NETWORK TECHNOLOGIES INCORPORATED
1275 Danner Dr Tel:330-562-7070
Aurora, OH 44202 Fax:330-562-1999
www.nti1.com

SERIMUX® SECURE

SERIMUX-SECURE-x

Secure Access Console Switch

Installation and Operation Manual

MAN008 Rev 2/10/2004

Warranty Information

The warranty period on this product (parts and labor) is one (1) year from the date of purchase. Please contact Network Technologies Inc at **(800) 742-8324** (800-RGB-TECH) or **(330) 562-7070** or visit our website at http://www.nti1.com for information regarding repairs and/or returns. A return authorization number is required for all repairs/returns.

COPYRIGHT

CHANGES

The material in this guide is for information only and is subject to change without notice. Network Technologies Inc reserves the right to make changes in the product design without reservation and without notification to its users.

TABLE OF CONTENTS

TABLE OF FIGURES

SERIMUX Model Support

This manual offers information on SERIMUX 32-port, 16-port, and 8-port models.

Key Features

The SERIMUX (console management) provides secure, flexible management of servers, routers, switches, and other networked devices. Key features include:

- SSH v1 and v2 for server and clients
- IP filtering
- Authentication using RADIUS, LDAP, TACACS+, Kerberos, and a local database
- Custom menuing
- System and port logging
- Microsoft Windows Server 2003 Special Administration Console (SAC) support
- A web interface that supports both HTTP and HTTPS and simplifies configuration

Materials

Materials Supplied with this kit:

- NTI SERIMUX-SECURE Secure Console Access Server
- RJ45 M/M UTP CAT5 Patch Cable
- Console Adapter RJ45-DB25 Female
- Console Adapter RJ45-DB25 Male
- Modem Adapter RJ45- DB25 Male
- Serial Adapter RJ45-DB9 Female
- RJ45 Diagnostic Loop back Plug
- Mounting Kit
- AC Power Cable
- This Owners Manual (on CD ROM)
- Quick Start Guide (also on CD ROM)
- Discovery Tool (on CD ROM)

Materials *Not* Supplied, but *REQUIRED*:

Ethernet cable is required to connect the SERIMUX to the network.

Note: In order to comply with FCC standards, the SERIMUX requires the use of a shielded Category 5 cable connected to the Ethernet Interface

User Groups

The SERIMUX comes with built-in user groups, defined by access levels. The following table lists user groups, their access rights, and default user names.

Group	Access Privileges		Configuration Privileges		Defaults	
--	**Ports**	**Command Line**	**Ports**	**System**	**Login**	**Password**
Root	Yes	Yes	Yes	Yes	root	dbps
System	Yes	Yes (read only)	Yes	Yes	admin	admin
Admin	Yes	No	Yes	No	-	-
User	Yes	No	No	No	-	-

Root and Admin Usernames and Passwords

The SERIMUX comes with two default users, root and system admin.

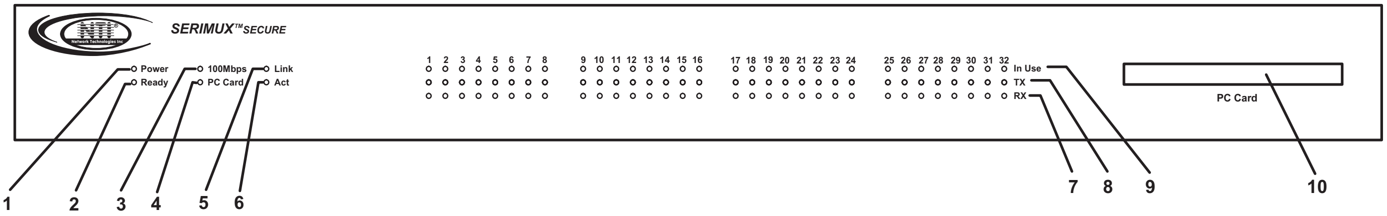
User Name	Default Password
root	dbps
admin	admin

Note: Root's password can be modified through the command line interface using the command `passwd`.

