to derive clock from either BITS or the cell bus

3. Follow the sequence below to set the OC12 transmit timing to either recovered or local/BITS. Recovered clock derives timing from the SONET stream. Local/BITS derives timing from the onboard oscillator. Repeat this step for both OC12s.

Select **System Management** ↵
Select **Configuration** ↵
Select **Slot** with OC12 ↵
Select **Transit Timing** ↵
Choose **Recovered** or **Local/BITS** ↵

Follow the sequence below to enable an alarm for loss of BITS clock. Do this for both OC-12c/STM-4cs.

Select **System Management** ↵
Select **Configuration** ↵
Select **Slot** with OC12 ↵
Select **BITS Clock Alarm Loss** ↵
Choose **Enable** or **Disable** ↵

The recommended configuration for maximum clocking stability is:

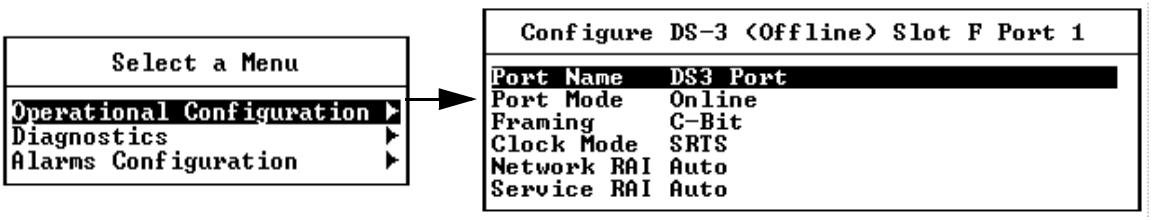
1. Connect BITS sources to NIM I/O A and NIM I/O B.
2. Select a Primary Reference Source (A or B), and then enable the clock loss alarm menu option on each OC-12c/STM-4c.
3. Configure the DS3 SAM to BITS clock mode.

   The equipment connected to the Broadmore 1750 OC-12c/STM-4c interface is configured to BITS and provides a BITS reference clock embedded in the SONET serial stream.
4. The Broadmore 1750 OC-12c/STM-4c Transmit timing option is set to recovered.

   In effect, the Broadmore 1750 OC-12c/STM-4c is loop timed off of the associated SONET device. Configuring the equipment in this manner allows the DS3 SAM to fallback on a clock derived from the associated SONET equipment's BITS, in the event of a BITS clock failure.

Unstructured DS3 SAM

Choose the slot containing the DS3 SAM to be configured to display a screen for port selection. The table below is a guide to configuration parameters. Operational, Diagnostics, and Alarm configuration are the three menu options. Descriptions of the configurable items are found in the following tables. Highlight each item and use the space bar to toggle available options for each. Save the configuration after making changes.



The following tables show the options available for each item, separated by operational configuration, diagnostics, and alarm configuration.

Table 7-2: Unstructured DS3 SAM Configuration Items

Item	Options	Comments
Port Name		A descriptive field to identify the port
Port Mode	**On-line** **Off-line**	This is a status field that can be toggled to **online** or **offline**. When the port is in offline status, it is not available to make calls, and passive SVCs are refused.
Framing	**C-bit** **M13** **Unframed**	**C-bit** is a framing mode using DS2 stuff bits associated with M23 multiplexing for other purposes such as Far End Alarm Control (FEAC) Channel. **M13** is a mode that maps 28 DS1s directly into the DS3. The DS1s do not exist independently as is the case when M23 multiplexing is used. **Unframed** requires a 44.736 Mbps input.
Clock Mode	**SRTS** **Adaptive** **Network** **BITS** **Loop**	**NOTE: SRTS is a proprietary timing algorithm and may ONLY be used with specific written prior permission from Carrier Access Corporation. Additional license fees may apply.** **SRTS**-This method measures the Service Clock input frequency against a network-wide ATM synchronization clock and sends the difference signals in the AAL1 header to the destination Broadmore 1700 circuit emulation interface. The different signals are then combined with the network-wide ATM synchronization clock to re-create the input service clock. If more than one ATM clock synchronization is present in the network, an alternate timing recovery method must be selected. For this method to work, the ATM network must be synchronized to a single network-wide clock source. User equipment should be configured to internal clock. **Adaptive Timing** –This technique maintains a pre-defined fill level in the Circuit Emulation Re-assembly buffer to control the timing output to user equipment. This method of timing recovery does not require a Synchronous ATM network and is used in applications where network wide synchronization is not available. **(Synchronous) Network**-This method of clock recovery derives timing from the ATM Network and propagates it to the CE Service Interface. The ATM network must be synchronized to a single source clock. User equipment should be configured to recover timing from the Broadmore 1700 CE service interface. **(Synchronous) Loop**-The Broadmore 1700 CE interface will derive clock from the attached DS3 user equipment and transmit from the CE interface at that rate. The user equipment should be configured for Internal timing if the Broadmore 1700 CE service interface is configured for Synchronous loop. **BITS**- (Building Integrated Timing Supply)- distributes standard timing to equipment within the central office. The Broadmore 1700 accepts BITS via either NIM IOM. The fallback for the primary BITS clock is the other BITS clock. The fallback for no BITS is the internal clock of the NIM.

Item	Options	Comments
Network RAI	**Auto** **X-bits 1** **X-bits 0**	Indication (RAI) configuration. Allows user configuration of the X-bits associated with C-bit parity framing. Auto makes it transparent; the other choices set the X-bits to either 1 or 0.
Service RAI	**Auto** **X-bits 1** **X-bits 0**	Indication (RAI) configuration. Allows user configuration of the X-bits associated with C-bit parity framing. Auto makes it transparent; the other choices set the X-bits to either 1 or 0.

Table 7-3: Unstructured DS3 SAM Diagnostics Configuration

Item	Options	Comments
Automatic FEAC Alarms	**Activate/Deactivate**	Activates or deactivates Far End Alarm and Control Channel (FEAC) alarms. FEAC alarms can only be active when the port is configured for C-bit parity framing. Activate to detect and transmit RAI as applicable and detect FEAC channel activate/deactivate commands
Network FEAC Loopback	**Activate/Deactivate**	Activate sends a FEAC command to the far end network equipment to go into network loopback. Deactivate sends a FEAC command to go out of network loopback. Only active when port is configured for C-bit parity. The receive code generated is DS3 Out of Frame (0000000).
Service FEAC Loopback	**Activate/Deactivate**	Activate sends a FEAC command to the far end service equipment to go into service loopback. Deactivate sends a FEAC command to go out of service loopback. Only active when port is configured for C-bit parity.
Network BERT Test	**Activate/Deactivate**	BERT test can only be performed when the port is configured for C-bit parity framing. Causes the port to generate a $2e^{23}$ pseudo-random test pattern to the ATM network.
Service BERT Test	**Activate/Deactivate**	Same as network BERT test except it goes to the service equipment. These tests can be monitored from CAMMI following the selection sequence: *system management → monitor activity →slot statistics→ DS3 SAM → Port # → Port Counters*

Item	Options	Comments
Network AIS	**Activate/Deactivate**	Sends Alarm Indication Signal to the network when activated.
Service AIS	**Activate/Deactivate**	Sends Alarm Indication Signal to the connected local service equipment when activated.
Loopback	**Normal** **Local** **Remote**	Normal is no loopback. Local sets a service side loopback (DS3) on the port. Remote sets a network side loopback (ATM) on the port. See diagram "Loopback Options" on page 5-20

Table 7-4: Unstructured DS3 SAM Alarm Configuration

Network Alarms	Options	Service Alarms
Cell Starvation	**Ignore/Major/Minor**	LOS
LOF	**Ignore/Major/Minor**	LOF
AIS	**Ignore/Major/Minor**	AIS
Idle	**Ignore/Major/Minor**	Idle
RAI	**Ignore/Major/Minor**	RAI
FEAC	**Ignore/Major/Minor**	FEAC
Sequence Errors	**Ignore/Major/Minor**	Line Code Violation
Excessive SNP Errors	**Ignore/Major/Minor**	Excessive SNP Errors
Excessive F-bit Errors	**Ignore/Major/Minor**	Excessive F-bit Errors
Excessive Parity Errors	**Ignore/Major/Minor**	Excessive Parity Errors
Excessive C-bit Errors	**Ignore/Major/Minor**	Excessive C-bit Errors
Excessive FEBE Errors	**Ignore/Major/Minor**	Excessive FEBE Errors

Follow the sequence below to set network alarms. DS3 alarms are set on a port basis with alarm definitions as shown.

Select **System Management** ↵
Select **Configure** ↵
Select **Slot** ↵
Select **Port** of interest ↵
Select **Alarm Configuration** ↵
Press **Network Alarms** or **Service Alarms** ↵
Use the space bar to toggle to the available options and press **Esc** to save the settings.

Table 7-5: Network Alarm Definitions

Network Alarm	Definition
Cell Starvation	Cell Starvation indicates there are no cells being received from the network side.
LOF	Loss Of Framing indicates that the framing alignment of the signal coming into the Broadmore 1700 from the ATM side has been lost.
AIS	This alarm indicates an Alarm Indication Signal is being received from the network side. When a network element receives a loss of signal, it is supposed to propagate an AIS alarm on its output. If this alarm is active, then an AIS alarm is being propagated to it. An AIS alarm is a validly framed DS3 signal consisting of a repeated 1010 data pattern.
Idle	An idle alarm means that an idle signal (validly framed DS3 signal with a repeated 1100 signal) is being detected on the network side.
RAI	The Remote Alarm Indicator (also known as a Yellow Alarm) is transmitted by setting the X bits to zero. This particular alarm indicates that a Yellow alarm has been sent across the ATM network and is being received by this DS3 port. In the DS3 port configuration screen, you can select the Network and Service side RAI as Auto, 1, or 0. Selecting “0” will cause the network RAI alarm to be activated, if the user has not selected to Ignore it.
FEAC	Far End Alarm and Control Channel.

Network Alarm	Definition
Sequence Errors	This alarm indicates that frames are out of sequence as they arrive at the DS3 port.
Excessive SNP Errors	SNP Errors are errors that occur in the Sequence Number Parity portion of the DS3 frame
Excessive F-bit Errors	The Excessive F-bit Errors alarm is triggered when the DS3 port receives F-bit errors at a rate of 1×10^{-4}
Excessive Parity Errors	The Excessive Parity Errors alarm will be triggered when the DS3 port receives parity errors at a rate of 1×10^{-4}
Excessive C-bit Errors	The Excessive C-bit Errors alarm will be triggered when the DS3 port receives C-bit errors at a rate of 1×10^{-4}
Excessive FEBE Errors	The Excessive FEBE (Far End Block Error) alarm is triggered when the DS3 port receives FEBEs at a rate of 1×10^{-4}

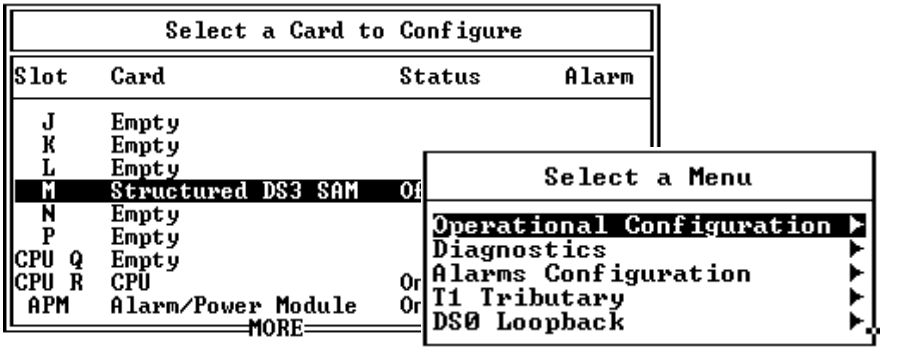
Table 7-6: Service Alarm Definitions

Service Alarm	Definition
LOS	Loss Of Signal indicates that there is no signal being input to the DS3 from the service side.
LOF	Loss of Framing indicates that the framing alignment of the signal coming into the Broadmore 1700 from the ATM side has been lost.
AIS	This alarm indicates that the DS3 port is receiving an Alarm Indication Signal from the attached equipment. AIS is a validly framed DS3 signal consisting of a repeated 1010 data pattern.
Idle	An idle alarm means that an idle signal (validly framed DS3 signal with a repeated 1100 signal) is being detected on the service side.
RAI	The Remote Alarm Indicator (also known as a Yellow Alarm) is transmitted by setting the X bits to zero. In this instance, the service side equipment is transmitting the RAI to the DS3 port.
FEAC	Far End Alarm and Control Channel.

Service Alarm	Definition
Line Code Violation	This alarm indicates that a long string of zeros is being received by the DS3 port from any attached equipment.
Excessive F-bit Errors	The Excessive F-bit Errors alarm is triggered when the DS3 port receives F-bit errors at a rate of 1×10^{-4}
Excessive Parity Errors	The Excessive Parity Errors alarm will be triggered when the DS3 port receives parity errors at a rate of 1×10^{-4}
Excessive C-bit Errors	The Excessive C-bit Errors alarm will be triggered when the DS3 port receives C-bit errors at a rate of 1×10^{-4}
Excessive FEBE Errors	The Excessive FEBE (Far End Block Error) alarm is triggered when the DS3 port receives FEBEs at a rate of 1×10^{-4}

Structured DS3 SAM

Choose the slot containing the structured DS3 SAM to be configured to display a screen for port selection. The table below is a guide to configuration parameters. Operational, Diagnostics, Alarm, T1 Tributary, and DS0 configuration are the menu options. Descriptions of the configurable items are found in the following tables. Highlight each item and use the space bar to toggle available options for each, and then save the configuration after making changes.



Use the following steps for configuring the SDS3.

Select **System Management** ↵
Select **Configure** ↵
Select **Slot** ↵
Select **Structured DS3 SAM** ↵
Select **one** of the following:
- *** Diagnostics** ↵
- *** T1 Tributary** ↵
- *** DS0 Loopback** ↵
- *** Operational Configuration** ↵
- *** Alarms Configuration** ↵

Use the space bar to toggle to the available options and press **Esc** to save the settings.

Table 7-7*: *Structured DS3 SAM Operational Configuration

Item	Options	Description
Port Name		A descriptive field to identify the port
Port Mode	**On-line** **Off-line**	This is a status field that can be toggled to offline, in which case the port will not be available to make calls and passive SVCs are refused.
Framing	**C-bit** **M13**	**C-bit** is a framing mode using DS2 stuff bits associated with M13 multiplexing for other purposes such as Far End Alarm Control (FEAC) Channel. **M13** is a mode that maps 28 DS1s directly into the DS3. The DS1s do not exist independently as is the case when M23 multiplexing is used.
Clock Mode	**Network** **BITS-Clock** **Loop**	**(Synchronous) Network**-This method of clock recovery derives timing from the ATM Network and propagates it to the CE Service Interface. The ATM network must be synchronized to a single source clock. User equipment should be configured to recover timing from the Broadmore 1750 CE service interface. **BITS-Clock** (Building Integrated Timing Supply)-distributes standard timing to equipment within the central office. The Broadmore 1750 accepts BITS via either NIM IOM. The fallback for the primary BITS clock is the other BITS clock. The fallback for no BITS is the internal clock of the NIM. **(Synchronous) Loop**-The Broadmore 1750 CE interface will derive clock from the attached SDS3 user equipment and transmit from the CE interface at that rate. The user equipment should be configured for Internal timing if the Broadmore 1750 CE service interface is configured for Synchronous loop.
Loopback	**Normal** **Local** **Remote**	Normal Mode is no loopback. Local Line Loopback sets a loopback to the service equipment.Remote Loopback sets a loopback to the ATM network.
Service RAI	**Auto** **X-bits 1** **X-bits 0**	Indication (RAI) configuration. Allows user configuration of the X-bits associated with C-bit parity framing. Auto makes it transparent; the other choices set the X-bits to either 1 or 0.

Table 7-8: Structured DS3 SAM Diagnostics Configuration

Item	Options	Description
Port Name		A descriptive field to identify the port
Port Mode	**On-line** **Off-line**	This is a status field that can be toggled to offline, in which case the port will not be available to make calls and passive SVCs are refused.
Framing	**C-bit** **M13**	**C-bit** is a framing mode using DS2 stuff bits associated with M13 multiplexing for other purposes such as Far End Alarm Control (FEAC) Channel. **M13** is a mode that maps 28 DS1s directly into the DS3. The DS1s do not exist independently as is the case when M23 multiplexing is used.
Clock Mode	**Network** **BITS-Clock** **Loop**	**(Synchronous) Network**-This method of clock recovery derives timing from the ATM Network and propagates it to the CE Service Interface. The ATM network must be synchronized to a single source clock. User equipment should be configured to recover timing from the Broadmore 1750 CE service interface. **BITS-Clock** (Building Integrated Timing Supply)-distributes standard timing to equipment within the central office. The Broadmore 1750 accepts BITS via either NIM IOM. The fallback for the primary BITS clock is the other BITS clock. The fallback for no BITS is the internal clock of the NIM. **(Synchronous) Loop**-The Broadmore 1750 CE interface will derive clock from the attached SDS3 user equipment and transmit from the CE interface at that rate. The user equipment should be configured for Internal timing if the Broadmore 1750 CE service interface is configured for Synchronous loop.
Loopback	**Normal** **Remote**	Normal Mode is no loopback. Remote Loopback sets a loopback to the service side.
Service RAI	**Auto** **X-bits 1** **X-bits 0**	Indication (RAI) configuration. Allows user configuration of the X-bits associated with C-bit parity framing. Auto makes it transparent; the other choices set the X-bits to either 1 or 0.

Item	Options	Description
Automatic FEAC Alarms	**Activate/Deactivate**	Activates or deactivates Far End Alarm and Control Channel (FEAC) alarms. FEAC alarms can only be active when the port is configured for C-bit parity framing. Activate to detect and transmit RAI as applicable and detect FEAC channel activate/deactivate commands
Service FEAC Loopback	**Activate/Deactivate**	Activate sends a FEAC command to the far end service equipment to go into service loopback. Deactivate sends a FEAC command to go out of service loopback. Only active when port is configured for C-bit parity.
Service AIS	**Activate/Deactivate**	Sends Alarm Indication Signal to the connected local service equipment when activated.

Table 7-9: Structured DS3 SAM Alarms

Service Alarms	Options
LOS	**Ignore/Major/Minor**
LOF	**Ignore/Major/Minor**
AIS	**Ignore/Major/Minor**
Idle	**Ignore/Major/Minor**
RAI	**Ignore/Major/Minor**
FEAC	**Ignore/Major/Minor**
Line Code Violation	**Ignore/Major/Minor**
Excessive F-bit Errors	**Ignore/Major/Minor**
Excessive Parity Errors	**Ignore/Major/Minor**
Excessive C-bit Errors	**Ignore/Major/Minor**
Excessive FEBE Errors	**Ignore/Major/Minor**

Follow the sequence below to set service alarms. DS3 alarms are set on a port basis with alarm definitions as shown.

Select **System Management** ↵
Select **Configure** ↵
Select **Slot** ↵
Select **Structured DS3 SAM** ↵
Select **Alarms Configuration** ↵
Select from the list of **Alarms** ↵
Use the space bar to toggle to the available options and press **Esc** to save the settings.

Table 7-10: Structured DS3 Service Alarm Definitions

Service Alarm	Definition
LOS	Loss Of Signal indicates that there is no signal being input to the DS3 from the service side.
LOF	Loss of Framing indicates that the framing alignment of the signal coming into the Broadmore 1750 from the ATM side has been lost.
AIS	This alarm indicates that the DS3 port is receiving an Alarm Indication Signal from the attached equipment. AIS is a validly framed DS3 signal consisting of a repeated 1010 data pattern.
Idle	An idle alarm means that an idle signal (validly framed DS3 signal with a repeated 1100 signal) is being detected on the service side.
RAI	The Remote Alarm Indicator (yellow alarm) is transmitted by setting the X bits to zero. In this instance, the service side equipment is transmitting the RAI to the DS3 port.
FEAC	Far End Alarm and Control Channel.
Line Code Violation	This alarm indicates that a long string of zeros is being received by the DS3 port from any attached equipment.

Service Alarm	Definition
Excessive F-bit Errors	The Excessive F-bit Errors alarm is triggered when the DS3 port receives F-bit errors at a rate of 1 x 10^{-4}
Excessive Parity Errors	The Excessive Parity Errors alarm will be triggered when the DS3 port receives parity errors at a rate of 1 x 10^{-4}
Excessive C-bit Errors	The Excessive C-bit Errors alarm will be triggered when the DS3 port receives C-bit errors at a rate of 1 x 10^{-4}
Excessive FEBE Errors	The Excessive FEBE (Far End Block Error) alarm is triggered when the DS3 port receives FEBEs at a rate of 1 x 10^{-4}

Table 7-11: Structured DS3 SAM DS1 Tributary Configuration

Item	Options	Description
Timing Recovery Service Clocking Mode	**SRTS Timing** **Synchronous Network** **Synchronous Loop**	Each option specifies a method of clock recovery that will be used for all recovery circuits on the port. **NOTE: SRTS is a proprietary timing algorithm and may ONLY be used with specific written prior permission from Carrier Access Corporation. Additional license fees may apply.**
Loopback	**Normal** **Remote**	Normal Mode is no loopback. Remote Loopback sets a loopback to the service side.

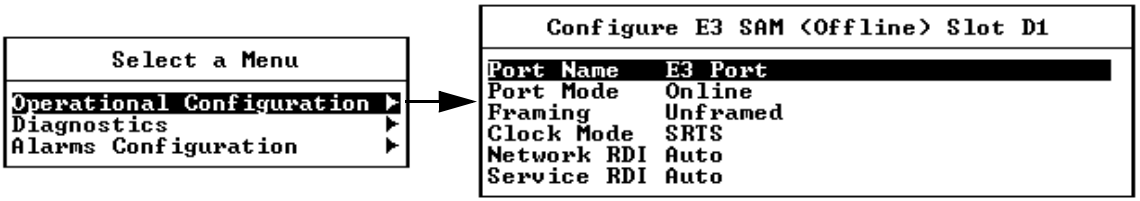
Item	Options	Description
CBR Service Type	**Structured No CAS** **Structured with CAS** **Unstructured**	Structured No CAS allows DS0 (fractional) allocation without Channel Associated Signalling (CAS). Structured with CAS allows DS0 allocation with CAS enabled, using robbed-bit signalling. Unstructured assigns all the timeslots to one VP/VC. Structured No CAS and Structured with CAS can assign a timeslot or group of timeslots to a VP/VC. Unstructured allocates all 24 DS0s to the DS1, using the entire DS1 bandwidth regardless of data content.
Frame Type	**Unframed** **Extended Superframe** **Superframe**	No framing occurs. Superframe groups 12 DS1 frames together. Extended Superframe groups 24 DS1 frames together. The equipment attached must be set to the same frame type as chosen here.
BERT	**Off** **21e-11 PRBS** **21e-15 PRBS** **21e-20 PRBS** **21e-23 PRBS**	BERT test can only be performed when the port is configured for C-bit parity framing. This causes the port to generate pseudo-random test patterns to the service side DS3 physical connection.

Table 7-12: Structured DS3 SAM DS0 Loopback Tributary Configuration

Item	Options	Description
DS0-0 (0-23)	**Normal** **Remote**	Normal Mode is no loopback. Remote Loopback sets a loopback to the service side.

Unstructured E3-3 SAM

Choose the slot containing the Unstructured E3 SAM to be configured to display a screen for port selection. The table below is a guide to configuration parameters. Operational, Diagnostics, and Alarm configuration are the three menu options. Descriptions of the configurable items are found in the following tables. Highlight each item and use the space bar to toggle available options for each. Save the configuration after making changes.



The next three pages show the options available for each item, separated by operational configuration, diagnostics, and alarm configuration.

Table 7-13: Unstructured E3-3 SAM Operational Configuration

Item	Options	Comments
Port Name		A descriptive field to identify the port
Port Mode	**On-line** **Off-line**	This is a status field that can be toggled to **off-line,** in which case the port will not be available to make calls and passive SVCs are refused.
Framing	**G.751** **G.832** **Unframed**	**G.751** is a European framing standard used for PDH applications. **G.832** is a European framing standard set by the ITU for transporting SDH elements on PDH network. **Unframed** requires a 44.736 Mbps input.
Clock Mode	**SRTS** **Adaptive** **Network** **BITS Clock** **Loop**	**NOTE: SRTS is a proprietary timing algorithm and may ONLY be used with specific written prior permission from Carrier Access Corporation. Additional license fees may apply.** **SRTS** measures the Service Clock input frequency against a network-wide ATM synchronization clock and sends the difference signals in the AAL1 header to the destination Broadmore 1750 circuit emulation interface. The different signals are then combined with the network-wide ATM synchronization clock to re-create the input service clock. If more than one ATM clock synchronization is present in the network, an alternate timing recovery method must be selected. For this method to work, the ATM network must be synchronized to a single network-wide clock source. User equipment should be configured to internal clock. **Adaptive Timing** maintains a pre-defined fill level in the Circuit Emulation Re-assembly buffer to control the timing output to user equipment. This method of timing recovery does not require a Synchronous ATM network and is used in applications where network wide synchronization is not available. **(Synchronous) Network** method of clock recovery derives timing from the ATM Network and propagates it to the CE Service Interface. The ATM network must be synchronized to a single source clock. User equipment should be configured to recover timing from the Broadmore 1750 CE service interface. **(Synchronous) Loop** CE interface will derive clock from the attached E3 user equipment and transmit from the CE interface at that rate. The user equipment should be configured for Internal timing if the Broadmore 1750 CE service interface is configured for Synchronous loop. **BITS-** (Building Integrated Timing Supply) distributes standard timing to equipment within the central office. The Broadmore 1750 accepts BITS via either NIM IOM. The fallback for the primary BITS clock is the other BITS clock. The fallback for no BITS is the internal clock of the NIM.

Item	Options	Comments
Network RDI	**Auto** **X-bits 1** **X-bits 0**	A Remote Defect Indication (RDI) is LOS or LOF detected on the attached equipment of the network side. **Auto** sets the RDI to automatically reflect whether or not an error is present. **1** sets an error to occur whether one is present or not. **0** indicates no errors even if one is present.
Service RDI	**Auto** **X-bits 1** **X-bits 0**	A Remote Defect Indication (RDI) is LOS or LOF detected on the attached equipment of the network side. **Auto** sets the RDI to automatically reflect whether or not an error is present. **1** sets an error to occur whether one is present or not. **0** indicates no errors even if one is present.

Table 7-14: Unstructured E3-3 SAM Diagnostics Configuration

Item	Options	Comment
Network BERT Test	**Activate/Deactivate**	BERT test can only be performed when the port is configured for C-bit parity framing. Causes the port to generate a $2e^{23}$ pseudo-random test pattern to the ATM network.
Service BERT Test	**Activate/Deactivate**	Same as network BERT test except it goes to the service equipment. These tests can be monitored from CAMMI following the selection sequence: *system management* → *monitor activity* →*slot statistics*→ *E3 SAM* → *Port #* → *Port Counters*
Network AIS	**Activate/Deactivate**	Sends Alarm Indication Signal to the network when activated.
Service AIS	**Activate/Deactivate**	Sends Alarm Indication Signal to the connected local service equipment when activated.
Loopback	**Normal** **Local** **Remote**	Normal is no loopback. Local sets a service side loopback (E3) on the port. Remote sets a network side loopback (ATM) on the port. See diagram “Loopback Options” on page 5-20

Table 7-15: Unstructured E3-3 SAM Alarm Configuration

Network Alarms	Options	Service Alarms
Cell Starvation	**Ignore/Major/Minor**	LOS
LOF	**Ignore/Major/Minor**	LOF
AIS	**Ignore/Major/Minor**	AIS
RDI	**Ignore/Major/Minor**	RDI
Sequence Errors	**Ignore/Major/Minor**	Line Code Violation
Excessive SNP Errors	**Ignore/Major/Minor**	Excessive F-bit Errors
Excessive F-bit Errors	**Ignore/Major/Minor**	Excessive Parity Errors
Excessive Parity Errors	**Ignore/Major/Minor**	Excessive FEBE Errors
Excessive FEBE Errors	**Ignore/Major/Minor**	

Follow the sequence below to set network alarms. E3 alarms are set on a port basis with alarm definitions as shown.

Select **System Management** ↵
Select **Configure** ↵
Select **Slot** with DS3 ↵
Select **Port** of interest ↵
Select **Alarm Configuration** ↵
Select **Network Alarms** ↵
Adjust settings using the spacebar ↵
Select **Escape** and save settings as desired ↵
Press **Service Alarms** ↵
Repeat the procedure to set and save Service Alarms ↵

Table 7-16: Unstructured E3-3 SAM Network Alarms

Network Alarm	Definition
Cell Starvation	Cell Starvation indicates there are no cells being received from the network side.
LOF	Loss Of Framing indicates that the framing alignment of the signal coming into the Broadmore 1750 from the ATM side has been lost.
AIS	This alarm indicates an Alarm Indication Signal is being received from the network side. When a network element receives a loss of signal, it is supposed to propagate an AIS alarm on its output. If this alarm is active, then an AIS alarm is being propagated to it. An AIS alarm is a validly framed E3 signal consisting of a repeated 1010 data pattern.
Idle	An idle alarm means that an idle signal (validly framed E3 signal with a repeated 1100 signal) is being detected on the network side.
RAI	The Remote Alarm Indicator (also known as a Yellow Alarm) is transmitted by setting the X bits to zero. This particular alarm indicates that a Yellow alarm has been sent across the ATM network and is being received by this E3 port. In the E3 port configuration screen, you can select the Network and Service side RAI as Auto, 1, or 0. Selecting “0” will cause the network RAI alarm to be activated, if the user has not selected to Ignore it.
FEAC	Far End Alarm and Control Channel.
Sequence Errors	This alarm indicates that frames are out of sequence as they arrive at the E3 port.
Excessive SNP Errors	SNP Errors are errors that occur in the Sequence Number Parity portion of the E3 frame
Excessive F-bit Errors	The Excessive F-bit Errors alarm is triggered when the E3 port receives F-bit errors at a rate of 1×10^{-4}
Excessive Parity Errors	The Excessive Parity Errors alarm will be triggered when the E3 port receives parity errors at a rate of 1×10^{-4}
Excessive C-bit Errors	The Excessive C-bit Errors alarm will be triggered when the E3 port receives C-bit errors at a rate of 1×10^{-4}
Excessive FEBE Errors	The Excessive FEBE (Far End Block Error) alarm is triggered when the E3 port receives FEBEs at a rate of 1×10^{-4}

Table 7-17: Unstructured E3-3 SAM Service Alarms

Service Alarm	Definition
LOS	Loss Of Signal indicates that there is no signal being input to the E3 from the service side.
LOF	Loss of Framing indicates that the framing alignment of the signal coming into the Broadmore 1750 from the ATM side has been lost.
AIS	This alarm indicates that the E3 port is receiving an Alarm Indication Signal from the attached equipment. AIS is a validly framed E3 signal consisting of a repeated 1010 data pattern.
Idle	An idle alarm means that an idle signal (validly framed E3 signal with a repeated 1100 signal) is being detected on the service side.
RAI	The Remote Alarm Indicator (also known as a Yellow Alarm) is transmitted by setting the X bits to zero. In this instance, the service side equipment is transmitting the RAI to the E3 port.
FEAC	Far End Alarm and Control Channel.
Line Code Violation	This alarm indicates that a long string of zeros is being received by the E3 port from any attached equipment.
Excessive F-bit Errors	The Excessive F-bit Errors alarm is triggered when the E3 port receives F-bit errors at a rate of 1×10^{-4}
Excessive Parity Errors	The Excessive Parity Errors alarm will be triggered when the E3 port receives parity errors at a rate of 1×10^{-4}
Excessive C-bit Errors	The Excessive C-bit Errors alarm will be triggered when the E3 port receives C-bit errors at a rate of 1×10^{-4}
Excessive FEBE Errors	The Excessive FEBE (Far End Block Error) alarm is triggered when the E3 port receives FEBEs at a rate of 1×10^{-4}

PVC Connection

Follow the selection process shown below to add a new PVC. The **Establish a PVC Call** screen appears for data entry.

Select **System Management** ↵
Select **Configure** ↵
Select **Configure PVC** ↵
Select **Insert** (shift +:) ↵

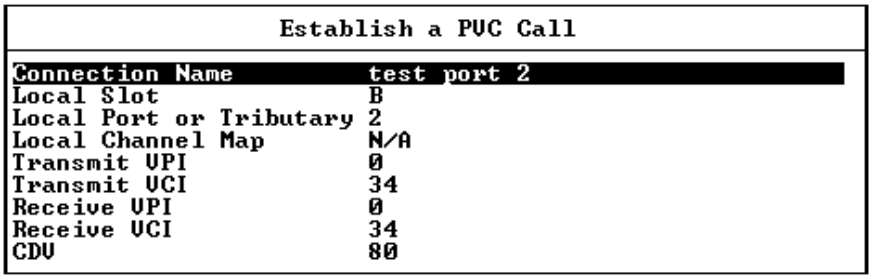


Table 7-18: PVC Configuration Items

Item	Definition
Connection Name	Press the space bar to select Connection Name and type a descriptive identifier (For example, **test port 2**).
Local Slot	The Local Slot is the chassis slot.
Local Port Number	Port number depends on the configuration.
Local Channel Map	Channel map depends on the configuration. Channel map only applies to the Structured DS3 SAMs. There is **no** channel mapping for the Unstructured DS3 or Unstructured E3, and this value will be displayed as N/A.
VP/VC (Transmit/ Receive)	The maximum settings for VP/VC are allocated using the Max VP/VC feature in System Services (see *"Max VP/VC" on page 7-20*). Table 7-1 on page 7-20 shows the valid VP/VC values.
CDV	Cell Delay Variation (CDV) is the difference between the expected arrival time and the actual arrival time of the next cell. This value is expressed in number of cells. The value can vary from 0 to 255. An initial value of 80 to 100 cells is recommended.

The VPI/VCI are locally significant and need to match on both ends of the PVC. Therefore the VPI/VCI must be provisioned identically on the ATM switch port.

NOTE: The transmit and receive VPI/VCI must be configured through the ATM switch. The procedure for this will vary by switch. Consult the ATM switch documentation to accomplish this configuration.

SVC Connection

Follow the selection process shown below to add a new SVC. The **Establish a Call** screen appears for data entry as shown below.

Select **System Management** ↵
Select **Configure** ↵
Select **Configure SVC** ↵

```
LINK UP                    SVC Connection Table Editor                    12
UniquePart              ¦--Local---¦ ¦-FarEnd--¦          Cause
DestAddr      State     CrdPrt Chan  CrdPrt Chan  VP/VC  Code Name

00807CFFEC23 Rel'd    D 5 00FFF000 D 5 FFF00000  0/   0  38 DS1 trib 5
00807CFFEA23 Active   D 7 00FFFFFF --- --------  0/ 191   0
```

From here, use the ***Insert*** (or ***shift:***) key to access the input screen below.

```
                          Establish a Call

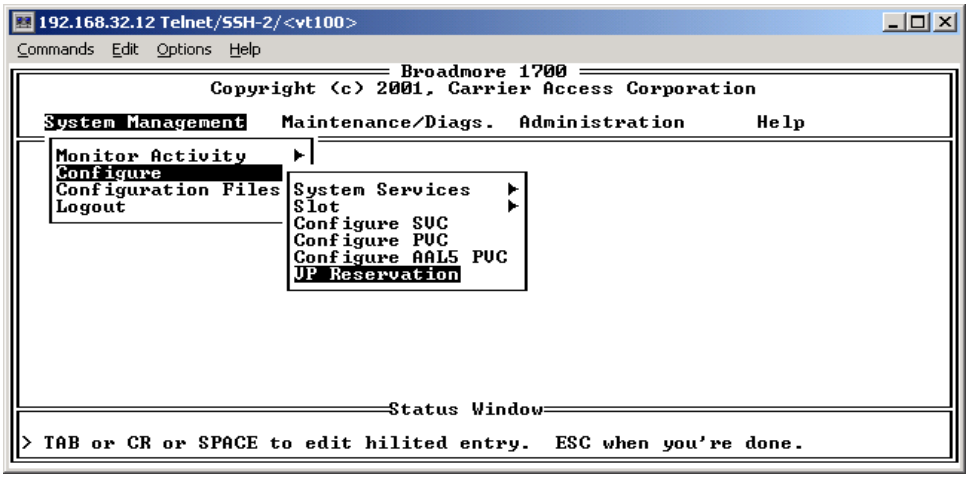
Connection Name           DS1 trib 5
Local Slot                D
Local Port or Tributary   5
Local Channel Map         ---------xxxxxxxxxxxxxxxxxxxxxxxx
Destination ATM Address   47000580FFE1000000F21A880900807CFFEC2300
Remote Slot               D
Remote Port or Tributary  5
Remote Channel Map        11111111111100000000000000000000
CDV                       80
```

Item	Definition
Connection Name	Press the space bar to select Connection Name and type a descriptive identifier (For example, **test port 2**).
Local Slot	The Local Slot is the chassis slot.
Local Port Number	The Port number depends on the configuration.
Local Channel Map	The Channel map depends on the configuration. Channel map only applies to the Structured DS3 SAMs. There is **no** channel mapping for the Unstructured DS3 and Unstructured E3 SAMs, and this value will be displayed as N/A.
VP/VC (Transmit/ Receive)	The maximum settings for VP/VC are allocated using the Max VP/VC feature in System Services (see *"Max VP/VC" on page 7-20*). Table 7-1 on page 7-20 shows the valid VP/VC values.
Destination ATM Address	Enter the Destination ATM address. To view the ATM Address List, enter**?**.
Remote Slot	The Remote Slot is the chassis slot of the remote unit.
Remote Port Number or Tributary	The Remote Port Number or Tributary depends on the configuration.
Remote Channel Map	The Remote Channel Map depends on the configuration.
CDV	Cell Delay Variation (CDV) is the difference between the expected arrival time and the actual arrival time of the next cell. This value is expressed in number of cells. The value can vary from 0 to 255. An initial value of 80 to 100 cells is recommended.

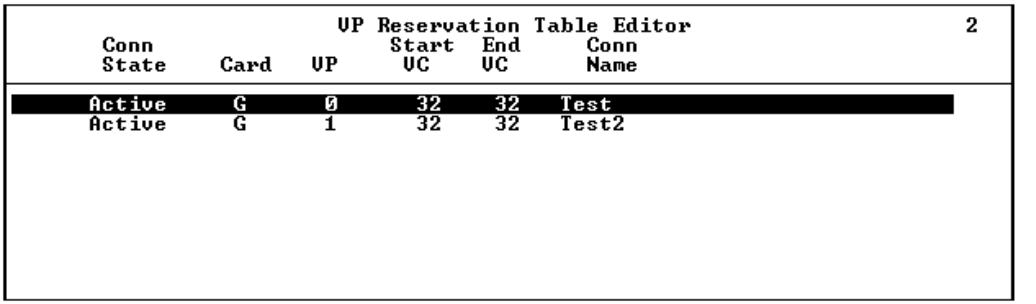
VP Reservation

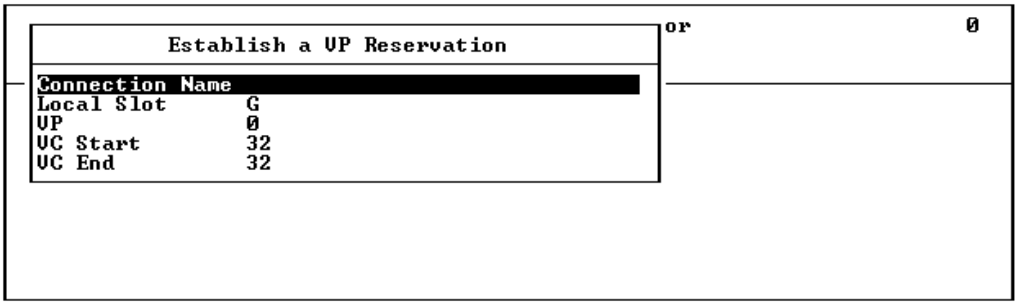
NOTE: The functionality described in this section is only available with Broadmore release 4.6 (or higher). To support this functionality, all ATM DS3, CBI, HSSI-CBI, OC-3c, or OC-12c modules in the chassis must be upgraded to the levels released with 4.6 (or higher). Firmware and instructions are provided on the upgrade CD.

VP Reservation allows you to reserve a block of up to 65,535 virtual channels (VCs) within a virtual path (VP). With this feature, you can set a VC range on a particular VP without having to set up all of the VC connections individually. You can define up to 40 VPs for reservation. This feature is available only on the ATM DS3, CBI, and HSSI-CBI modules.



The VP Reservation Table Editor is shown below. Press the Enter key to edit or clear an existing connection or create a new connection, then follow the on-screen instructions.





VP Reservation settings are described on the following page.

Item	Comments
Connection Name	Press the space bar to select Connection Name and type a descriptive identifier (For example, **test port 2**).
Local Slot	The Local Slot is the chassis slot.
VP	The range is 0 to one less than the value set for maximum VPs (see *"Max VP/VC" on page 7-20* for valid values). If the Max VP/VC value is set to 2/65536, the VP number must be set to 0; a value of 1 is invalid. **NOTE:** A maximum of 40 VPs can be defined for reservation.
VC Start	The default range is 32 to the value set for maximum VCs (see *"Max VP/VC" on page 7-20* for valid values). VC numbers can start at 1 if the VP is not set to 0.
VC End	The default range is 32 to the value set for maximum VCs (see *"Max VP/VC" on page 7-20* for valid values). VC numbers can start at 1 if the VP is not set to 0.

System Configuration

- Save Configuration ... *7-70*
- Restore Configuration ... *7-71*
- Delete Configuration ... *7-71*
- Set Power-on Default ... *7-72*
- Save Card Defaults ... *7-72*
- Restore Card Defaults ... *7-72*

The system configuration is quickly accessed via the configuration files as shown below. There is a special option to save a configuration for powerup. This configuration will automatically load with the application of power to the Broadmore 1750 after a power interruption.

Select **Save Configuration** to save the current configuration and choose an appropriate file name when asked. This should be done after each significant configuration change so that the configuration can be quickly re-established at a later time.

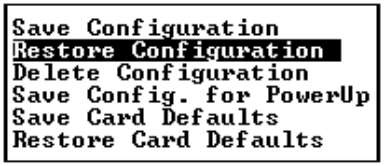
Save Configuration

Follow the selection sequence below to save the current configuration. Enter an appropriate file name (for example: 17may3pm). This file can then be used to return to the current system configuration.

Select **System Management** ↵
Select **Configuration Files** ↵
Select **Save Configuration** ↵

Restore Configuration

Select **Restore Configuration** to restore a previously saved configuration as shown below.



The Restore Configuration results in the tear-down of all calls, configuration of all modules, and establishment of all calls found in the named configuration. The UNI must be UP to restore a configuration file containing one (or more) SVC. Follow the sequence below to check UNI status. If necessary, configure UNI before restoring the configuration.

Select **System Management** ↵
Select **Monitor Activity** ↵
Select **Connections** ↵
Select **UNI Status** ↵

Delete Configuration

Follow the selection sequence below to delete the current configuration. Answer Yes to the confirmation notice. Use caution as this configuration cannot be restored once it has been deleted

Select **System Management** ↵
Select **Configuration Files** ↵
Select **Delete Configuration** ↵

Set Power-on Default

Select **Save Config. for PowerUp** to save a particular configuration for system power-up. Select **Save Config. for PowerUp** as shown below to retain the current configuration for PowerUp.

Select **System Management** ↵
Select **Configuration Files** ↵
Select **Save Config. For PowerUp** ↵

Save Card Defaults

Select **Save Card Defaults** to save the default configuration for the specific card.

Select **System Management** ↵
Select **Configuration Files** ↵
Select **Save Card Defaults** ↵
Select **Slot** ↵
Select **'Yes' to save the defaults** ↵

Restore Card Defaults

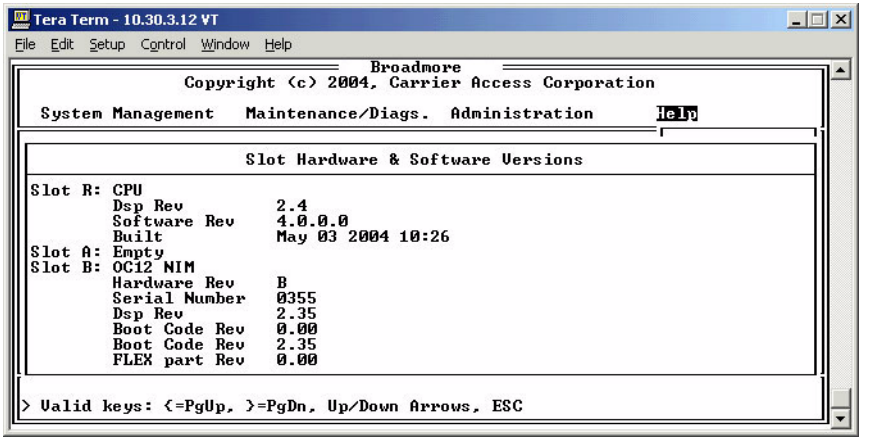
Select **Restore Card Defaults** to restore the default configuration for the specific card. This selection causes the following actions:

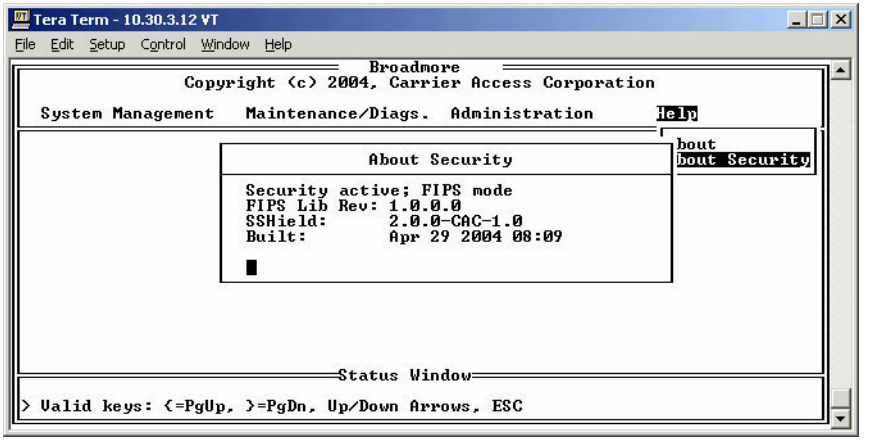
- Deletes all existing connections
- Reads the configuration file and restores the card port settings
- Reads the configuration file again and sets up any SVC/PVCs

Select **System Management** ↵
Select **Configuration Files** ↵
Select **Restore Card Defaults** ↵
Select **Slot** ↵
Select **'Yes' to restore the card defaults** ↵

Help

The Help main menu item has two pull-down items: *About* and *About Security*. Choose *About* to obtain the hardware and software version data. This information is important when contacting customer service. Choose *About Security* to display the security mode and software version numbers.