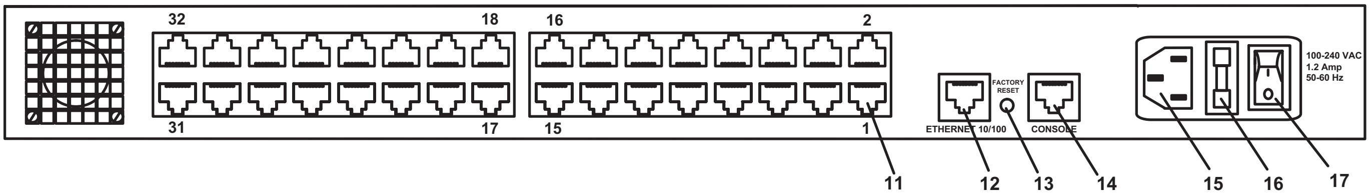
Adding Port Administrators and Users

The system administrator and root user can add port administrators and users easily with the web interface by choosing System administration > User administration > Add user.   Root's password must be modified from the command line using the command `passwd`.

Front View of SERIMUX-Secure



Rear View of SERIMUX-SECURE



Features and Functions

1. Power LED- Indicates SERIMUX is powered up
2. Ready- Indicates SERIMUX is ready to run
3. 100Mbps LED- for visual indication that a 100Base-TX connection has been detected
4. PC Card LED- visual indication that a PCMCIA device is running
5. Link LED-   visual indication of a connection to an ethernet network
6. ACT LED- visual indication of any activities, either transmitting or receiving data, through SERIMUX
7. RX LED- indicates the port is receiving data
8. TX LED- indicates the port is transmitting data
9. In Use- indicates the port has a connection an is enabled
10. PC Card- For attachment of optional PCMCIA device (memory card, LAN Card, or modem card)
11. RJ45 Connector- For attachment of devices to be connected by SERIMUX
12. RJ45 Connector- Ethernet 10/100- for connection to Ethernet LAN
13. Factory Reset- button to enable user reset to factory default settings
14. Console- RJ45 Connector- For attachment of local access user console
15. IEC Power Socket- for connection of power cord
16. Fuse- Overcurrent protection fuse
17. Power ON/OFF switch

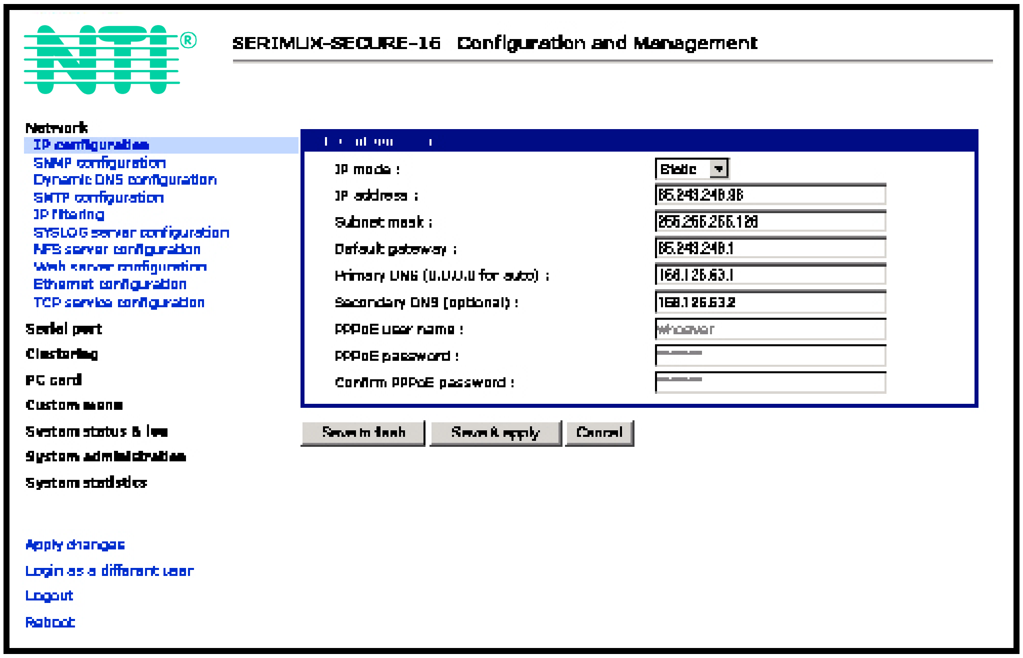
Ways to Configure the SERIMUX

This section discusses the three ways to configure the SERIMUX, web interface, configuration menu, and command line interface.

Web Interface

The web interface provides an easy way to configure the SERIMUX. The root user and system administrator can configure all features from it. Port administrators can configure ports, including port clustering, but cannot modify system settings. Users cannot use the web interface for configuration. To access the web interface, enter the SERIMUX IP address or host name in a browser's URL window. The default IP address is 192.168.161.5.   The following page is displayed after log in.

Note: The SERIMUX web interface features HTTPS for secure access

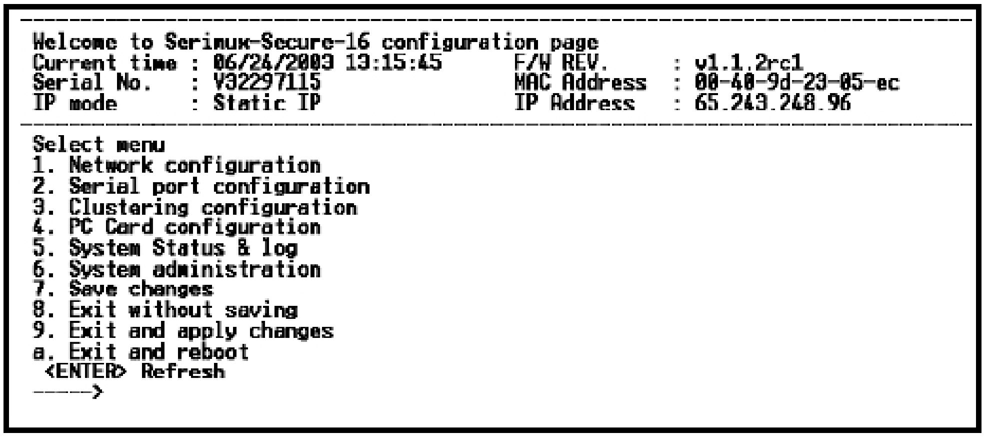


IP mode : Static
IP address : 65.243.248.96
Subnet mask : 255.255.255.128
Default gateway : 65.243.248.1
Primary DNS (0.0.0.0 for auto) : 168.126.63.1
Secondary DNS (optional) : 168.126.63.2
PPPoE user name : whoever
PPPoE password :
Confirm PPPoE password :

Figure 1- SERIMUX SECURE WEB Interface- Main menu

Configuration Menu

The root user and system administrator have full access to the configuration menu from a Telnet session or a serial connection through the console port. Functionality is similar to the web interface, with the exception of custom menus, which can be created only from the web interface. The configuration menu is presented to system administrators automatically. Root users access it by entering the command `configmenu`. Port administrators can access this menu but can modify serial port configuration only. Users cannot access this menu.



```
------------------------------------------------------------------------------
Welcome to Serimux-Secure-16 configuration page
Current time : 06/24/2003 13:15:45         F/W REV.      : v1.1.2rc1
Serial No.   : V32297115                    MAC Address   : 00-40-9d-23-05-ec
IP mode      : Static IP                    IP Address    : 65.243.248.96
------------------------------------------------------------------------------
Select menu
1. Network configuration
2. Serial port configuration
3. Clustering configuration
4. PC Card configuration
5. System Status & log
6. System administration
7. Save changes
8. Exit without saving
9. Exit and apply changes
a. Exit and reboot
 <ENTER> Refresh
----->
```

Figure 2- SERIMUX-SECURE Telnet Session- Configuration menu

Command Line Interface

The command line interface can be accessed from a Telnet session or from the console port. The root user always has access to this interface. The system administrator can be granted read-only permission as well. No other users can access the command line interface.