CHAPTER 8

Maintenance and Troubleshooting

In this Chapter

- Statistics ... *8-2*
- Troubleshooting ... *8-15*
- Repair/Replacement ... *8-30*
- General Maintenance ... *8-39*
- Summary of Front Panel LEDs ... *8-44*

Statistics

- Chassis Statistics ... *8-2*
- OC-12c/STM-4c NIM Statistics ... *8-3*
- Alarm Overview ... *8-4*
- Slot Statistics for NIM/SAM Cards ... *8-4*
- 24-Hour Statistics ... *8-13*
- PLOA/AAL5 Statistics ... *8-14*

Statistics are available to monitor the Broadmore 1750 operation at the chassis, individual module, or connection level. Thus, the statistics provide a good initial indication of performance and a means to isolate any problems that may arise.

Chassis Statistics

Statistics are monitored by following the sequence shown below to view the chassis statistics shown.

Select **System Management** ↵
Select **Monitor Activity** ↵
Select **ATM by Chassis** ↵

```
                    Chassis ATM Cell and AAL5 Statistics

#  Rx Cells    Tx Cells    Errors      #  Rx Cells    Tx Cells    Errors
A 14602427    15258240    4734        H 0           0           0
B 0           0           0           J 0           0           0
C 0           0           0           K 0           0           0
D 422102037   422241660   0           L 0           0           0
E 0           0           0           M 0           0           0
F 0           0           0           N 0           0           0
G 0           0           0           P 0           0           0
                                      Q 322350      108060      4
Q RxPkt:  143177        TxPkt:  69175         PktTimeout: 0
Q CelDrp: 0             BadVpc: 0             SizeError:  0
Q BadCrc: 1             EopErr: 0             NonZeroGFC: 3
```

OC-12c/STM-4c NIM Statistics

Slot statistics provide specific module level information. Follow the sequence below to select an OC-12c/STM-4c and view the statistics shown on the next page.

Select **System Management** ↵
Select **Monitor Activity** ↵
Select **Slot statistics** ↵
Select **OC-12 NIM** (slot A shown) ↵

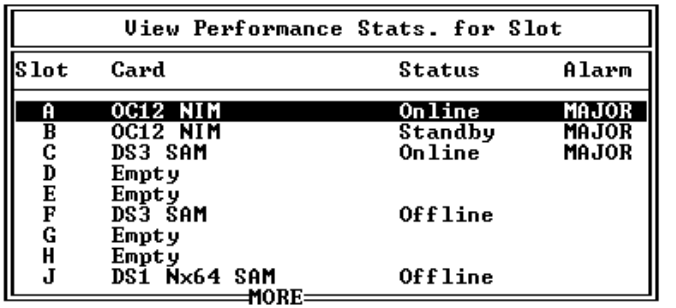
OC-12 NIM (Online) Slot A Statistics

	CV	ES	SES	SEFS/UAS	LF	SLOS
Near Section	0	21923	21923	21923		
Near Line	0	0	0	0	0	
Near Path	0	0	0	0	0	
Far Line	0	0	0	0	0	
Far Path	0	0	0	0	0	

Transmitted Cells: 0
Received Cells: 0
Uncorrected HEC Errors: 0
Corrected HEC Errors: 0
Protect Switch Count: 1 BITS A : Absent BITS B : Absent
Protect Switch Duration: 23896 Seconds: 10

Alarm Overview

When the slot selection screen (below) appears, the last column provides an alarm overview. This screen is accessed from either the monitor activity or configuration path and gives an indication for each slot of any major or minor alarm. From ***Monitor Activity***, select the slot for more detailed alarm information. From ***Configuration***, select the slot for more detailed alarm configuration information.



Slot Statistics for NIM/SAM Cards

- Unstructured DS3 and Unstructured E3 SAM Statistics ... *8-5*
- Unstructured E3 SAM Statistics ... *8-8*
- Structured DS3 SAM Statistics ... *8-9*

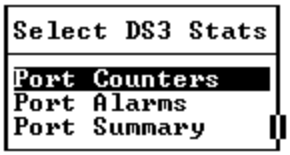
Statistics are maintained for each SAM port. The statistics for each of the ports is displayed on the following pages.

Unstructured DS3 and Unstructured E3 SAM Statistics

Operational statistics are provided in accordance with RFC 1407. Statistics for the Unstructured DS3 and Unstructured E3 are shown in separate windows below.

Unstructured DS3 Statistics

For Unstructured DS3 SAMs, the most recent 24 hours of statistical data is maintained in a separate file. This data is presented in 15-minute increments by port in spreadsheet format.



Use the following steps to view the Unstructured DS3 SAM statistics

Select **System Management** ↵
Select **Monitor Activity** ↵
Select **Slot Statistics** ↵
Select **DS3 slot** ↵
Select **Port** ↵
Select one of the following statistics to view:
- *** Port Counters**
- *** Port Alarms**
- *** Port Summary**

Statistics for the Unstructured DS3 SAM are shown below.

```
                    DS3 SAM (Online) Slot C Port 1 Counters

Tx Cells 2991263019              Rx Cells 176919

Network Errors                   Service Errors                Major Alarm YES
SEQ Errors     0                 BPV Errors     0              Minor Alarm YES
SNP Errors     0                 EXZ Errors     0
F-BIT Errors   0                 F-BIT Errors   0
PARITY Errors  0                 PARITY Errors  0
C-BIT Errors   0                 C-BIT Errors   0
FEBE Errors    0                 FEBE Errors    0
BERT Errors    0                 BERT Errors    0
```

The alarm display below has two columns to differentiate network and service errors.

```
                    DS3 SAM (Online) Slot C Port 1 Alarms

Network Cell Starvation  On       Service LOS                  On
        LOF              On               LOF                  On
        AIS              Off              AIS                  Off
        IDLE             Off              IDLE                 Off
        RAI              Off              RAI                  On
        FEAC Alarm       Off              FEAC Alarm           Off
        XS SEQ Errors    Off              Line Code Violation  On
        XS SNP Errors    Off              XS F-BIT Errors      Off
        XS F-BIT Errors  Off              XS Parity Errors     On
        XS Parity Errors Off              XS C-BIT Errors      On
        XS C-BIT Errors  Off              XS FEBE Errors       On
        XS FEBE Errors   Off
```

```
                    DS3 SAM (Online) Slot C Port 1 Summary

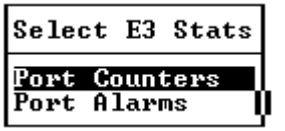
S-PES  0                    N-PES  0                 UNDER FLOW  364
S-PSES 0                    N-PSES 0                 OVER FLOW   0
S-SEFS 364                  N-SEFS 364
S-UAS  364                  N-UAS  362
S-AS   0                    N-AS   0
S-LCV  1661580              N-SNP  0
S-PCV  830790               N-PCV  0
S-CCV  830790               N-CCV  0
S-CES  0                    N-CES  0
S-CSES 0                    N-CSES 0
S-LES  362                  N-SEQ  0
Seconds Recorded 362
```

The standard error terms (such as PES for P-Bit Error Seconds) have a preceding letter, either S or N. The S represents the Service side of the DS3, and the N for the Network side. The display is divided into two columns, service and network, for clarity. Definitions are provided below for reference.

Term	Definition
AS	Available Seconds
CCV	C-bit Coding Violation
CES	C-bit Errored Seconds
CSES	C-bit Severely Errored Seconds
LCV	Line Coding Violation
LES	Line Errored Seconds
PCV	P-bit Coding Violation
PES	P-bit Errored Seconds
PSES	P-bit Severely Errored Seconds
SEFS	Severely Errored Framing Seconds
SEQ	Sequence Errors
SNP	Sequence Number parity
UAS	Unavailable Seconds

Unstructured E3 SAM Statistics

For Unstructured E3 SAMs, the most recent 24 hours of statistical data is maintained in a separate file. This data is presented in 15-minute increments by port in spreadsheet format



Use the following steps to view the Unstructured E3 SAM statistics

Select **System Management** ↵
Select **Monitor Activity** ↵
Select **Slot Statistics** ↵
Select **E3 SAM** ↵
Select **Port** ↵
Select one of the following statistics to view:
- *** Port Counters**
- *** Port Alarms**

Statistics for the Unstructured E3 SAM are shown below.

E3 SAM (Offline) Slot D Port 1 Counters

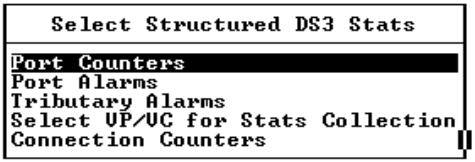
Tx Cells 75160			Rx Cells 75160		
Network Errors			Service Errors		Major Alarm NO
SEQ Errors	0		BPV Errors	0	Minor Alarm NO
SNP Errors	0		EXZ Errors	0	
F-BIT Errors	0		F-BIT Errors	0	
BIP Errors	0		BIP Errors	0	
FEBE Errors	0		FEBE Errors	0	
BERT Errors	0		BERT Errors	0	

```
                    E3 SAM (Offline) Slot D Port 1 Alarms

Network Cell Starvation  Off       Service LOS                  Off
        LOF              Off               LOF                  Off
        AIS              Off               AIS                  Off
        RDI              Off               RDI                  Off
        XS SEQ Errors    Off               Line Code Violation  Off
        XS SNP Errors    Off               XS F-BIT Errors      Off
        XS F-BIT Errors  Off               XS BIP Errors        Off
        XS BIP Errors    Off               XS FEBE Errors       Off
        XS FEBE Errors   Off
```

Structured DS3 SAM Statistics

Operational statistics are provided in accordance with RFC 1407. Counters, alarms, and a summary are shown in separate windows following the sequence below. For Structured DS3 SAMs, the most recent 24 hours of statistical data is maintained in a separate file. This data is presented in 15-minute increments by port in spreadsheet format.



Use the following steps to view the Structured DS3 SAM statistics. Statistics for the Structured DS3 SAM statistics are shown below.

Select **System Management** ↵
Select **Monitor Activity** ↵
Select **Slot Statistics** ↵
Select **Structured DS3 SAM** ↵
Select one of the following statistics to view:
* **Port Counters**
* **Port Alarms**
* **Tributary Alarms**
* **Select VP/VC for Statistics Collection**
* **Connection Counters**

```
                Structured DS3 SAM (Offline) Slot E Counters

Service Errors

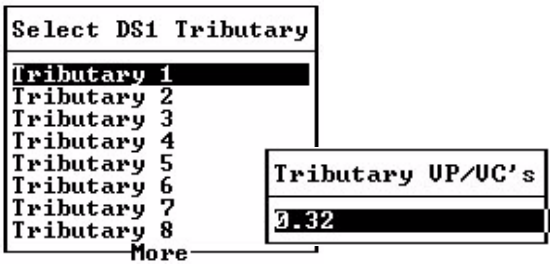
BPV Errors       0                    Major Alarm NO
EXZ Errors       0                    Minor Alarm NO
F-BIT Errors     0
PARITY Errors    0                    Tx Cells    0
C-BIT Errors     0                    Rx Cells    0
FEBE Errors      0
```

```
   Structured DS3 SAM (Offline) Slot M Alarms

LOS                    Off
LOF                    Off
AIS                    Off
IDLE                   Off
RAI                    Off
FEAC Alarm             Off
Line Code Violation    Off
XS F-BIT Errors        Off
XS Parity Errors       Off
XS C-BIT Errors        Off
XS FEBE Errors         Off
```

```
                Structured DS3 SAM (Offline) Slot M Alarm Detail

    AIS  Cell Starve      AIS  Cell Starve      AIS  Cell Starve
 1                    12                   23
 2                    13                   24
 3                    14                   25
 4                    15                   26
 5                    16                   27
 6                    17                   28
 7                    18
 8                    19
 9                    20
10                    21
11                    22
```




```
                Structured DS3 SAM (Online) Slot E VP=0 VC=32

Rx Cells:                    0   Tx Cells:                 7611
   Seq Errors:               0      Cond Cells:               0
   Snp Errors:               0      Suppressed Cells:         0
   Dropped Cells:            0
   Lost Cells:               0
   Overruns:                 0
   Ptr Reframes:             0
   Ptr Parity Errors:        0
   Misinserted Cells:        0
   Underruns:                0
```

```
                Structured DS3 SAM (Online) Slot E VP=0 VC=32

Rx Cells:                       0   Tx Cells:                    7611
   Seq Errors:                  0      Cond Cells:                  0
   Snp Errors:                  0      Suppressed Cells:            0
   Dropped Cells:               0
   Lost Cells:                  0
   Overruns:                    0
   Ptr Reframes:                0
   Ptr Parity Errors:           0
   Misinserted Cells:           0
   Underruns:                   0
```

```
              Structured DS3 SAM (Offline) Slot C Bert test detail

   SYNC       BER count      SYNC       BER count      SYNC       BER count
 1 PAT Sync       82181  12  NO Sync           0  23 PAT Sync      118501
 2  NO Sync           0  13 PAT Sync       73972  24  NO Sync           0
 3 PAT Sync       85316  14  NO Sync           0  25 PAT Sync       83267
 4  NO Sync           0  15 PAT Sync       74711  26  NO Sync           0
 5 PAT Sync       65138  16  NO Sync           0  27 PAT Sync       92485
 6  NO Sync           0  17 PAT Sync       90835  28  NO Sync           0
 7 PAT Sync       81501  18  NO Sync           0
 8  NO Sync           0  19 PAT Sync       89911
 9 PAT Sync       79214  20  NO Sync           0
10  NO Sync           0  21 PAT Sync       91917
11 PAT Sync       86540  22  NO Sync           0
```

```
                    SDS3 SAM (Offline) Slot C Port Summary

PES  0                      PSES   0
CES  0                      F-CES  213
CSES 0                      F-CSES 213
CCV  845963346              F-CCV  390728613
SEFS 0
LCV  1463724225
PCV  75245484
LES  213
UAS  213                    F-UA   0


Seconds Recorded 213
```

24-Hour Statistics

Statistics for the most recent 24-hour period are maintained for DS3 modules. Statistics for each port are maintained in a file that may be transferred via **FTP** to a PC and viewed, using a spreadsheet program such as Microsoft Excel. The files are in the **STATS** directory, and named according to the following sequence:

STATS\DS3C1.STA
STATS\DS3C2.STA
STATS\DS3C3.STA
STATS\DS3F1.STA (and so on)

The C1 represents slot C port 1, C2 represents slot C port 2, and F1 represents slot F port 1.

Statistics are maintained according to the following:

A file is created when a PVC or SVC is activated on a port.

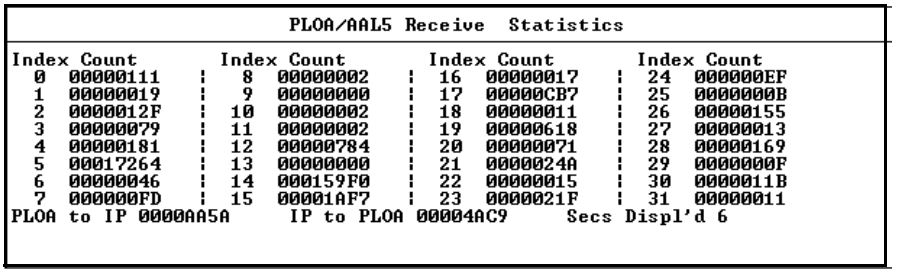
- Statistics for a port are not recorded after the associated PVC is released.
- Statistics are PVC and SVC dependent. When a PVC or SVC is established on a port previously in use, the old statistics are moved to a “discard directory” and new statistics are maintained.
- The discard directory only retains statistics for the most recently released PVC or SVC on any given port.

Use a standard spreadsheet program (such as Excel) to open a statistics file. Adjust the column widths as necessary to match the printer/paper size in use so that the data may be displayed on a single sheet of paper.

PLOA/AAL5 Statistics

Follow the sequence below to select and view the PLOA/AAL5 statistics shown.

Select **System Management** ↵
Select **Monitor Activity** ↵
Select **PLOA/AAL5 Statistics** ↵



PLOA/AAL5 Receive Statistics

Index	Count	Index	Count	Index	Count	Index	Count
0	00000111	8	00000002	16	00000017	24	000000EF
1	00000019	9	00000000	17	00000CB7	25	0000000B
2	0000012F	10	00000002	18	00000011	26	00000155
3	00000079	11	00000002	19	00000618	27	00000013
4	00000181	12	00000784	20	00000071	28	00000169
5	00017264	13	00000000	21	0000024A	29	0000000F
6	00000046	14	000159F0	22	00000015	30	0000011B
7	000000FD	15	00001AF7	23	0000021F	31	00000011

PLOA to IP 0000AA5A IP to PLOA 00004AC9 Secs Displ'd 6

Troubleshooting

- LED Alerts ... *8-15*
- Error Codes ... *8-16*
- Redundancy ... *8-16*
- CPU Sync ... *8-17*
- Problem Isolation ... *8-18*
- Port Loopback ... *8-19*
- Failure Recovery ... *8-21*
- Alarm Response/Reset ... *8-22*
- Flowchart ... *8-22*

Troubleshooting is the process of isolating the cause of a problem so that corrective action can be taken. Steps in this process narrow the focus of attention to the problem area. Documentation at each step in the process provides a valuable aid for further analysis.

NOTE: The steps below should be completed by a qualified technician. These steps assume that the technician will follow basic circuit troubleshooting logic or contact Customer Service when in doubt. Keep written records for each action taken to aid in re-creation if necessary.

LED Alerts

Front panel LED displays provide alerts by module as summarized in the table on *"Summary of Front Panel LEDs" on page 8-44*. Each LED is labeled for identification.

LEDs are basic three-color displays: **red, amber, green.** The basic LED interpretation follows accepted practice of *green* for normal operation; **amber** for minor alert; and *red* for major alert.

Error Codes

The software system will recognize and return both system and setup errors. These error codes provide troubleshooting clues for the user and Customer Service use in solving configuration and system errors. If a software error is returned to the display screen, follow the procedure below:

1. Record the error exactly as it appears on the screen.
2. Complete the troubleshooting flow chart in this chapter to isolate and/or correct any problem before going to step 3.
3. Contact Customer Service for assistance. Have the error message and other pertinent information (e.g., system log) readily available.

NOTE: The remainder of this chapter is based upon the assumption that there are no system or setup software errors. Therefore, it is important to clear all such errors before proceeding.

Redundancy

The Broadmore 1750 configuration has redundancy that serves to minimize system downtime. Troubleshooting alerts for redundant components are clearly indicated on the LEDs as explained below:

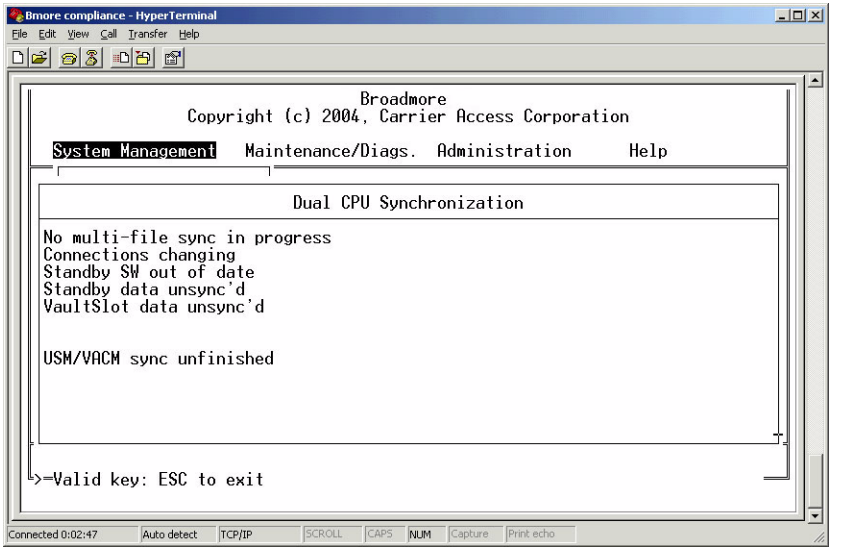
- Power supply: a problem to either module is indicated by LED and log entry. The unit can be replaced without impact to system operation.
- NIM: a problem will give a fault on the online NIM with log entry and the backup assumes control so a module replacement can be done without impact to system operation.
- SAM: the 1:N protection SAM in slot P takes over for the faulty unit that can then be replaced without further impact to system operation. A log entry is also provided to alert the operator.
- CPU Sync: a problem synchronizing files between redundant CPUs (see below).

CPU Sync

Follow the sequence below to view the CPU synchronization status between redundant CPUs. This screen shows the progress of a normal CPU Sync and will refresh every few seconds. The messages usually do not indicate any problem but can be useful if troubleshooting is required. When a CPU sync is in progress, the screen will list the number of files remaining and the current file name being synchronized. The files listed on the left side are those that would inhibit a controlled switchover.

NOTE: See also *"Synchronizing CPU" on page 7-35*.

Select **System Management** ↵
Select **Monitor Activity** ↵
Select **CPU Sync** ↵



Problem Isolation

Once you have determined that a problem exists, perform the following steps to isolate the problem for repair:

1. Check to ensure power is available to all modules.
2. Review the LED displays to determine if any module is in an alarm state. Evaluate the alarms and isolate the problem to the extent possible.
3. Review the slot configuration and look at the individual ports. Evaluate any information to further isolate the problem.

   Select **System Management** ↵
   Select **Monitor** ↵
   Select **Slot** ↵
   Select the slot of interest ↵
   Select individual ports ↵
   Observe **Data**

4. Check wiring to ensure connected equipment cables are properly installed and secured. Do not assume the problem is internal to the Broadmore 1750.
5. Check module(s) **Configuration** from the **System Management** pull-down menu. Choose the slot of interest and verify that the configuration is correct for each port.
6. Use loopbacks (below) to pinpoint circuit connectivity problems.
7. Use the flowcharts that follow to pinpoint hardware problems.

Port Loopback

The loopback function is the primary troubleshooting aid for isolation of circuit connectivity problems, both internal and external to the Broadmore 1750. Loopback is available on both the NIM and SAM. There are three loopback options on each SAM module, four on each NIM, see Figure 8-1. These loopbacks are set as a card configuration function (see *"Module Configuration" on page 7-37* for details).

Loopbacks provide a means to verify that circuit paths are functioning correctly. For example, setting the SAM remote loopback, will take user equipment transmit data (Tx) and send it to user equipment receive data (Rx). If a check of the user equipment indicates good Tx and Rx, the problem is not between the SAM and user equipment but somewhere else in the circuit. This logic can then be extended through the entire circuit until problems are isolated and corrected.

The NIM has four loopback options:

1. Normal: no loopback.
2. Local: The user equipment data is looped back after processing by the SONET circuitry on the NIM.
3. Remote: The ATM network data is looped back before passing through the NIM
4. Terminal: The user equipment data is looped back after passing through the NIM framer, but before the Line Interface Unit, LIU.

CAUTION! THE TERMINAL OPTION IS RESERVED FOR CARRIER ACCESS ENGINEERS AND SHOULD NOT BE USED.

The SAM has three loopback options:

1. Normal state is no loopback.
2. Remote: user equipment data is looped back after passing through the SAM LIU.
3. Local: ATM network data is looped back to the network after local processing by the NIM but before passing through the SAM LIU to user equipment.

These loopback options are shown graphically on the next page. The top view shows a simple circuit without any loopbacks. The middle view shows NIM loopbacks breaking the circuit connectivity. SAM loopbacks are shown in the following figure.

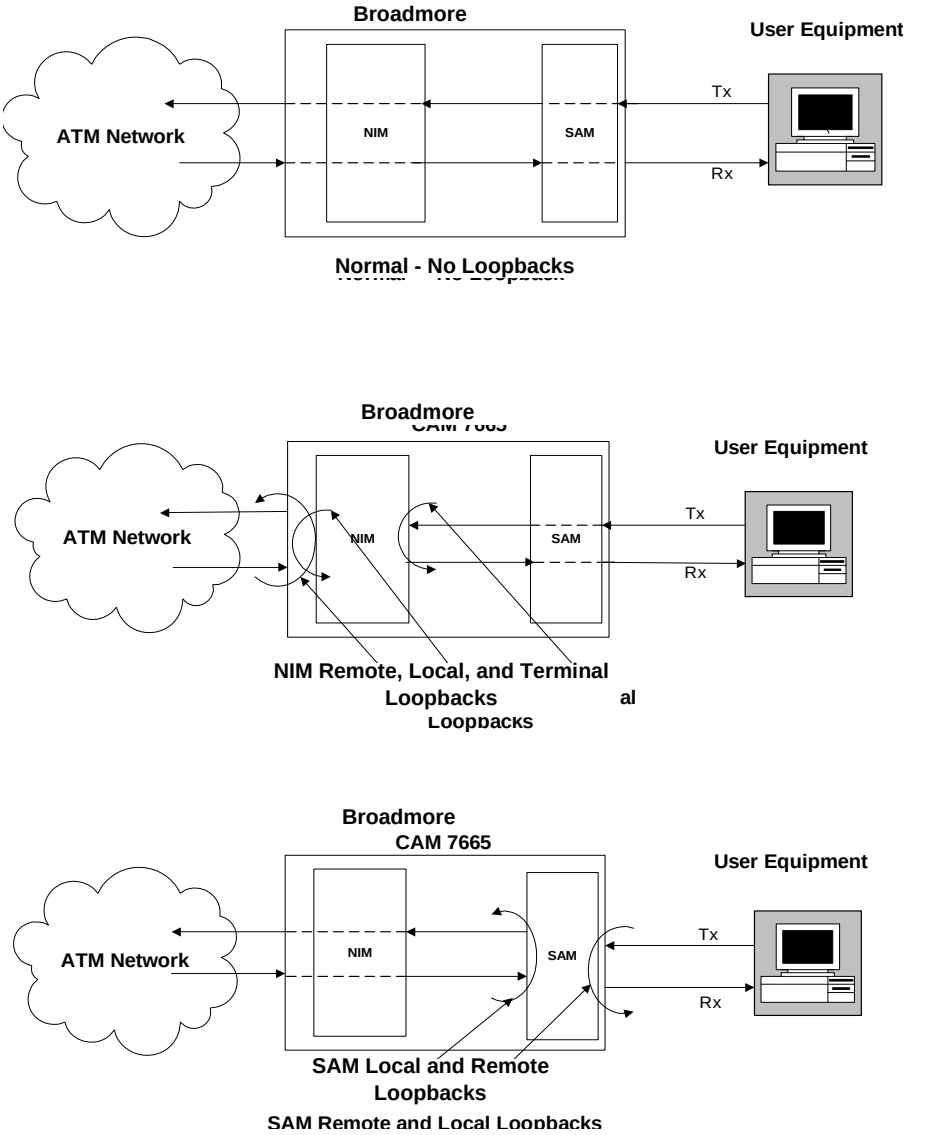


Figure 8-1: Loopback Options

Failure Recovery

Failure recovery is the sequence of events necessary to bring the Broadmore 1750 back to fully operational status after an unexpected service interruption. Throughout the recovery process, specific problems should be corrected following the troubleshooting flowchart (see Figure 8-2). The steps in failure recovery are:

1. Ensure sufficient stable electrical power is available to both the Broadmore 1750 and the control station. Observe successful completion of POST.
2. Establish communications from the control station to the Broadmore 1750. Login and view alarm LEDs. Correct all hardware problems before proceeding.
3. The Broadmore 1750 will automatically load the configuration that was saved for power-up. PVC and originated SVC connections will be re-established to the ATM backbone. Far-end originated SVCs must be re-established from the far end. Alternate previous system configurations may be loaded if they were saved. This is accomplished following the sequence below.

   Select **System Management** ↵
   Select **Configuration Files** ↵
   Select the saved file to restore ↵

4. Monitor activity for individual slots and for the ATM connection.
5. Verify configuration of the NIM(s). Validate parameter settings with the ATM switch if in doubt. Check the timing options and other parameters. Change as necessary to eliminate any errors.
6. Verify configuration of the installed SAMs. Monitor individual slots.
7. Monitor activity for the ATM connection. Select individually defined circuits to edit or connect and monitor the respective port.

The failure recovery process is a logical sequence of events to restore connectivity. With monitoring and corrective action at each step, the process includes:

- Providing power to the Broadmore 1750 and control station
- Establishing connectivity between the Broadmore 1750 and control station
- Loading the Broadmore 1750 configuration
- Establishing ATM connectivity
- Establishing individual circuit connectivity

Alarm Response/Reset

Alarms are designed into the Broadmore 1750 to provide the initial indication of a communications problem and to help isolate the problem. For example, a major alarm from a SAM identifies the specific module that will focus response efforts. The following flowchart approach to troubleshooting is based upon the initial alarm indication. The alarm response is a three-step process:

1. Troubleshoot to isolate the cause.
2. Complete corrective action to eliminate the alarm condition.
3. Return system to full operation and document the events.

Alarms are designed as real-time alerts. Thus, elimination of the alarm condition will automatically reset the associated alarm.

Flowchart

The top-level troubleshooting flowchart is shown on the below. LED indicators are the basis for entry into the flowchart, which will lead to the most likely problem(s) and recommended solution(s). The control system alarm indication can also be used as an entry point. In either case, use of this flowchart provides a logical approach to troubleshooting in the event that a problem is encountered.

CAUTION! SOME STEPS IN THE FOLLOWING FLOWCHART MAY CAUSE DISRUPTION IN SERVICE.

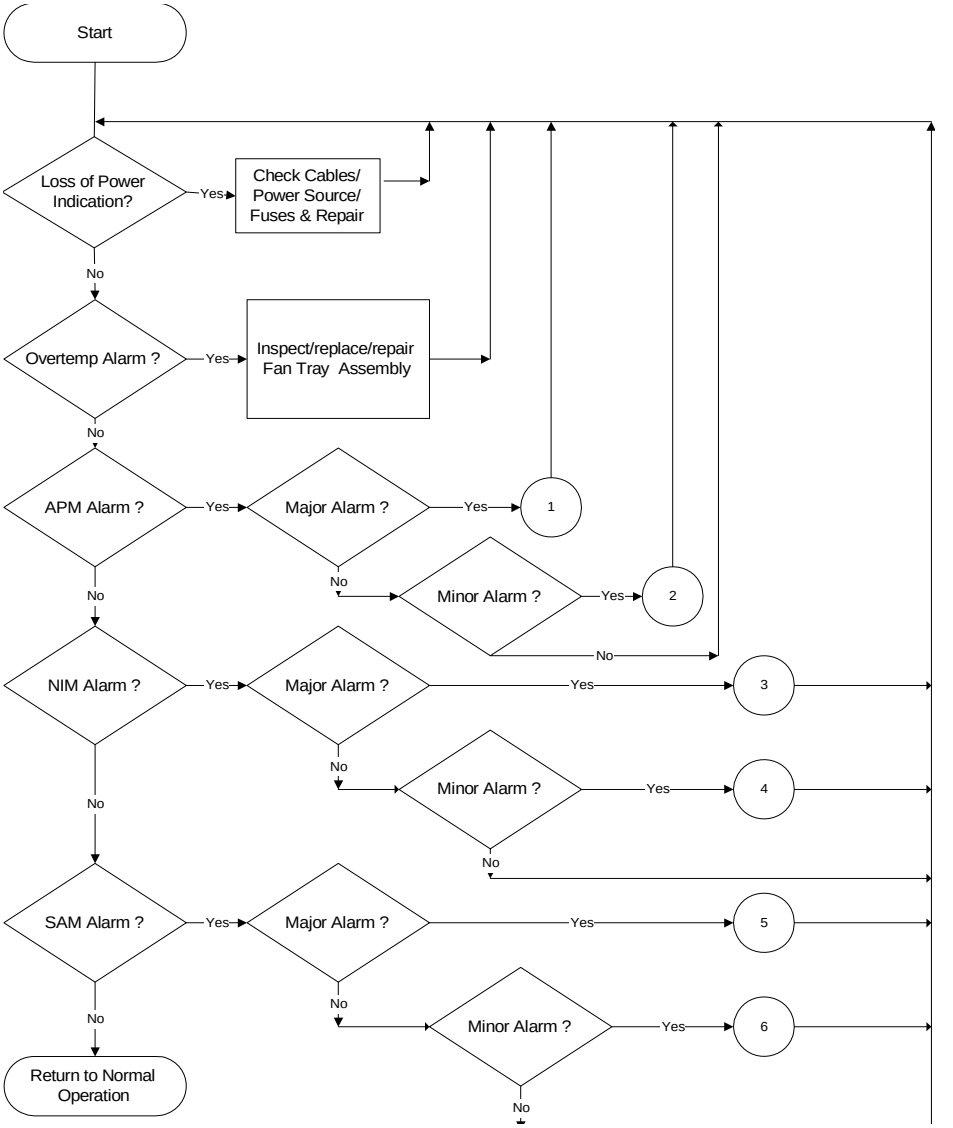


Figure 8-2: Troubleshooting Flowchart Based On LEDs

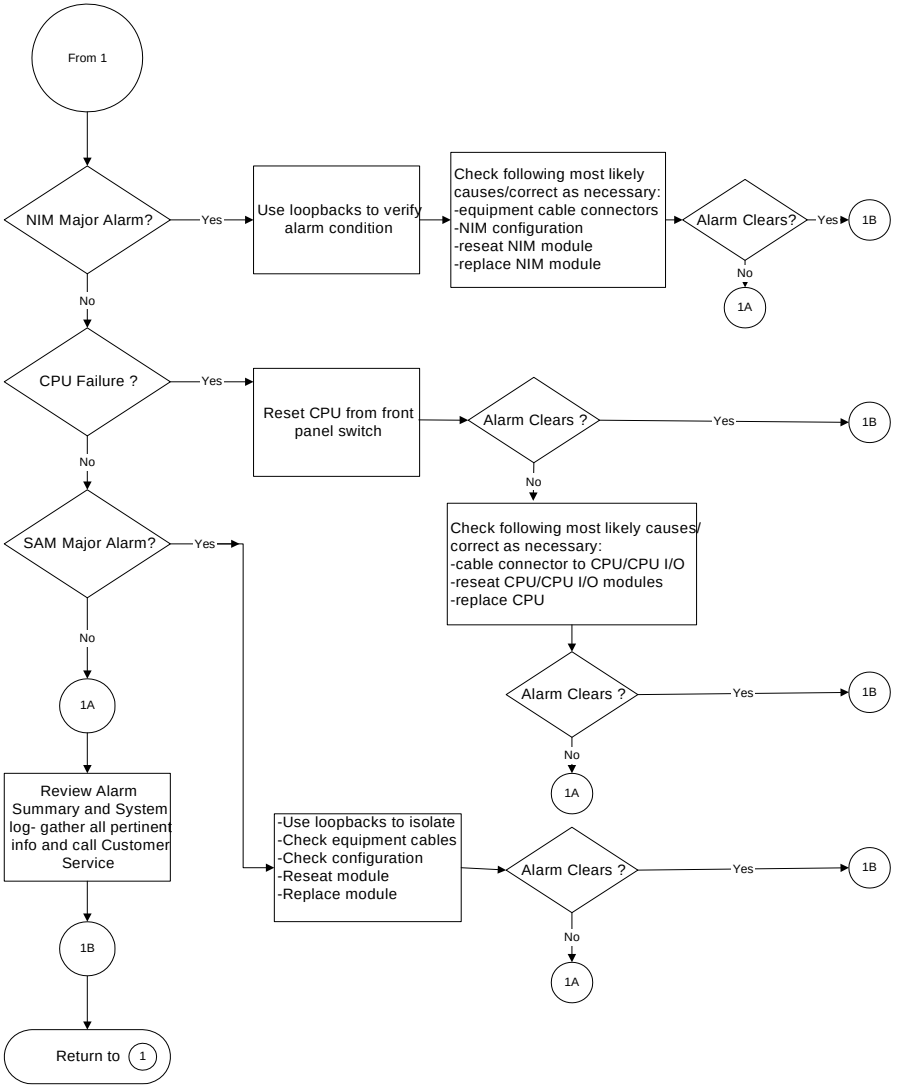


Figure 8-3: APM Major Alarm Troubleshooting Flowchart

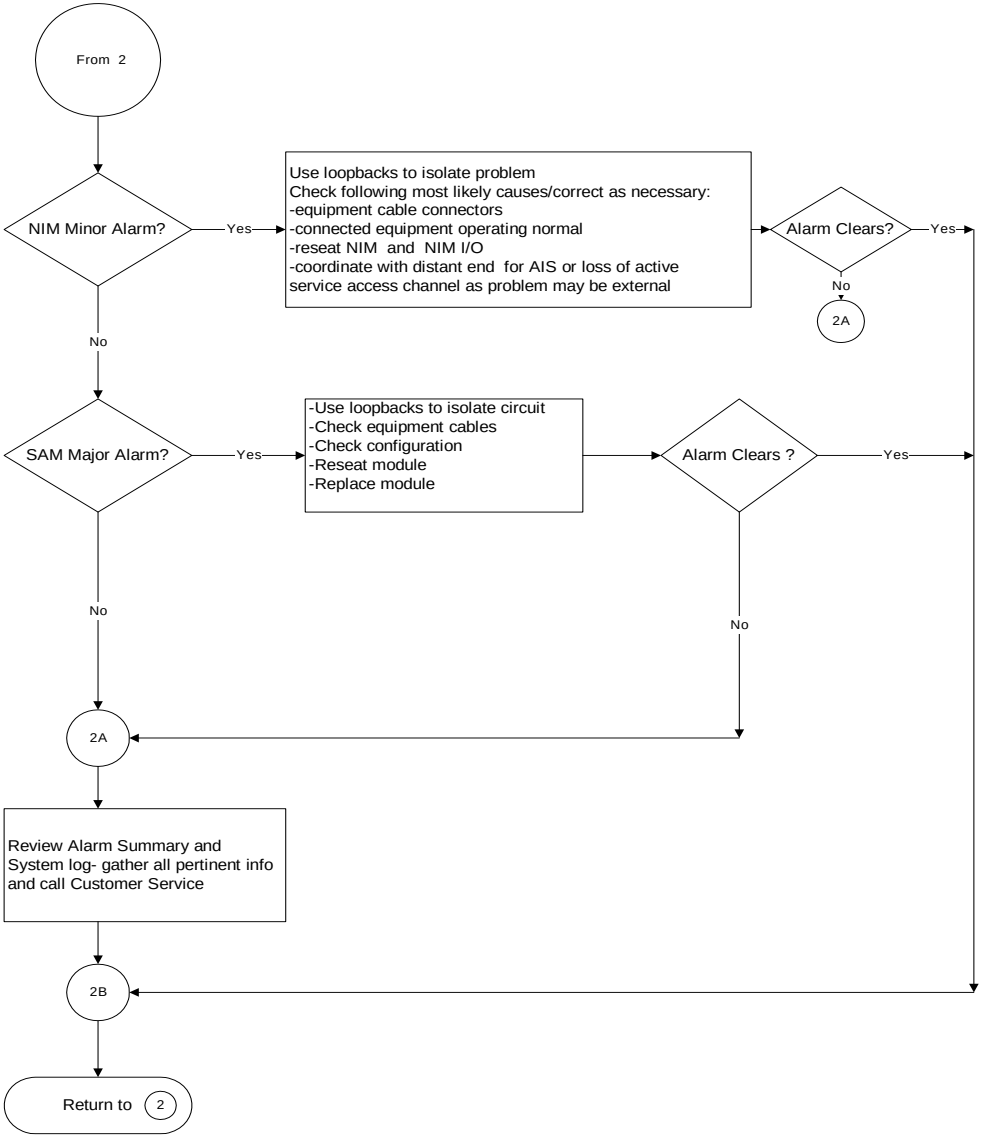


Figure 8-4: APM Minor Alarm Troubleshooting Flowchart

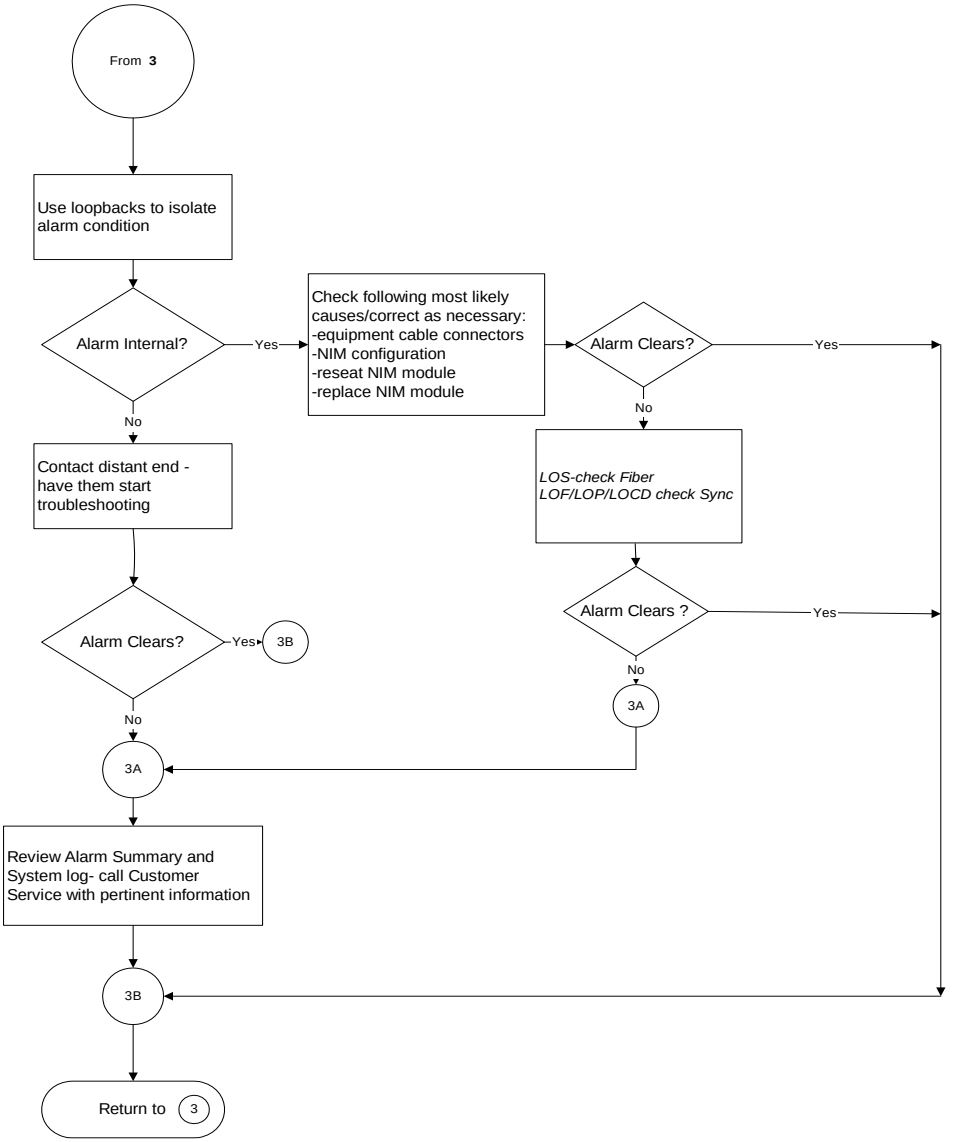


Figure 8-5: NIM Major Alarm Troubleshooting Flowchart

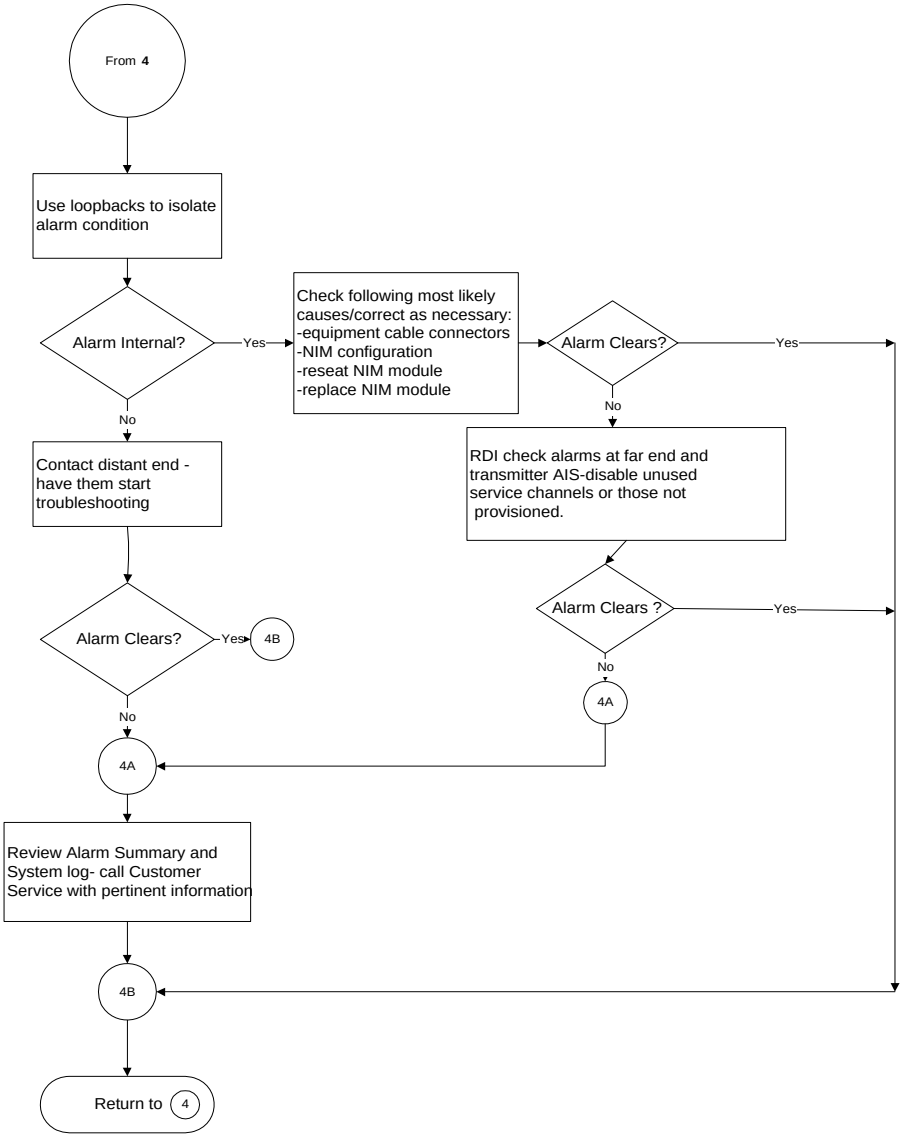


Figure 8-6: NIM Minor Alarm Troubleshooting Flowchart

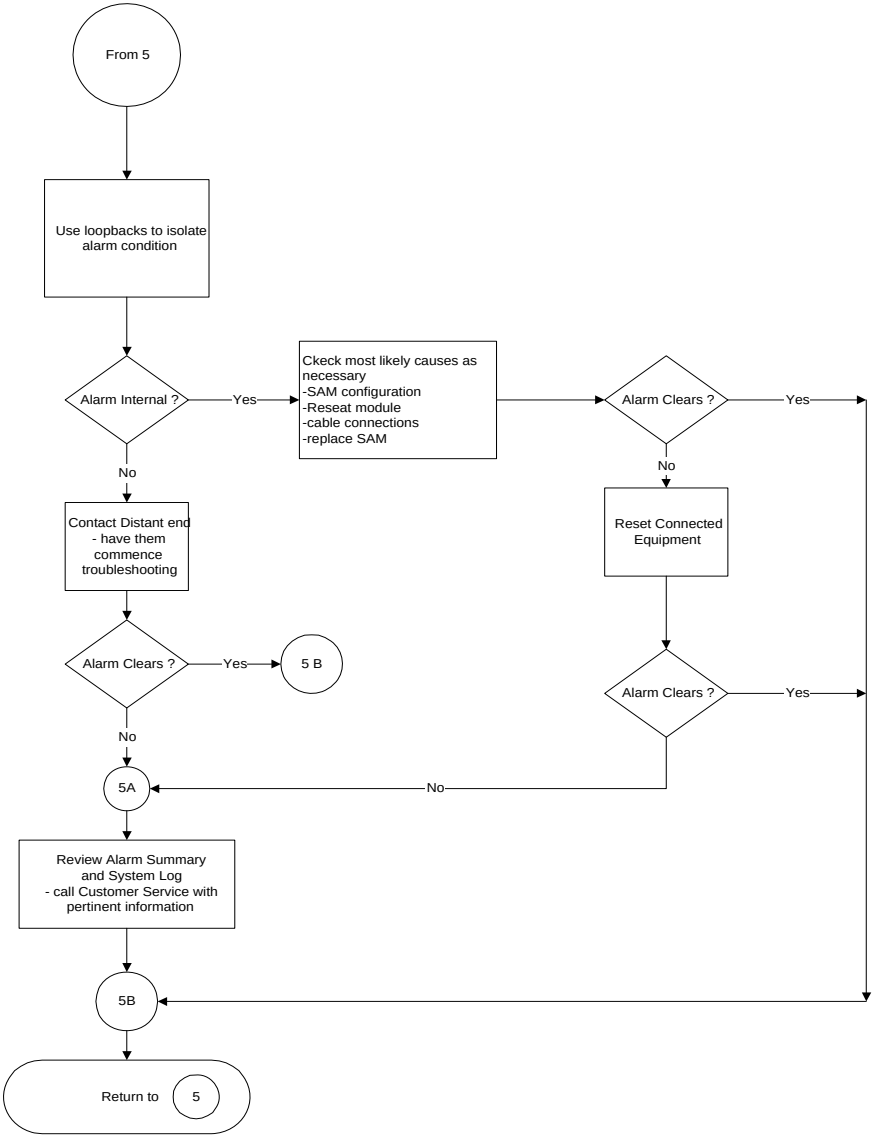


Figure 8-7: SAM Major Alarm Troubleshooting Flowchart

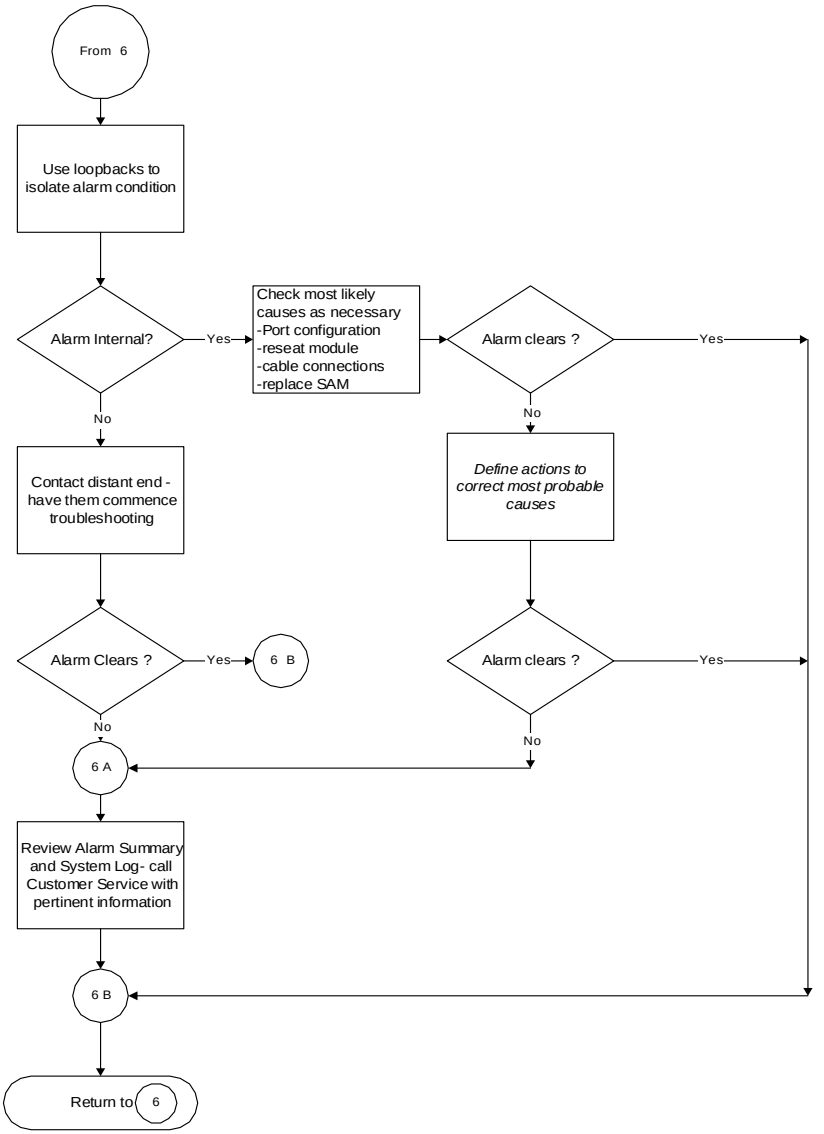


Figure 8-8: SAM Minor Alarm Troubleshooting Flowchart

Repair/Replacement

- Power Supply ... *8-31*
- NIM Replacement ... *8-32*
- SAM Replacement ... *8-33*
- IOM Replacement ... *8-34*
- CPU Replacement ... *8-35*
- CPU IOM Replacement ... *8-36*
- Fan Replacement ... *8-36*
- Integrated Fan/Alarm Module Replacement ... *8-37*
- Fan Filter Cleaning and Replacement ... *8-39*

All repair/replacement actions should be accomplished by a qualified technician familiar with the Broadmore 1750 system. The majority of repairs involve troubleshooting and the replacement of a module or card.

WARNING! **USE ESD PRECAUTIONS: WEAR AN ESD GROUNDING STRAP WHILE HANDLING ANY CARDS OR ACCESSING THE INSIDE OF THE BROADMORE 1750. FAILURE TO FOLLOW ESD PROCEDURES MAY DAMAGE SENSITIVE COMPONENTS AND VOID THE WARRANTY.**

CAUTION! **MODULE REMOVAL AND INSERTION – ON A POWERED-UP SYSTEM, WAIT AT LEAST 15 SECONDS AFTER ANY MODULE REMOVAL OR INSERTION TO ALLOW THE SYSTEM TO STABILIZE. FAILURE TO FOLLOW THIS PROCEDURE MAY RESULT IN SYSTEM ERRORS REQUIRING TOTAL SYSTEM REBOOT. WHEN INSTALLING A REPLACEMENT CPU IN A REDUNDANT CPU SYSTEM, DO NOT REBOOT OR POWER DOWN THE SYSTEM BEFORE CPU SYNCHRONIZATION IS COMPLETE AS INDICATED BY A SOLID STATUS LIGHT.**

Power Supply

The Broadmore 1750 receives –48 VDC power at the chassis rear from a user-provided source. Repair/replacement of this source is external to the scope of this manual.

Optionally, the Broadmore 1750 may be configured with a dual AC power supply. When an AC power source is used, the following steps are required to repair/replace a power supply module. The power supply is usually mounted directly below the Broadmore 1750. The power supply design facilitates module replacement without any wiring or power disruption.

1. Ensure that a replacement module is available.
2. Identify the problem module by front panel indicator that will not be illuminated and a software alarm will be received at the control station. Additionally, the integrated fan/alarm module front panel will give a no-power indication (from *green* to *off*) for the defective module.
3. Turn the power switch ***off*** for the defective power module. Loosen the front panel screws and remove the defective module by pulling it straight out the front. Fully insert the replacement module, ensuring proper alignment. Turn the power switch ***on*** and the front panel should display *green.* The power modules are hot-swappable. This replacement will not impact Broadmore 1750 operation due to the built-in redundancy feature.
4. Tighten the front panel retainer screws to hold the new module in place.
5. Contact Customer Service and return the defective module for repair.

NIM Replacement

There are no field repairable items on a NIM. In a redundant configuration, replacement of a NIM will not impact user ATM network connectivity. In a single NIM configuration, all ATM connectivity will be disrupted during card replacement. Follow the steps below to replace a NIM.

1. Ensure that a replacement module is available.
2. Remove the chassis front cover. The Broadmore 1750 retains power; individual NIMs may be removed/replaced without power disruption to other modules.
3. Remove the fiber connection and loosen retaining screws at the top and bottom of the NIM to be replaced.
4. Use the installed ejectors to unseat the NIM from the midplane. This is done by simultaneously pushing up on the top ejector and down on the bottom ejector.
5. Remove the defective NIM by pulling it straight out the front.
6. Insert the replacement NIM, ensuring correct alignment with the card guides and midplane connector.
7. Firmly press the new NIM into place so that it is fully seated with the midplane connector. Tighten both retaining screws (finger tight only) and install the fiber connection.
8. The new NIM will automatically configure to the last known configuration of the slot where installed. In a single NIM system (non-redundant), originated SVCs and PVCs will be re-connected per the current connection list. The far end must originate the re-connection of incoming SVCs. Monitor activity for the ATM connection to ensure proper operation
9. Replace the chassis front cover.
10. Return the defective NIM for repair. Contact Customer Service for a Return Material Authorization (RMA) number and detailed procedures.

SAM Replacement

There are no field repairable items on a SAM. All user equipment connected to the defective SAM will lose ATM connectivity during replacement. Equipment connected via other SAM(s) will not have an ATM service disruption. Follow the steps below to replace a SAM:

1. Ensure that you have a replacement module.
2. Remove the chassis front cover. The Broadmore 1750 retains power; individual SAM cards may be removed/replaced without service disruption to other modules.
3. Loosen retaining screws at the top and bottom of the SAM to be replaced.
4. Use the installed ejectors to unseat the SAM from the midplane. This is done by simultaneously pushing out on the ejectors.
5. Remove the defective SAM by pulling it straight out the chassis front.
6. Insert the replacement SAM, ensuring correct alignment with the card guides and midplane connector.
7. Firmly press the new SAM into place so that it is fully seated with the midplane connector. Tighten both retaining screws (finger tight only). The new card configuration will be identical to the last configuration for the installed slot.
8. Replace the chassis front cover.
9. Return the defective SAM for repair. Contact Customer Service for an RMA number and procedures.

IOM Replacement

There are no field repairable items on an IOM. All user equipment connected to the defective IOM will lose ATM connectivity during replacement. Equipment connected via other IOM(s) will not have an ATM service disruption. Follow the steps below to replace an IOM:

1. Ensure that you have a replacement module.
2. Remove the chassis rear cover. The Broadmore 1700 CABB retains power; individual IOM cards may be removed/replaced without service disruption to other modules.
3. Remove and tag the cables on the IOM to be replaced.
4. Loosen retaining screws at the top and bottom of the IOM to be replaced.
5. Use the installed ejectors to unseat the IOM from the midplane. This is done by simultaneously pushing out on the ejectors.
6. Remove the defective IOM by pulling it straight out the chassis.
7. Insert the replacement IOM, ensuring correct alignment with the card guides and midplane connector.
8. Firmly press the new IOM into place so that it is fully seated with the midplane connector. Tighten both retaining screws (finger tight only). The new card configuration will be identical to the last configuration for the installed slot.
9. Reconnect the cables to the IOM.
10. Replace the chassis rear cover.
11. Return the defective IOM for repair. Contact Customer Service for an RMA number and procedures.

CPU Replacement

CAUTION! **WHEN INSTALLING A REPLACEMENT CPU IN A REDUNDANT CPU SYSTEM, DO NOT REBOOT OR POWER DOWN THE SYSTEM BEFORE CPU SYNCHRONIZATION IS COMPLETE AS INDICATED BY A SOLID STATUS LIGHT.**

NOTE: Each CPU card has a battery that should be replaced periodically. See Appendix B, *Spare Parts List* for part number information.

There are no field-repairable items on the CPU card. In a single CPU system, there will be a disruption of system control and administration during card replacement. In a redundant CPU system, user PVCs through the ATM network remain intact during replacement of a CPU. In a single CPU system, the CPU will reboot and all PVC service is interrupted. Follow the steps below to replace a CPU Card.

1. Ensure that you have a replacement module.
2. Remove the chassis front cover.
3. Loosen retaining screws at the top and bottom of the CPU card to be replaced. The Broadmore 1750 retains power; the CPU card may be removed/replaced without service disruption to other modules.
4. Use the installed ejectors to unseat the CPU card from the midplane. This is done by simultaneously pushing up on the top ejector and down on the bottom ejector.
5. Remove the defective CPU card by pulling it straight out chassis front.
6. Insert the replacement CPU card, ensuring correct alignment with the card guides and midplane connector.
7. Firmly press the new CPU card into place so that it is fully seated with the midplane connector. Tighten both retaining screws (finger tight only).

NOTE: The new CPU card will come configured. Any necessary updates will be announced.

8. Replace the chassis front cover.

9. Return the defective CPU card for repair. Contact Customer Service for an RMA number and detailed procedures.

CPU IOM Replacement

There are no field-repairable items on the CPU IOM. This module does contain a unique part of the Ethernet address such that the Broadmore 1750 system must be alerted to the module change in order to restore service. Only replace the standby CPU or CPU IOM on a redundant system. This will ensure correct programming of the IP, CIP, LANE and ATM address information.

1. Ensure that you have a replacement CPU IOM with remote reboot jumpers set correctly.
2. Follow the CAMMI sequence on the next page to signal CPU IOM removal.
3. Loosen top and bottom retaining screws, use ejectors to unseat the module, and pull it straight out to remove.
4. Insert the replacement CPU IOM, ensuring alignment with the guides and midplane connector. Tighten both retaining screws (finger tight only).
5. Return the defective CPU IOM for repair. Contact Customer Service for an RMA number and detailed procedures.

Fan Replacement

There are no field-repairable items on the fan tray assembly. The air filters are removable for routine cleaning. Removal and replacement of the fan assembly will not impact normal Broadmore 1750 operations. This replacement should be completed quickly to avoid possible overheating of Broadmore 1750 components. Follow the steps below to replace the fan assembly.

1. Ensure that you have a replacement fan tray assembly.
2. Loosen retaining screws on both sides of the fan assembly to be replaced.
3. Remove the defective fan assembly from below the chassis by pulling it straight out.
4. Insert the replacement fan assembly, ensuring alignment in the side guides.

5. Firmly press the new fan assembly into place so that it is fully seated. Tighten both retaining screws (finger tight only).
6. Return the defective fan assembly for repair. Contact Customer Service for an RMA number and procedures.

Integrated Fan/Alarm Module Replacement

The integrated fan/alarm module has two replaceable fuses. Follow the steps below to replace a fuse.

1. Fuses and spares are located on the integrated fan/alarm module IOM accessed from the chassis rear. Remove the rear cover to access the fuses.
2. Blown fuses are removed by pulling directly out.
3. Remove a spare fuse by pulling directly out. Insert the replacement fuse(s) in reverse to the one(s) removed.
4. Obtain replacement spare fuse(s) locally. Use only 7.5 Amp (Bussman part # GMT7.5) or equivalent.

CAUTION! FUSES ARE ONE-TIME USAGE ITEMS. IF THE FUSE BLOWS A SECOND TIME, CIRCUIT DAMAGE MAY BE MORE EXTENSIVE, AND IT MAY BE NECESSARY TO DISCONNECT POWER TO THE ENTIRE BROADMORE 1750 CHASSIS AND REPLACE THE INTEGRATED FAN/ALARM MODULE. ALL CIRCUITS WILL EXPERIENCE A DISRUPTION DURING INTEGRATED FAN/ALARM MODULE REPLACEMENT.

Follow the steps below to replace an integrated fan/alarm module.

1. Ensure that a replacement module is available.
2. Remove the chassis front cover.
3. Loosen retaining screws at the top and bottom of the integrated fan/alarm module card to be replaced.
4. Use the installed ejectors to unseat the integrated fan/alarm module card from the midplane. This is done by simultaneously pushing up on the top ejector and down on the bottom ejector.

5. Remove the defective integrated fan/alarm module card by pulling it straight out the chassis front.
6. Insert the replacement integrated fan/alarm module, ensuring correct alignment with the card guides and midplane connector.
7. Firmly press the new integrated fan/alarm module into place so that it is fully seated with the midplane connector. Tighten the retaining screw (finger tight only).
8. Replace the chassis front cover.
9. Return the defective integrated fan/alarm module for repair. Contact Customer Service for an RMA number and procedures.

General Maintenance

- Fan Filter Cleaning and Replacement ... *8-39*
- Maintenance/Diagnostics ... *8-40*
- Engineering Analysis ... *8-42*

The Broadmore 1750 is designed to provide continuous service with minimal maintenance provided operational conditions remain within specifications. Cooling fans are included in the Broadmore 1750 to aid in heat dissipation. The fan tray has two air filters, one on each fan. Complete the fan filter cleaning procedure below on a monthly basis, or more often if the filters are excessively dirty. It is not necessary to power down the Broadmore 1750 for this routine maintenance.

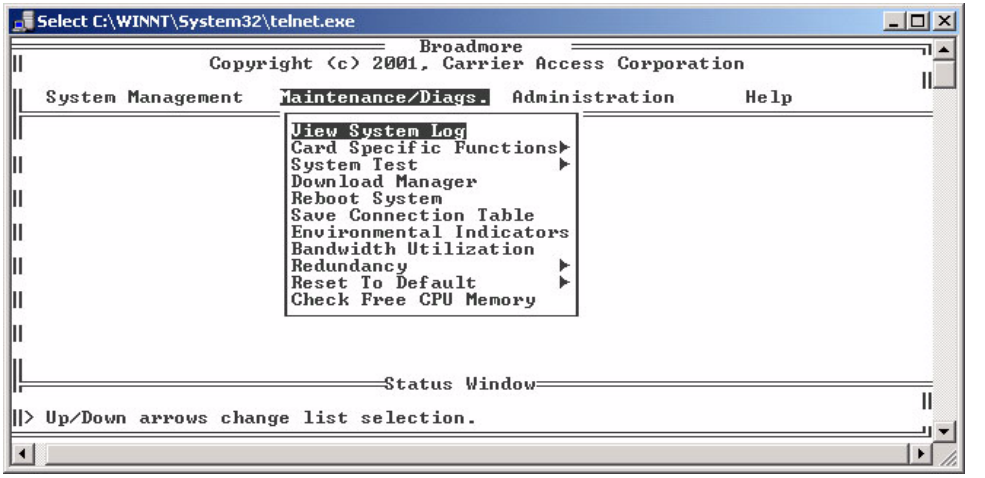
Fan Filter Cleaning and Replacement

1. Loosen screws and remove the chassis front cover.
2. Loosen screws and remove the fan tray by pulling on the Center handle.
3. Remove the fan filters from the bottom of the tray. Each filter snaps out of place.
4. The filters are re-usable. Wash them in a mild soapy solution, clean thoroughly, and dry completely. Additional filters may be obtained from the manufacturer, Globe Motors (part # FFM745) or Customer Service. Filters may be replaced with new ones.
5. Snap the filters back into place.
6. Re-install the fan tray, being careful to align it in the guides provided. Ensure the fans are operating properly, then tighten the screws to hold the fan tray in place.
7. Replace the chassis front panel and secure retaining screws.

NOTE: This is the only routine maintenance required for the Broadmore 1750.

Maintenance/Diagnostics

CAMMI provides access to several maintenance and test functions under the Maintenance/Diagnostics main menu. These items are explained below.



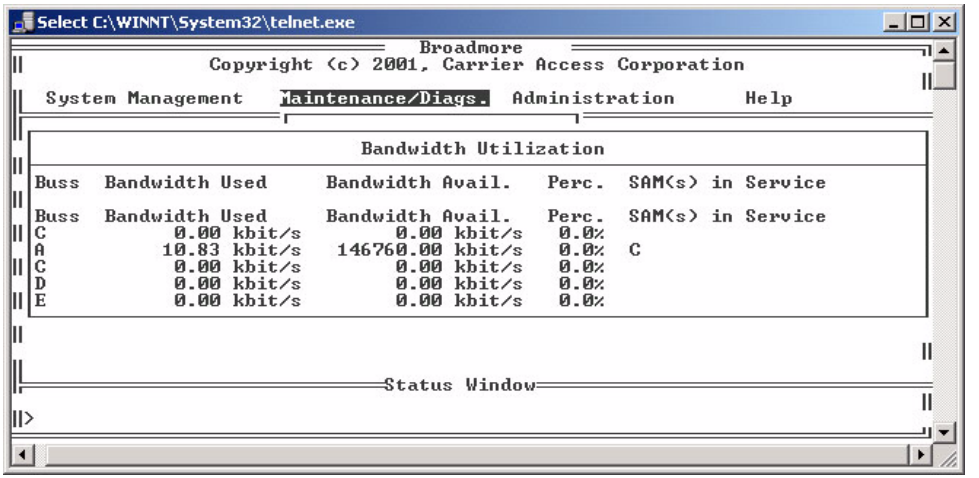
View System Log provides a historical record of events, such as configuration, establishing a PVC, or other action that affects service. Messages are filtered by privilege level. All messages are displayed at the Supervisor level, many of which can only be interpreted by Carrier Access engineers.

Environmental Indicators will display the current status of power, fan, and BITS clocks. This display, shown below, does not indicate fan removal.

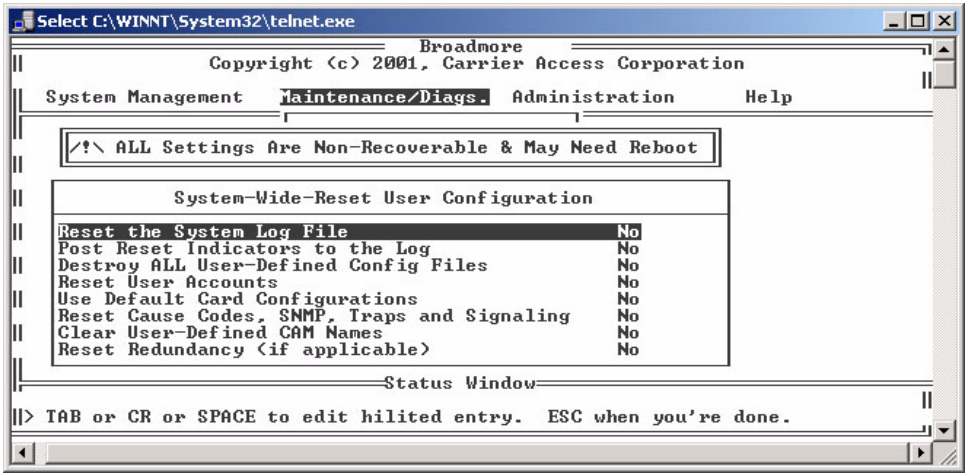
```
System Status

Power source A missing!
Power source B present.
Chassis fan operational.
Bits On card A :Present
Bits On card B :Present
```

Bandwidth Utilization displays the amount of bandwidth being used, the remaining bandwidth available, and the percentage used. This can be recalculated by pressing 'R' when the screen displays.



Reset to Defaults allows you to reset the Broadmore 1750 to the factory defaults settings.



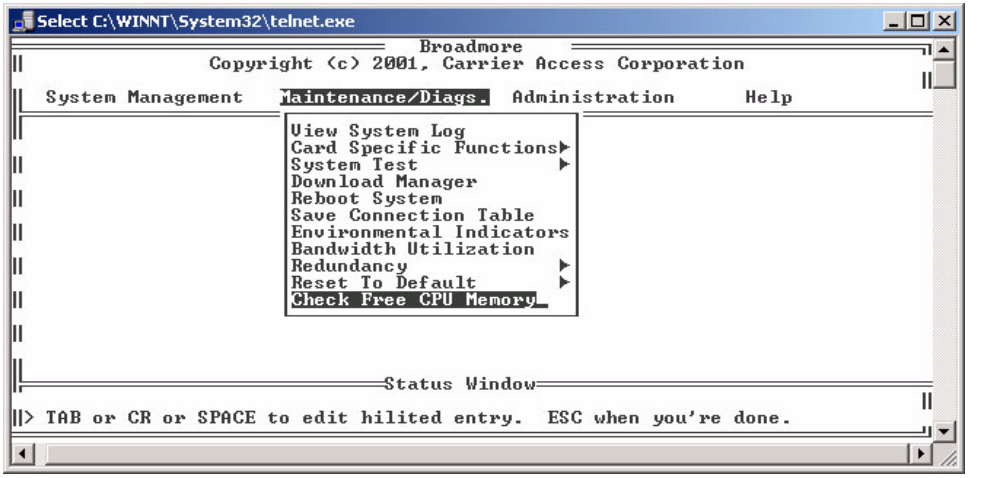
Engineering Analysis

There are several options under the **Maintenance/Diags**. menu reserved for use by Carrier Access engineers. A brief description is provided to aid in understanding the system. These commands should only be used in close coordination with Carrier Access engineers.

Card Specific Functions leads to individual card diagnostics where you **Peek and Poke** various information fields.

System Test runs a preconfigured test and displays statistical results. The **Asserts** option will activate additional software traps to provide more detailed information.

Check Free CPU Memory will display the free memory available as shown below. This is valuable information for coordination with Carrier Access engineers.



Download Manager is used to download new software. Instructions are provided with any new software distributed.

Reboot System reboots the CPU and uses the system setting in place prior to the reboot. This option is necessary when downloading new software revisions or changing your system's IP address. The changes you make to system settings will not take effect until you reboot.

Save Connection Table will preserve the current connection data in a text file format so that it can be viewed using any standard text editor.

Summary of Front Panel LEDs

The following table provides descriptions of the front panel LEDs for the Broadmore 1750.

Module	LED Display	LED Color	Definition
APM	Major Alarm	Red	Major fault for 2.5 seconds
		None	No major alarm
	Minor Alarm	Amber	Minor alarm for 2.5 seconds
		Not Lit	No minor alarm
	*Over Temp	Red	* Not supported at this time.
		Not Lit	
	Power	Green	-48 volts power is present
		Not Lit	No power present
	Power Fail A/B	Red	
		Not Lit	
NIM	Fault	Red	Major alarm detected for 2.5 seconds
		Amber	Minor alarm detected for 2.5 seconds
		Green	Normal, no fault condition
	On-Line	Red-flashing	NIM failed POST, not ready
		Amber	NIM passed POST and in standby
		Green	NIM is online, normal
	LOS	Red	Loss of Signal
		Green	Acceptable optical receive power for 10 seconds
SAM	Fault	Red	Major alarm detected for 2.5 seconds
		Amber	Minor alarm detected for 2.5 seconds
		Green	Normal, no fault condition
		Not Lit	Out of service
	On-line	Red	SAM failed POST, not ready
		Amber	offline or standby
		Green	Normal, no fault condition
	Alarm	Red	Major

Module	LED Display	LED Color	Definition
		Amber	Minor
		Green	Normal, enabled
		Not Lit	Out of service
CPU	Master	Green	online as master
		Amber	Standby
	On-line Activity	Amber	Normal activity

CHAPTER 9

Command Line Interface

In this Chapter:

- CLI Access ... *9-2*
- Creating and Running Scripts ... *9-4*
- Port Configuration ... *9-6*
- Monitor ... *9-8*
- About Command ... *9-9*

CLI Access

The Command Line Interface (CLI) provides much the same functional control of the Broadmore 1750 as the CAMMI program. CLI commands are entered as text. The command prompt displays the current location from the cascading menu structure that parallels CAMMI. Therefore, a working knowledge of CAMMI makes navigation through CLI easier.

NOTE: Use CAMMI for administrative features such as changing passwords or identifying new users.

Use the following steps for CLI Access.

1. Log into the Broadmore 1750 operating system, pSoS, using a valid user name and password.

NOTE: At this point, you can type 'help' to view a list of commands. You can also type 'help *command*' to obtain help on any of the listed commands.

2. At the 1750> prompt, type 'cli' and press enter. The prompt changes to cli> for successful access to the CLI program.

NOTE: The security mode and user privilege level determines the CLI commands available to each operator.

3. Type **?** and press enter at any prompt to display the available commands, both general and for the current command level.
   - General commands apply at all levels.
   - quit: exits the CLI program
   - up: moves up one level in the command structure
   - clear: removes data from the screen except the last line, which is displayed at the top of the screen

Enter commands that are not case sensitive as they appear when viewed using the **?** query. The spelling must be correct.

Example:

At the cli > prompt, enter **?** to display a list of available commands. At this point, the level commands are:

- sys
- maintain
- about

General commands are:

- up
- clear
- quit
- ? (help)

The level commands correspond with the CAMMI main menu except for the administrative function, which is not implemented in CLI.

Creating and Running Scripts

To reduce the time required to configure one or more Broadmores, you can script a series of CLI commands that can be saved to a file, uploaded to the Broadmore, and executed as needed.

You can use a text editor or a terminal emulation program to create a script file. For example, using a terminal emulator such as Symantec Procomm®, you can perform the following steps to create a script and save it to a file.

Select **Tools** ↵
Select **Scripts** ↵
Select **Start Recorder** ↵
Enter the appppropriate sequence of **CLI** commands
Select **Stop Recorder** ↵
Save the script as <filename> of choice

A script file must meet the following requirements:

- Each command must begin on a new line.
- Comments or unused configuration settings must begin with a semicolon (**;**). When the Broadmore's script interpreter encounters a semicolon, all remaining text on the line is ignored.
- The file must be named as follows:

  `filename.scp`

See Appendix G for a list of Broadmore commands.

NOTE: Do not use the following command in a script:

`showi`

This command is "show interactive" for the system log and requires user input. If necessary, use the `show` command instead.

To upload and run a script file:

1. Log in to the Broadmore using FTP or SFTP. See *"FTP Login" on page 10-21* or *"SFTP Login" on page 11-43* for instructions.
2. Using your FTP or SFTP software, upload the script file to the **script** directory on the Broadmore's online CPU.
3. Log into the Broadmore's operating system using a valid user name and password. At the 1750> prompt, enter the following command:

   `runscript` *`filename`*

NOTE: On a redundant Broadmore, you must also load and run the script file on the standby CPU.

After you issue the `runscript` command, the script interpreter switches to the CLI> prompt and executes all commands from the script file in sequence. Each command is displayed as if you were manually entering it during a normal session.

If the script interpreter encounters an error, it continues to attempt to interpret each successive line until it can execute a valid command. If no valid commands can be executed before the end of the file, review the error displayed to resolve the problem.

It is recommended that all logs be reviewed after at least the first time a script is executed to ensure that the script performed as intended.

NOTE: Depending upon the load on the Broadmore's CPU, you may need to insert delays between some commands in a script. For example, when using a 'deleteall' command, you may need to insert a delay before attempting to reconfigure the same resources. You may also need delays when configuring a large number of PVCs in a row. Depending upon system load, delays of up to 30 seconds may be necessary between some script commands. To insert a delay between script commands, use the following command:

`sleep(`*`n`*`)`

where *n* = 1 to 30 seconds.

Port Configuration

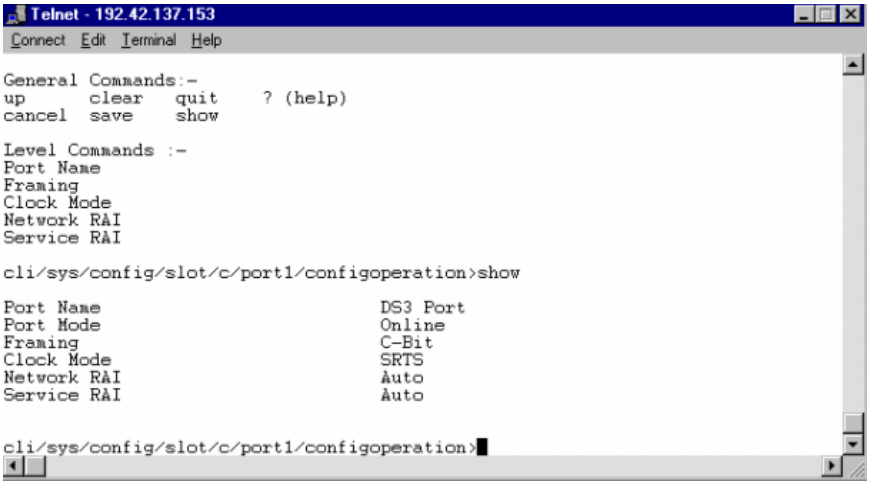
This example shows how to use CLI to configure a DS3 port. Follow the steps below from the initial CLI screen to access the configuration items. The steps shown below must be entered in sequence one-at-a-time. CLI does not support going directly to the last screen via a single entry (e.g., a single entry of sys/config/slot/c/port1/ configoperation/show will give an error for unrecognized entry).

Enter **sys** ↵	response is	cli/sys>
Enter **config** ↵	response is	cli/sys/config>
Enter **slot** ↵	response is	cli/sys/config/slot>
Enter **c** ↵	response is	cli/sys/config/slot/c>
Enter **port1** ↵	response is	cli/sys/config/slot/c/port1>
Enter **configoperation** ↵	response is	cli/sys/config/slot/c/port1/configoperation>
Enter **show** ↵	response is the screen shown on the next page	

Each parameter can be revised. For example, to change the port name to “DS3Port”, you would enter:

```
Port name  DS3 port
```

Then type **show** and press Enter to see that the change has taken effect.



Note that the above general commands have two additional items: cancel and save. The normal way to leave any screen is to enter up, which takes you to the previous command level. However, this is not allowed on this screen because configuration data has been altered. This data must be either discarded (cancel) or retained (save) before proceeding.

The command **cardstatus** will display a list of all Broadmore 1750 slots with the module installed. Cardstatus is available when you are in either of the following command levels:

cli/sys/config/slot

cli/sys/monitor/slot

Monitor

Use Monitor to display system operation statistics. The CLI command string to monitor and show port counters is displayed below. Note that an additional command, reset, is available. Reset will zero all counters. This was done as the first command in the display below.

```
cli/sys/monitor/slotstats/c/port2/counters>reset

cli/sys/monitor/slotstats/c/port2/counters>show

DS3 SAM (Online) Slot C Port 2 Counters
Tx Cells 311228                  Rx Cells 311227

Network Errors                Service Errors                Major Alarm YES
SEQ Errors     0              BPV Errors     8670           Minor Alarm NO
SNP Errors     0              EXZ Errors     8670
F-BIT Errors   0              F-BIT Errors   8670
PARITY Errors  0              PARITY Errors  7420
C-BIT Errors   0              C-BIT Errors   7439
FEBE Errors    8670           FEBE Errors    510
BERT Errors    0              BERT Errors    0

cli/sys/monitor/slotstats/c/port2/counters>
```

About Command

The About command, accessed from the initial CLI> prompt will provide information about each slot, including:

- Type module
- Module serial number
- Hardware revision
- Software revision

The information displayed is tailored for the type of module. This information is particularly valuable when contacting Customer Service.

CHAPTER 10

Security Management

In this Chapter:

- Security Features ... *10-2*
- Security Guidance ... *10-3*
- Logging In ... *10-5*
- Log-in Banner ... *10-6*
- System Clock ... *10-7*
- Network Time Protocol ... *10-8*
- Managing Users and Audit Trails ... *10-10*
- IP ICMP Messages ... *10-17*
- SNMP Messages ... *10-18*
- Shell Commands (Non-FIPS Mode) ... *10-19*
- FTP Login ... *10-21*

Security Features

The Broadmore provides the following security features:

- User ID and password authentication
- Four levels of user privileges for accessing command functions
- Configuration activity audit trails
- Enable/disable SNMP and ICMP messages
- SNMPv3 USM/VACM
- Log-in Banner for special user instructions

Only the Network Administrator (SuperUser) can create and modify user accounts, set access privileges, and monitor user activity audit trails. The Broadmore requires that users log into the Broadmore through Telnet and FTP.

NOTE: Be sure to use the appropriate fonts and screen settings to maintain the proper screen appearance.

Security Guidance

- **Receipt and Inspection** – Broadmore components containing operating system software are packaged and sealed at the factory with tamper-proof security tape. Upon receipt, carefully examine the security sealing tapes on the shipping containers for any signs of tampering. (See *"Receipt" on page 3-2*.)
- **Security** – Broadmore components containing operating system software (CPU modules, memory modules, and storage media) should be handled in accordance with applicable security procedures.
- **Initial Login** – The Broadmore is shipped with a default username and password for logging in the first time. A SuperUser should log in the first time to configure the Broadmore for secure operation.
  For maximum security, perform the following steps:
  (1) configure IP access (via ethernet, LANE, or CIP)
  (2) create a temporary SuperUser account
  (4) delete the public SYSADMIN account and log out
  (5) after logging in securely, you can safely create user accounts and configure the Broadmore for secure operation.
- **Security Modes** – The Broadmore is shipped with security turned off. Only a SuperUser can change the FIPS and SecurID modes. If these security modes are required, see next chapter.
- **Potential Security Vulnerabilities**
  (1) The Broadmore accepts loose source routed IP packets, so it is recommended that source routed packets be dropped on routers and firewalls. (See manufacturer's instructions.)
  (2) The Broadmore RS-232 COM 1 serial port used for "Craft Access" does not immediately terminate a management session if a user disconnects without typing "exit". During the following timeout period, another user can connect without logging into the RS-232 port and other users are denied access through the ethernet port. It is recommended that all accounts be created with "Remote Access" only, except for one failsafe SuperUser account with "Craft Access." The craft password should be stored safely in the NOC. When needed, the SuperUser can log into the craft port, fix things, change the password, log out, and store the new password back in the NOC.

- **System Clock** – The system clock is used to time stamp all events recorded in the system log and user audit log. To set the system clock, see *"System Clock" on page 10-7*.

- **User Administration** – The Broadmore authenticates users by identification and role-based access privilege levels and maintains an audit trail activity log. Only a SuperUser can assign users and access levels, set the minimum number of characters required for user names and passwords (user ID rules), and clear the system log. The security officer must ensure that all users change their passwords periodically in accordance with local security practice.
  (1) It is recommended that passwords be changed at least once every 6 months. Users must be instructed to use a random combination of all the usable characters for passwords.
  (2) It is recommended that all users, access privileges, and role assignments be reviewed periodically or whenever a personnel termination, transfer, or role change occurs.

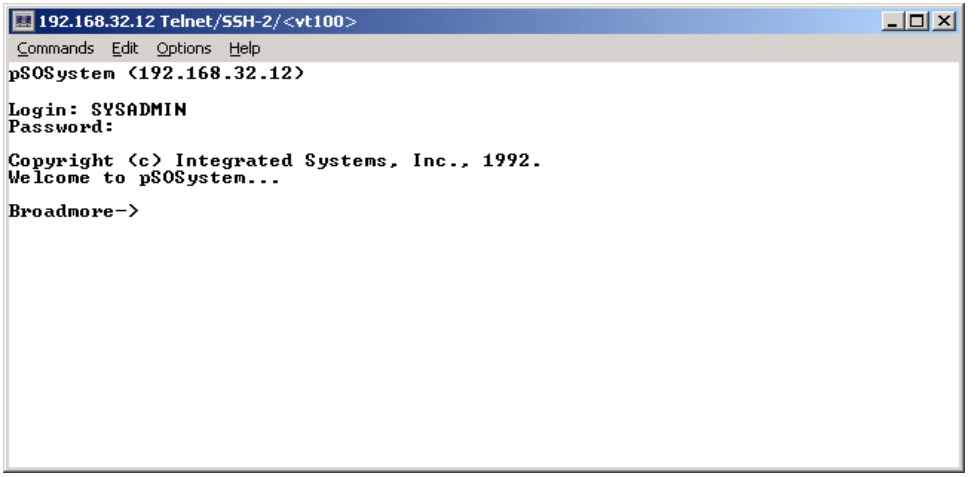
- **Audit Trails** – Audit trails must be enabled for FIPS mode.
  The cryptographic module provides a system log and user audit log. The audit log (audit.txt) records user actions while the system log (sys.log) records system events and configuration changes.
  A SuperUser has access to pSOS shell commands that can overwrite the system and audit log files. This misuse of shell commands to corrupt the audit trail is strictly prohibited and removes the Broadmore from the evaluated configuration. It is recommended that user audit trails be examined periodically in accordance with local security practice to determine if the Broadmore is being accessed by unauthorized users or during nonstandard hours, or if the configuration is being accessed or altered in an inappropriate manner. For example, every third consecutive attempted login failure produces an entry in the system log.

Logging In

The following example uses the Windows telnet client software.

To log into the Broadmore:

1. Open a telnet window.
2. Type in the Hostname and Username. The Hostname is the IP address of the Broadmore, and the Username is **admin**.
3. Select Keyboard Interactive from the Primary pull-down menu in the Authentication panel.
4. Click Connect.



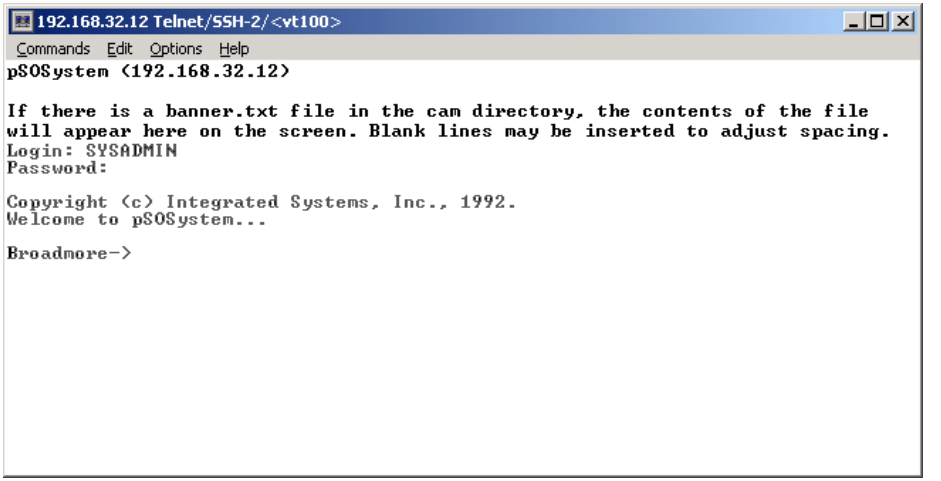
NOTE: For initial system installation, the factory default user name is **SYSADMIN** and the password is **INITIAL**. To ensure network security, a network administrator (SuperUser) must create new user names and passwords. See *"Managing Users and Audit Trails" on page 10-10*.