Ways of Accessing the SERIMUX: Overview

There are four ways to access the SERIMUX including:

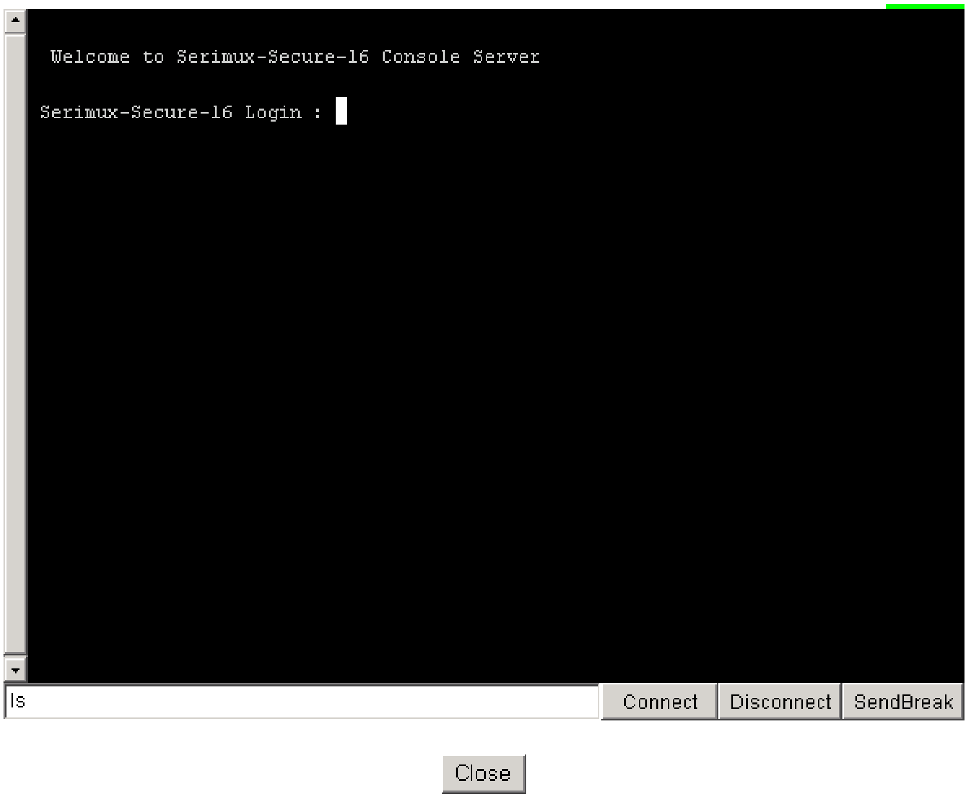
- Web Interface
- Port Access Menu
- Direct Port Access
- Custom Menus

Web Interface Access Menu

The web interface menu provides easy and convenient access to ports. All users can access the menu by entering the SERIMUX IP address or host name in a web browser's URL window.

To access a port from the web interface, do the following:

1. Access the web interface.
2. Choose Serial port > Connection.
3. Choose a port by clicking in the appropriate icon.
   A Java applet or Telnet window opens with a login prompt.



```
 Welcome to Serimux-Secure-16 Console Server

Serimux-Secure-16 Login :
```

Figure 3- WEB Interface- Port login screen

Port Access Menu

The Port Access Menu provides access to ports. It is accessible to all users through the web interface, Telnet and SSH sessions, and remote modem access. The information that follows shows how to access this menu.

Access Type	Permissions	Procedure
Web interface	Any user can use This method.	1. Access the web interface. 2. Choose Serial port > Connection > Port access menu connection. 3. Log in.
Telnet	Any user can use This method.	1. Telnet to the SERIMUX specifying its IP address and port 7000. Example: `Telnet 192.168.15.7 7000` 2. Log in.
Command line	Root	From the command line, issue the portaccessmenu command. Example: `portaccessmenu`

Direct Port Access

Users can connect directly to a properly configured port through a Telnet or SSH session. Configuration requirements include setting the Host Mode to Console Server Mode and the Protocol to either Telnet or SSH. Ports, by default, are set to Console Server Mode and Telnet. Use the information that follows to make a Telnet or SSH connection to a port:

Type	Command Syntax	Example Connection to Port 3
Telnet	`telnet` *`ip-address tcp-port`* where *ip-address* is the SERIMUX's IP address and *tcp-port* is the Listening TCP port for a port	`telnet 192.168.15.7 7003`
SSH	ssh *user-name@ ip-address tcp-por*t where *user-name* is a user's name, *ipaddress* is the SERIMUX's IP address and *tcp-port* is the Listening TCP port for a port	`ssh admin@ 192.168.15.7 7003`

Note: The example assumes that the Listening TCP port is 7003, the default for port 3.

Custom Menus

Custom menus are created by either root or the system administrator to limit a user's access to specific ports. For more information, see "Making Custom Menus" on page 36.

Saving and Applying Changes

In the web interface, the user can save and apply configuration changes in two ways. With the one-step method, choose "Save & apply" and changes are saved and applied enabling them to take effect immediately. With the two-step method, choose "Save to flash," which immediately saves changes but the changes do not take effect until choosing "Apply changes." This might be more efficiently used if multiple changes are being made. The following topics describe how to do each of these operations.

One Step: Save and Apply Changes

To save and apply changes immediately, choose the Save & apply button.

Two-Step: Save to Flash and then Apply Changes

To save multiple changes but apply changes once, do the following:

1. Choose the Save to flash button after each configuration change.
2. When finished changing the configuration, choose the Apply changes link, which is located on the main menu.

Getting Started

Introduction

This chapter covers basic configuration topics. Included is information on assigning IP settings, enabling secure access with the web interface, accessing the unit through SSH, and adding and removing users.

Note: Initial setup is described in the Quick Start Guide included with the product packaging.

Assigning IP Settings from the Console Port

To use the console port to assign IP settings, do the following:

1. Connect the console port on the rear panel of the SERIMUX to a serial port on a workstation using the Ethernet console cable and DB-9 adapter packaged with the SERIMUX. (See Fig. 4) **The default IP address is 192.168.161.5.**