5. When Broadmore user login message displays, type the Login and Password. You will need to press Enter after each.

   After successfully logging into the Broadmore user's list, the Broadmore command prompt displays.

Log-in Banner

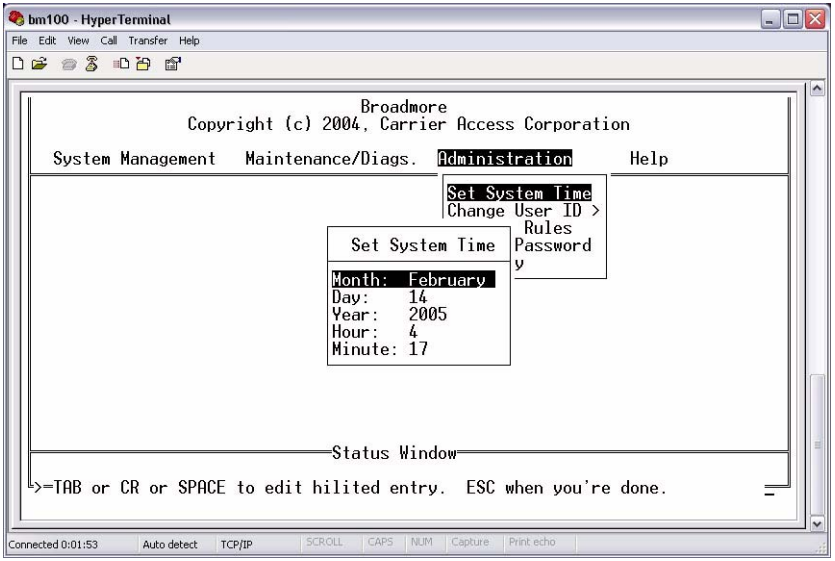
The Broadmore provides the ability to insert a customizable banner that will appear when a user logs in. The banner is a simple way to provide special instructions to the user. A SuperUser can implement this feature by using ftp or SFTP to download a banner text file, named **banner.txt**, to the Broadmore **cam** directory. When a shell login is requested, the contents of the banner file (if any) will be dumped to the screen just ahead of the login prompt, as in the following example.



System Clock

The Broadmore CPU system clock provides the time and date stamp used for system logs, events, and audit trails. A SuperUser must set the system clock either manually after powering up the Broadmore or configure the Broadmore to use a network timing source (see *"Network Time Protocol" on page 10-8*).

Select Set System Time from the Administration menu. Then set the Month, Day, Year, Hour, and Minute to the correct values. When finished, press Escape and select Yes to change the system clock.



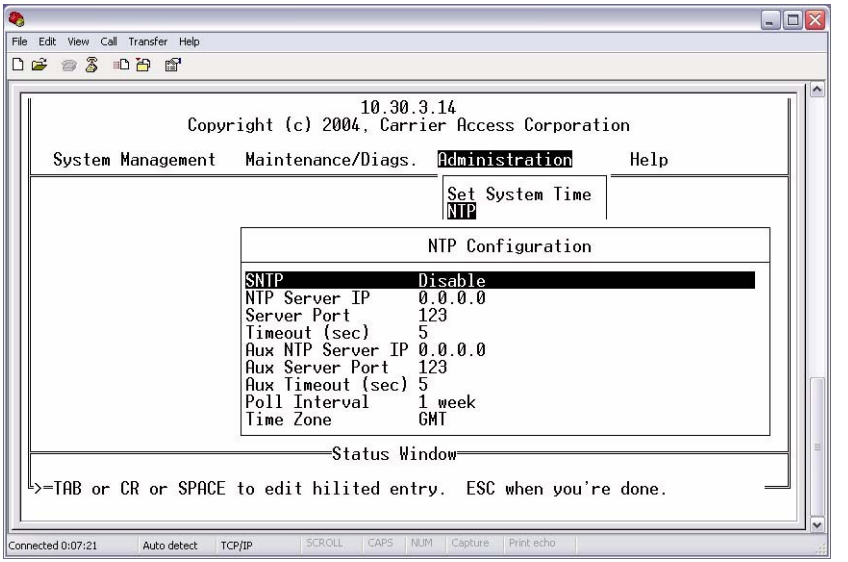
NOTE: Changing the system clock is an event recorded in the system log (see *"System Log" on page 10-15*).

Network Time Protocol

The Broadmore CPU system clock provides the time and date stamp used for system logs, events, and audit trails. A SuperUser must set the system clock either manually after powering up the Broadmore (see *"System Clock" on page 10-7*) or configure the Broadmore to use a network time source as described below. The Broadmore uses Simple Network Time Protocol (SNTP), which is an Internet standard for periodically synchronizing the system clocks connected to an IP network.

If the clock uses the NTP source, the system clock will be automatically synchronized to the NTP source when power is reapplied to the Broadmore.

Select NTP from the Administration menu. Then set the following parameters to the desired values. When finished, press Escape and select Yes to accept the changes.



Item	Options	Comments
SNTP	Enable, Disable	When enabled, the Broadmore system clock will be synchronized to the network time source.
NTP Server IP		The IP address of the primary network time source.
Server Port	0 to 32767	
Timeout (sec)	1 to 100	The time to wait for a response from the primary network time source.
Aux NTP Server IP		The IP address of the auxiliary network time source, to be used if a request to the primary network time source exceeds the timeout period.
Aux Server Port	0 to 32767	
Aux Timeout (sec)	1 to 100	The time to wait for a response from the auxiliary network time source.
Poll Interval	1 hr, 8 hr, 1 day, 1 week	Determines how often the Broadmore will request an update from the NTP source. The default is 1 week.
Time Zone	GMT or specific zone	The default is Greenwich Mean Time (GMT) but you can choose among 24 international time zones.

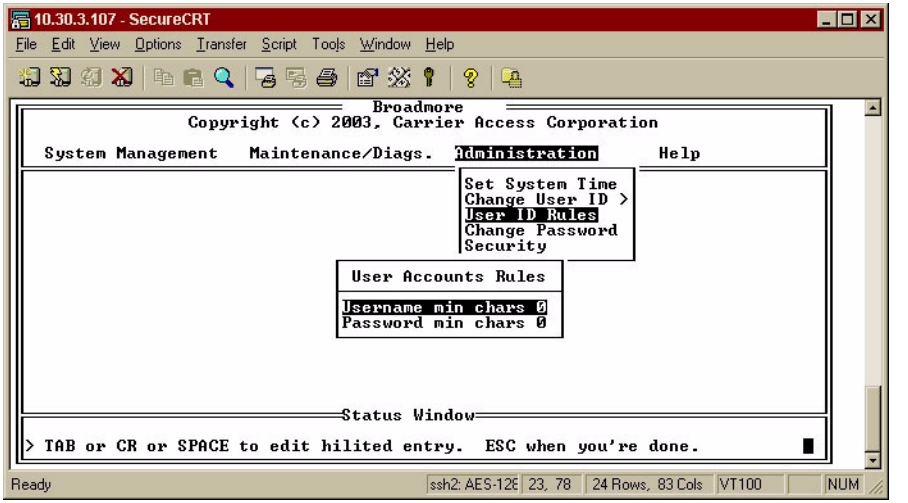
Managing Users and Audit Trails

- User ID Rules ... *10-10*
- Change User ID ... *10-11*
- User Audit Trails ... *10-13*

User ID Rules

A SuperUser can set the minimum allowable number of characters in user names and passwords by selecting User ID Rules from the Administration menu.

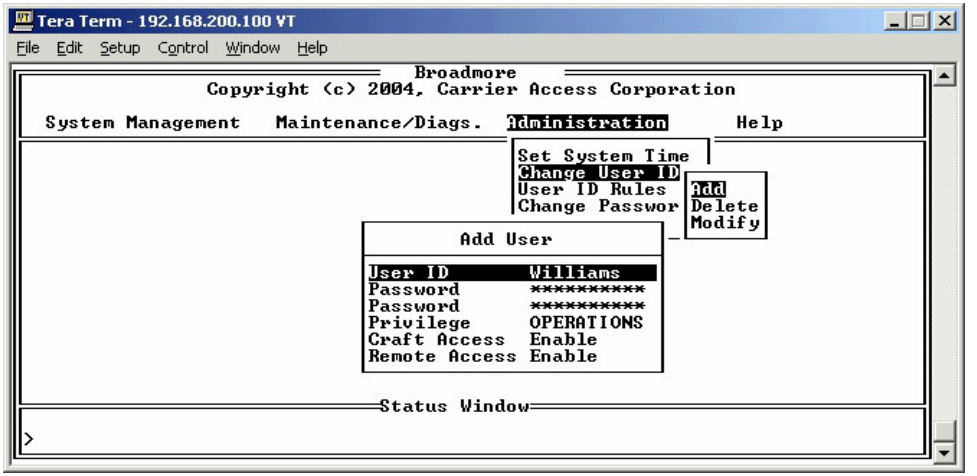
From this menu, select the Username or Password and enter the required minimum number of characters.



Change User ID

The Change User ID menu allows a SuperUser to add, delete, and modify user IDs. (Any user can change their own password using the Change Password menu.)

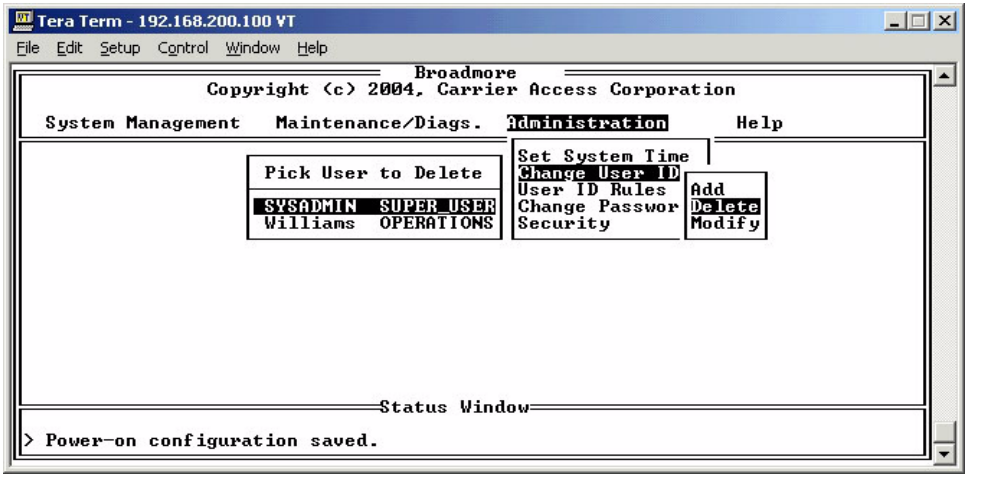
Adding a User



Enter the following information for each user that is added.

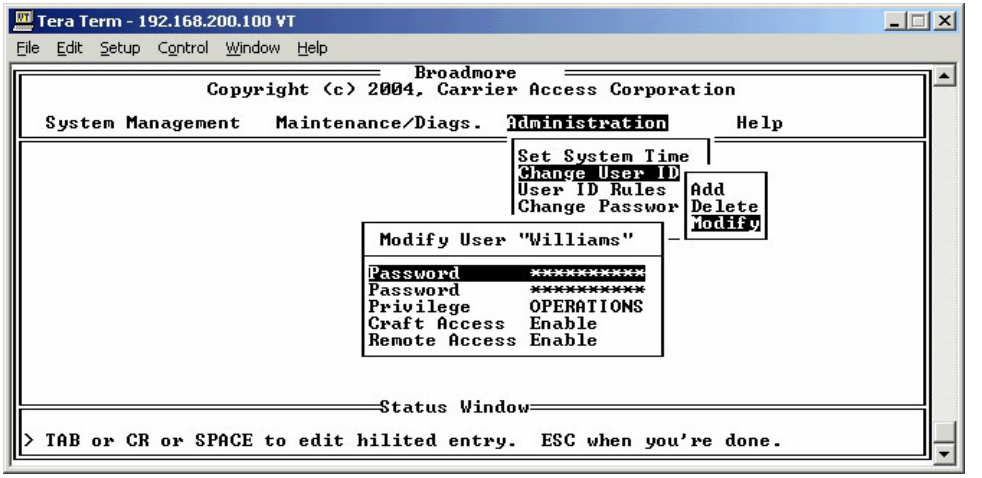
Item	Options	Comments
User ID		A unique user identifier
Password/ Password		A unique password for the user and a second password field to confirm
Privilege	BROWSER OPERATIONS SYS_ADMIN SUPER_USER	The level of user access. See *"User Security Configuration" on page 7-23.*
Craft Access	Enable, Disable	Access through the serial port on the front of the CPU.
Remote Access	Enable, Disable	Access through telnet, secure shell login, ftp or secure ftp.

Deleting a User



After you select the user to be deleted, a confirmation message appears. Select Yes to delete the user, or No to exit without making any changes.

Modifying a User



After you select the user to be modified, enter the appropriate information in the

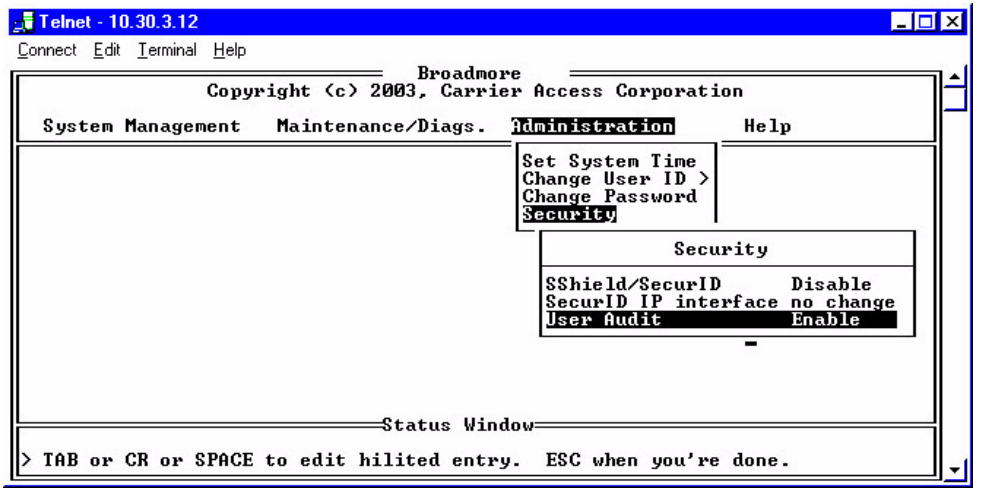
Modify User fields. See *"Adding a User" on page 10-11* for more information on the individual fields.

User Audit Trails

NOTE: It is recommended that audit trails remain disabled until deployment of the Broadmore with the anticipated "power up" configuration is complete. This prevents the audit logging of numerous initial installation configuration changes. Only a SuperUser can enable or disable this function or use shell commands to access the audit file.

Only a SuperUser can enable or disable this function or use shell commands to access the audit files.

Audit Trails protect a Broadmore by providing traceability of who performed procedures on the unit, what procedures were performed, and when they took place. The Broadmore local audit trail logs changes to configuration parameters and user logins.



NOTE: The audit file is located in the **cam** directory. The craft port will allow **cat**, **head**, or **tail** commands in the non-FIPS mode.

NOTE: Audit files can be up to 200k bytes, with the most recent data being located at the end of the file. Use the **tail** command to display the end of the file. For detailed examination, it is best to upload the file via FTP.

To display the audit file, at the Broadmore > prompt, enter the following commands:

cd cam ↵

tail audit.txt ↵

An example of the output is provided below.

```
Copyright (c) Integrated Systems, Inc., 1992.
Welcome to pSOSystem...

Broadmore->cd cam
Broadmore->tail audit.txt
08/08/2002 10:36:59 Q SYSADMIN:Security:User Audit=Enable
08/08/2002 10:37:53 Q SYSADMIN:Reboot System
08/09/2002 08:42:10 Q SYSADMIN:Create VP Reservation:"Test", slot G, vp 0, vcSt2
08/09/2002 08:45:22 Q SYSADMIN:Create VP Reservation:"Test2", slot G, vp 1, vcS2
08/09/2002 09:07:25 Q SYSADMIN:General Properties:Bandwidth Meter=Enable
Broadmore->
```

User audit files record the following information for each user action:

- date
- time
- online CPU (Q or R) or standby CPU (q or r)
- user name
- event type
- short description of the event

Once the **audit.txt** file is full, the file is automatically closed, the name is changed to **audit_o.txt**, in case a SuperUser wants to access the old file via FTP. A new file is then opened named **audit.txt** and new data is written to that file.

Deleting Audit Trails

A user can delete the contents of the system log by using the CAMMI (Maintenance/Diags, View System Log, Delete command) or the corresponding CLI command. However, this only deletes the events that can be viewed by their access level.

Archiving Audit Trails

A SuperUser can archive the **audit.txt** and **audit_o.txt** files using an FTP client to copy the files to another computer or storage device. After logging in with FTP, navigate to the **cam** directory and locate the audit.txt and audit_o.txt files.

System Log

The system log file **sys.log** is a circular file that contains a recent history of system users, events, and alarms. Old records are overwritten by new records. The log file identifies the currently active CPU and any user currently logged into the Broadmore. All users can use the CAMMI interface to view those system events permitted by their access role (see *"Maintenance and Troubleshooting" on page 8-1*). Only a SuperUser can copy or delete the sys.log file. After logging in using an FTP client, navigate to the **cam** directory and locate the sys.log file. The system log can be deleted and archived in much the same way as the audit log files.

For example, the SuperUser can delete the **sys.log** file by using the **del** shell command, as in the following example.

cd cam ↵

del sys.log ↵

Rather than using FTP, a SuperUser can also display or delete the system log through the Command Line Interface.

To display the system log, log into the Broadmore and enter the following commands at the Broadmore prompt:

cli ↵

maintain ↵

systemlog ↵

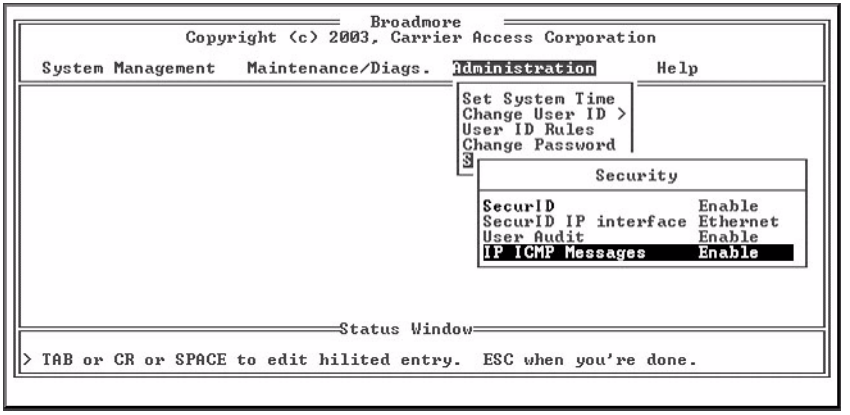
showi ↵

You can then navigate through the system log by following the instructions appearing at the bottom of the window.

To delete the system log, enter **clearlog** instead of **showi**.

IP ICMP Messages

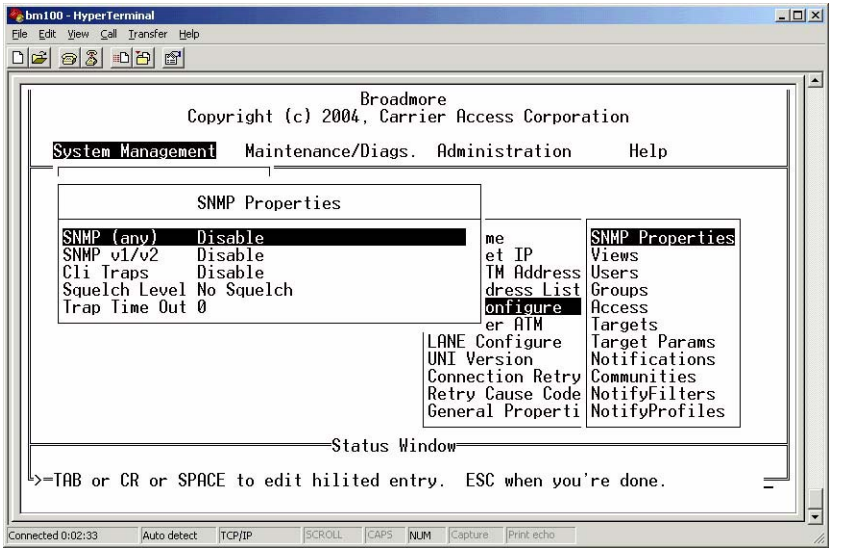
You can use the Internet Control Message Protocol selection to enable or disable all ICMP messages for Internet Protocols such as ping or echo. Disabling ICMP is a common defense against denial-of-service attacks using ping floods.



SNMP Messages

You can use the SNMP Properties selection to enable or disable SNMP messages. The Broadmore supports older SNMP v1 and v2, as well as newer SNMPv3 protocols. You have the option to disable only SNMPv1 and v2 messages, or all SNMP messages.

Only a SuperUser or SysAdmin can access or change these properties (see *"SNMP Properties" on page 12-3*).



Select **System Management** ↵
Select **Configure** ↵
Select **System Services** ↵
Select **SNMP Configure** ↵
Select **SNMP Properties** ↵

Shell Commands (Non-FIPS Mode)

Shell commands are UNIX-like commands provided by the embedded pSOS operating system. Command syntax is available using the “help” command. Authorized Access to each command is based on the user privilege level.

FIPS Mode

The Broadmore is shipped with FIPS mode security turned off. A SuperUser can use the **fipsmode** shell command to enable FIPS mode operation (see *“Security Management (FIPS Mode)” on page 11-1*).

Authorized Access to Shell Commands

The following table lists the authorized commands available to each access privilege level when operating in non-FIPS mode.

User ID → **↓ Authorized Services**	**Super_User**	**Sys_Admin**	**Operations**	**Browser**
arp	•	•		
cammi (start GUI interface)	•	•	•	•
cat	•	•	•	
cd	•	•	•	
cli	•	•	•	•
cmp	•	•	•	
comp	•	•	•	
copy	•	•	•	
cp	•	•	•	
del	•	•	•	
dir	•	•	•	
du	•	•		
echo	•	•	•	•
fipsmode	•			

User ID → ↓ Authorized Services	Super_User	Sys_Admin	Operations	Browser
head	●	●	●	
help	●	●	●	●
ifconf	●	●		
ls	●	●	●	
md	●	●		
mem	●			
mkdir	●	●		
move	●	●	●	
mv	●	●	●	
netstat	●	●		
ping	●	●	●	●
pwd	●	●	●	●
rd	●	●	●	
resetSecurID	●	●		
resetSecurIDIp	●	●		
rm	●	●	●	
rmdir	●	●	●	
route	●	●		
savert	●	●		
scp	●	●		
selftest	●			
setbaud	●	●	●	
setenv	●	●		
settimeout	●	●		
setwrite	●	●	●	
sigmem	●			
sshdSessionShow	●	●		
sshdShow	●	●		
tail	●	●	●	

User ID → ↓ Authorized Services	Super_User	Sys_Admin	Operations	Browser
touch	•	•		
zeroize	•			

FTP Login

Users can login using ftp to access Broadmore administrative functions over IP.

To log in to the Broadmore:

1. Open your ftp program. The Connect window opens.
2. Enter the IP address of the Broadmore.
3. Enter the Username: **SYSADMIN** (the username is case sensitive).
4. Enter the Password: (example) **jsmith** – the default password for new installations is **INITIAL** (passwords are case sensitive).

CHAPTER 11

Security Management (FIPS Mode)

In this Chapter:

- Security Features ... *11-2*
- Security Guidance ... *11-3*
- Authentication and Identification ... *11-6*
- Authorized Services ... *11-7*
- Key Management ... *11-8*
- Logging In ... *11-9*
- Log-in Banner ... *11-13*
- System Clock ... *11-14*
- Network Time Protocol ... *11-15*
- Changing Security Modes ... *11-17*
- User Administration and Audit Trails ... *11-26*
- Shell Commands (FIPS Mode) ... *11-34*
- SFTP Login ... *11-43*
- SecurID Features ... *11-49*
- Residual Data and Memory Volatility ... *11-50*

Security Features

This release of the Broadmore includes the Broadmore/SSHield Management Module, which is a FIPS 140-2 validated software-only module that meets the security requirements of Federal Information Processing Standard PUB 140-2. The Broadmore/SSHield Management Module enables the secure operation and control of the Broadmore's ATM configuration parameters via a command line interface (CLI) or menu based interface (CAMMI). TeamF1's SSHield provides security by means of the SSH (IETF SECSH) protocol to ensure that network connections are secure.

A detailed description of the Broadmore security features are provided in the "Broadmore/SSHield Management Module Version 4.0 Security Policy" available at the following web sites:

- *http://www.carrieraccess.com/support/* under the Broadmore documents
- *http://csrc.nist.gov/cryptval/* under the Validation Lists

When the FIPS Security option is enabled on the Broadmore, the following security features are available:

- RSA SecurID® authentication (optional, see *"SecurID Features" on page 11-49*)
- Private management data paths using SSHield for CLI/CAMMI sessions and Secure File Transfer Protocol (SFTP)
- Configuration activity audit trails
- Zeroize command for decommissioning one or both CPUs

Enabling FIPS mode security disables FTP and Telnet access. Users must log in using secure client replacements such as SecureCRT® and SecureFX®. A secure terminal emulator is required to enter a secure Broadmore system. Although many secure terminal emulators are available, SecureCRT is recommended.

NOTE: Be sure to use the appropriate fonts and screen settings to maintain the proper screen appearance.

Additional security-relevant features include:

- Enable/disable SNMP and ICMP messages
- SNMPv3 USM/VACM
- Log-in Banner for special user instructions

Security Guidance

- **Receipt and Inspection** – Broadmore components containing FIPS 140-2 validated software are packaged and sealed at the factory with tamper-proof security tape. Upon receipt, carefully examine the security sealing tapes on the shipping containers for any signs of tampering. (See *"Receipt" on page 3-2*.)
- **Security** – Broadmore components containing FIPS 140-2 validated software (CPU modules, memory modules, and storage media) should be handled in accordance with applicable security procedures.
- **Initial Login** – The Broadmore is shipped with a default username and password for logging in the first time. A SuperUser (Crypto Officer) should log in the first time to configure the Broadmore for secure operation.
  For maximum security, perform the following steps:
  (1) configure IP access (via ethernet, LANE, or CIP)
  (2) install security keys
  (3) create a temporary SuperUser account
  (4) delete the public SYSADMIN account
  (5) enable FIPS mode and reboot the system
  (6) after logging in securely, you can safely create user accounts and configure the Broadmore for secure operation.
- **Security Modes** – The Broadmore is shipped with security turned off. Only a SuperUser can change the FIPS and SecurID modes (see *"Changing Security Modes" on page 11-17*).

- **Potential Security Vulnerabilities**
  (1) Disabling fipsmode deletes existing user access accounts and cryptographic keys and reverts the Broadmore to the factory default SuperUser ID and password, which can deny management access and compromise security. No one can log in till the Broadmore is rebooted. It is recommended that the fipsmode be changed only during initial setup and decommissioning.
  (2) The Broadmore accepts loose source routed IP packets, so it is recommended that source routed packets be dropped on routers and firewalls. (See manufacturer's instructions.)
  (3) The Broadmore RS-232 COM 1 serial port used for "Craft Access" does not immediately terminate a management session if a user disconnects without typing "exit". During the following timeout period, another user can connect without logging into the RS-232 port and other users are denied access through the ethernet port. It is recommended that all accounts be created with "Remote Access" only, except for one failsafe SuperUser account with "Craft Access." The craft password should be stored safely in the NOC. When needed, the SuperUser can log into the craft port, fix things, change the password, log out, and store the new password back in the NOC.

- **Initialization and Verification** – When the Broadmore is powered up in the FIPS mode, the FIPS 140-2 validated software will perform a self-test to verify software integrity and cryptographic functions. To verify that the Broadmore is operating in FIPS mode, see *"Help About Security" on page 11-17*.

- **Key Management** – A DSA private hosts key is required for SSH2 connection to the Broadmore. A default key is provided for use in initializing the Broadmore after installation at the customer site. The SuperUser should change this key before making the Broadmore operational and change it periodically in accordance with local security practice.

- **System Clock** – The system clock is used to time stamp all events recorded in the system log and user audit log. To set the system clock, see *"System Clock" on page 11-14*.

- **User Administration** – The Broadmore authenticates users by identification and role-based access privilege levels and maintains an audit trail activity log. Only a SuperUser can assign users and access levels, set the minimum number of characters required for user names and passwords (user ID rules), and clear the system log. The security officer must ensure that all users change their passwords periodically in accordance with local security practice.
  (1) It is recommended that passwords be changed at least once every 6 months. Users must be instructed to use a random combination of all the usable characters for passwords.
  (2) It is recommended that all users, access privileges, and role assignments be reviewed periodically or whenever a personnel termination, transfer, or role change occurs.

- **Audit Trails** – Audit trails must be enabled for FIPS mode.
  The cryptographic module provides a system log and user audit log. The audit log (audit.txt) records user actions while the system log (sys.log) records system events and configuration changes.
  A SuperUser has access to pSOS shell commands that can overwrite the system and audit log files. This misuse of shell commands to corrupt the audit trail is strictly prohibited and removes the Broadmore from the evaluated configuration. It is recommended that user audit trails be examined periodically in accordance with local security practice to determine if the Broadmore is being accessed by unauthorized users or during nonstandard hours, or if the configuration is being accessed or altered in an inappropriate manner. For example, every third consecutive attempted login failure produces an entry in the system log.

- **Decomissioning and Sanitizing** – The **zeroize** command is not intended for normal operational use. It is intended as a security measure (per FIPS 140-2 requirements) to allow a SuperUser to completely remove all security-sensitive data that may be required before decommissioning a CPU. Turning off FIPS mode will erase Critical Security Parameters (CSPs) but does not erase the FIPS validated operating software. For additional information on sanitizing the equipment, see *"Residual Data and Memory Volatility" on page 11-50*.

Authentication and Identification

The cryptographic module supports distinct operator roles and enforces the separation of these roles using identity-based operator authentication that requires a Username and Password, and optional SecurID.

The SecurID option has no effect on FIPS 140-2 compliance. When SecurID is enabled, operators must also enter a SecurID token before they can gain access to the Broadmore. The SecurID token is a number that may be constant or change every minute, and it is verified by an RSA Authentication Manager deployed at the customer site.

A username and password are always required to log in, whether or not SecurID is enabled. The mandatory username is an alphanumeric string of characters whose minimum length can be set by the Security Officer. The password is a string of characters from the 94 printable and human-readable characters whose length can be set by the Crypto Officer.

Passwords be changed at least once every 6 months and that users be instructed to use a random combination of all the usable characters for passwords.

Upon successful authentication, the role and privilege level are selected based on the identity (username) of the operator. At the end of a session, the operator should log off, though the user is automatically logged off after a configurable period of inactivity.

Role	Privilege Level	Authorized Functions
User	Browser	User is able to look at most all data plane information but is not able to affect anything. To protect security data, no file access is permitted. This role cannot access the security settings.
	Operations	User is able to perform data plane configurations, such as defining PVCs, SVCs, configuring service card parameters. To protect security data, no file access is permitted under this privilege level. This role cannot access the security settings.
	SysAdmin	User is able to perform global configuration operations such as redundancy. To protect security data, no file access is permitted. This role cannot access the security settings.
Crypto Officer	SuperUser	This role is required to manage system accounts, use SFTP, and alter security settings. Only users at this privilege level may turn FIPS mode on or off.

Authorized Services

The following table lists the authorized services available to each privilege level.

User ID → ↓ Authorized Services	Super_User	Sys_Admin	Operations	Browser
SecureCRT (SSH2 terminal client)	•	•	•	•
SecureFX (SSH2 SFTP client)	•			
Change User ID	•			
Change own password	•	•	•	•
System Services	•	•		
Connection Retry	•	•	•	
Establish connections	•	•	•	
Delete connections	•	•	•	
Configure modules	•	•	•	
Maintenance/Diagnostics	•	•		
View System Log	•	•	•	•
Environmental Indicators	•	•	•	•
Boot/Reboot system or card	•	•		
Card diagnostics	•			
System test	•			
Check free CPU memory	•			
View configuration statistics	•	•	•	•
Security management including user accounts, audit trail, and zeroizing	•			
Change Files using shell commands	•			

NOTE: For a complete list, see *"Authorized Access to Shell Commands" on page 11-41*.

Key Management

A DSA private hosts key is required for SSH2 connection to the Broadmore.

Default DSA Key

During manufacture, a default **host_dsa** key file is placed in the **/SSHD** directory of the Broadmore CPU. This default key is intended only for use in initializing the Broadmore after installation at the customer site and should be changed by the SuperUser (Crypto Officer) before making the Broadmore operational.

NOTE: The DSA hosts key can only be replaced by the SuperUser while the Broadmore is in the FIPS mode.

Generating DSA Key Pairs

DSA keys can be generated on a UNIX or Windows host, using key generation utilities provided as a part of the ssh clients/server software of various vendors.

OpenSSH provides ssh-keygen to generate DSA keys on a UNIX or Windows host. The ssh-keygen program can be downloaded from the URL http://www.openssh.org.

The following example shows how to generate the **host_dsa** key on a UNIX host or on a Windows PC running Cygwin.

```
$ ssh-keygen -t dsa -f host_dsa -N "" -C <comments>
```

Installing the DSA Key

With the Broadmore in FIPS mode, the SuperUser can use an SSH2 client (such as SecureFX) to log into the Broadmore/SSHield module and install the **host_dsa** key in the **/SSHD** directory on the Broadmore CPU.

NOTE: After installing the DSA key, the Broadmore must be rebooted in order for the change to take effect.

Logging In

NOTE: If FIPS mode is currently turned off, you must follow the non-FIPS mode instructions for *"Logging In" on page 10-5*.

Broadmore units are shipped from the factory with SecurID turned off and FIPS mode turned off. After logging into the Broadmore, the Crypto Officer can configure the Broadmore to use SecurID, if desired.

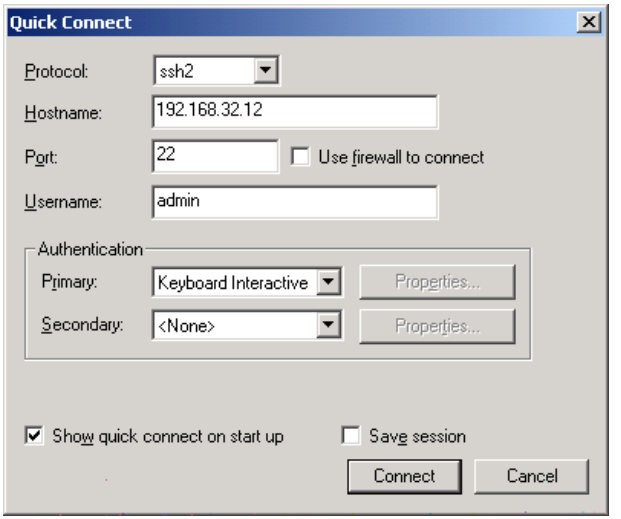
Using both SecurID and FIPS mode with the Broadmore provides a two-stage login. First, users log in using RSA SecurID. Then they can log into the Broadmore/SSHield Management Module.

Logging in with SecurID Disabled

The following example uses SecureCRT as the secure client software.

To log into the Broadmore:

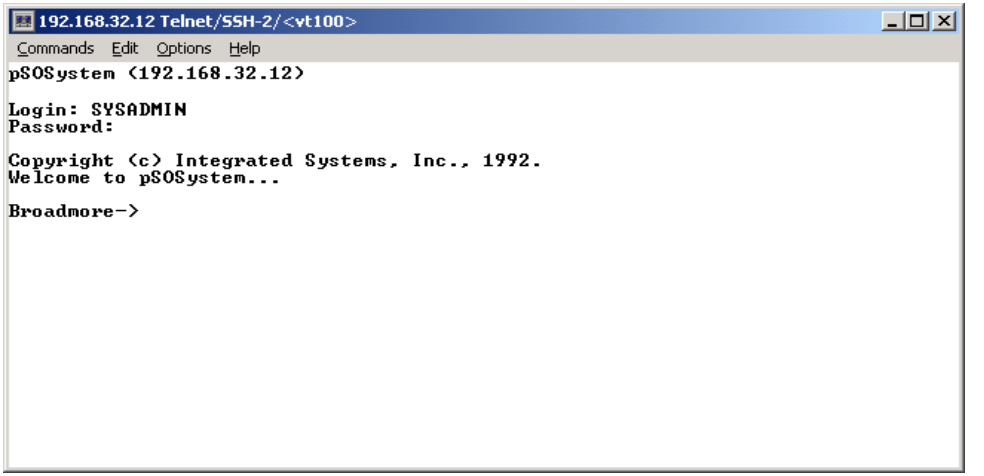
1. Open SecureCRT. The Quick Connect window opens.



2. Select ssh2 from the Protocol pull-down menu.

3. Type in the Hostname and Username. The Hostname is the IP address of the Broadmore, and the Username is the Broadmore user name.
4. Click Connect.
5. When the Broadmore Login message appears, type in the Login and Password. You will need to press Enter after each. (The factory defaults for the initial installation are **SYSADMIN** and **INITIAL**.)

   After successfully logging in, the Broadmore command prompt displays.

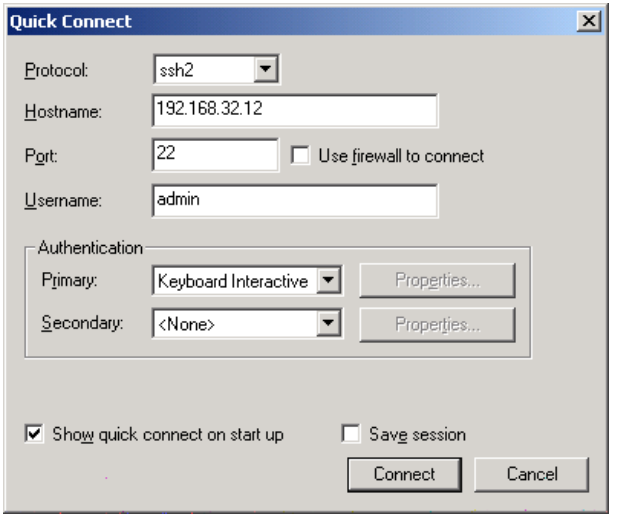


Logging in with SecurID Enabled

The following example uses SecureCRT as the secure client software.

To log into the RSA SecurID server:

1. Open SecureCRT. The Quick Connect window opens.

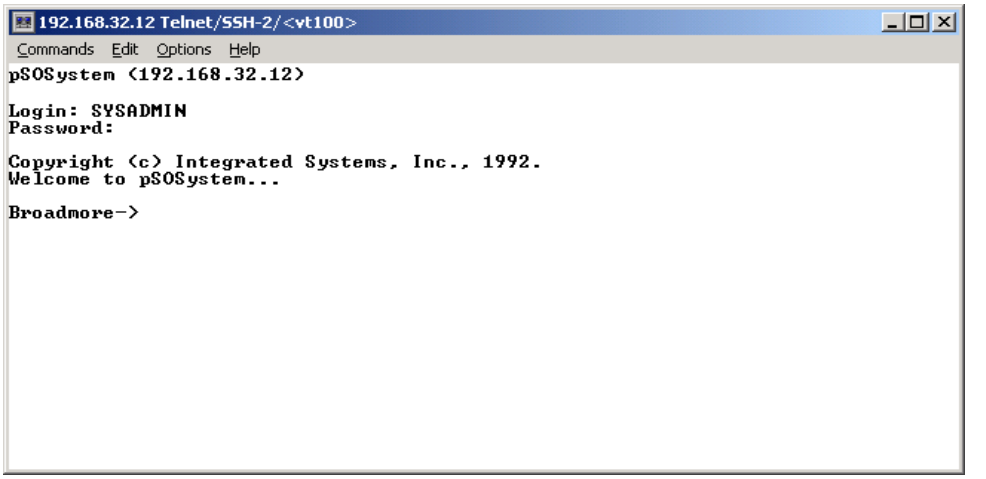


2. Select ssh2 from the Protocol pull-down menu.
3. Type in the Hostname and Username. The Hostname is the IP address of the Broadmore, and the Username is the SecurID user name that is configured on the RSA SecurID server with a token assigned to it.
4. Select Keyboard Interactive from the Primary pull-down menu in the Authentication panel.
5. Click Connect.

The Keyboard Interactive Authentication opens.

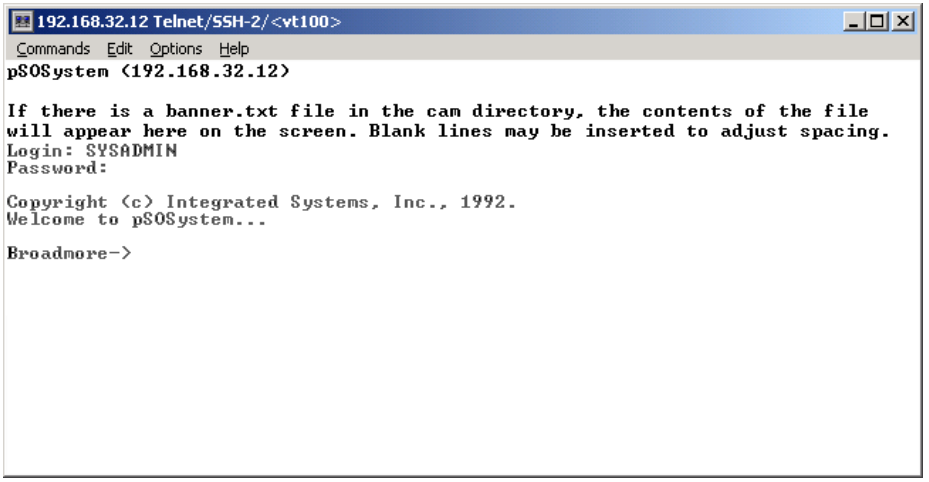


6. Type in the SecurID passcode, and click OK.
7. After successfully logging into SecurID, the Broadmore login displays.
8. Type the Login and Password. You will need to press Enter after each. (The factory defaults for the initial installation are **SYSADMIN** and **INITIAL**.) After successful login, the Broadmore command prompt appears.



Log-in Banner

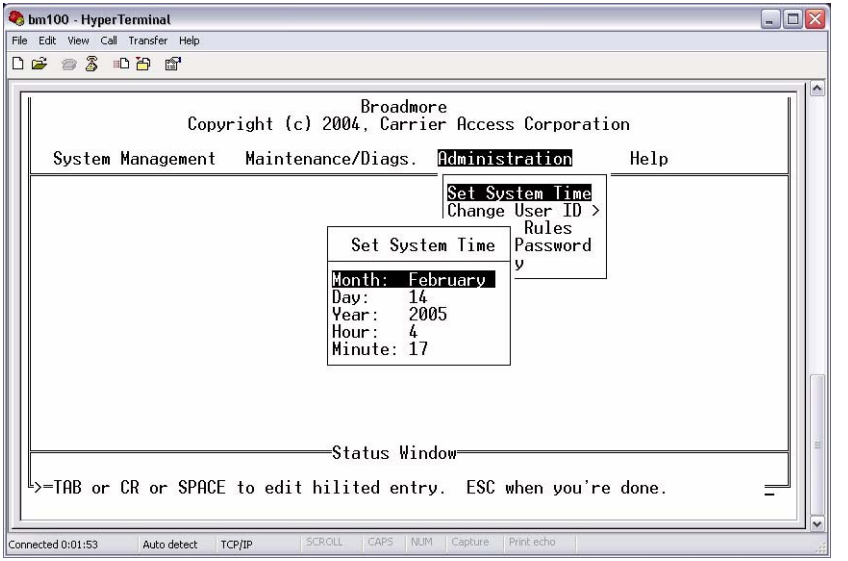
The Broadmore provides the ability to insert a customizable banner that will appear when a user logs in. The banner is a simple way to provide special instructions to the user. A SuperUser can implement this feature by using ftp or SFTP to download a banner text file, named **banner.txt**, to the Broadmore **cam** directory. There is no limit to the size of this file. When a shell login is requested, the contents of the banner file (if any) will be dumped to the screen just ahead of the login prompt, as in the following example.



System Clock

The Broadmore CPU system clock provides the time and date stamp used for system logs, events, and audit trails. A SuperUser must set the system clock either manually after powering up the Broadmore or configure the Broadmore to use a network timing source (see *"Network Time Protocol" on page 11-15*).

Select Set System Time from the Administration menu. Then set the Month, Day, Year, Hour, and Minute to the correct values. When finished, press Escape and select Yes to change the system clock.