Rear View of SERIMUX-SECURE

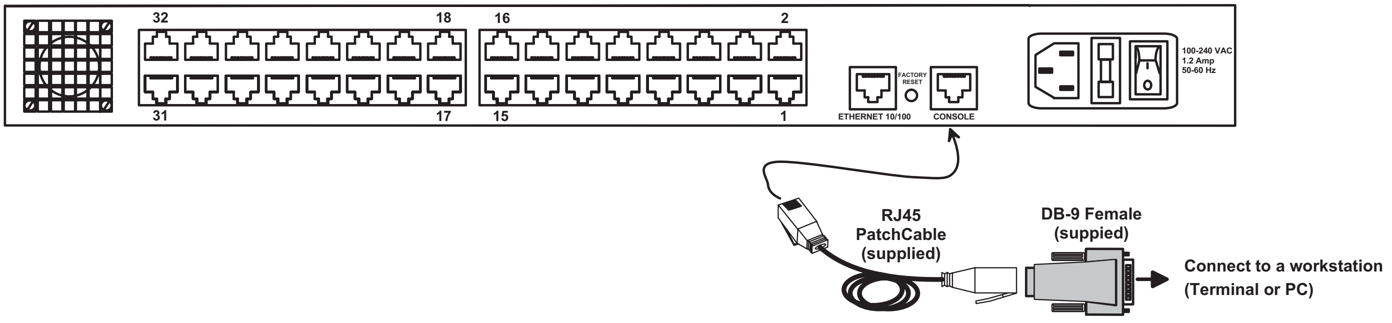


Figure 4- Attach a workstation to the console port

2. Configure a terminal emulation program, such as HyperTerminal, using the following settings:

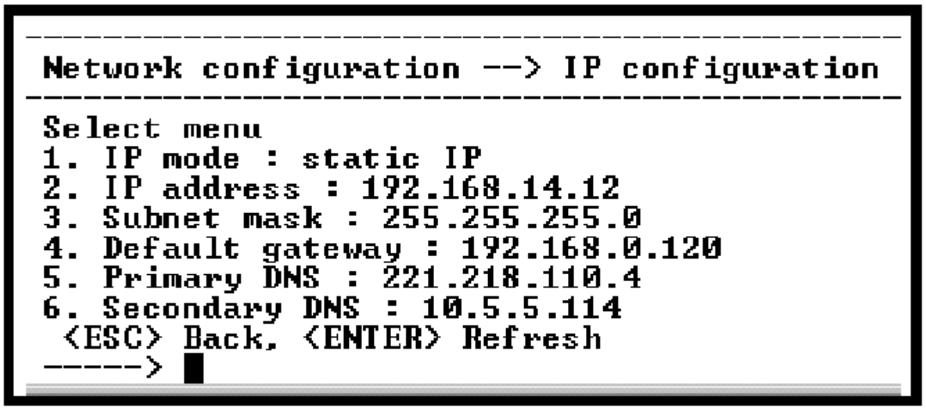
bps = 9600
data bits = 8
parity = none
stop bits = 1
flow control = none.

3. Establish a connection to the console port and press Enter to get a command prompt.
4. At the login prompt, log in as **admin**.
   The default password for admin is admin.

   The Configuration menu appears.

5. Enter the following to navigate to the IP configuration:
   a. 1 for Network configuration
   b. 1 for IP configuration
   c. The numbers for the individual IP settings.

   The following menu is displayed.



```
---------------------------------------------
 Network configuration --> IP configuration
---------------------------------------------
 Select menu
 1. IP mode : static IP
 2. IP address : 192.168.14.12
 3. Subnet mask : 255.255.255.0
 4. Default gateway : 192.168.0.120
 5. Primary DNS : 221.218.110.4
 6. Secondary DNS : 10.5.5.114
  <ESC> Back, <ENTER> Refresh
 -----> 
```

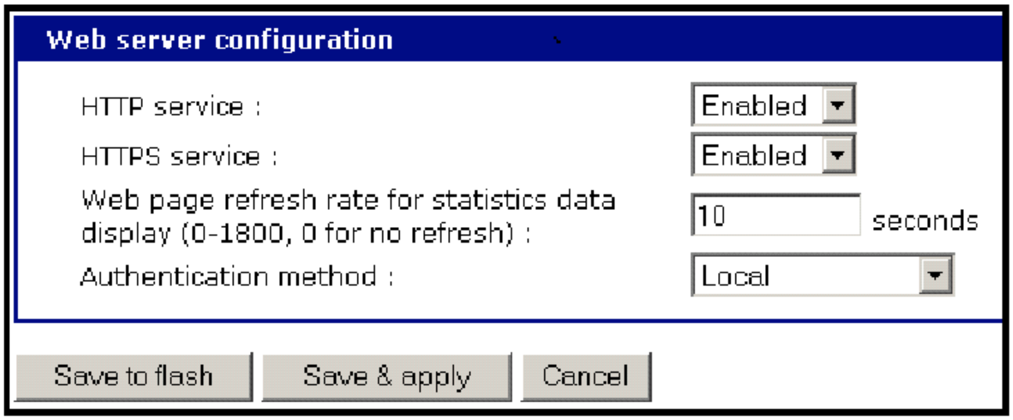
Figure 5- The IP configuration menu

6. Press ESC when done to return to the main configuration menu.
7. Enter number 9 to exit and apply changes.
   Changes are saved and applied immediately. There is no need to reboot.

Configuring HTTP and HTTPS

By default HTTP and HTTPS are enabled on the SERIMUX device. To modify these settings, do the following:

1. Enter the IP address for the SERIMUX in a web browser's URL.
2. Choose Web server configuration from the Network Configuration heading on the web interface menu.
3. Choose Enabled or Disabled.
4. Set the desired refresh rate for statistics data. The default value is 10 seconds.
5. Choose an authentication method for accessing the web interface. The default is local.
6. To save and apply changes, choose Save & apply.



Web server configuration

HTTP service : Enabled

HTTPS service : Enabled

Web page refresh rate for statistics data display (0-1800, 0 for no refresh) : 10 seconds

Authentication method : Local

Figure 6- Enable Web server HTTP/HTTPS service

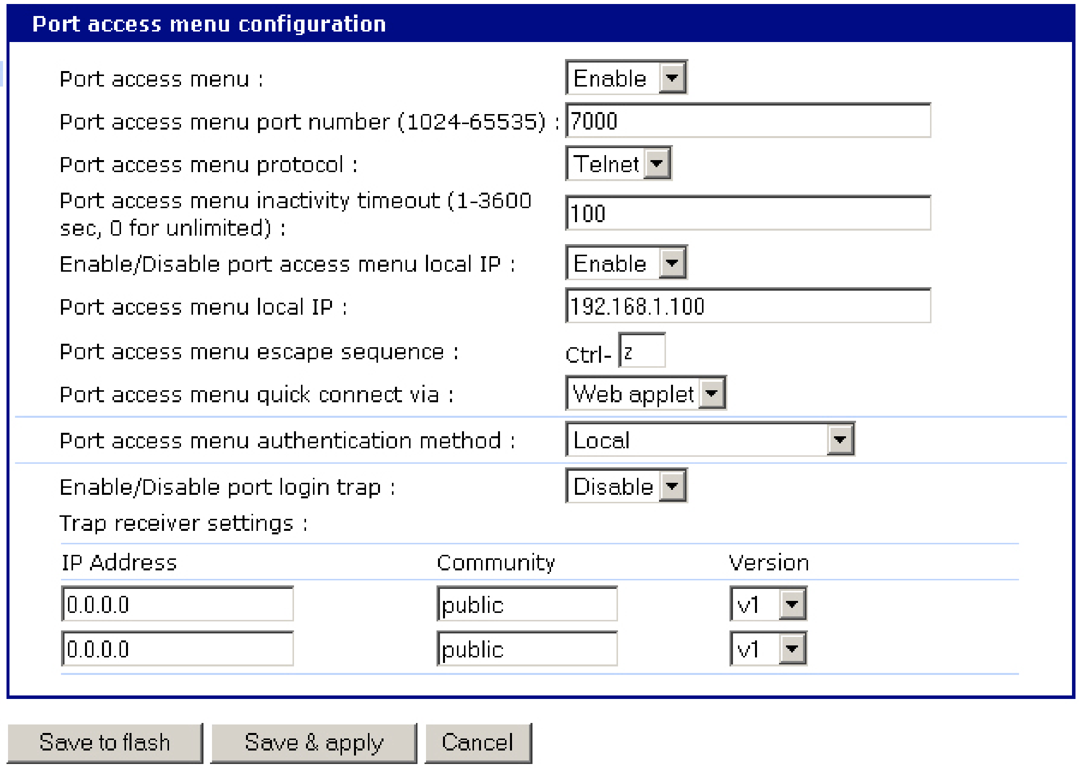
Configuring for SSH

Options

The Port Access Menu and individual ports can be configured for SSH.

Configuring the Port Access Menu for SSH

1. Access the web interface.
2. Log in as root, admin, or a member of the port administration group.
   The default password for root is **dbps**,
   The default password for admin is **admin**.
3. Choose Serial port > Configuration > Port access configuration menu.
   The Port access configuration menu appears.
4. Choose SSH as the Port access menu protocol.



Port access menu configuration

Port access menu :	Enable
Port access menu port number (1024-65535) :	7000
Port access menu protocol :	Telnet
Port access menu inactivity timeout (1-3600 sec, 0 for unlimited) :	100
Enable/Disable port access menu local IP :	Enable
Port access menu local IP :	192.168.1.100
Port access menu escape sequence :	Ctrl- z
Port access menu quick connect via :	Web applet
Port access menu authentication method :	Local
Enable/Disable port login trap :	Disable

Trap receiver settings :

IP Address	Community	Version
0.0.0.0	public	v1
0.0.0.0	public	v1