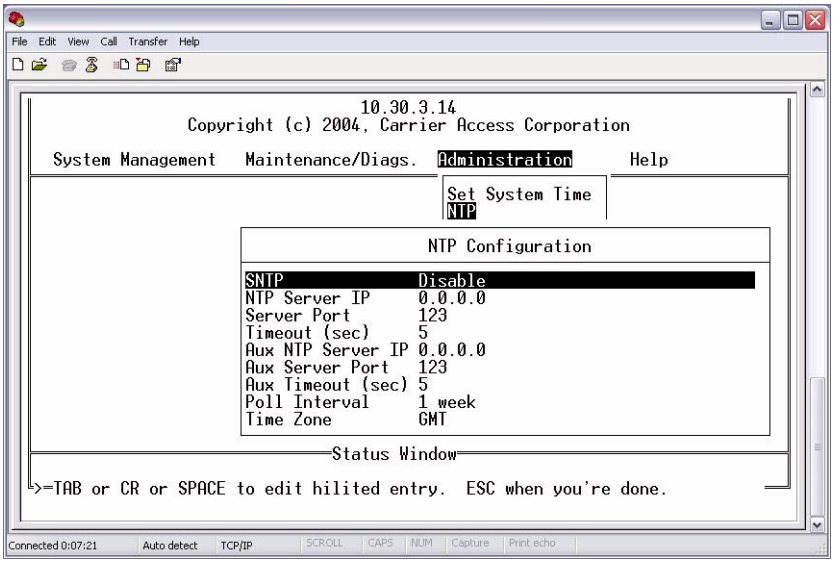
NOTE: Changing the system clock is an event recorded in the system log (see *"System Log" on page 11-32*).

Network Time Protocol

The Broadmore CPU system clock provides the time and date stamp used for system logs, events, and audit trails. A SuperUser must set the system clock either manually after powering up the Broadmore (see *"System Clock" on page 11-14*) or configure the Broadmore to use a network time source as described below. The Broadmore uses Simple Network Time Protocol (SNTP), which is an Internet standard for periodically synchronizing the system clocks connected to an IP network.

If the clock uses the NTP source, the system clock will be automatically synchronized to the NTP source when power is reapplied to the Broadmore.

Select NTP from the Administration menu. Then set the following parameters to the desired values. When finished, press Escape and select Yes to accept the changes.



Item	Options	Comments
SNTP	Enable, Disable	When enabled, the Broadmore system clock will be synchronized to the network time source.
NTP Server IP		The IP address of the primary network time source.
Server Port	0 to 32767	
Timeout (sec)	1 to 100	The time to wait for a response from the primary network time source.
Aux NTP Server IP		The IP address of the auxiliary network time source, to be used if a request to the primary network time source exceeds the timeout period.
Aux Server Port	0 to 32767	
Aux Timeout (sec)	1 to 100	The time to wait for a response from the auxiliary network time source.
Poll Interval	1 hr, 8 hr, 1 day, 1 week	Determines how often the Broadmore will request an update from the NTP source. The default is 1 week.
Time Zone	GMT or specific zone	The default is Greenwich Mean Time (GMT) but you can choose among 24 international time zones.

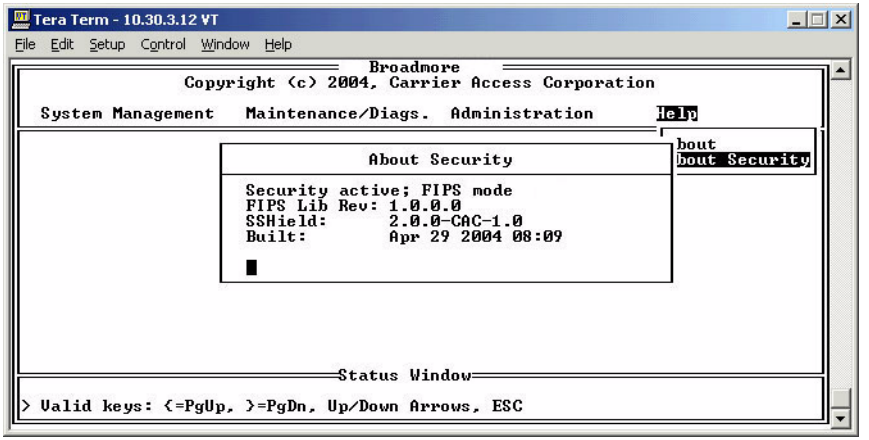
Changing Security Modes

- Help About Security ... *11-17*
- Enabling FIPS Mode ... *11-18*
- Disabling FIPS Mode ... *11-20*
- Enabling SecurID ... *11-21*
- Disabling SecurID ... *11-24*
- IP ICMP Messages ... *11-24*
- SNMP Messages ... *11-25*

Only a Crypto Officer (SuperUser) can change the security modes. The Broadmore is shipped from the factory with FIPS mode and SecurID turned off. The security modes can only be changed after successfully logging into the Broadmore while operating in the current mode configuration (see *"Logging In" on page 11-9*).

Help About Security

Any user, regardless of security level, can use this command. Selecting Help About Security from the main menu will display the current FIPS mode setting and the version numbers of the security software included in the Broadmore.



Item	Comments
FIPS Mode Active	Broadmore is in FIPS 140-2 validated operating mode
Security inactive; non-FIPS mode	Broadmore is not in FIPS approved operating mode
FIPS Lib Rev	Version of FIPS Library.
SSHield	Version of SSHield software
Built	Build date of SSHield software

Enabling FIPS Mode

Only a Superuser (Crypto Officer) can change the security modes. The Broadmore is shipped from the factory with FIPS mode turned off. The security mode can only be changed after successfully logging into the Broadmore for the first time, by performing the following steps.

1. Log into the online CPU (Broadmore primary IP address) with a conventional terminal emulator such as Telnet (see *"Logging In" on page 10-5*).
2. Enable FIPS mode by entering the following command at the Broadmore prompt:
   fipsmode on ↵
3. Set the session timeout for the Broadmore craft port by entering the following command:
   settimeout <hh:mm:ss> ↵
   Example: **settimeout 00:05:00** sets the timeout to 5 minutes.
   The current value can be displayed by entering **settimeout** by itself.

NOTE: The SSH session timeout is fixed at 5 minutes.

4. Reboot the Broadmore for the change to take effect by entering the following commands at the Broadmore prompt:
   cli ↵
   maintain ↵
   redundancy ↵
   cpu ↵
   rebootstandby ↵
   releasecpu ↵

NOTE: The above command sequence reboots the standby CPU (if any) and then the online CPU. In a redundant system, both CPUs must be rebooted into the FIPS mode. Rebooting the online CPU will terminate the current management session. After reboot, the previous standby CPU will normally become the online CPU. It may take several minutes for the ARP tables in the network to refresh before you can log into the online CPU.

5. Verify that the Broadmore is in FIPS mode by logging in with an SSH terminal emulator such as SecureCRT (see *"Logging In" on page 11-9*). If you must use Telnet, the Broadmore is not in FIPS mode.
6. Start up the CAMMI interface by entering the following command at the Broadmore prompt:
   cammi ↵
7. After logging in, also verify that the Broadmore is in FIPS mode by observing that the CAMMI *Help / About Security* screen shows that FIPS mode is active (see *"Help About Security" on page 11-17*).
8. Select *Administration / User ID Rules* and set the username and password minimum length values (see *"User ID Rules" on page 11-26*).

NOTE: The Broadmore will only enforce the minimum length values when creating new user accounts. Old accounts are not affected. The Superuser (Crypto Officer) must ensure that all user accounts meet FIPS 140-2 requirements.

Disabling FIPS Mode

Only a Superuser (Crypto Officer) can change the security modes. The security mode can only be changed after successfully logging into the Broadmore, then performing the following steps.

CAUTION! DISABLING FIPSMODE WILL DELETE EXISTING USER ACCESS ACCOUNTS AND CRYPTOGRAPHIC KEYS AND REVERT THE BROADMORE TO THE FACTORY DEFAULT SUPERUSER ID AND PASSWORD, WHICH CAN DENY MANAGEMENT ACCESS AND COMPROMISE SECURITY. NO ONE CAN LOG IN REMOTELY TILL THE BROADMORE IS REBOOTED.

1. Log into the online CPU (Broadmore primary IP address) with a secure SSH terminal emulator such as SecureCRT (see *"Logging In" on page 11-9*).
2. Disable FIPS mode by entering the following shell command at the Broadmore prompt:
   fipsmode off ↵
3. Reboot the Broadmore for the change to take effect by entering the following commands at the Broadmore prompt:
   cli ↵
   maintain ↵
   redundancy ↵
   cpu ↵
   rebootstandby ↵
   releasecpu ↵

NOTE: The above command sequence reboots the standby CPU (if any) and then the online CPU. In a redundant system, both CPUs must be rebooted into the non-FIPS mode. Rebooting the online CPU will terminate the current management session. After reboot, the previous standby CPU will normally become the online CPU. It may take several minutes for the ARP tables in the network to refresh before you can log into the online CPU.

4. Log into the Broadmore using a conventional terminal emulator such as Telnet (see *"Logging In" on page 10-5*).
5. Start up the CAMMI interface by entering the following command at the Broadmore prompt:
   cammi ↵
6. Verify that the Broadmore is not in FIPS mode by observing that the CAMMI *Help / About Security* screen shows that FIPS mode is inactive.

Enabling SecurID

NOTE: SecurID is only available when FIPS mode is turned on (see *"Enabling FIPS Mode" on page 11-18*). Only the online CPU can be accessed when SecurID is enabled.

Only a Superuser (Crypto Officer) can change the security modes. The Broadmore is shipped from the factory with SecurID turned off. The security mode can only be changed after successfully logging into the Broadmore while in its current security mode.

SecurID requires that the Broadmore CPUs be set up for use with a SecurID server. Each CPU must be set up one at a time. In a redundant system, one CPU must be temporarily removed while the other is being set up.

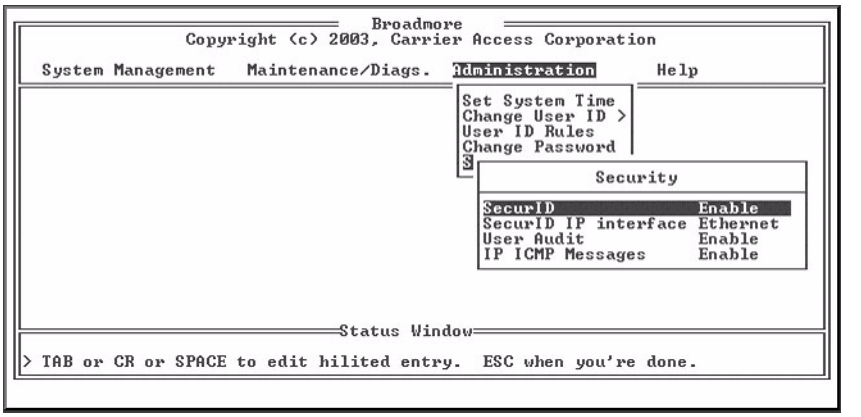
SecurID requires the following:

- RSA SecurID server version 5.0 or higher
- SSH terminal emulator, such as SecureCRT
- SFTP software, such as SecureFX
- Ethernet connection to both CPUs

1. If the Broadmore has two CPUs, remove the CPU that is not on line.

Setting up the first CPU

2. Using an SSH terminal emulator, log into the online CPU and ensure that the Broadmore is operating in FIPS mode (see *"Help About Security" on page 11-17*). If FIPS mode is not enabled, follow the procedure in *"Enabling FIPS Mode" on page 11-18* to turn on FIPS mode and then reboot the Broadmore.
3. On the SecurID server, create an Agent Host for the Broadmore and a **sdconf.rec** file.
4. Using SFTP software, put the **sdconf.rec** file into the **securid** directory of the Broadmore's online CPU.
5. Using the CAMMI *Administration / Security* menu, select SecurID and press the space bar choose Enable. Select SecurID Interface and press the space bar to choose Ethernet. (See figure below.)
6. If the step 5 was successful, the first CPU is set up correctly and you are ready to use SecureID with that CPU. If step 5 was not successful, do not proceed until the problem is fixed.



Item	Options	Comments
SecurID	Enable, Disable	This feature is described in the Carrier Access *RSA SecurID Ready Implementation Guide* for the Broadmore 500, 1700, and 1750. This guide also describes how to manipulate the security options in the "sdopts.rec" file.
SecurID IP Interface	No change, IP, LANE, CIP	If you choose "no change," any pre-existing sdopts.rec file will not be affected. If no sdopts.rec file exists, the system will default to ethernet IP. If you choose another option, the system will create an sdopts.rec file with your selection.

Setting up the second CPU

7. Using SFTP software, get the following three files from the **secureid** directory for use in setting up the second CPU: **sdconf.rec**, **secret**, and **sdopts.rec**.
8. Remove the first CPU and insert the second CPU into the chassis.
9. Using an SSH terminal emulator, log into the second CPU and ensure that the Broadmore is operating in FIPS mode (see *"Help About Security" on page 11-17*). If FIPS mode is not enabled, follow the procedure in *"Enabling FIPS Mode" on page 11-18* to turn on FIPS mode and then reboot the Broadmore.
10. Using SFTP software, put the three files (copied in step 7) into the **secureid** directory of the second CPU: **sdconf.rec**, **secret**, and **sdopts.rec**.
11. Using the CAMMI Administration/Security menu, select SecurID and press the space bar choose Enable. Select SecurID Interface and press the space bar to choose Ethernet.
12. Log out and log back in using your SecurID credentials.
13. If the proceeding step was successful, you can now insert both CPUs.

Disabling SecurID

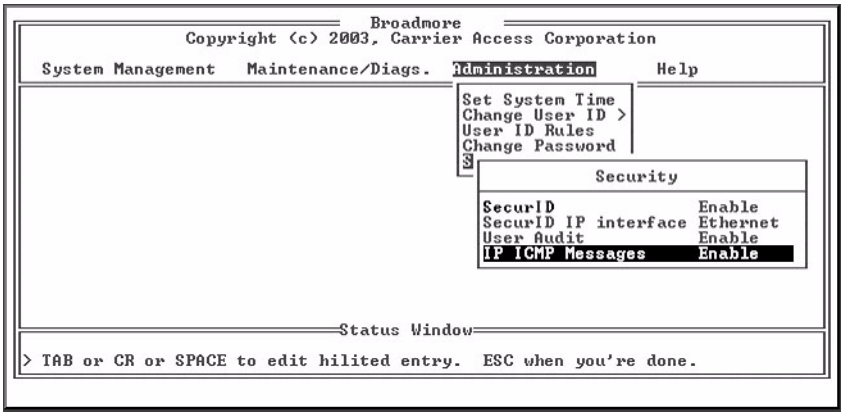
NOTE: SecurID is only available when FIPS mode is turned on (see *"Enabling FIPS Mode" on page 11-18*). Only the online CPU can be accessed when SecurID is enabled.

Only a Superuser (Crypto Officer) can change the security modes. The Broadmore is shipped from the factory with SecurID turned off. The security mode can only be changed after successfully logging into the Broadmore while in its current security mode.

1. Using the CAMMI *Administration / Security* menu, select SecurID and press the space bar choose Disable.
2. The next time you log into the Broadmore, you will not have to provide any SecurID credentials.

IP ICMP Messages

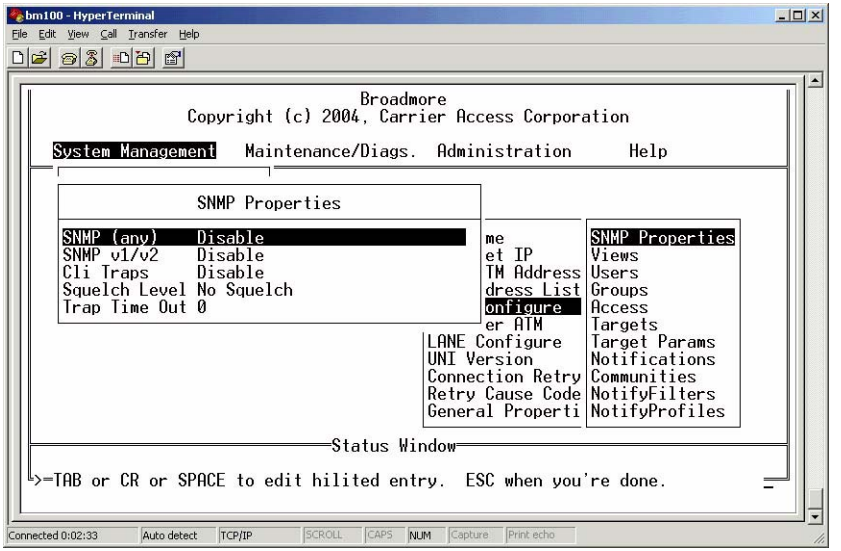
You can use the Internet Control Message Protocol selection to enable or disable all ICMP messages for Internet Protocols such as ping or echo. Disabling ICMP is a common defense against denial-of-service attacks using ping floods.



SNMP Messages

You can use the SNMP Properties selection to enable or disable SNMP messages. The Broadmore supports older SNMP v1 and v2, as well as newer SNMPv3 protocols. You have the option to disable only SNMPv1 and v2 messages, or all SNMP messages.

Only a SuperUser or SysAdmin can access or change these properties (see *"SNMP Properties" on page 12-3*).



Select **System Management** ↵
Select **Configure** ↵
Select **System Services** ↵
Select **SNMP Configure** ↵
Select **SNMP Properties** ↵

User Administration and Audit Trails

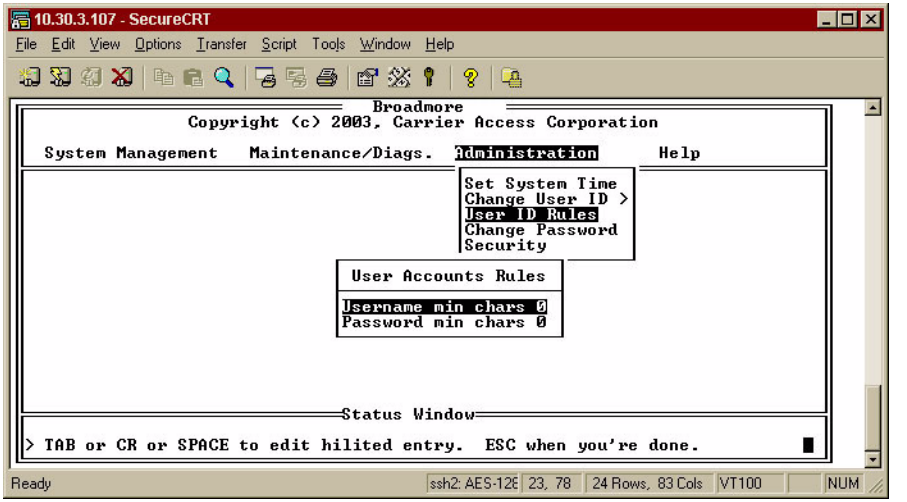
- User ID Rules ... *11-26*
- Change User ID ... *11-27*
- User Audit Trails ... *11-30*

User ID Rules

A SuperUser can set the minimum allowable number of characters in user names and passwords by selecting User ID Rules from the Administration menu.

From this menu, select the Username or Password and enter the required minimum number of characters. These values must be set to at least 6 characters to satisfy FIPS 140-2 security requirements.

NOTE: The Broadmore will only enforce the minimum length values when creating new user accounts. Old accounts are not affected. It is up to the Superuser (Crypto Officer) to ensure that all user accounts meet FIPS 140-2 security requirements.

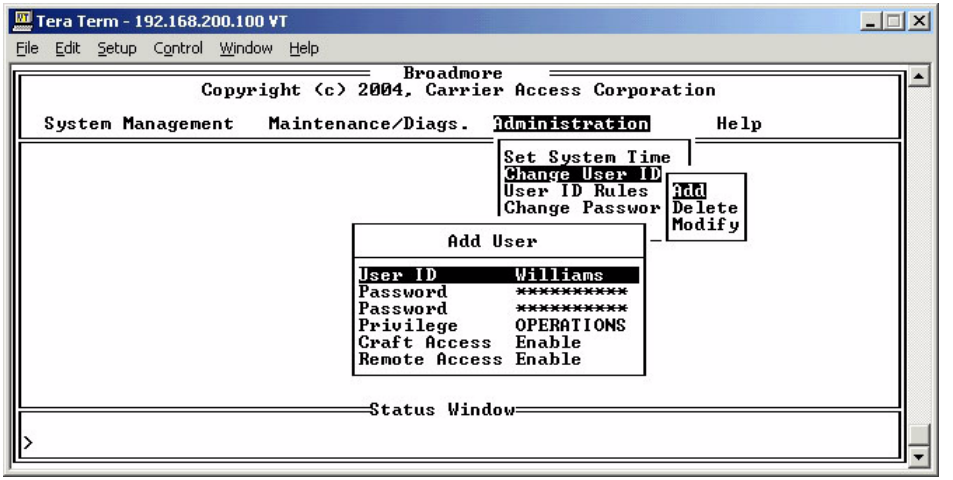


Change User ID

The Change User ID menu allows a SuperUser to add, delete, and modify user IDs.

NOTE: After logging in, any user can change their own password using the Change Password menu.

Adding a User

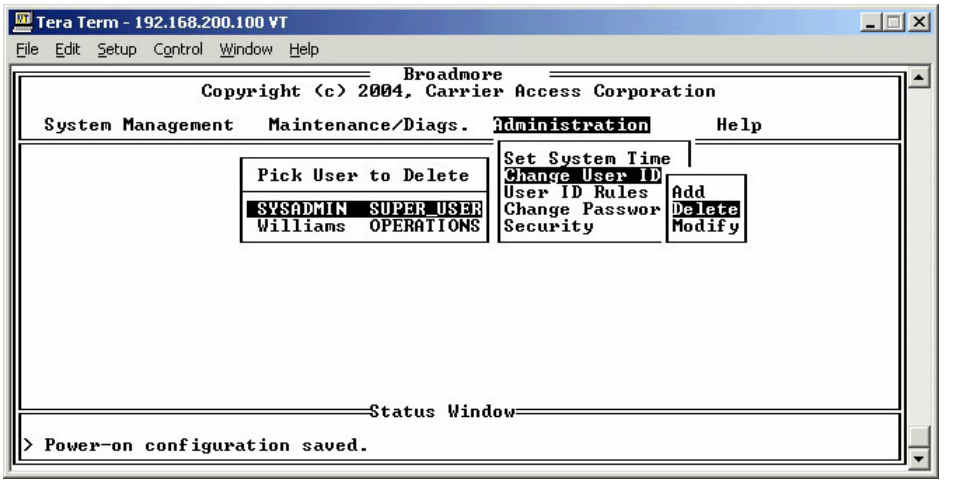


Enter the following information for each user that is added.

Item	Options	Comments
User ID		A unique user identifier
Password/ Password		A unique password for the user and a second password field to confirm
Privilege	BROWSER OPERATIONS SYS_ADMIN SUPER_USER	The level of user access. See *"User Security Configuration" on page 7-23.*

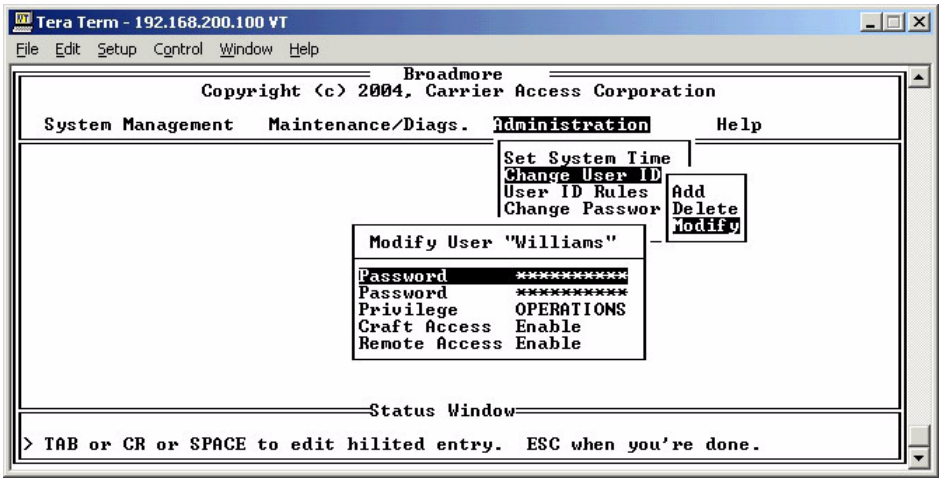
Item	Options	Comments
Craft Access	Enable, Disable	Access through the serial port on the front of the CPU.
Remote Access	Enable, Disable	Access through the Ethernet port on the CPU IOM.

Deleting a User



After you select the user to be deleted, a confirmation message appears. Select Yes to delete the user, or No to exit without making any changes.

Modifying a User



After you select the user to be modified, enter the appropriate information in the Modify User fields.

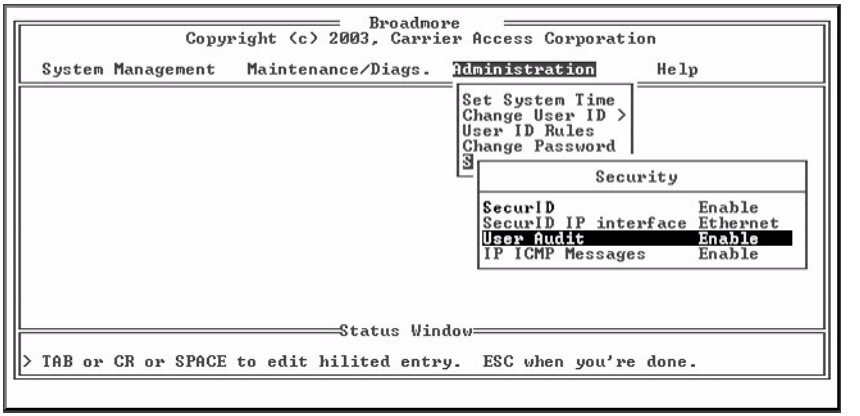
Item	Options	Comments
User ID		A unique user identifier
Password/ Password		A unique password for the user and a second password field to confirm
Privilege	BROWSER OPERATIONS SYS_ADMIN SUPER_USER	The level of user access. See *"User Security Configuration" on page 7-23.*
Craft Access	Enable, Disable	Access through the serial port on the front of the CPU.
Remote Access	Enable, Disable	Access through telnet, secure shell login, ftp or secure ftp.

User Audit Trails

NOTE: It is recommended that audit trails remain disabled until deployment of the Broadmore with the anticipated "power up" configuration is complete. This prevents the audit logging of numerous initial installation configuration changes. Only a SuperUser can enable or disable this function or use shell commands to access the audit file.

Only a SuperUser can enable or disable this function or use shell commands to access the audit files.

Audit Trails protect a Broadmore by providing traceability of who performed procedures on the unit, what procedures were performed, and when they took place. The Broadmore local audit trail logs changes to configuration parameters and user logins.



NOTE: The audit file is located in the **cam** directory and can only be accessed via SSH2. The craft port does not allow **cat**, **head**, or **tail** commands in the FIPS mode.

NOTE: Audit files can be up to 200k bytes, with the most recent data being located at the end of the file. Use the **tail** command to display the end of the file. For detailed examination, it is best to upload the file via FTP or SFTP.

To display the audit file, at the Broadmore > prompt, enter the following commands:

cd cam ↵

tail audit.txt ↵

An example of the output is provided below.

```
Copyright (c) Integrated Systems, Inc., 1992.
Welcome to pSOSystem...

Broadmore->cd cam
Broadmore->tail audit.txt
08/08/2002 10:36:59 Q SYSADMIN:Security:User Audit=Enable
08/08/2002 10:37:53 Q SYSADMIN:Reboot System
08/09/2002 08:42:10 Q SYSADMIN:Create VP Reservation:"Test", slot G, vp 0, vcSt2
08/09/2002 08:45:22 Q SYSADMIN:Create VP Reservation:"Test2", slot G, vp 1, vcS2
08/09/2002 09:07:25 Q SYSADMIN:General Properties:Bandwidth Meter=Enable
Broadmore->
```

User audit files record the following information for each user action:

- date
- time
- online CPU (Q or R) or standby CPU (q or r)
- user name
- event type
- short description of the event

Once the **audit.txt** file is full, the file is automatically closed, the name is changed

to **audit_o.txt**, in case a SuperUser wants to access the old file via SecureFX in SFTP mode. A new file is then opened named **audit.txt** and new data is written to that file.

Deleting Audit Trails

A user can delete the contents of the system log by using the CAMMI (Maintenance/Diags, View System Log, Delete command) or the corresponding CLI command. However, this only deletes the events that can be viewed by their access level.

Archiving Audit Trails

A SuperUser can archive the **audit.txt** and **audit_o.txt** files using an SSH2 FTP client such as SecureFX to copy the files to another computer or storage device. After logging in with SecureFX, navigate to the **cam** directory and locate the audit.txt and audit_o.txt files.

System Log

The system log file **sys.log** is a circular file that contains a recent history of system users, events, and alarms. Old records are overwritten by new records. The log file identifies the currently active CPU and any user currently logged into the Broadmore. All users can use the CAMMI interface to view those system events permitted by their access role (see *"Maintenance and Troubleshooting" on page 8-1*). Only a SuperUser can copy or delete the sys.log file. After logging in using an SSH2 FTP client such as SecureFX, navigate to the **cam** directory and locate the sys.log file. The system log can be deleted and archived in much the same way as the audit log files.

For example, the SuperUser can delete the **sys.log** file by using the **del** shell command, as in the following example.

cd cam ↵

del sys.log ↵

Rather than using FTP, a SuperUser can also display or delete the system log through the Command Line Interface.

To display the system log, log into the Broadmore and enter the following commands at the Broadmore prompt:

cli ↵

maintain ↵

systemlog ↵

showi ↵

You can then navigate through the system log by following the instructions appearing at the bottom of the window.

To delete the system log, enter **clearlog** instead of **showi**.

Shell Commands (FIPS Mode)

- fipsmode ... *11-34*
- selftest ... *11-34*
- settimeout ... *11-35*
- sshdShow ... *11-35*
- sshdSessionShow ... *11-37*
- scp ... *11-38*
- resetSecurID ... *11-39*
- zeroize ... *11-40*
- Authorized Access to Shell Commands ... *11-41*

Shell commands are UNIX-like commands provided by the embedded operating system. Command syntax is available using the "help" command. Authorized Access to each command is based on the user privilege level.

fipsmode

NOTE: The procedure for using this command is given in *"Enabling FIPS Mode" on page 11-18*.

The FIPS mode can only be changed by a SuperUser (Crypto Officer). At the Broadmore prompt, type **fipsmode** (to see current value) or **fipsmode on** (to enable) or **fipsmode off** (to disable). After executing this command, the Broadmore must be rebooted for the change to take effect.

selftest

Self-tests of the FIPS algorithms are performed automatically during power-up. A SuperUser (Crypto Officer) can perform a manual self-test at any time. At the Broadmore prompt, type **selftest**. The following message will be displayed if all tests pass.

```
AES Passed
DES Passed
TDES Passed
```

```
DSA Passed
FIPS 186-2 RAND Passed
RSA Passed
SHA1 Passed
IMAGE SIG VERIFY Passed
HMAC-SHA1 Passed
```

NOTE: If a manually initiated self-test results in a self-test failure, the management module will reboot.

NOTE: A FIPS algorithm self-test failure will immediately disable all management connections, as required by FIPS-2. The Broadmore will continue to carry existing ATM communications traffic across the data plane but the operating configuration can not be changed until the unit is repaired.

settimeout

A SuperUser (Crypto Officer) can set the session timeout for the Broadmore craft port for user inactivity. The command syntax is:

settimeout <hh:mm:ss>

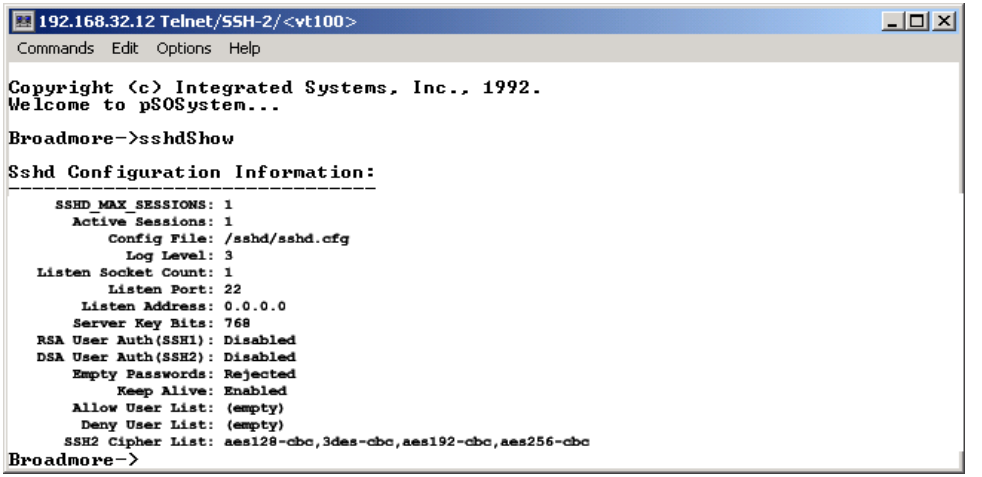
Example: **settimeout 00:05:00** will set the timeout to 5 minutes.

Entering **settimeout** by itself will display the current value.

NOTE: The SSH session timeout is fixed at 5 minutes.

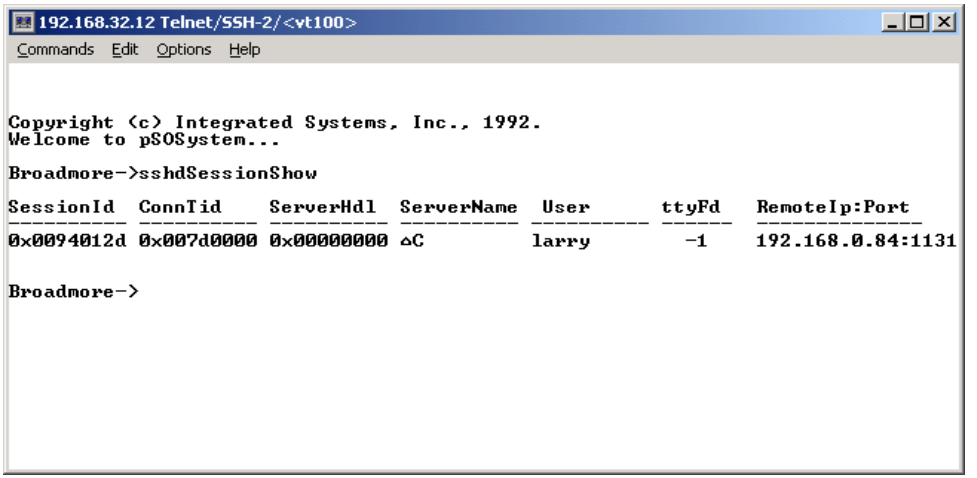
sshdShow

A SuperUser (Crypto Officer) can access the SSHD configuration information, at the Broadmore prompt, by typing **sshdShow**. An example of the output is provided in the following graphic.


192.168.32.12 Telnet/SSH-2/<vt100>
Commands Edit Options Help
Copyright (c) Integrated Systems, Inc., 1992.
Welcome to pSOSystem...
Broadmore->sshdShow
Sshd Configuration Information:
SSHD_MAX_SESSIONS: 1
Active Sessions: 1
Config File: /sshd/sshd.cfg
Log Level: 3
Listen Socket Count: 1
Listen Port: 22
Listen Address: 0.0.0.0
Server Key Bits: 768
RSA User Auth(SSH1): Disabled
DSA User Auth(SSH2): Disabled
Empty Passwords: Rejected
Keep Alive: Enabled
Allow User List: (empty)
Deny User List: (empty)
SSH2 Cipher List: aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
Broadmore->>

sshdSessionShow

A SuperUser (Crypto Officer) can access the information about current active ssh server sessions, at the Broadmore prompt, by typing **sshdSessionShow**. An example of the output is provided in the following graphic.



Item	Comments
Session ID	Session ID
ConnTid	Task ID of the sshd server handling the connection
ServerTid	Session server task spawned for the connection
ServerName	Session server name
User	Connecting user's name
ttydFd	fd available to the server task for IO with the sshd connection task
RemoteIp:Port	IP and port of the remote system

scp

A SuperUser (Crypto Officer) can copy files to a specific directory, using the secure copy (scp) command.

Using SCP

The scp client can be invoked from a target-OS shell by running scp and passing all options as parameter strings. Examples are provided below.

To copy a file, **local_file**, on the target to a remote server, **my_server**, use the following command:

```
-> scp <local_file> my_self@my_server:<local_file_new>
```

To to copy files from the remote server, **my_server**, to the target, **local_file**, use this command:

```
-> scp my_self@my_server:/<dir>/<file> /<dir>/<new_file>
```

To display a list of options and usage information use the "**-h**" command.

```
-> scp -h
```

Enabling Debug Messages

A SuperUser (Crypto Officer) can enable Debug by using the "-v" option. An example is provided below.

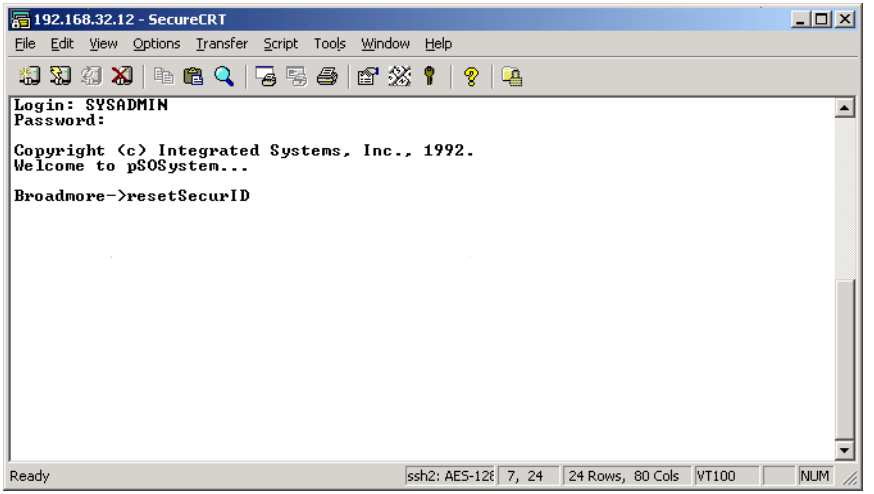
```
-> scp -v [local_file] user_name@remote:[remote_file]
```

NOTE: For more information about shell commands and general information about session privacy, go to www.openssh.org.

resetSecurID

A SuperUser (Crypto Officer) can use the resetSecurID command to reset the node secret file. This command is necessary if the system administrator has, for example, changed the server and needs to get a fresh node secret file.

At the Broadmore> prompt, type resetSecurID as shown in the following figure, and then press Enter.



The node secret file resets, and the screen returns to the prompt. There is no output with this command.

zeroize

WARNING! **THE ZEROIZE COMMAND WILL DECOMMISSION THE CPU MODULE AND MAKE IT INOPERABLE (THE CPU WILL NOT REBOOT). THIS COMMAND WILL PERMANENTLY ERASE ALL CRITICAL SECURITY PARAMETERS AND CPU DISK-ON-CHIP MEMORY. A ZEROIZED CPU CONTAINS NO SECURITY DATA OR OPERATING SYSTEM SOFTWARE. A ZEROIZED CPU CAN BE RETURNED TO THE FACTORY FOR REPAIR.**

This command is not intended for normal operational use. It is intended as a security measure (per FIPS 140-2 requirements) to allow a SuperUser (Crypto Officer) to completely remove all security-sensitive data that may be required before decommissioning a CPU. This command has two options:

- To zeroize only the standby CPU, type **zeroize standby**
  This option is intended primarily for decommissioning a defective CPU module.
- To zeroize both CPUs, type **zeroize global** which will first zeroize the standby CPU and then the online CPU. This option is intended for decommissioning the entire Broadmore system.

Authorized Access to Shell Commands

The following table lists the authorized commands available to each access privilege level when operating in FIPS mode.

User ID → ↓ Authorized Services	Super_User	Sys_Admin	Operations	Browser
arp	•4	•		
cammi (start GUI interface)	•	•	•	•
cat	•			
cd	•	•	•	
cli	•	•	•	•
cmp	•			
comp	•			
copy	•			
cp	•			
del	•			
dir	•	•	•	
du	•	•		
echo	•	•	•	•
fipsmode	•			
head	•			
help	•	•	•	•
ifconf	•	•		
ls	•	•	•	
md	•	•		
mem	•			
mkdir	•			
move	•			
mv	•	•		
netstat	•	•		
ping	•	•	•	•

User ID → ↓ Authorized Services	Super_User	Sys_Admin	Operations	Browser
pwd	●	●	●	●
rd	●			
resetSecurID	●			
resetSecurIDIp	●			
rm	●			
rmdir	●			
route	●	●		
savert	●	●		
scp	●			
selftest	●			
setbaud	●	●	●	
setenv	●	●		
settimeout	●			
setwrite	●			
sigmem	●			
sshdSessionShow	●			
sshdShow	●			
tail	●			
touch	●	●		
zeroize	●			

SFTP Login

Users can login using SFTP to access Broadmore administrative functions the same way as ftp. With SFTP, the data is encrypted as it flows to and from the Broadmore over IP.

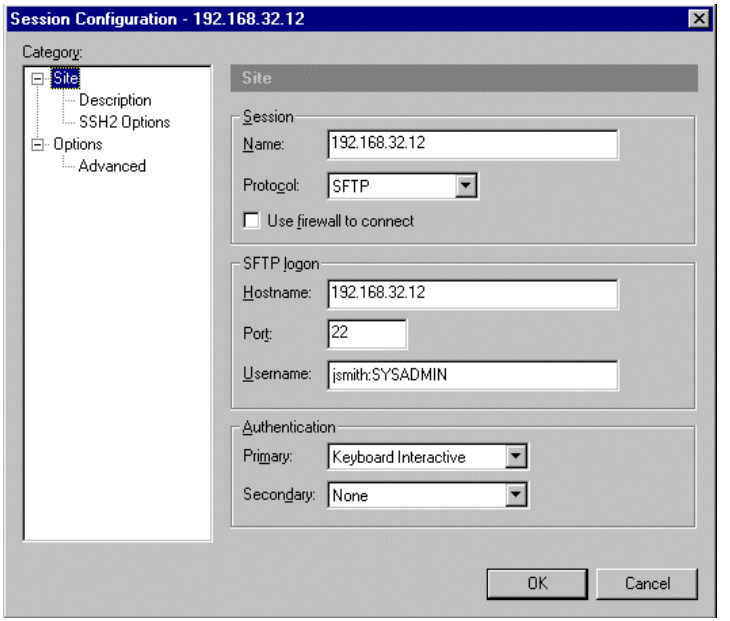
The following procedure provides an example of how to login using SFTP using SecureFX.

Logging in with SecurID Disabled

To log in to RSA SecurID and the Broadmore:

1. Open SecureFX. The Connect window opens.
2. Right-click on the connection you want to use, and select Properties.

   The Session Configuration window opens.



3. In the Session panel, type the IP address of the Broadmore, and select SFTP from the Protocol pull-down menu.

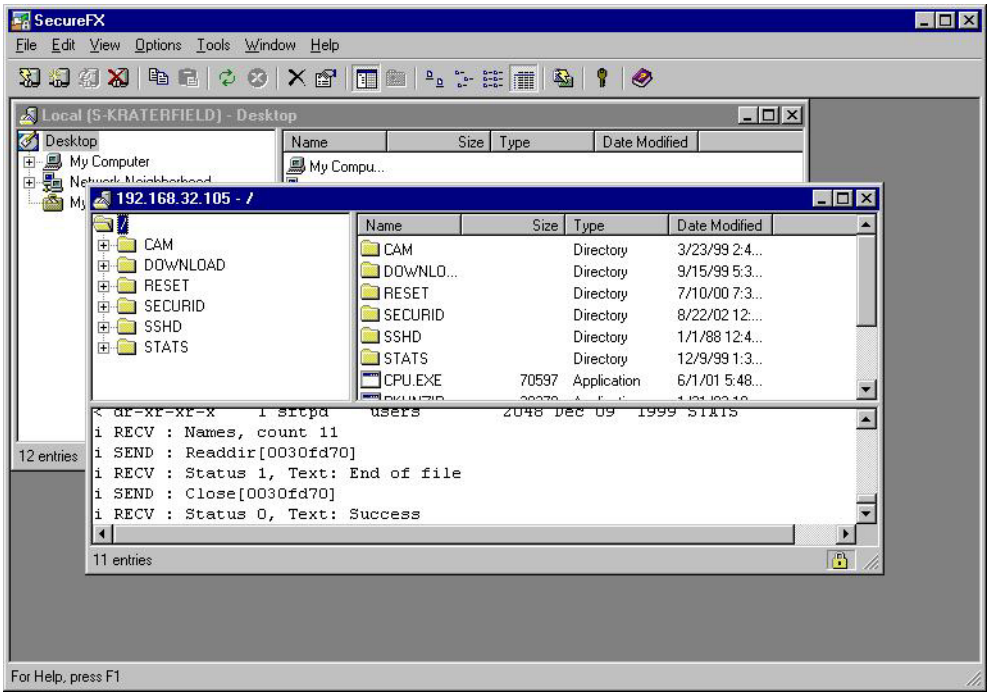
NOTE: Some secure ftp clients do not allow a colon as the first character. The following step works with SecureFX.

4. In the SFTP logon panel, type in the Hostname and Username. The Hostname is the IP address of the Broadmore; the Username is Broadmore local user name prefixed by a colon (for example, **:SYSADMIN**).
5. Select Keyboard Interactive from the Primary pull-down menu in the Authentication panel.
6. Click OK. The following prompt appears:



7. Type in the local Broadmore password, and click OK.

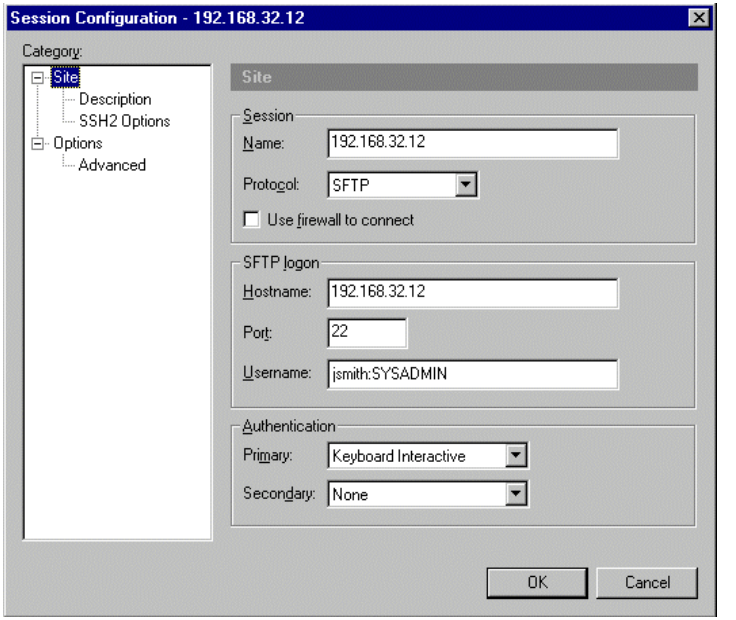
   After successfully logging in, the SecureFX window appears as shown in the following graphic.


SecureFX
File Edit View Options Tools Window Help
Local (S-KRATERFIELD) - Desktop
Desktop
My Computer
Name Size Type Date Modified
192.168.32.105 - /
CAM
DOWNLOAD
RESET
SECURID
SSHD
STATS
Name Size Type Date Modified
CAM Directory 3/23/99 2:4...
DOWNLO... Directory 9/15/99 5:3...
RESET Directory 7/10/00 7:3...
SECURID Directory 8/22/02 12:...
SSHD Directory 1/1/88 12:4...
STATS Directory 12/9/99 1:3...
CPU.EXE 70597 Application 6/1/01 5:48...
i RECV : Names, count 11
i SEND : Readdir[0030fd70]
i RECV : Status 1, Text: End of file
i SEND : Close[0030fd70]
i RECV : Status 0, Text: Success
11 entries
12 entries
For Help, press F1

Logging in with SecurID Enabled

To log in to RSA SecurID and the Broadmore:

1. Open SecureFX. The Connect window opens.
2. Right-click on the connection you want to use, and select Properties. The Session Configuration window opens.



3. In the Session panel, type the IP address of the Broadmore, and select SFTP from the Protocol pull-down menu.
4. In the SFTP logon panel, type in the Hostname and Username. The Hostname is the IP address of the Broadmore; the Username is The SecurID user name and Broadmore local user name joined together with a colon between and no spaces (for example, **jsmith:SYSADMIN**).
5. Select Keyboard Interactive from the Primary pull-down menu in the Authentication panel.

6. Click OK. The following prompt appears:



7. Click OK. The Keyboard Interactive Authentication window opens.

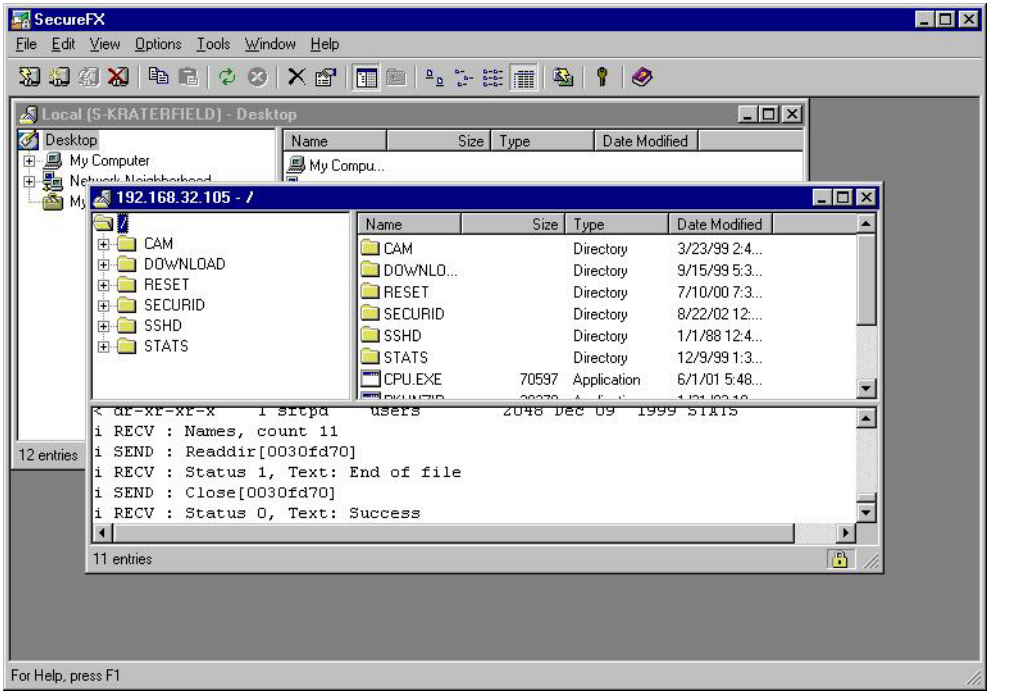


8. Type in the SecurID passcode, and click OK. A second Keyboard Interactive Authentication window opens.



9. Type in the local Broadmore password, and click OK.

   After successfully logging into SecurID, the SecureFX window appears as shown in the following graphic.


SecureFX
File Edit View Options Tools Window Help
Local (S-KRATERFIELD) - Desktop
Desktop
My Computer
Name Size Type Date Modified
My Compu...
12 entries
192.168.32.105 - /
CAM
DOWNLOAD
RESET
SECURID
SSHD
STATS
Name Size Type Date Modified
CAM Directory 3/23/99 2:4...
DOWNLO... Directory 9/15/99 5:3...
RESET Directory 7/10/00 7:3...
SECURID Directory 8/22/02 12:...
SSHD Directory 1/1/88 12:4...
STATS Directory 12/9/99 1:3...
CPU.EXE 70597 Application 6/1/01 5:48...
< dr-xr-xr-x 1 sftpd users 2048 Dec 09 1999 STATS
i RECV : Names, count 11
i SEND : Readdir[0030fd70]
i RECV : Status 1, Text: End of file
i SEND : Close[0030fd70]
i RECV : Status 0, Text: Success
11 entries
For Help, press F1

SecurID Features

SecurID is an option that may be used to help authenticate a user prior to logging into the Broadmore/SSHield Management Module. SecurID does not use FIPS approved algorithms but using SecurID does not in any way affect the security provided by the FIPS-2 validated Broadmore/SSHield Management Module.

Feature	Details
RSA Authentication Methods Supported	Native SecurID
RSA Authentication Manager/Agent Library Version	5.0.2
RSA Authentication Manager 5 Locking	Yes
Replica RSA Authentication Manager Support	Full Replica Support
Secondary RADIUS/TACACS+Server Support	N/A
Location of Node Secret on Client	\securid\securid
RSA Authentication Manager Agent Host Type	Net OS Agent
SecurID User Specification	All remote users
SecurID Protection of Administrators	No

Residual Data and Memory Volatility

- Non-Volatile Memory ... *11-50*
- Network Interfaces ... *11-51*
- Sanitation Procedures ... *11-51*

This notice summarizes relevant security concerns associated with the movement of sensitive data through any Broadmore ATM Multiplexer and subsequent re-deployment of these products into open environments. Should there be any questions or concerns regarding this notice, please contact Carrier Access Corporation customer support at 800-786-9929.

Non-Volatile Memory

The modules used in the Broadmore each contain one or more of the following types of non-volatile memory: removable Disk-on-Chip, removable and non-removable Flash memory. There is no internal data path or mechanism provided in a Broadmore to permit network data streams to be recorded onto non-volatile media. Such unintended or hostile actions on the part of the Broadmore could only be enabled by the surreptitious alteration of the device's embedded firmware and hardware. Thus, adequate physical security and access controls are required to prevent hostile implementation of "other" (non-Carrier Access provided) firmware and hardware.

With Release 4.0, Broadmore received FIPS 140-2 validation (see certificate #478 posted under the Validation Lists at *http://csrc.nist.gov/cryptval/*). When operated properly, this version of software contains "zeroize" commands that reformats the Disk-on-Chip and destroys all stored configuration and sensitive data. It also contains a start-up routine that verifies that no surreptitious software has been loaded. See the *Broadmore/SSHield Management Module Security Policy* for more information.

The Broadmore also has a limited amount of cell buffering implemented via random access memory (RAM). This memory implementation is entirely volatile and will be immediately lost upon power-down. Data that has been buffered in the Broadmore RAM cannot be recovered under any circumstances after power-down.

Network Interfaces

Network Interface Modules (NIMs) are installed in the Broadmore ATM Multiplexer and provide an interface to the ATM network. Each NIM contains non-volatile Flash memory for storing run-time code. These chips are not physically accessible from the ATM data path and thus cannot store data that passes through the Broadmore.

Sanitation Procedures

The following table summarizes procedures for all Broadmore modules when removing them from authorized areas to open areas.

Product Release	Product Type	Sanitation Procedure
Release 3.8 and earlier	Broadmore Unit	Power Off for 24 hours Remove Disk-on-Chip from CPU
	Network Interface Modules	Power Off for 24 hours
	CPU	Power Off for 24 hours Remove Disk-on-Chip from CPU
Release 4.0 and later	Broadmore Unit	FIPS Zeroize Global/Standby Power Off for 24 hours
	Network Interface Modules	Power Off for 24 hours
	CPU	FIPS Zeroize Standby Power Off for 24 hours

CHAPTER 12

SNMP Configuration

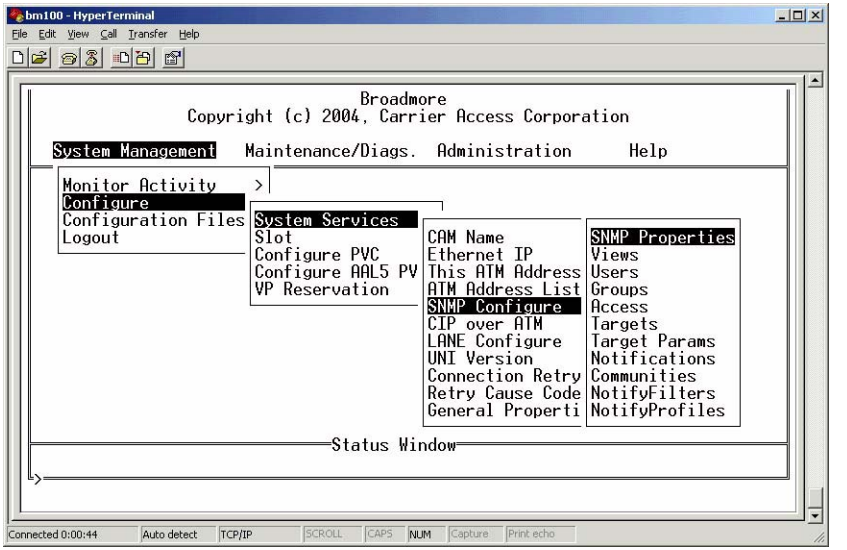
In this Chapter:

- SNMP Overview ... *12-2*
- SNMP Properties ... *12-3*
- USM/VACM Configuration ... *12-6*
- Trap Configuration ... *12-28*

SNMP Overview

Simple Network Management Protocol (SNMP) is a plain-text service with no access to any critical security parameters (CSPs). The Broadmore supports SNMP v1, v2, and v3. Follow the sequence below to configure the SNMP parameters.

NOTE: SNMPv3 configuration must be performed through CAMMI. Do not use the CLI to configure SNMPv3 parameters.

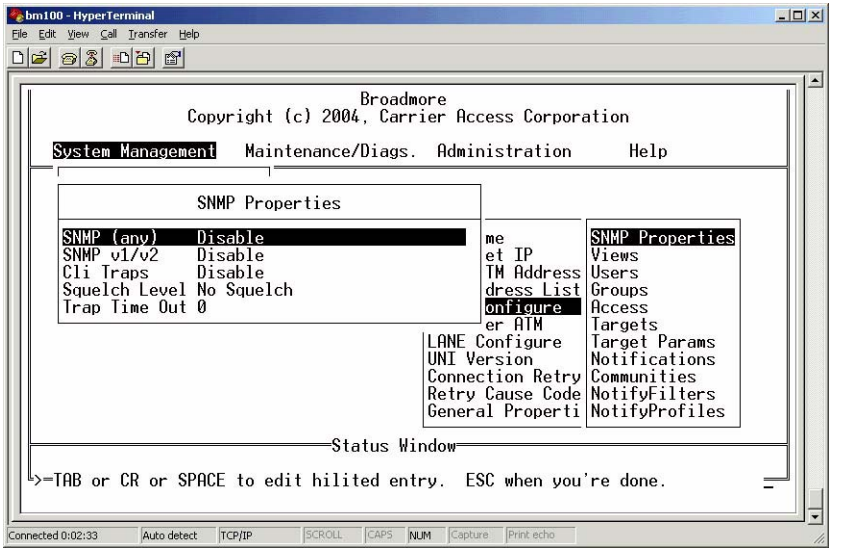


Select **System Management** ↵
Select **Configure** ↵
Select **System Services** ↵
Select **SNMP Configure** ↵
Select the item you want to configure.
With each selection, confirm your changes and press *Esc* to exit.

SNMP Properties

These settings can only be accessed and changed by a SuperUser or SysAdmin. SNMP properties allow the user to control SNMP operation.

.



Select **System Management** ↵
Select **Configure** ↵
Select **System Services** ↵
Select **SNMP Configure** ↵
Select **SNMP Properties** ↵
Select the item you want to configure.
With each selection, confirm your changes and press *Esc* to exit.

The following table lists the SNMP property selections.

Item	Options	Comments
SNMP (any)	Enable, Disable	Enables or disables all SNMP messages.
SNMP v1/v2	Enable, Disable	Enables or disables only SNMP v1 and v2 messages. SNMPv3 messages are enabled.
CLI Traps	Enable, Disable	This selection is a switch (enable/disable) that allows you to view trap messages when logged into CLI. When enabled, trap messages will echo to the screen when they occur.
Squelch Level	Below Current Level, Equal or Below Current Level, No Squelch	The Broadmore is shipped with the squelch level set at “below current level.” The Squelch level allows you to control the trap volume with a single “level” setting. The severity of the last “state” trap is remembered, and future traps will be sent only if the setting for the squelch level permits their severity. Only traps with matching “set” and “clear” instances become the “outstanding” trap for squelching. These are limited to the traps for card/port major and minor alarms. Each port will attempt to “set” a trap when an alarm first trips, in the absence of squelching, and a matching “clear” will be sent when that port's alarms dissipate.
Trap Time Out	0-3600	Enter Time Out as a value in minutes between 0 and 3600. When a trap triggers, it may be squelched if there is an outstanding trap of serious priority. The Timeout value guards against an old trap that is no longer relevant preventing any future traps. The timeout value guards against an old, no longer relevant trap preventing any future traps. When the time expires, the outstanding trap is discarded. Enter Timeout as a value in seconds between 0 and 3600 (60 minutes) with 1200 (20 minutes) as a recommended initial value.

Example: Squelching Traps

The system will be delivered from the factory with the squelch level at “below current level”. All individual traps will be enabled, with the following severities:

Critical

- Failure reboot
- NIM major alarm

Major

- SAM major alarm
- Slot failure
- Uni up/down

Minor

- SAM minor alarm
- NIM minor alarm

Inform

- Card insert/removed
- NIM switchover
- CPU switchover
- Restore
- User reboot
- Cold Start

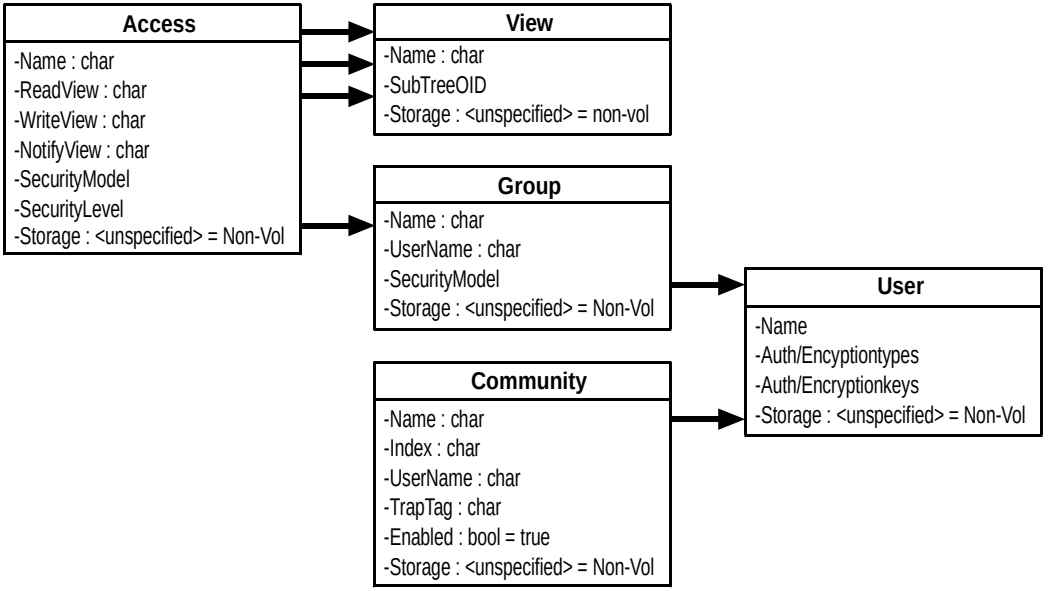
This squelch configuration will send a single “critical” trap if a NIM fiber breaks, and will prevent cascading traps like “NIM switchover” (in a redundant NIM system) from sending dozens of SAM port notifications caused by the switchover. Normally, if you get a trap on a single port of a SAM, you would get traps for all the other ports and all the other SAMs. But with the squelch at “equal or below current level”), the notifications are throttled back to 1 trap for all SAMs.

USM/VACM Configuration

- Users ... *12-8*
- Groups ... *12-13*
- Views ... *12-16*
- Access ... *12-19*
- Communities ... *12-24*

SNMPv3 supports the User-based Security Model (USM) and View-based Access Control Model (VACM). These settings can only be accessed and changed by a SuperUser (Crypto Officer).

Broadmore Implementation of USM/VACM



USM provides authentication and privacy services for SNMPv3. USM provides improved security over SNMPv1 and SNMPv2 by adding encryption and synchronized time indicators. Although USM uses cryptography to support the underlying protocol, it is a plain-text service and does not provide the level of data confidentiality or protection required by FIPS-2. Consequently, it should be treated like any other plain-text service port.

USM uses loosely synchronized monotonically increasing time indicators to defend against certain message stream modification attacks. Automatic clock synchronization mechanisms based on the protocol are specified without dependence on third-party time sources and concomitant security considerations.

VACM is an architecture for viewing and controlling users. VACM defines the access control policy that determines which users can access which subset of MIB objects in the Broadmore. VACM also defines the type of access (Read/Write) over a view.

The Broadmore organizes the USM/VACM into four tables or *entities*: Views, Users, Groups, and Access. With each entity, the following *actions* are associated:

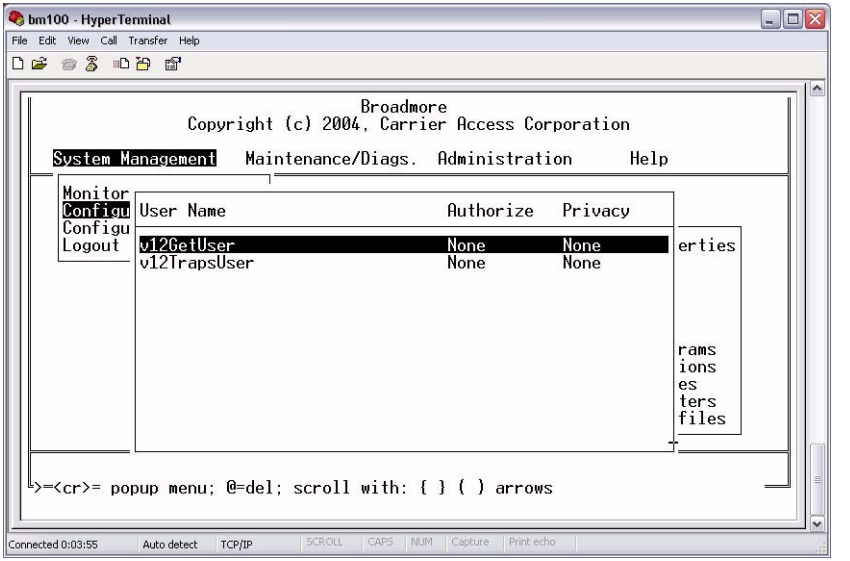
- Edit – used to modify an existing User, View, Group or an Access entry
- Copy – used to copy the information for an existing User, View, Group or an Access entry as a basis for a new one
- Delete – used to delete an existing User, View, Group or an Access entry
- New – used to add a new User, View, Group or an Access entry
- Validate Table – used to check table entries for consistency with other tables.

The Communities table supports the coexistence of SNMP v1, v2, and v3 access described in RFC 2576. The Communities table supports v1/v2 get, set, and trap requests within USM/VACM.

NOTE: When configuring USM/VACM, please note the consequences of selecting certain “Storage Type” parameters in the tables. “Permanent” entries cannot be deleted except by deleting the entire SNMP configuration and rebooting. “Read Only” entries can only be edited or removed by deleting the entire SNMP configuration and rebooting.

Users

This selection allows you to control users and their access privileges. Once this menu option is chosen, a list of existing users will be displayed. The screen below shows the two predefined users.

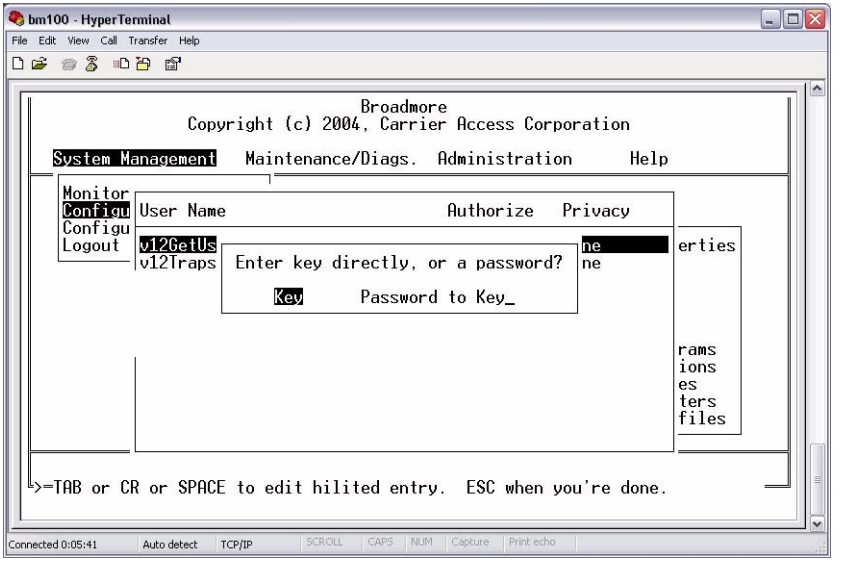


Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **SNMP Configure** ↵
Select **Users** ↵
Select one of the following:

* **Edit** ↵, edit the User information
* **Copy** ↵, (to put a copy of the information into the list)
* **Delete** ↵, delete an existing User
* **New** ↵, enter a new User
* **Validate Table** ↵, check table entries for consistency

With each selection, confirm your changes and press *Esc* to exit.

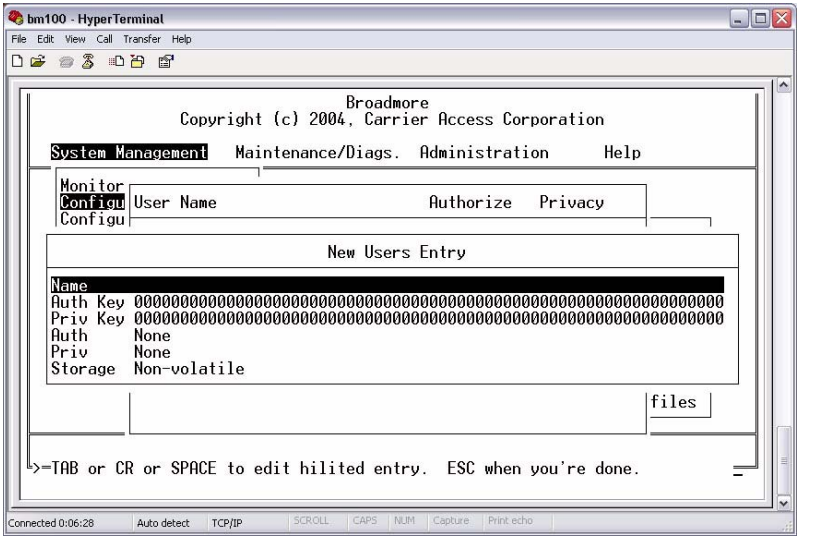
When adding a new user (either through *New* or *Copy* action), the system will present an option to either enter the Authentication and Privacy (Encryption) Key either directly (Key) or as a Password (Password to Key), as shown below.



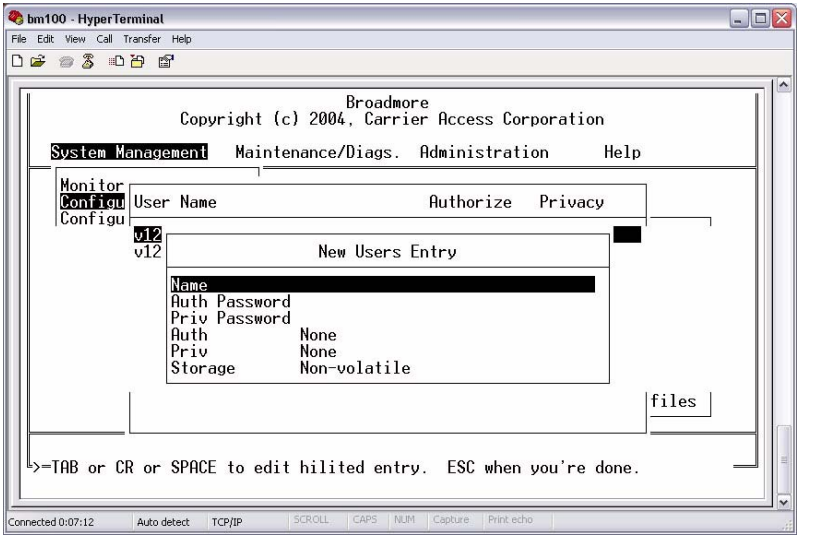
In case you choose to enter the key information as a password, the system will internally generate a key value corresponding to the password entered and maintain that information for the user. This is done because some SNMP clients use keys for authentication and encryption, while others use passwords. For clients that use passwords, a user needs to be created with passwords for the Authentication and Encryption parameters. After choosing either “Key” or “Password to key”, press “OK” and fill in the parameters described in the table above to define the new user, as shown in the following New Users Entry screen.

NOTE: When editing a user who has been created with a password for Authentication and Privacy, you can only edit the resulting key. This is because Broadmore converts the password to a key while saving the user information and does not maintain any record of the original password that had been entered.

Screen for entering User Key



Screen for entering User Password



Use the Esc key to exit this menu. If you have made any changes to the Users information the system will ask you for confirmation on whether you want to accept the changes or not.

NOTE: The entries in the User table are not actual users of the system. These usernames cannot be used for authentication in order to access the Broadmore administration functionality.

The following table describes the selections.

Item	Options	Comments
User Name	string	A unique value for User Name, 1 to 30 characters.
Auth Key	string	Key to be used for authorizing a SNMP user to the Broadmore system.
Priv Key	string	Key to be used to encrypt SNMP traffic.
Auth Password	string	Password to be used for authorizing SNMP user.
Priv Password	string	Password to be used to encrypt SNMP traffic.
Auth	None SHA MD5	Authentication protocol used.
Priv	None AES DES 3DES	Protocol used to encrypt SNMP data between a client and Broadmore SNMP agent.
Storage	Volatile Non-volatile Permanent Readonly Other	Settings lost without power. Settings remembered after reboot. Settings can not be deleted. Settings can not be changed.

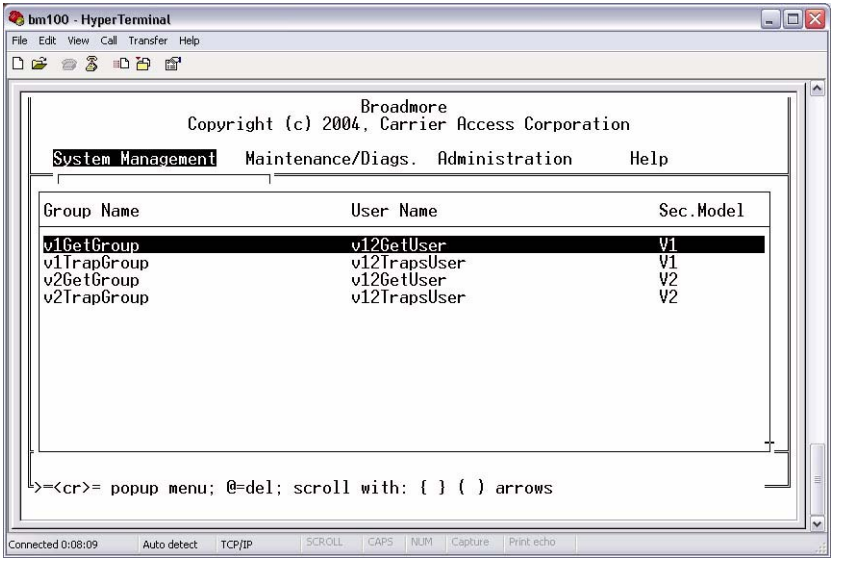
User Edit Rules

The following table describes which parameters can be modified in a Users table entry.

Item	Edit Allowed
User Name	No
Auth Password	No
Priv Password	No
Auth	Yes
Priv	Yes
Storage	Yes

Groups

The VACM model supports the concept of categorizing *users* into *groups*. A group is a unique pair defined by the parameters “User Name” and “Security Model” (see table below). The screen below shows the four predefined groups.



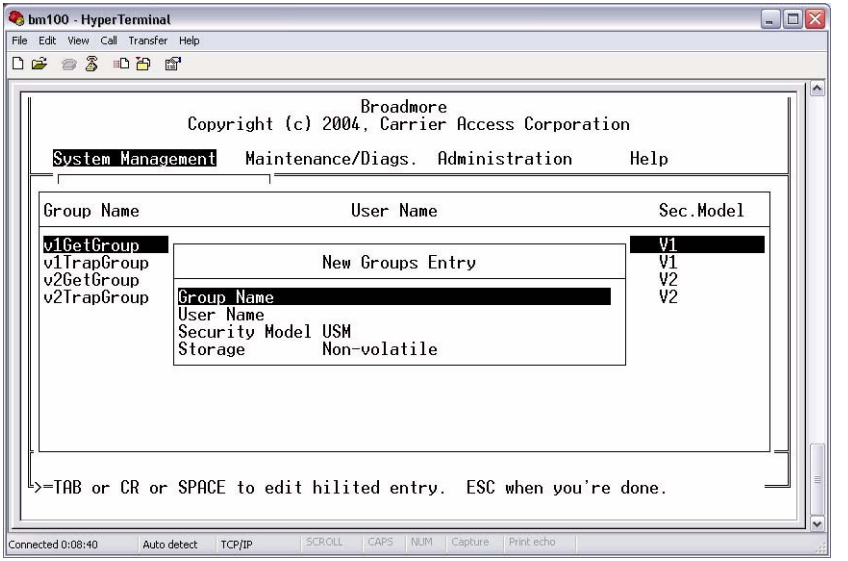
Follow the sequence below to modify the list.

Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **SNMP Configure** ↵
Select **Groups** ↵
Select one of the following:

* **Edit** ↵, edit the Group information
* **Copy** ↵, (to put a copy of the information into the list)
* **Delete** ↵, delete an existing Group
* **New** ↵, enter a new Group
* **Validate Table** ↵, check table entries for consistency

With each selection, confirm your changes and press *Esc* to exit.

Once this menu option is chosen, a list of existing groups will be displayed. To choose the required action on groups, highlight any of the existing entries and press the Enter key. The screen below shows the New Groups Entry.



The following table describes the selections.

Item	Options	Comments
Group Name	string	value for Group Name, 1 to 30 characters.
User Name	string	value for User Name, 1 to 30 characters.
Security Model	V1 V2 USM	The Security Model used in processing an SNMP query from a client. This parameter can be used to restrict access to the managed objects based on the security model set for a group.
Storage	Volatile Non-volatile Permanent Readonly Other	Settings lost without power. Settings can be changed. Settings can not be deleted. Settings can not be changed.

Use the Esc key to exit this menu. If you have made any changes to the user information, the system will prompt you for confirmation on whether you want to accept the changes or not.

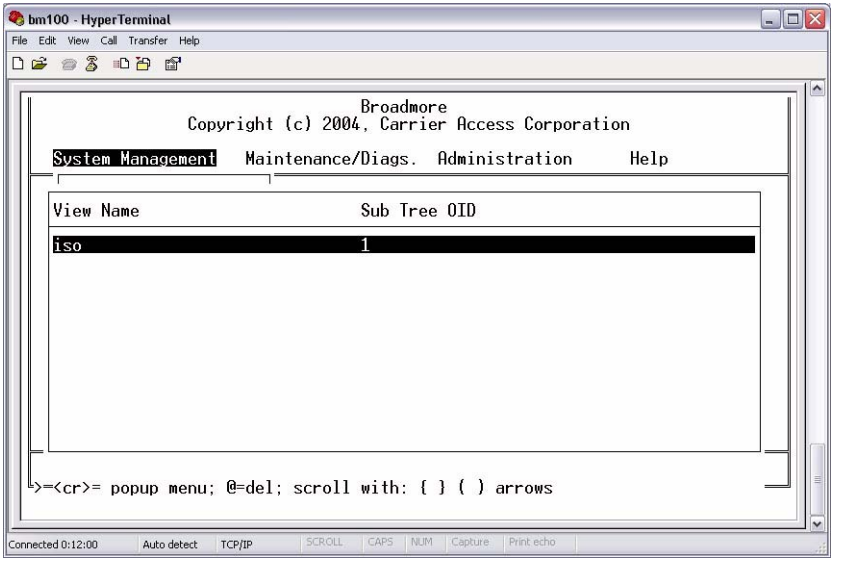
Group Edit Rules

The following table describes which parameters can be modified in a Groups table entry.

Item	Edit Allowed
Group Name	Yes
User Name	No
Security Model	No
Storage	Yes

Views

This selection allows you to create a views and assign object identifiers. The screen below shows the predefined “iso” view.

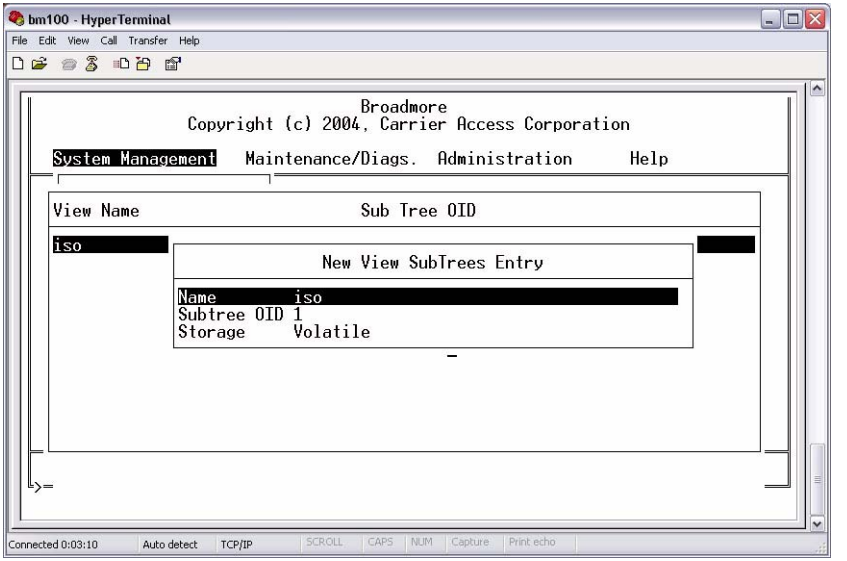


Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **SNMP Configure** ↵
Select **Views** ↵
Select one of the following:

* **Edit** ↵, edit the View information
* **Copy** ↵, (to put a copy of the information into the list)
* **Delete** ↵, delete an existing View
* **New** ↵, enter a new View
* **Validate Table** ↵, check table entries for consistency

With each selection, confirm your changes and press *Esc* to exit.

Once this menu option is chosen, a list of existing groups will be displayed. To choose the required action on groups, highlight any of the existing entries and press the Enter key. The following shows the New View SubTrees Entry screen.



The managed objects in Broadmore are organized in a tree structure, known as a MIB tree, based on the OID (Object Identifier) of each object. A view defines a particular subtree in this MIB tree. For example, one view could be defined to be over the MIB subtree represented by the OID 1.3.6 while another could be over the subtree represented by OID 1.3.6.1. Of these two views, the latter is more restrictive as it has fewer managed objects under it. A view could also be defined to be one specific OID in the entire MIB tree of managed objects. The following shows the New View SubTrees view.

The following table describes the selections

Item	Options	Comments
Name	string	Unique value for View Name, 1 to 30 characters. Default is “iso” standard.
Subtree OID	string	Unique value for Object Identifier, such as “1.3.6”.

Item	Options	Comments
Storage	Volatile Non-volatile Permanent Readonly Other	Settings lost without power. Settings can be changed. Settings can not be deleted. Settings can not be changed.

Use the Esc key to exit this menu. If you have made any changes to the Users information, the system will prompt you for confirmation on whether you want to accept the changes or not.

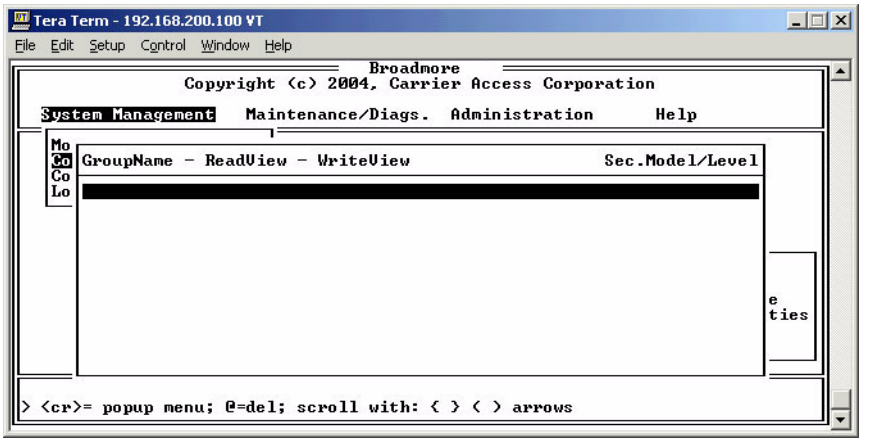
View Edit Rules

The following table describes which parameters can be modified in a Views table entry.

Item	Edit Allowed
Name	No
Subtree OID	Yes
Storage	Yes

Access

This selection allows you to control access to each Group.

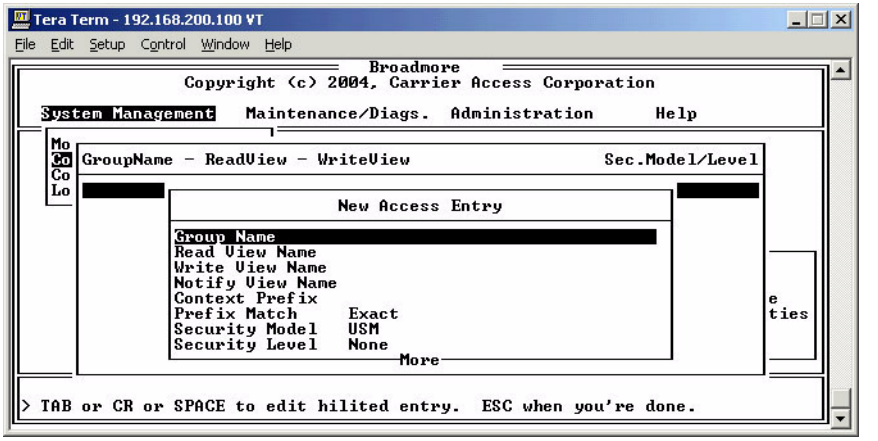


Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **SNMP Configure** ↵
Select **Access** ↵
Select one of the following:

* **Edit** ↵, edit the Group information
* **Copy** ↵, (to put a copy of the information into the list)
* **Delete** ↵, delete an existing Group
* **New** ↵, enter a new Group
* **Validate Table** ↵, check table entries for consistency

With each selection, confirm your changes and press *Esc* to exit.

Once this menu option is chosen, a list of existing access entries will be displayed. To choose the required action on an entry, highlight any of the existing entries and press the Enter key. The following shows the New Access Entry screen.



The Access entries implement the SNMP access policy for the Broadmore. For more details, see *Access Policy* below. The access table is used to enforce fine-grained access rights that form an access policy. The access list is used to define the parts of the MIB tree that are available for either read or write, for specific combinations of group and security models. It also defines whether an incoming SNMP request needs authentication and whether SNMP messages need to be encrypted.

The following table describes the selections.

Item	Options	Comments
Group Name	string	A group name from the Groups in the system, 1 to 30 characters.
Read View Name	string	A view name from the Views in the system, 1 to 30 characters. The Read View Name is for “get” access.
Write View Name	string	A view name from the Views in the system, 1 to 30 characters. The Write View Name is for “set” access.

Item	Options	Comments
Notify View Name	string	A view name from the Views in the system, 1 to 30 characters. The Notify View Name is for traps and notifications.
Context Prefix	string	A string, 1 to 30 characters. The interpretation depends on the value of the Prefix Match. If not specified, the default is an empty string, "".
Prefix Match	Exact Prefix	Exact – the contextName must match the Context Prefix. Prefix – only the initial substring of the contextName must match the Context Prefix.
Security Model	V1 V2 USM	The Security Model used in processing an SNMP query from a client. This parameter can be used to restrict access to the managed objects based on the security model set for a group.
Security Level	None AuthnoPriv AuthPriv	None – the incoming request requires no authentication or encryption. AuthnoPriv – authentication is required but SNMP messages will not be encrypted. AuthPriv – authentication is required and SNMP messages are encrypted.
Storage	Volatile Non-volatile Permanent Readonly Other	Settings lost without power. Settings can be changed. Settings can not be deleted. Settings can not be changed.

Use the Esc key to exit this menu. If you have made any changes to the Users information the system will prompt you for confirmation on whether you want to accept the changes or not.

Access Edit Rules

The following table describes which parameters can be modified in a Access table entry.

Item	Edit Allowed
Group Name	No
Read View Name	Yes
Write View Name	Yes
Notify View Name	Yes
Security Model	No
Security Level	No
Storage	Yes

Access Policy

The USM/VACM configuration defines the complete access policy in effect for incoming SNMP requests in the system. SNMP users and a Security model define a SNMP group. Each Group along with a View defines one element of the Access Policy as defined in the Access table. When an SNMP request comes to the system, the system first determines which group the user sending the request belongs to. This is done by looking up the username and the Security model used (V1, V2 or USM) in the SNMP request. Once the group is determined the system looks up the Access table entries and decides:

- whether the authentication and encryption is required for the SNMP query. This is determined by looking up the “Security Level” parameter in the Access table. Authentication is verified based on the information in the User table parameters “Auth Key” or “Auth Password”. In case encryption is required, the key defined by User table parameters “Priv Key” or “Priv Password” is used.

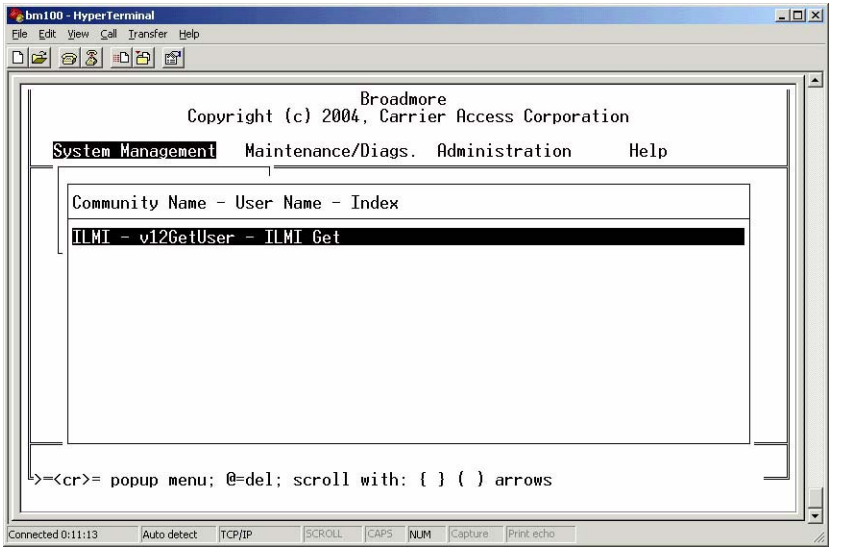
- whether the user sending the SNMP request is eligible to get or set the MIB variable. This is determined by looking up the “Read” and “Write” parameters of the Access table
- the exact set of MIB variables (managed objects) that will be visible to the user. This is determined by the Views table entries.
- access based on the security model set in Groups and Access table.

NOTE: In addition to the standard MIBs, the Broadmore includes enterprise MIBs that are specific to its operation.

Communities

Broadmore supports SNMPv1 and SNMPv2 through the SNMPv3 co-existence model. SNMPv1 and SNMPv2 community strings can be defined using the following menu option. Broadmore permits up to 20 entries in this table.

These settings can only be accessed and changed by a SuperUser.



Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **SNMP Configure** ↵
Select **Communities** ↵
Select one of the following:

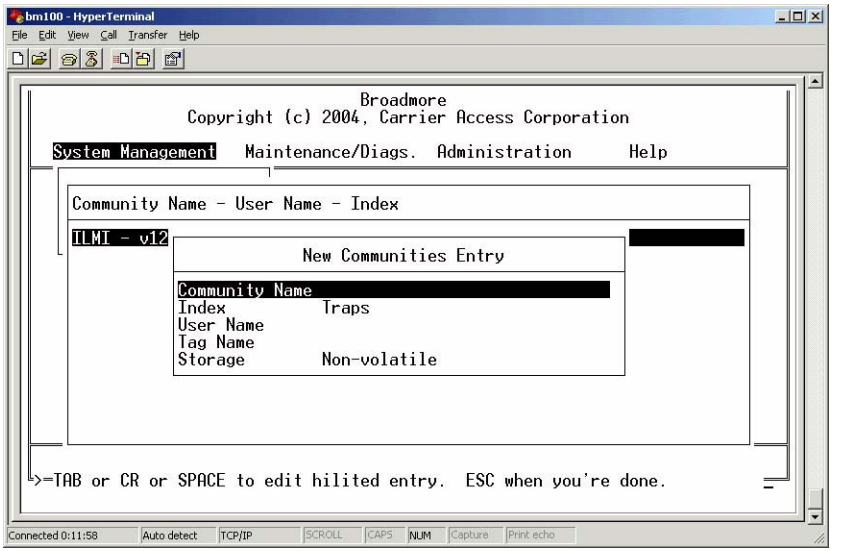
* **Edit** ↵, edit the Community information
* **Copy** ↵, (to put a copy of the information into the list)
* **Delete** ↵, delete an existing Community
* **New** ↵, enter a new Community
* **Validate Table** ↵, check table entries for consistency

With each selection, confirm your changes and press *Esc* to exit.

NOTE: Selecting the Validate command on this table will check each "User Name" value for existence in the "usmUserTable" and check each Tag Name for existence in the "snmpNotifyTable".

NOTE: So that the Broadmore properly registers with the ATM Switch, the Broadmore automatically creates an "ILMI" community with predefined Views, Users, Groups, and Access. These properties are read-only.

ILMI (Interim Local Management Interface) is an independent industry standard used for configuration of ATM interfaces. Although it is based on SNMP, ILMI communication actually occurs using a transport other than IP that traverses only the physical ATM link. ILMI is essential to functions such as ATM auto-discovery and LANE (LAN Emulation).



Use the Esc key to exit this menu. If you have made any changes to the Community information the system will ask you for confirmation on whether you want to accept the changes or not.

The following table describes the selections.

Item	Options	Comments
Community Name	string	SNMPv1 and SNMPv2 Community Name, 1 to 30 characters. The Community Name is used with the User Name and Tag Name to determine get, set, and trap access.
Index	string	The Index permits the table to specify the same actual string multiple times. A particular Index must be unique.
User Name	string	Value for User Name, 1 to 30 characters.
Tag Name	string	Value for Tag Name, 1 to 30 characters. Must be same as in Notify table if this community will be used in notifications. Leave empty if used only for get and set access.
Storage	Volatile Non-volatile Permanent Readonly Other	Settings lost without power. Settings can be changed. Settings can not be deleted. Settings can not be changed.

There are several ways to set up communities, so automatically setting all of them up will unnecessarily limit the customer's flexibility.

Example 1: Use the same "public" string for every get/set/trap

- Create a user "v1v2GetSetUser" with all the get/set privilege you desire using the appropriate view, user, group, and access table entries. In this case, the "access" record would have both the read and write views filled in.
- Create a community name "public" with index "GetSet" and an empty "Tag", and specify the user "v1v2GetSetUser"
- Create a community name "public" with index "Trap" and tag "Trap". Specify the predefined user "v12TrapsUser".

Example 2: Use a different string for “set”

- Create a user “v1v2SetUser” with all the set privilege you desire using the view, user, group, and access tables
- Create a community name “private” with index “Set” and no tag. Specify the user “v1v2SetUser”.
- Create a community name “public” with index “Trap” and tag “Trap”. Specify the predefined user “v12TrapsUser”.
- Create a community name “public” with index “Get” and no tag. Specify the predefined user “v12Getuser”.

In fact, you can create as many get and/or set community strings as you desire, provided that they map back to users with the privileges you desire and they all have arbitrarily unique index fields. For example, if you wished to have three different “get” community strings, you might use the index values “Get1”, “Get2”, “Get3”.

Trap Configuration

- Trap Detection Overview ... *12-28*
- Trap Management Overview ... *12-29*
- Table Usage ... *12-32*
- Targets ... *12-33*
- Target Parameters ... *12-35*
- Notifications ... *12-37*
- Notify Filters ... *12-40*
- Notify Profiles ... *12-42*

Trap Detection Overview

The Broadmore supports trap-directed notifications. This means that the Broadmore can automatically send a notification message to a network manager when a certain trap event occurs. This is much more efficient than having to continually poll each device on a network to check if it is working properly.

The Broadmore can send the following kinds of trap notifications:

- Major/Minor Alarms for each module and port – each “set” alarm is matched by a “clear”, indicating the states of the fault LEDs on the chassis or module
- Module inserted or removed from the chassis
- Slot failure
- UNI up/down
- Redundancy switchover
- File restores by the user – a user audit event
- Reboots by the user – a user audit event
- Reboots from system failure
- Cold start – a generic trap

Traps are a valuable network management tool for monitoring system status. However, to realize their full value, the system should post only those conditions requiring action by maintenance personnel. Otherwise, a fundamental system problem might create an avalanche of related traps, resulting in further degradation of the network.

Network operations organizations also have varying policies on what conditions to monitor and what alarm severities to assign to each condition.

The Broadmore gives selective control over traps to mitigate these issues.

- Squelching traps following a serious outstanding trap, to focus attention only on that “first fault.”
- Enabling or disabling individual traps, to match local monitoringpolicies.
- Adjusting individual traps severities works in concert with the “squelch” setting to control traps volume. This severity setting is completely independent from the major/minor indication in some of the traps names.

Trap Management Overview

SNMP traps are managed by a “Notification Originator” – a software application that makes decisions based on events and the contents of various SNMP tables. If the decision is to send a notification message, the Notification Originator assembles the relevant trap information into a Protocol Data Unit (PDU) and sends the PDU to a network manager at a target address.

SNMPv3 uses SNMPv2 PDUs and also adds target address tables that tell the Notification Originator which targets should be sent notifications with given Object IDs (OIDs) in them. For example, a particular event may cause a *linkDown* or a *warmStart* notification. You can specify that the *linkDown* message be sent to a specific entity or a group of entities in the target address table.

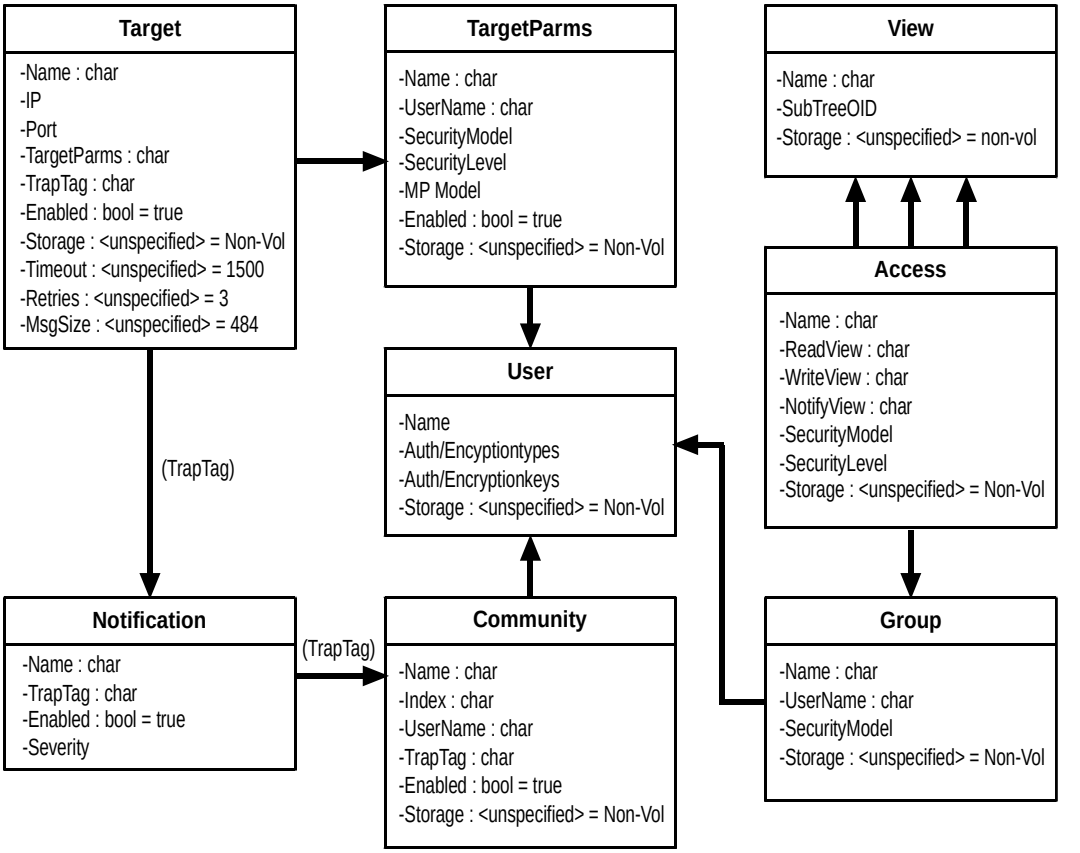
To define targets, the Notification Originator application uses the SNMP Notify and target tables. The target tables include filter and profile tables that are used to determine if specific notifications should be sent to entities in the target address table. Other tables are used for defining parameters that are needed in SNMPv3 PDUs, such as the Security Model, the Security Level, and the Security Name.

The Notification Originator uses the various tables in two ways:

- to identify the targets to send information to, including the priority of one type or event over another
- to create the PDU that will be sent.

The idea is to organize the information into specific tables that can be tied to other tables, as shown in the figure below. All the target addresses used by notifications and proxies are put into one table. Another table is used to identify which elements belong to the notifications. The target parameter table contains the information for creating SNMPv3 PDUs. Other tables are used to identify which notifications should go to which targets. When the Notification Originator creates an INFORM or v2TRAP PDU for SNMPv3, as opposed to locating proper targets, it takes information from the target address table and the target params table.

Broadmore Implementation of SNMP tables in RFCs 2273 and 2573.



The sequence of events in using these tables is as follows:

1. An event occurs and the Notification Originator goes to work.
2. The Notification Originator uses the notify table to identify possible targets to which to send a message. These are only possible targets because there may be notification filters setup to identify a subset of these possible targets that will be sent the message.
3. If no filters are set up (that is, no entry is in the snmpNotifyFilterProfileTable corresponding to this target), the Notification Originator can create and send the PDU(s). The process is then done.
4. If filters are on but the Notification Originator cannot find an entry for any of the specific targets, no PDUs can be sent. The process is then done.
5. If filters on and we have a filter entry, the Notification Originator checks the filter to see if it is set to include or exclude this target. If the filter is set to exclude this target, then the message need not be sent to this target.
6. If filters are on and the filter associated with the target provides a mask, the mask is used to see if this trap event can be sent to this target. The mask allows the Notification Originator to check if the OID of the trap and snmpTrapOID.0 matches the subtree that is in the notify filter table. That way, it can check for a certain event to send to a target, such as a warmStart message only.
7. Finally, using information from the target params table that is accessed from the target address table, the Notification Originator checks the target address (user information) to see if the entity has view privileges for the object. If the view is okay, the PDU(s) are sent. Either way, the process is completed. Views are checked whether or not filters exist.

Table Usage

The following summarizes the way that the SNMP tables are used.

User Management:

- User, Community, View, Access, and Group Tables (from VACM)

Format for the PDU to send (also used for Proxies):

- Target Address Table – contains domain and addressing information, timeout and retry information, and a tag list (snmpTargetAddrTagList) to define where to send notifications (and to forward proxied messages). There is also a link into the Target Params table.
- Target Params Table – contains the definition of parameters such as the Message Processing Model, the Security Model, the Security Level, and the Security Name to build and SNMPv3 PDU.

Tables to identify targets and provide finer selection of events to send:

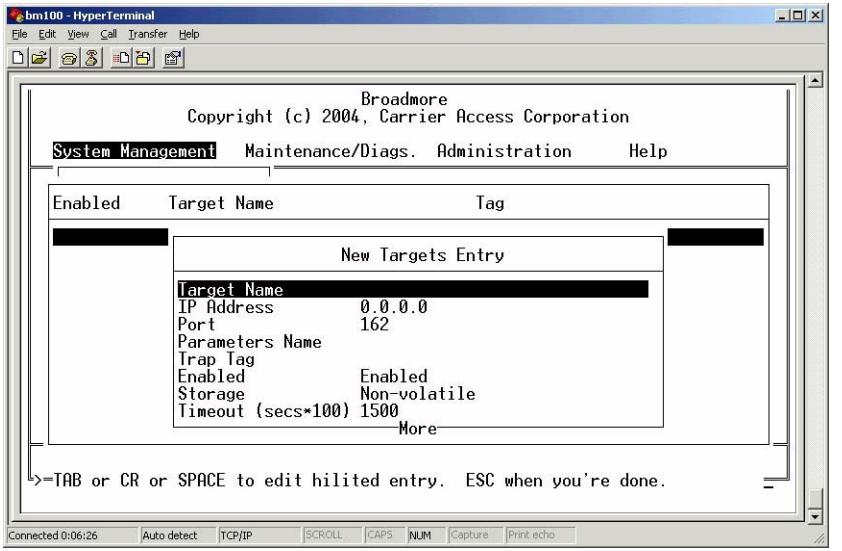
- Notifications Table – how to group targets to send notifications and what type of notification to send
- Notify Filter Profile Table – a list of filters used by a notification for finer grained control over trap destinations
- Notify Filter Table – filters to limit the number of notifications generated for a particular target

NOTE: The Broadmore predefines some SNMP v1/v2 trap parameters to ensure proper operation with ATM switches. For example, there is a predefined v1/v2 “get” user that can be added to a community (such as “public”) in the communities table.

NOTE: When configuring traps, please note the consequences of selecting certain “Storage Type” parameters in the tables. “Permanent” entries cannot be deleted except by deleting the entire SNMP configuration and rebooting. “Read Only” entries can only be edited or removed by deleting the entire SNMP configuration and rebooting.

Targets

This selection allows you to enter up to 10 target IP addresses to receive trap notifications. The screen below shows the New Targets Entry.



Follow the sequence below to modify the list.

Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **SNMP Configure** ↵
Select **Targets** ↵
Select one of the following:

* **Edit** ↵, edit the Target information
* **Copy** ↵, (to put a copy of the information into the list)
* **Delete** ↵, delete an existing Target
* **New** ↵, enter a new Target
* **Validate Table** ↵, check table entries for consistency

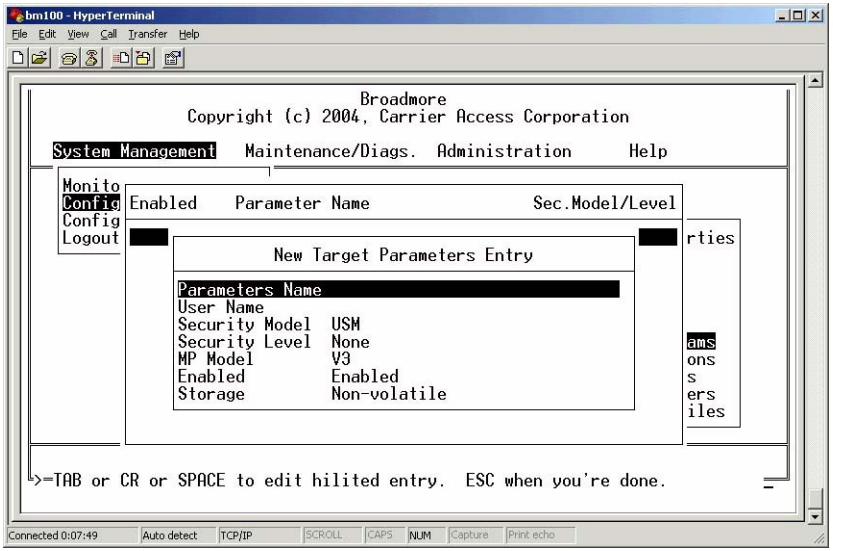
With each selection, confirm your changes and press *Esc* to exit.

The following table describes the selections.

Item	Options	Comments
Target Name		A unique value for Target Name, 1 to 30 characters.
IP Address		Format xxx.xxx.xxx.xxx where xxx is a decimal number, 0 to 255
Port		A number between 1024 and 65535.
Parameter Name		A unique value for Parameter Name, 1 to 30 characters.
Trap Tag		A unique value for Trap Tag, 1 to 30 characters.
Enabled	Enabled Disabled	Enables/disables this target.
Storage	Volatile Non-volatile Permanent Readonly Other	Settings lost without power. Settings can be changed. Settings can not be deleted. Settings can not be changed.
Timeout (secs*100)		Enter Timeout as a value in hundredths of a second. For example, 1500 represents 15 seconds. This value indicates the expected maximum round trip time for communicating with the IP address defined by this target. When a message is sent to this address, and a response (if one is expected) is not received within this time period, it may assumed that the response will not be delivered.
Retries		The number of times to attempt sending the notification.
Max Message Size		TBD

Target Parameters

This selection allows you to enter the kind of protocol and security to be used for the target destinations. The screen below shows the New Target Parameters Entry.



Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **SNMP Configure** ↵
Select **Target Params** ↵
Select one of the following:

* **Edit** ↵, edit the Target Parameter information
* **Copy** ↵, (to put a copy of the information into the list)
* **Delete** ↵, delete an existing Target Parameter
* **New** ↵, enter a new Target Parameter
* **Validate Table** ↵, check table entries for consistency

With each selection, confirm your changes and press *Esc* to exit.

NOTE: Selecting **Validate Table** will check that each Parameter Name in this table exists in the Notify Profiles table.

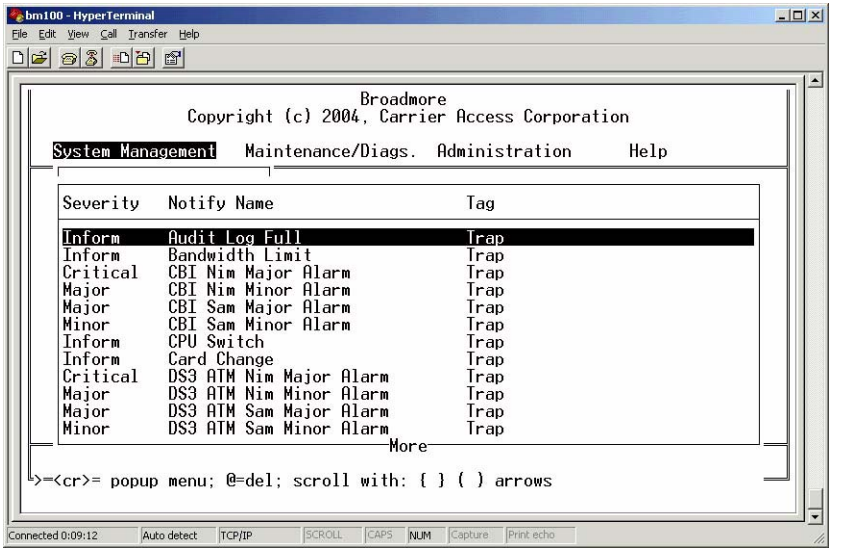
The following table describes the selections.

Item	Options	Comments
Parameter Name	string	Value for Parameter Name, 1 to 30 characters. **Note:** This entry must agree with the Parameters Name in the Notify Profiles table (see *"Notify Profiles" on page 12-42*).
User Name	string	Value for User Name, 1 to 30 characters.
Security Model	V1 V2 USM	The Security Model used in processing an SNMP query from a client. This parameter can be used to restrict access to the managed objects based on the security model set for a group.
Security Level	None AuthnoPriv AuthPriv	None – the incoming request requires no authentication or encryption. AuthnoPriv – authentication is required but SNMP messages will not be encrypted. AuthPriv – authentication is required and SNMP messages are encrypted.
MP Model	V1 V2 V3	Message Processing model
Enabled	Enabled Disabled	Enables/disables this target parameter.
Storage	Volatile Non-volatile Permanent Readonly Other	Settings lost without power. Settings can be changed. Settings can not be deleted. Settings can not be changed.

Notifications

This selection displays a list of all available trap events that can be used for notifications. These entries automatically appear in the MIB “snmpNotifyTable” accessible by a remote manager. The notification names cannot be changed but individual traps can be enabled and assigned a tag name and a severity level. The severity is reported as a variable with the trap, and also works in concert with the squelch level (in SNMP Properties) to keep traps appropriately throttled.

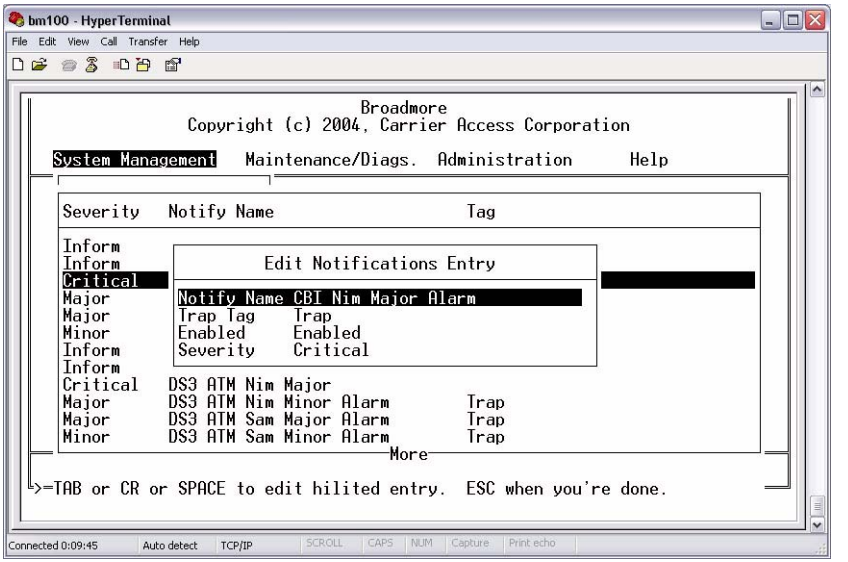
Follow the sequence below to enable or disable each trap type in the list. Save the configuration when asked to activate the SNMP trap reporting.



Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **SNMP Properties** ↵
Select **Notifications** ↵

NOTE: Entries in this table cannot be added or deleted, only edited. The storage type for these entries is automatically configured to “permanent”.

The screen below shows the Edit Notifications Entry.



The following table describes the selections

Item	Options	Comments
Notify Name		This parameter cannot be changed.
Trap Tag	string	The default name is “Trap”. If remote managers are to receive all traps, there is no need to modify the Trap Tag. Different tag names would be useful if responsibility for trap management was subdivided by trap types such that a specific destination was only responsible for a partial set of traps.
Enabled	Enabled Disabled	Enables/disables this notification.

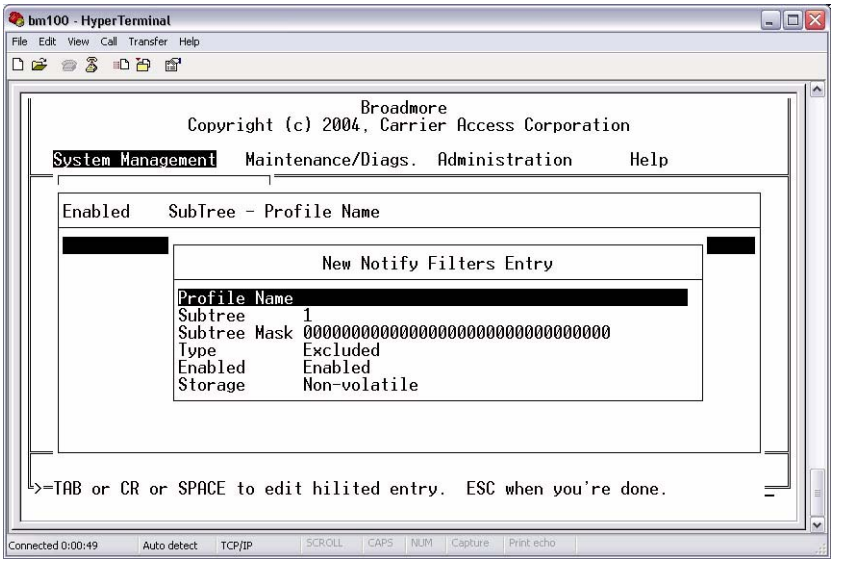
Item	Options	Comments
Severity	Critical Major Minor Inform	Reboot failure, NIM major alarm. SAM major alarm, slot failure, Uni up/down. SAM minor alarm, NIM minor alarm. Card insert/removed, NIM switchover, CPU switchover, restore, user reboot.

NOTE: "Severity" is an attribute only available for Broadmore enterprise traps; it is not described in the RFCs. Severity is reported as a variable with the trap. To configure trap severity from a remote SNMP manager, use the Broadmore enterprise MIB table "snmpTrapTypeTable".

Notify Filters

Entries may be completely maintained using the cammi Notify Filters table (which is a direct representation of "snmpNotifyFilterTable") or via a remote SNMP manager. This table allows finer grained control over trap reports. Broadmore permits up to 20 entries in this table. An empty table is acceptable.

These settings can only be accessed and changed by a SuperUser.



Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **SNMP Configure** ↵
Select **Notify Filters** ↵
Select one of the following:

* **Edit** ↵, edit the Filter information
* **Copy** ↵, (to put a copy of the information into the list)
* **Delete** ↵, delete an existing Filter
* **New** ↵, enter a new Filter
* **Validate Table** ↵, check table entries for consistency

With each selection, confirm your changes and press *Esc* to exit.

NOTE: Selecting **Validate Table** will check that each Profile Name in this table exists in the Notify Profiles table.

The Notify Filters table is used to avoid sending traps for specific mib variables. Each variable in the VarBindList is checked against the Subtree. If a match occurs, the trap is not sent.

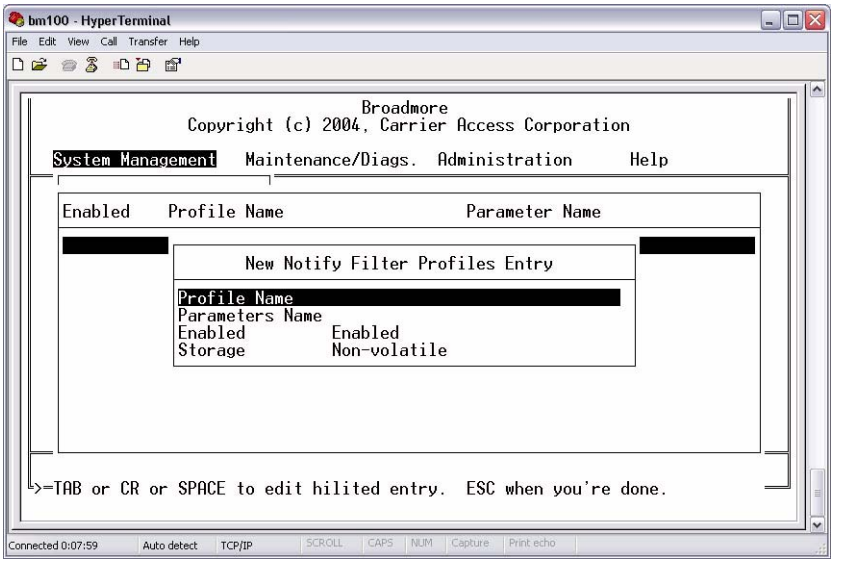
The following table describes the selections.

Item	Options	Comments
Profile Name	string	Value for Profile Name, 1 to 30 characters. **Note:** This entry must agree with the Profle Name in the Notify Profiles table (see *"Notify Profiles" on page 12-42*).
Subtree	bit string	The MIB tree address indicating the branch nodes to be filtered.
Subtree Mask	bit string	The "mask" is a bit string where a "1" ignores the corresponding OID bit and a "0" indicates a wild card match for the corresponding OID bit. A string of all "1" bits will accept any OID.
Type	Included Excluded	Must be same as in Notify table.
Enabled	Enabled Disabled	Enables/disables this filter.
Storage	Volatile Non-volatile Permanent Readonly Other	Settings lost without power. Settings can be changed. Settings can not be deleted. Settings can not be changed.

Notify Profiles

Entries may be completely maintained using the cammi Notification Profiles table (which is a direct representation of “snmpNotifyFilterProfileTable”) or via a remote SNMP manager. This table allows finer grained control over trap reports. Broadmore permits up to 20 entries in this table. An empty table is acceptable.

These settings can only be accessed and changed by a SuperUser.



Select **System Management** ↵
Select **Configuration** ↵
Select **System Services** ↵
Select **SNMP Configure** ↵
Select **Notify Profiles** ↵
Select one of the following:

* **Edit** ↵, edit the Profile information
* **Copy** ↵, (to put a copy of the information into the list)
* **Delete** ↵, delete an existing Profile
* **New** ↵, enter a new Profile
* **Validate Table** ↵, check table entries for consistency

With each selection, confirm your changes and press *Esc* to exit.

NOTE: Selecting **Validate Table** will check that each Parameter Name in this table exists in the Target Parameters table.

The only reason for this table is to allow more than one notify filter with the same Profile Name and different subtree, so that "profile_name" + "subtree" is the key into the Notify Filter table. When a "profile_name" is found in the Notify Profiles table, the Notify Filter table is searched for all entries having the same "profile_name".

The following table describes the selections.

Item	Options	Comments
Profile Name	string	Value for Profile Name, 1 to 30 characters.
Parameter Name	string	Value for Parameter Name, 1 to 30 characters. **Note:** This entry must agree with the Parameters Name in the Target Parameters table (see *"Target Parameters" on page 12-35*).
Enabled	Enabled Disabled	Enables/disables this profile.
Storage	Volatile Non-volatile Permanent Readonly Other	Settings lost without power. Settings remembered after reboot. Settings can not be deleted. Settings can not be changed.

APPENDIX A

Technical Specifications

In this Appendix:

- Broadmore 1750 Platform ... *A-2*
- Broadmore Modules ... *A-6*

Broadmore 1750 Platform

System Architecture

- Mid-plane architecture
- Internal Stratum 3E clock with dual BITS clock inputs
- Redundant CPUs, NIMs, SAMs, backplane, power supplies
- OC-12c/STM-4c ATM network interfaces
- Up to 80 T1s, 60 E1s, 11 DS-3s, or 12 E3s per chassis

Management

- RS-232/V.24 async craft port
- SNMP v1, v2, v3 (RFC 1213, RFC 3414, MIB II)
- IPv4 and IPv6 ready Controller
- In-band management:

  LAN Emulation Client

  CLIP (RFC-1577)
- Out-of-band management:

  10Base-T Ethernet port

  RS-232/V.24 async craft port
- Management interface:

  Command Line Interface (CLI)

  Text-based menu-driven
- Optional security features:

  FIPS 140-2 approved Secure Shell (SSH) v2.0

  RSA SecurID® User Client v5.0.2

Network Standards

- ATM Forum compliant AAL1 and AAL5 QoS
- ATM Forum compliant SVCs and PVCs
- ATM Forum Circuit Emulation Service v2.0 (CES)
- ITU-T and ANSI compliant UNI 3.0, 3.1, and 4.0 Signaling
- ATM Forum compliant ILMI 4.0
- Network Timing Protocol Client per RFC 1305

Redundancy

- System Level:

  Backplane: redundant segment protection

  Dual Power -48 VDC power rails to each card

- Interface Level:

  CPUs: 1:1

  NIMs: 1+1 SONET APS per Telcordia™ GR-253-CORE with Digital Protection Switching

  SAMs: 1:N

  Dual BITS clock inputs with internal Stratum 3E holdover clock

Alarms

- Dry contacts for major and minor alarms
- LEDs indicating major and minor alarms
- User-defined alarm configuration
- SNMP trap generation for user-defined alarms

Testing & Diagnostics

- Network loop-backs (structured DS3: DS3 port; unstructured DS3, E3 port)
- Service loop-backs (structured DS3: DS3 port, tributary and DS0; unstructured DS3, E3)
- Internal BERT generation and monitoring (structured DS3, unstructured DS3, E3)
- FEAC loop-back generation and detection

Power

- –48 VDC dual inputs, labeled A and B
- 240 W maximum for fully populated system

  10 watts per NIM

  8 watts per SAM

  20 watts per CPU
- Fused at 7.5 A, each input
- Alarm power module, 1 slot

  Over-voltage threshold: 58 ± 1.5 VDC
  Under-voltage threshold: 38 ± 0.72 VDC
- Optional Dual Redundant AC Power Supply, external

Regulatory Approvals

- FCC Part 15, Class A radiated emissions
- ANSI/UL 60950, CSA-C22.2 NO. 60950-00
- FIPS-140-2 Validated
- Joint Interoperability Test Command (JITC) Certified
- DISA Information Assurance (IA) Tested
- Network Equipment Building Standard (NEBS) Validated, Level 3

Physical

- 17-slot chassis
- Card slots: 1 to 12 SAMs, 1 or 2 NIMs, 1 or 2 CPUs, 1 alarm power module
- Rack mountable in 19 in (48.26 cm) or 23 in (58.42 cm) racks
- Dimensions:

  17.5 in (H) x 17.25 in (W) x 15.3 in (D)

  44.45 cm (H) x 43.82 cm (W) x 38.86 cm (D)
- Weight: 31 lb. (14.1 kg) empty, 48 lbs (21.8 kg) fully loaded

Environment

- Operating temperature range: 50 °F to 122 °F (10 °C to 50 °C)
- Storage temperature range: –4 °F to 158 °F (–20 °C to 70 °C)
- Relative humidity (non-condensing) range: 5% to 80%

Broadmore Modules

OC-12c Network Interface Modules (NIMs)

- SONET/ SDH OC-12c/ STM-4c 622.08 Mbps: network synchronization
- Single mode and multi-mode options
- Optical connectors type: SC
- Premise Reach:

  Type - multi-mode

  Wavelength - 1300 nm

  Tx Output power - greater than or equal to –18.0 dBm

  Rx sensitivity - less than or equal to –28.0 dBm
- Intermediate Reach:

  Type - single-mode

  Wavelength - 1300nm

  Tx Output power - greater than or equal to –11.0 dBm

  Rx sensitivity- less than or equal to –28.0 dBm

DS3 (T3) Structured Circuit Emulation SAM

- 1 port per card
- BNC connector access on rear panel IOM
- CES Version 2 (AAL1) and ITU-T recommendation I.363:

  Structured (N x 64) DS3: (1 to 672 ATM PVCs or SVCs per port)
- DS3 options: C Bit parity, M13
- Clocking: Network, BITS, Adaptive, SRTS, Loop

NOTE: SRTS is a proprietary timing algorithm and may ONLY be used with specific written prior permission from Carrier Access Corporation. Additional license fees may apply.

DS3 Unstructured Circuit Emulation SAM

- 3 ports per card
- BNC connector access on rear panel IOM
- Unstructured CES Version 2 (AAL1) and ITU-T recommendation I.363
- DS3 options: C Bit parity, clear channel
- Clocking: Network, BITS, Adaptive, SRTS, Loop

NOTE: SRTS is a proprietary timing algorithm and may ONLY be used with specific written prior permission from Carrier Access Corporation. Additional license fees may apply.

E3 Unstructured Circuit Emulation SAM

- 3 ports per card
- BNC connector access on rear panel IOM
- Unstructured CES Version 2 (AAL1) and ITU-T recommendation I.363
- E3 options: clear channel
- Clocking: Network, BITS, Adaptive, SRTS, Loop

NOTE: SRTS is a proprietary timing algorithm and may ONLY be used with specific written prior permission from Carrier Access Corporation. Additional license fees may apply.

APPENDIX B

Spare Parts List

The most common spare parts are listed below. The fan filters and fuse/fuse cover assemblies may be ordered from Carrier Access Corporation or directly from the manufacturer. The manufacturer's name and part numbers are provided for these items.

Contact your local Sales Account Manager for the latest availability and pricing information. Please have your system model and serial number available when calling to facilitate service. In the unlikely event that a part not listed above is required, the Customer Support Center will provide detailed information on replacing the component.

P/N	Description	Page
7660-022	Fan Tray Assembly	
7660-023	Module, Alarm/Power (APM)	
7660-034	Module, Unstructured DS3 SAM, CE, 3-Port	
7660-045	Module, Unstructured E3 SAM, 3 Port	
7660-110	Module, OC-12/STM-4, NWK INTFC, IR, FC	
7660-114	Module, OC-12/STM-4, IR, SC	
7660-206	Module, CPU with FIPS, Ethernet and SAR	
7660-403	Module, DS3 SAM IOM, 3-Port	
7660-404	Module, SAM IOM, 8 RJ48 Connectors	
7660-406	Module, NIM IOM	
7660-410	Module, Protection IOM	
7660-411	Module, CPU IOM	
7660-416	Module, Structured DS3 SAM IOM, 1 BNC Port	
7660-672	Module, Structured DS3 SAM	
51670066-01	LapLink Cable, PC to Broadmore 1750 serial port cable with DB9-F and DB25-F connectors on both ends	
034-0016	CPU-2 Replacement Battery, Panasonic VL1220-1HF or equivalent	
Bussman #GMT7.5	Bussman 7.5 Amp Fuse	
Bussman #GMT-X	Bussman Fuse Cover	
Globe Motors #FFM745	Globe Motors Fan Filter	

APPENDIX C

Software Error Messages

In this Appendix:

- Overview
- System Errors
- Setup Errors

Overview

Error messages are displayed for a number of reasons. In many cases an error message is the result of normal operation and no operator action is required. The messages shown below are divided into two groups: SYSTEM ERRORS and SETUP ERRORS. Typically, the SETUP ERRORS are configuration problems which the user can correct through normal operations as noted in chapters three and four. SYSTEM ERRORS provide clues about system operation which are meant primarily for Carrier Access Customer Support analysis.

NOTE: System errors may be observed during normal operation. These errors may be an indication of events which are not necessarily a problem. Evaluate the Broadmore 1750 operation according to *"Maintenance and Troubleshooting" on page 8-1*, when in doubt.

```
/*
* Error codes used primarily by the Configuration Manger.
*
* These codes are in a range not used by pSOS. For codes not in
this
* list, see the pSOS manual.
*/
```

System Errors

The user cannot address these errors. Contact Carrier Access Customer Support.

```
MALLOC_FAILED              = 0x1000
   NULL_POINTER             = 0x1001
   NOT_A_NIM                = 0x1002
   NOT_A_SAM                = 0x1003
   BAD_ATMIFNUM             = 0x1004
      /* Illegal value for atmIfNum */
ENTRY_ZERO_NOT_RESERVED = 0x1005
      /* Connection table entry 0 must be
                          * reserved for use by error handling
                          * code. NO_ATM_IF_INDEX must = 0!
                         */
   LIKELY_MEMORY_LEAK       = 0x1006
   NONSENSICAL_STATE        = 0x1007
      /* "Impossible" state of affairs found */
   UNREACHABLE_CODE         = 0x1008
      /* Unreachable code reached! */
   OUTBOUND_MSG_TOO_LONG    = 0x1009
     /* Msg to a DSP is too long   */
   INBOUND_MSG_TOO_LONG     = 0x1010
     /* Msg from a DSP is too long */
   TRANSMIT_ERROR           = 0x1011
     /* Error transmitting data to a card */
   INVALID_QUEUE_NUMBER     = 0x1012
    /* Invalid message queue number */
```

Setup Errors

These errors can usually be corrected by the user.

```
BAD_OC3_INPUT_PARAMETER    = 0x1101
BAD_OC3_FRAME_TYPE         = 0x1102
BAD_OC3_CLOCK_MODE         = 0x1103
BAD_OC3_LASER_STATE        = 0x1104
BAD_OC3_SCAMBLE_CONTROL    = 0x1105
BAD_OC3_BIPFEBE_OPTION     = 0x1106
BAD_OC3_PLSCRAMBLE_OPTION = 0x1107
BAD_OC3_XTABLE_FORMAT      = 0x1108
BAD_OC3_RESET_OPTION       = 0x1109
BAD_OC3_LOOP_MODE          = 0x110a
BAD_OC3_ACTION_ID          = 0x110b

BAD_NX64_ACTION_ID         = 0x110c
BAD_NX64_INPUT_PARAMETER   = 0x110d
BAD_NX64_LINE_CODE_FORMAT = 0x110e
BAD_NX64_TIMING_SOURCE     = 0x110f
BAD_NX64_LOOPMODE          = 0x1110
BAD_NX64_LINE_LENGTH       = 0x1111
BAD_NX64_FRAME_TYPE        = 0x1112
BAD_NX64_TRANSMIT_ALARM    = 0x1113
BAD_NX64_DIAG_CONTROL      = 0x1114
BAD_NX64_SERVICE_TYPE      = 0x1115

INVALID_SLOT_NUMBER        = 0x1116
NULL_SDU_POINTER           = 0x1117
CONFIGURE_ITEM_QSEND_ERR   = 0x1118
CONFIGURE_ITEM_ERROR       = 0x1119
READ_NX64SAMFILE_ERROR     = 0x111a
READ_OC3NIMFILE_ERROR      = 0x111b
WRITE_NX64SAMFILE_ERROR    = 0x111c
```

```
WRITE_OC3NIMFILE_ERROR    = 0x111d
DATABASE_CREATION_ERROR   = 0x111e
WRITE_7665INIFILE_ERROR   = 0x111f
CONMAN_RETRIES_EXCEEDED   = 0x1120

SVCS_CARDTYPE_MISMATCH    = 0x1121

WRONG_RX_TX_DATALEN       = 0x1122
WRONG_LOAD_XTABLE_DATALEN = 0x1123
VPVC_NOT_TRANSLATABLE     = 0x1124
   /* VP/VC incompatible with the
          * current OC3 Translation Table
          * Address Format.
          */
NIM_NOT_FOUND             = 0x1125
CONNECTION_LIMIT_REACHED  = 0x1126
   /* Connection table is full */
CHANNELS_ALREADY_IN_USE   = 0x1127
       /*VC related errors */
SIG_LINK_NOT_READY        = 0x1128
INVALID_PORT_NUMBER       = 0x1129
INVALID_CHANNEL_NUMBER    = 0x112a
INVALID_CHANNEL_MAP       = 0x112b
INVALID_ATM_IFINDEX       = 0x112c
   /* Connection not found
        * or ifIndex was not as expected. */
CONNECTION_IN_USE         = 0x112d
    /* Connection in use; request not
          * allowed at this time.*/
INVALID_DSS                = 0x112e
INVALID_SDU_DATAWORD_LEN   = 0x112f
PVCS_CARDTYPE_MISMATCH     = 0x1130
    /* PVCs not supported for card type */
```

```
INVALID_INTERNAL_VCI      = 0x1131
INVALID_CALL_IDENT        = 0x1132
INVALID_CARD_TYPE         = 0x1133
CONFIG_DEFAULTS_USED      = 0x1134
INVALID_MESSAGE_TYPE      = 0x1135
UNKNOWN_ACTION_ID         = 0x1136
```

APPENDIX D

Sample Network with RFC 1577 Configuration

This Appendix provides a sample network configuration to explain how the Classic IP (CIP) over ATM functions. CIP provides the path for control of remote Broadmore 1750s from a master control station over the ATM network.The three possible configurations are shown in the figure on the next page. These are:

1. The master control station has Ethernet access to the Broadmore 1750 (Broadmore 1750 #1).
2. The master control station does not have Ethernet access to the Broadmore 1750 and the Broadmore 1750 does not have an Ethernet local control station (Broadmore 1750 # 2).
3. The master control station does not have Ethernet access to the Broadmore 1750 and the Broadmore 1750 has an Ethernet local control station (Broadmore 1750 #3).

The objective is for the master control station to be able to communicate with all three Broadmore 1750s. This is done by creating a subnet over the ATM. This subnet consists of the three Broadmore 1750s; with each having a unique CIP Ethernet address as shown. Broadmore 1750 #1 has Ethernet connectivity with the master control station. The ARP server, which is the ATM switch or a suitable

device on the ATM network, maintains the Logical IP Subnetwork (LIS) as explained in the CIP over ATM section of Chapter 4.

Ethernet traffic for Broadmore 1750 #1 goes through the gateway directly to Broadmore 1750 #1. Ethernet traffic for Broadmore 1750 #2 and Broadmore 1750 #3 is routed by the gateway to Broadmore 1750 #1. The server uses LIS data to convert the IP address to an ATM address; the traffic is then sent over the ATM to the destination Broadmore 1750 where it is interpreted and acted upon as required.

Broadmore 1750 #2 has no Ethernet connection and its gateway is set to null. This Broadmore 1750 sends all Ethernet traffic over the ATM (to Broadmore 1750 #1) by default. Broadmore 1750 #1 then forwards the traffic to the gateway and ultimately to the appropriate Ethernet address.

Broadmore 1750 #3 has an Ethernet gateway (local control station in example diagram on next page). However, traffic to the master control station will not be delivered since the local control station has no Ethernet route to the master control station. A static route is added to Broadmore 1750 #3. This static route sends the response to all traffic from the master control station back to it via a static route using LIS conversion.

This use of CIP over ATM provides inband control of remote Broadmore 1750s. After initial setup, this configuration is essentially transparent to the master control station.

The master control station addresses:

Broadmore 1750 #1 by IP address,

Broadmore 1750 #2 by CIP address,

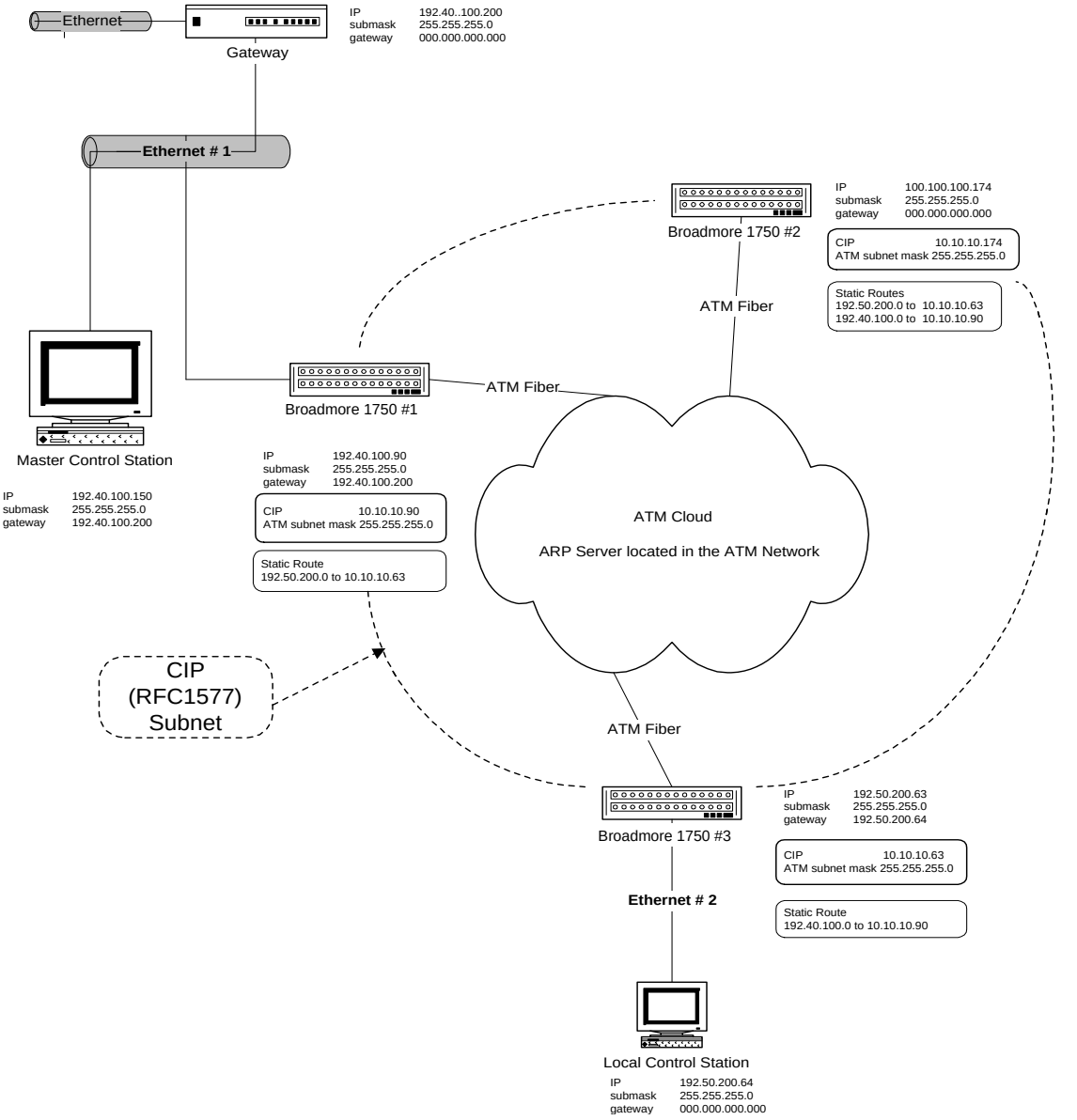
Broadmore 1750 #3 by CIP address.

Broadmore 1750 #3 addresses its local control station by IP address and the master control station via static route and Broadmore 1750 #1.

The master control station addresses
Broadmore 1750 #1 as IP 192.40.100.90,
Broadmore 1750 #2 as CIP 10.10.10.174, and
Broadmore 1750 #3 as CIP 10.10.10.63.

The local control station addresses Broadmore 1750 #3 as IP 192.50.200.63.

Sample Network with RFC 1577 Classic IP (CIP) Over ATM



APPENDIX E

Chassis Differences

Broadmore Chassis Differences

This user manual covers the 7665-17B and 7665C chassis. The 7665C chassis is the newest chassis in the Broadmore series and has the most functionality. There is also a 17A chassis.

Hardware Differences

Major differences between chassis include mid-plane wiring, alarm/power modules, and fan trays as shown in the following table.

Chassis	Major Assemblies	Part Nos.	Comments
7665-17A	Alarm & Power Module	7660-021	No I/O module
	Fan Tray	7660-022	2-wire connection
7665-17B	Alarm & Power Module	7660-023	Requires I/O module
	Alarm & Power Module I/O	7660-025	
	Fan Tray	7660-024	4-wire connection
7665-17C	Alarm & Power Module	7660-023	Requires I/O module
	Alarm & Power Module I/O	7660-025	
	Fan Tray	7660-024	4-wire connection

The 17A and 17C chassis used in the Broadmore 1700 provide the same functionality and support the same NIM, SAM, and CPU modules. The 17C chassis also uses the improved Alarm & Power Module and Fan Tray assemblies as the 17B chassis.

The 17B chassis used in the Broadmore 1750 provides 1:4 SAM redundancy and has been NEBS tested with the OC-12 NIM (7660-114 or 7660-113) and the Un-Structured DS3 SAMs (7660-034 or 7660-672).

Software Differences

Software release v3.4.1 was introduced to support the 7665-17C chassis used in the Broadmore 1700. However, software release 3.4.1 and higher can be used on all Broadmore chassis.

The CPU module can be moved between different chassis but it must be configured to recognize the chassis in which it is installed. The chassis version is specified by the presence of a file pointer in the \CAM directory. For example, a 7665-17C chassis is identified by the presence of a file named CAM7665.17C in the \CAM directory. Similarly, the 17A and 17B chassis are identified by the files CAM7665.17A and CAM7665.17B.

To change the file pointer in the CPU, perform the following steps:

1. Log in as a Superuser. The default login is: ***SYSADMIN*** and password: ***INITIAL***
2. From the operating system prompt, enter ***cd cam***
3. Type ***dir*** and look for one of the following files: ***CAM7665.17A***, ***CAM7665.17B***, or ***CAM7665.17C***
4. If the file name does not correspond to the chassis in which the CPU is installed, the file must be renamed. For example, to change the chassis version from 17A to 17C, enter the following command: ***mv CAM7665.17A CAM7665.17C***
5. If no file can be found, it can be created using the touch command. For example, to create a file for the 17C chassis, enter the command: ***touch CAM7665.17C***

A CPU shipped with a Broadmore 500 will have the file CAM7665.5, which tells the CPU to recongnize only the first 5 module slots. This file can also be changed as described above if the CPU is installed in a different chassis.

APPENDIX F

IPv6 Support

In this Appendix:

- Overview ... *F-2*
- Configuring IPv6 Addresses for Network Interfaces ... *F-2*
- Pinging over IPv6 ... *F-4*
- Testing route6 Application ... *F-5*

Overview

This Appendix provides methods for demonstrating IPv6 functionality on Broadmore.

You can find more test methods in the Product Application Notice: Broadmore IPv6 (PAN-07-0001), which is available on the Customer Support website.

Configuring IPv6 Addresses for Network Interfaces

When the system boots up, an IPv6 address of link-local scope is configured on all the network interfaces. This section provides steps to configure a network interface.

Adding an IPv6 Address

To set the IPv6 address on the Ethernet interface, from the Broadmore shell issue the command **`ifconf6`** with the argument **`-a`**. For example:

```
Broadmore-> ifconf6 1 -a 3ffe:0:0:13::5
```

The above command sets the IPv6 address **`3ffe:0:0:13::5`** on the Ethernet interface **`1`**.

Displaying an Address

Check the interface configuration.

```
Broadmore->ifconf6 1

     Interface Name            : 1
     Index number              : 2
     Type                      : ETHERNET
     Inet6 Address             : fe80::2e0:97ff:fe6b:7ffe
     Prefix Mask               : ffff:ffff:ffff:ffff::
     Flags                     : 0 <>
     Inet6 Address             : 3ffe:0:0:13::5
     Prefix Mask               : ffff:ffff:ffff:ffff::
     Flags                     : 0 <>
```

```
Physical Address          : 00:e0:97:6b:7f:fe
MTU  Size                 : 1500
Packets received          : 23
Packets sent              : 2
Mcast Packets received    : 0
Mcast Packets sent        : 0
Total Bytes received      : 1480
Total Bytes sent          : 64
Input errors              : 0
Output errors             : 0
Packets dropped on input  : 0
Flags  : 0xa8e1 <BROADCAST,RUNNING,UP,MULTICAST>
```

Deleting an IPv6 Address

To delete the IPv6 address from an Ethernet interface, from the Broadmore shell issue the command **`ifconf6`** with the argument **`-d`**. For example:

```
Broadmore->ifconf6 1 -d 3ffe:0:0:13::5
```

Pinging over IPv6

To ping a remote host over IPv6, issue the command **ping6**. The remote host must also be configured with an IPv6 address of global scope and must be in the same subnet as the Broadmore.

Pinging an IPv6 Host

The following example shows a **ping6** operation to a host with an IPv6 address **3ffe:0:0:13::4**. The subnet in this case is 3ffe:0:0:13::x.

```
Broadmore->ping6 -c 1 3ffe:0:0:13::4
PING6(56=40+8+8 bytes) 3ffe:0:0:13::4
16 bytes from 3ffe:0:0:13::4, icmp_seq=0 hlim=64
--- ping6 statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
```

Ping the Loopback Interface Address

```
Broadmore->ping6 -c 10 -s 1000 ::1

PING6(1048=40+8+1000 bytes) ::1
1008 bytes from ::1, icmp_seq=0 hlim=64
1008 bytes from ::1, icmp_seq=1 hlim=64
1008 bytes from ::1, icmp_seq=2 hlim=64
1008 bytes from ::1, icmp_seq=3 hlim=64
1008 bytes from ::1, icmp_seq=4 hlim=64
1008 bytes from ::1, icmp_seq=5 hlim=64
1008 bytes from ::1, icmp_seq=6 hlim=64
1008 bytes from ::1, icmp_seq=7 hlim=64
1008 bytes from ::1, icmp_seq=8 hlim=64
1008 bytes from ::1, icmp_seq=9 hlim=64

--- ping6 statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
```

Testing route6 Application

This section provides examples for adding, deleting and displaying routes.

Adding an IPv6 Route

To add an IPv6 route, issue the Broadmore command **`route6.`** The following example adds a default route on the Broadmore:

```
Broadmore->route6 add default gateway 3ffe:0:0:13::4
```

Adding a Host Route

The following example adds a host route on the Broadmore:

```
Broadmore->route6 add host dst 3ffe:0:0:14::41 gateway
3ffe:0:0:13::4
```

Adding a Network Route

The following example adds a network route on the Broadmore:

```
Broadmore->route6 add net dst 3ffe:0:0:14:: gateway
3ffe:0:0:13::4prefixlen 64
```

Showing all IPv6 routes configured in the Broadmore

To display all the IPv6 routes configured in the system, issue the command **route6** with option **-a**. For example:

```
Broadmore->route6 -a

Destination        Gateway            Flags    Refcnt   Use      Interface

-------------------------------------------------------------------------------
-------------------------------------
::
        3ffe:0:0:13::4
                                     10803    0        0        1
-------------------------------------
::1
        ::1
                                     200005   0        0        6
-------------------------------------
3ffe:0:0:13::
        3ffe:0:0:13::5
                                     101      1        0        1
-------------------------------------
fe80:1::
        fe80:1::1
                                     10001    0        0        6
-------------------------------------
fe80:2::
        fe80:2::2e0:97ff:fe6b:7ffe
                                     101      0        0        1
-------------------------------------
ff01::
        ::1
                                     800001   0        0        6
-------------------------------------
ff02:1::
        ::1
                                     800101   0        0        6
-------------------------------------
ff02:2::
        fe80:2::2e0:97ff:fe6b:7ffe
                                     800101   0        0        1
-------------------------------------
-------------------------------------------------------------------------------
```

Deleting the Default Route

The following example deletes the default route on the Broadmore:

```
Broadmore->route6 delete default gateway 3ffe:0:0:13::4
```

Deleting a Host Route

The following example deletes a host route on the Broadmore:

```
Broadmore->route6 delete host dst 3ffe:0:0:14::41 gateway
3ffe:0:0:13::4
```

Deleting a Network Route

The following example deletes a network route on the Broadmore:

```
Broadmore->route6 delete net dst 3ffe:0:0:14:: gateway
3ffe:0:0:13::4 prefixlen 64
```

APPENDIX G

Broadmore Command List

In this Appendix:

- Commands Available at the Command Prompt
- Commands Available at the CLI Prompt

Commands Available at the Command Prompt

The commands listed below are available immediately after you log into the Broadmore.

Type ‘help’ at the command prompt to view the list of commands. You can also type ‘help *command*’ to obtain help on any of the listed commands.

arp
cammi
cat
cd
chargen6tcp
chargen6udp
cli
cmp
comp
copy
cp
daytime6tcp
daytime6udp
del
dir
du
echo
fipsmode
head
help
icmp6StatsShow
ifconf
ifconf6
in6AddrShow
ip6StatsShow
ls
mbStatsShow
md
netStackUdpStatsShow
netstat
ping
ping6
prefixListShow
pwd
rd
resetSecurID
resetSecurIDIp
rm
rmdir
route
route6
savert
scp
selftest
setbaud
setenv
settimeout
setwrite
showconfig
sigmem
snmpinit
sntpGet
sntpShow
sshdSessionShow
sshdShow
tail

mem	tc6
mkdir	timeoutStatsShow
move	touch
mv	ts6
nd6Cache	uc6
netStackTcpPcbShow	us6
netStackUdpPcbShow	zeroize

See *"Shell Commands (Non-FIPS Mode)" on page 10-19* and *"Shell Commands (FIPS Mode)" on page 11-34* for information about the availability of commands based on user access level.

Commands Available at the CLI Prompt

The commands listed below are available at the cli> prompt.

Type ? at the command prompt to view the list of commands.

General Commands

up cls quit ? (help)

Level Commands

sys maintain about

GLOSSARY

Acronyms and Abbreviations

AAL	ATM Adaptation Layer
AIS	Alarm Indication Signal
ANSI	American National Standards Institute
APM	Alarm Power Module
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
AS	Available Seconds
ATM	Asynchronous Transfer Mode
AWG	American Wire Gage
BITS	Building Integrated Timing System
Bps	Bits Per Second

C	Centigrade
CAM	Communications Access Multiplexer
CAMMI	CAM Management Interface
CBES	C-Bit Errored Seconds (network)
CBR	Constant Bit Rate
CCV	C-Bit Coding Violation
CDVT	Cell Delay Variation Tolerance
CES	C-Bit Errored Seconds
CES	Circuit Emulation SAM
CIP	Classic IP
CLI	Command Line Interface
CPU	Central Processor Unit
CSES	C-Bit Severely Errored Seconds
DSP	Digital Signal Processor
DS-n	Digital Signal level *n*
EIA	Electronic Industries Alliance
ESD	Electrostatic Discharge
FCC	Federal Communications Commission
FEAC	Far End Alarm Control
FTP	File Transfer Protocol

GUI	Graphical User Interface
IOM	Input Output Module
IP	Internet Protocol
IR	Intermediate Reach
LCV	Line Coding Violation
LED	Light-Emitting Diode
LES	Line Errored Seconds
LIS	Logical IP Subnetwork
LIU	Line Interface Unit
LOCD	Loss of ATM Cell Delineation
LOF	Loss of Frame
LOP	Loss of Pointer
LOS	Loss of Signal
MAC	Media Access Control
MBR	Multi-bit-rate
Mbps	Megabits per second
MIB	Management Information Base
NEBS	Network Equipment Building System
NIM	Network Interface Module

OC-n	Optical Carrier level *n*
PC	Personal Computer
PCB	Printed Circuit Board
PCMCIA	Personal Computer Memory Card International Association
PCV	P-Bit Coding Violation
PES	P-Bit Errored Second
PLOA	Protocol Layer Over ATM
POST	Power On Self Test
PSES	P-Bit Severely Errored Seconds
PWR	Power
RDI	Remote Defect Indicator
RMA	Return Material Authorization
RX	Receive
SAM	Service Access Module
SAR	Segmentation and Reassembly
SEFS	Severely Errored Framing Seconds
SEQ	Sequence Errors
SG	Signal Ground
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network

TBD	To Be Determined
TX	Transmit
UAS	Unavailable Seconds
UNI	User Network Interface
VGA	Video Graphics Adapter
VOM	Volt Ohm Meter

Glossary of Terms

ATM Adaptation Layer (AAL)

Type 1 AAL functions in support of constant bit rate, time-dependent traffic such as voice or video (default in CES-CBR configuration).

Type 2 AAL undefined by International Standards bodies. Its anticipated use is for variable bit rate video transmission.

Type 3/4 AAL functions in support of variable bit rate, delay-tolerant data traffic requiring some sequencing and/or error detection support. This was originally two AAL types, i.e., connection-oriented data traffic requiring minimal sequencing or error detection support.

Type 5 AAL functions in support of variable bit rate, delay-tolerant connection-oriented data traffic requiring minimal sequencing or error detection support.

Broadband Bearer Capability

A bearer class field that is part of the initial address message.

BCOB Broadband Connection Oriented Bearer -- information in the SETUP message that indicates the type of service requested by the calling user.

BCOB-A Bearer Class A -- indicated by ATM end user in SETUP message for connection-oriented, constant bit rate service. The network may perform internetworking based on AAL information element (default in CES-CBR configuration).

BCOB-C Bearer Class C -- indicated by ATM end user in SETUP message for connection-oriented, variable bit rate service. The network may perform internetworking based on AAL information element.

BCOB-X Bearer Class X -- indicated by ATM end user in SETUP message for ATM transport service where AAL, traffic type, and timing requirements are transparent to the network.

Constant Bit Rate

An ATM service category that supports a constant or guaranteed rate to transport services such as video or voice as well as circuit emulation requiring rigorous timing control and performance parameters.

Circuit Emulation Service (CES)

The ATM Forum circuit emulation service interoperability specification provides interoperability agreements for supporting constant bit rate (CBR) traffic over ATM networks that comply with the other ATM Forum interoperability agreements. Specifically, this specification supports emulation of existing TDM circuits over ATM networks.

End-to-End Timing Requirements

Timing requirements that address the restrictions on the amount of time a cell can take in getting from source to destination.

Point-to-Point Connection

A connection with two endpoints (default in CES-CBR configuration).

Point-to-Multipoint Connection

A collection of associated ATM VC or VP links, with associated endpoint nodes, with the following properties:

1. One ATM link, called the Root Link, serves as the root in a simple tree topology. When the Root Node sends information, all the remaining nodes on the connection, called the Leaf Nodes, receive copies of the information.
2. Each of the Leaf Nodes on the connection can send information directly to the Root Node. The Root Node cannot distinguish which Leaf is sending information without additional (higher layer) information.
3. The Leaf Nodes cannot communicate directly to each other with this connection type.

Quality of Service (QoS)

A QoS class can have specified performance parameters (specified QoS class) or no specified performance parameters (unspecified QoS class). QoS classes are inherently associated with a connection. A specified QoS class specifies a set of performance parameters and the objective values for each performance parameter identified. Examples of performance parameters that could be in a QoS class are:

1. Cell Loss Ratio
2. Cell Transfer Delay
3. Cell Delay Variation

A specified QoS class provides a quality of service to an ATM virtual connection (VCC or VPC) in terms of a subset of ATM performance parameters defined in Section 3 of Appendix A of the ATM Forum UNI v3.1 specifications. Initially, each service provider should define objective values for a subset of the ATM performance parameters for at least one of the Service Classes (Service Class A, B, C, or D) from ITU-T recommendation I.362 in a reference configuration that may depend on mileage and other factors.

QoS Classes are currently defined as:

Class 1: supports a QoS that will meet Service Class A performance requirements (circuit emulation, constant bit rate video). Should yield performance comparable to current digital private line performance.

Class 2: supports a QoS that will meet Service Class B performance requirements (variable bit rate audio and video). Intended for video and audio in teleconferencing and multi-media applications using packets.

Class 3: supports a QoS that will meet Service Class C performance requirements (connection-oriented data transfer). Intended for interoperation of connection-oriented protocols, such as Frame Relay.

Class 4: supports a QoS that will meet Service Class D performance requirements (connectionless data transfer). Intended for interoperation of connectionless protocols, such as IP or SMDS.

User Plane Connection

Signaling operates in the control plane (doing control-type functions such as setting up the connection). After signaling is finished, it drops out of the way and the established connection is used to move data. This moving of payload data is done in the user plane. Control and user planes are parts of the conceptual model of ATM.

Variable Bit Rate

An ATM Forum defined service category supporting variable bit rate data traffic with average and peak traffic parameters.

INDEX

Numerics

1 to 1 Protection 7-26
1 to n Protection 7-25
1+1 Protection 7-25
24-Hour Statistics 8-13
–48 VDC Power, Connecting 6-14

A

About Command, CLI 9-9
AC Power Supply Connections 6-12
AC Power Supply Tray 4-8
Access
    Chassis 5-5, 5-15
    Clearance 4-3
    CLI 9-2
    USM/VACM 12-19
Access Edit Rules, SNMPv3 12-22
Access Policy, SNMPv3 12-22
Address
    ATM IP 7-15
    Server 7-15
Aggregation and Backhaul, TDM Circuit . . . 2-3
Alarm
    Overview 8-4
    Port Connections 6-5
Alarm Power Module 1-10, 1-24
    IOM 1-25
Alarms 1-9
APM 1-24
    Configuration 1-10
    Installation 5-10
    IOM 1-25
    IOM Installation 5-12
    Slots 1-10
Application Planning Guide 2-2
Applications 1-3
APS 7-25
Architecture, System 1-7, 2-6
Archiving Audit Trails 10-15, 11-32
AS 8-7
ATM 7-14
    Address 7-11
    Bandwidth per Cell Bus 2-11
    Bandwidth per Module 2-12
    Interfaces 1-4
    IP Address 7-15
    Network Loading 2-12
    Payload Scramble Mode 7-39
    Subnet Mask 7-15
ATM by Chassis 8-2
Audit Trails 10-10, 10-13, 11-26, 11-30
    Archiving 10-15, 11-32
    Deleting 10-15, 11-32
    System Log 10-15, 11-32
Authentication 11-6
Authorized Access to Shell Commands . 10-19, 11-41
Authorized Services 11-6
Automatic
    FEAC Alarms 7-45, 7-53

B

Backhaul, TDM Circuit Aggregation and . . . 2-3
Bandwidth per Cell Bus, ATM 2-11
Bandwidth per Module, ATM 2-12
Banner Text 10-6, 11-13
Basic Features 2-2
Battery, CPU-2 Replacement 2-16
BER 7-28
Bit Error Rate 7-28
BITS 7-44, 7-51, 7-52, 7-58
    Clock Alarm Loss 7-39
    Jumpers 5-9
    Timing Redundancy 7-40
BITS Interface Connections 6-7
Brackets, Mounting 4-5
Broadmore 1750
    Chassis 2-15
    Options 2-16
    Spares 2-16
Broadmore Power Input Connector 6-14
Broadmore/SSHield Management Module . . 1-5
Bus
    ATM Bandwidth per Cell 2-11
    Configuration 2-8

C

Cable
    Serial Port 2-16
Cable Management 6-3
Cabling and Compliance Requirements 6-4
CAM
    CONFIG, CURRENT 7-3
    CONFIG, DEFAULTS 7-3
    CONFIG, User Name 7-3
    Name 7-8
CAMMI Access 7-7
C-bit 7-44, 7-51, 7-52, 7-58
CBR
    Service Type 7-56
CCEVS iii
CCV 8-7
Cell
    Starvation 7-47, 7-60, 7-61
Cell Bus
    ATM Bandwidth 2-11
    Configuration 2-8
Cell Starvation 7-46
Central Processing Unit 1-10
CES 8-7
Change Password 10-11
Changing Security Modes 11-17
Chassis 1-8
    Access 5-5, 5-15
    Broadmore 1750 2-15
    Cover Removal 5-5
    Cover Removal, Front 5-15
    Cover Replacement 5-13, 5-16
    Grounding 4-7
    Installation 4-1, 4-4
    Statistics 8-2
CIP 7-4
    IP Address 7-34
    Over ATM 7-14
Circuit Aggregation and Backhaul, TDM . . . 2-3
Circuit Resiliency, Mission-Critical 2-4
Clearance, Installation 4-3
CLI
    Access 9-2
    Monitor Commands 9-8
    Port Configuration 9-6
    Scripts 9-4
Clock
    Mode 7-44, 7-51, 7-52, 7-58
    System 10-7, 10-8, 11-14, 11-15
Communities, SNMP 12-24
Compliance iii
    DISA Validated iv
    FCC Requirements iii

FIPS 140-2 Validated iv
JITC Validation iv
National Electrical Code v
NEBS Validation v
Compliance Requirements 6-4
Configuration 1-10
APM 1-10
Broadmore 1750 7-1
Cell Bus 2-8
CLI Port 9-6
Guidelines
OC-12c NIM 2-9, 2-10
IOM 1-10
NIM 1-10
SAM 1-10
SAM, Protection 1-10
Configure
DS3 SAM, Structured 7-50
DS3 SAM, Unstructured 7-43
E3 SAM, Unstructured 7-57
IP 7-9
Module 7-37
OC-12c 7-39
Specific Modules 7-38
STM-4c 7-39
Connection
PVC 7-63
Retry 7-13
Connections
–48 VDC Power 6-14
AC Power Supply 6-12
Alarm Port 6-5
BITS Interface 6-7
CPU IOM 6-11
Ethernet 6-11
NIM IOM 6-8
Optical Interface 6-6
Power Supply 6-12
Remote Shutdown 6-11
SAM IOM 6-8
Serial Port 6-11
Structured DS3 IOM 6-10
Unstructured DS3-3 IOM 6-9
User Equipment 6-8
Connector, Broadmore Power Input 6-14
Contact Information 2-15
Cover
Fuse, Part Number 2-16
Removal 5-5, 5-15
Replacement 5-13, 5-16
CPU 1-10, 1-22, 7-4, 7-11, 7-34
Configuration 1-10
Disk-On-Chip, Replacement 2-16
Install Single or Dual 7-36
Installation 5-10
IOM 1-23
IOM Connections 6-11
IOM Installation 5-12
IP Address 7-34
Reboot Standby 7-36
Redundancy 7-33
Release Control 7-36
Slots 1-10
Sync 8-17
Sync Data and SW 7-35
System Log 7-34
CPU-2 Replacement Battery 2-16
CSES 8-7

D

Damage Report 3-3
Date
System 10-7, 11-14
Debug Messages, scp 11-38
Default
DSA Key 11-8
Delete
Configuration 7-71

User 10-12, 11-28
Deleting Audit Trails 10-15, 11-32
DISA Validated iv
Disk-On-Chip, Part Number 2-16
DS3
IOM 1-17, 1-20
Structured 1-19
SAM
Structured 1-18
Alarm Configuration 7-53
Configuration 7-50, 7-51
Diagnostics 7-52
Diagnostics Configuration 7-52
Loopback Configuration 7-56
Operational Configuration 7-58
Statistics 8-9
Tributory Configuration 7-55
Unstructured 1-15
Alarm Configuration 7-60
Configuration 7-43
Diagnostics 7-45, 7-59
Operational Configuration 7-44
Statistics 8-5
DS3 IOM
Connections, Structured 6-10
DS3-3 IOM
Connections, Unstructured 6-9
DSA Key
Default 11-8
Installing 11-8
Pairs, Generating 11-8

E

E3
IOM 1-17, 1-20
SAM 1-16
Unstructured
Configuration 7-57
E3-3 IOM
Connections, Unstructured 6-9
ELAN Name 7-18
Electrical Requirements 6-3
Electrostatic Discharge (ESD) Precautions . viii
Enabling 11-18
Equipment Connections, IOM 6-8
Errors
Messages, Software C-1
Setup C-4
System C-3
Ethernet 7-4, 7-14
Connections 6-11
Excessive
C-bit Errors . 7-46, 7-48, 7-49, 7-53, 7-55, ...7-61, 7-62
F-bit Errors . 7-46, 7-48, 7-49, 7-53, 7-55, ...7-60, 7-61, 7-62
FEBE Errors 7-46, 7-48, 7-49, 7-53, 7-55, ...7-60, 7-61, 7-62
Parity Errors . 7-46, 7-48, 7-49, 7-53, 7-55, ...7-60, 7-61, 7-62
SNP Errors 7-46, 7-48, 7-60, 7-61

F

Factors
Installation 4-3
Installation Planning 2-13
System Planning 2-6
Fan Filter 2-16
Fan Tray 1-9, 2-16
Installation 5-1, 5-15
Installation Procedure 5-14
FCC Requirements iii
FEAC 7-46, 7-47, 7-48, 7-54, 7-61, 7-62
Features
Alarms 1-9
Basic 2-2
Chassis 1-8

Fan Tray 1-9
Grounding 1-9
Modules 1-10
Power 1-9
Redundancy 1-9
System 1-7
File Access 1-6
Filter, Fan, Part Number 2-16
FIPS 140-2 Validated iv
FIPS Interface 1-5
FIPS Mode 10-19
Disabling 11-20
Enabling 11-18
Frame Type 7-56
Framing 7-44, 7-51, 7-52, 7-58
Type 7-39
FTP 7-23, 8-13
Fuse
Cover 2-16
Number 2-16

G

Gateway 7-10
General Instructions 6-8
Generating DSA Key Pairs 11-8
GR-253-CORE 7-28
Grounding 1-9
Chassis 4-7
Group Edit Rules 12-15
Group Edit Rules, SNMPv3 12-15
Groups, USM/VACM 12-13
Guide
Application Planning 2-2
Ordering 2-1, 2-15
Planning 2-1
Guidelines
OC-12c NIM Configuration 2-9, 2-10

H

Hardware Revision, Showing 9-9
Help About Security 11-17

I

ICMP Messages 10-17, 11-24
Idle 7-46, 7-47, 7-48, 7-54, 7-61, 7-62
Individual
Modules, NIM and IOM 2-17
Modules, SAM and IOM 2-18
Information, Contact 2-15
Input Connector, Broadmore Power 6-14
Input/Output Module 1-10
Inspection of Goods 3-3
Install Single or Dual CPU 7-36
Installation
APM 5-10
APM IOM 5-12
Chassis 4-1
Clearance 4-3
CPU 5-10
CPU IOM 5-12
Factors 4-3
Fan 5-1
Fan Tray 5-15
Fan Tray, Procedure 5-14
Guide 5-6
Module 5-1, 5-3
Module Procedures 5-3
NIM 5-9
NIM IOM 5-11
Planning Factors 2-13
Precautions 4-2, 5-2
SAM 5-10
SAM IOM 5-11
SAM IOM, Protection 5-11
Sequence, Modules 5-8
Tools 4-4, 5-15
Tools, Module 5-5

Installing the DSA Key 11-8
Instructions, General 6-8
Interface
BITS Connections 6-7
Optical Connections 6-6
Interfaces 1-4
ADT 1-4
FIPS 1-5
Logical 1-6
Management 1-5
Physical 1-6
Security 1-5
User 1-6
User Equipment 1-4
IOM
Alarm Power Module 1-25
APM 1-25
Configuration 1-10
CPU 1-23
DS3, Structured 1-19
DS3, Unstructured 1-17, 1-20
E3-3, Unstructured 1-17, 1-20
NIM 1-14
Protection 1-21
Replacement 8-34
IOM Connections
CPU 6-11
Structured DS3 6-10
Unstructured DS3-3 6-9
Unstructured E3-3 6-9
User Equipment 6-8
IP
Address 7-14, 7-34
ICMP Messages 10-17, 11-24
Traffic 7-14
IP Address
CPU 7-34
IPv6
Addresses
Adding F-2
Configuring F-2
Deleting F-3
Displaying F-2
Pinging F-4
Routes
Adding F-5
Displaying F-6
IPv6 Ready iv

J

JITC Validated iv
Jumpers
BITS 5-9
Reboot 5-12
Resync 5-11

K

Key
DSA 11-8
Management 11-8
Map 7-6

L

LANE 7-4, 7-34
Configuration 7-17
Configuration Items 7-18
IP Address 7-18, 7-34
Version 7-18
LapLink Cable 2-16
LCV 8-7
LECS ATM Address 7-18
LES 8-7
ATM Address 7-18
Line
Code Violation 7-49, 7-54, 7-62
LIS 7-14

Loading, ATM Network 2-12
Local/BITS Timing 7-40
Locations
Module 5-6
LOF . .7-46, 7-47, 7-48, 7-54, 7-60, 7-61, 7-62
Log
System 10-15, 11-32
Logging In 10-5, 11-9
Logging in
with SecurID Disabled 11-9
with SecurID Enabled 11-11
Logical
Interfaces 1-6
IP Subnetwork 7-14
Login
SFTP 10-21, 11-43
Log-in Banner 10-6, 11-13
Loopback 7-46, 7-51, 7-52, 7-55, 7-59
Mode 7-39
LOS 7-48, 7-54, 7-62

M

M13 . . . . . 7-44, 7-51, 7-52, 7-58
MAC 7-11
Maintenance 8-1
Management Interfaces 1-5
Management, Cable 6-3
Managing Users 10-10
Media Access Control 7-11
Memory
Non-Volatile 11-50
Messages, Software Error C-1
Mission-Critical
Circuit Resiliency 2-4
Modifying a User 10-12, 11-29
Module
ATM Bandwidth per 2-12
Configuration 1-10, 7-37
Configure, How to 7-38
Descriptions 1-12
Individual, NIM and IOM 2-17
Individual, SAM and IOM 2-18
Installation 5-1, 5-3
Installation Overview 5-4
Installation Procedures 5-3
Installation Sequence 5-8
Locations 5-6
NIM and IOM Sets 2-17
NIM, Individual 2-17
Options
NIM 2-17
SAM 2-18
Redundancy 7-25
SAM and IOM, Individual 2-18
SAM and IOM, Sets 2-18
Serial Number 9-9
Monitor Activity
ATM by Chassis 8-2
CPU Sync 8-17
Mounting Brackets 4-5

N

National Electrical Code Requirements v
NEBS Validated v
Network 7-45
AIS 7-46, 7-59
Alarm 7-47, 7-61
BERT Test 7-45, 7-59
FEAC Loopback 7-45
Interface Connections, Optical 6-6
Interface Module 1-10
Interface Module, Options 2-17
Loading, ATM 2-12
RAI 7-45, 7-59
Network Interfaces 11-51
NIM 7-25, 7-38
Configuration 1-10

Configuration Guidelines
OC-12c 2-9, 2-10
Installation 5-9
IOM 1-14
IOM Connections 6-8
IOM Installation 5-11
IOMs 7-40
OC-12c 1-13
Options 2-17
Redundancy 7-26
Sets 2-17
Slots 1-10
Statistics 8-4
STM-4c 1-13
Non-reverting Protection Mode 7-25
Non-Volatile Memory 11-50
Notices vii
Notifications, Target 12-37
Notify
Filters, SNMP 12-40
Profiles, SNMP 12-42
NTP 10-8, 11-15

O

OC-12c
BITS/Timing Redundancy 7-40
Configuration 7-39
NIM 1-13
NIM Configuration Guidelines . . 2-9, 2-10
Port Mode 7-39
Statistics 8-3
Optical Interface Connections 6-6
Options
Broadmore 1750 2-16
Network Interface Module 2-17
Network Interface Module (NIM) 2-17
Service Access Module 2-18
Service Access Module (SAM) 2-18
Ordering Guide 2-1, 2-15
Overview 7-2
Module Installation 5-4
SNMP 12-2

P

Password 7-7, 7-10
PCV 8-7
Peak Cell Rate 7-15
PES 8-7
Physical Interfaces 1-6
Planning Factors
Installation 2-13
System 2-6
Planning Guide 2-1
Application 2-2
PLOA/AAL5 8-14
Port
Configuration 9-6
Mode 7-44, 7-51, 7-52, 7-58
Name 7-44, 7-51, 7-52, 7-58
Port Connections, Alarm 6-5
Port Connections, Serial 6-11
Power 1-9, 6-3
AC Power Supply Tray 4-8
Power Input Connector 6-14
Power Supply
Redundancy 7-24
Power Supply Connections 6-12
Optional AC 6-12
Power, Connecting –48 VDC 6-14
Power-on
Default 7-72
Power-up 7-3
Precautions
Electrical Installation 6-2
Installation 4-2, 5-2
Product Description 1-1
Protection
Definitions 7-25

IOM 1-21
SAM IOM Installation 5-11
Protection IOM 1-10
PSES 8-7
Purpose 1-2
PVC
Connection 7-63
Input Screen 7-63

R

Rack Mounting 4-4
Procedure 4-6
RAI . . . 7-46, 7-47, 7-48, 7-54, 7-60, 7-61, 7-62
Reboot Jumpers 5-12
Reboot Standby CPU 7-36
Receipt of Goods 3-2
Receipt of Product 3-1
Received 7-40
Redundancy 1-9
Module 7-25
Release CPU Control 7-36
Remote Shutdown Connections 6-11
Remove Chassis Cover, Front 5-15
Remove Chassis Covers 5-5
Replace Chassis Cover, Front 5-16
Replace Chassis Covers 5-13
Report Damage 3-3
Requirements
Cabling and Compliance 6-4
Electrical 6-3
resetSecurID 11-39
Residual Data and Memory Volatility 11-50
Resiliency, Mission-Critical Circuit 2-4
Restore Configuration 7-71
Resync Jumpers 5-11
Reverting, Protection Mode 7-25
RFC 1577 . . . . . 7-4, 7-14
RS-232 7-4
RSA SecurID Authentication 11-2

S

Safety Information vi
SAM 7-38
Configuration 1-10
Configuration, Protection 1-10
DS3, Structured 1-18
DS3, Unstructured 1-15
E3 1-16
Installation 5-10
IOM Connections 6-8
IOM Installation 5-11
IOM, Protection, Installation 5-11
Sets 2-18
Slots 1-10
Statistics 8-4
Sanitation Procedures 11-51
SAR 1-22
Save Configuration 7-70
scp 11-38
Screen Display Annotation 7-5
Scripts, CLI 9-4
SD 7-28
SecureCRT 1-5
SecureFX 1-5
SecurID
Authentication 11-2
Disabling 11-24
Enabling 11-21
Features 11-49
Security
Audit Trails 10-13, 11-30
Change User ID 10-11, 11-27
Changing Modes 11-17
Features 10-2, 11-2
Guidance 10-3, 11-3
Help About 11-17
Interface 1-5
Logging In 10-5, 11-9

Residual Data and Memory Volatility 11-50
Sanitation Procedures 11-51
Shell Commands 10-19, 11-34
SNMP Overview 12-2
SEFS 8-7
SEQ 8-7
Sequence Errors 7-46, 7-48, 7-60, 7-61
Serial
Number, Module 9-9
Port Connections 6-11
Port. LapLink Cable 2-16
Server Address 7-15
Service
AIS 7-46, 7-53, 7-59
Alarm 7-48, 7-54, 7-55, 7-62
BERT Test 7-45, 7-59
Clocking Mode 7-55
FEAC Loopback 7-45, 7-53
RAI 7-45, 7-59
Service Access Module 1-10
Service Access Module Options 2-18
Service Access Module, Protection 1-10
settimeout 11-35
Setup Errors C-4
SFTP Login 10-21, 11-43
Shell Commands 10-19, 11-34
Authorized Access 10-19, 11-41
fipsmode 10-19
Shutdown Connections, Remote 6-11
Signal
Degradation (SD) 7-28
Slot
Statistics 8-4
Slots
APM 1-10
CPU 1-10
NIM 1-10
SAM 1-10
SNMP 7-4
Access 12-19
Access Edit Rules 12-22
Access Policy 12-22
Communities 12-24
Configuration 12-1
Group Edit Rules 12-15
Groups 12-13
Notifications 12-37
Notify Filters 12-40
Notify Profiles 12-42
Overview 12-2
Properties 12-3
Target Parameters 12-35
Targets 12-33
Trap Configuration 12-28
User Edit Rules 12-12
Users 12-8
USM/VACM Configuration 12-6
View Edit Rules 12-18
Views 12-16
SNMP Messages 10-18, 11-25
SNP 8-7
SNTP 10-8, 11-15
Software 6-15
Error Messages C-1
Revision, Showing 9-9
Upgrades 1-6
SONET 7-26
Tx 7-39
Spares
Broadmore 1750 2-16
SRTS 7-44, 7-58
sshdSessionShow 11-37
sshdShow 11-35
SSHield 11-2
Statistics 8-2
24-hour 8-13
DS3, Structured 8-9

DS3, Unstructured 8-5
Monitor, CLI 9-8
NIM 8-4
OC-12c/STM-4c 8-3
PLOA/AAL5 8-14
SAM 8-4
Slot 8-4
STM-4c
BITS/Timing Redundancy 7-40
Configuration 7-39
Port Mode 7-39
Statistics 8-3
STM-4c NIM 1-13
Structured
DS3 IOM 1-19
DS3 IOM Connections 6-10
DS3 SAM 1-18
Subnet 7-10
Mask 7-18
Supply Connections
AC Power 6-12
DC Power 6-14
Power 6-12
SVC
Connection 7-65
Input screen 7-65
SVCs 7-13
Sync
CPU Data and SW 7-35
Sync CPU Data and SW 7-35
Sync CPU Data Only 7-35
Sync Operating SW 7-35
System
Architecture 1-7, 2-6
Clock 10-7, 10-8, 11-14, 11-15
Configuration 7-70
Errors C-3
Features 1-7
Log 7-34
Planning Factors 2-6
Services Configuration 7-8
System Log 10-15, 11-32

T

Target
Notifications, SNMP 12-37
Parameters 12-35
Targets, SNMP 12-33
TDM Circuit Aggregation and Backhaul . . . 2-3
Telnet 7-4
Threshold 7-28
Time
System 10-7, 11-14
Timing
BITS 7-40
Tools 6-3
Fan Tray Replacement 5-15
Installation 4-4, 5-15
Module Installation 5-5
Transmit Timing 7-39
Trap
Configuration 12-28
Table Usage 12-32
Troubleshooting 8-1

U

UAS 8-7
UNI Version 7-19
Unpacking 3-2
Unstructured
DS3 IOM 1-17, 1-20
DS3 SAM 1-15
E3-3 IOM 1-17, 1-20
E3-3 SAM 1-16
Unstructured DS3-3 IOM Connections 6-9
Unstructured E3-3 IOM Connections 6-9
Upgrades
Software 1-6

User
- Administration 11-26
- Change ID 10-11, 11-27
- Deleting 10-12, 11-28
- Equipment Interfaces 1-4
- ID Rules 10-10, 11-26
- Interface Requirements 7-4
- Interfaces 1-6
- Modifying 10-12, 11-29
- Security Configuration 7-23

User Edit Rules 12-12
User Edit Rules, SNMPv3 12-12
Users
- Managing 10-10
- USM/VACM 12-8

USM/VACM
- Access 12-19
- Configuration 12-6
- Groups 12-13
- Users 12-8
- Views 12-16

V

Validation
- DISA iv
- FIPS 140-2 iv
- JITC iv
- NEBS v

View Edit Rules, SNMPv3 12-18
Views, USM/VACM 12-16
Virtual Channel 7-20
Virtual Path 7-20

W

Warranty ix
- Limitations x
- Procedure ix
- Product Returns xii

Z

zeroize 11-40

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP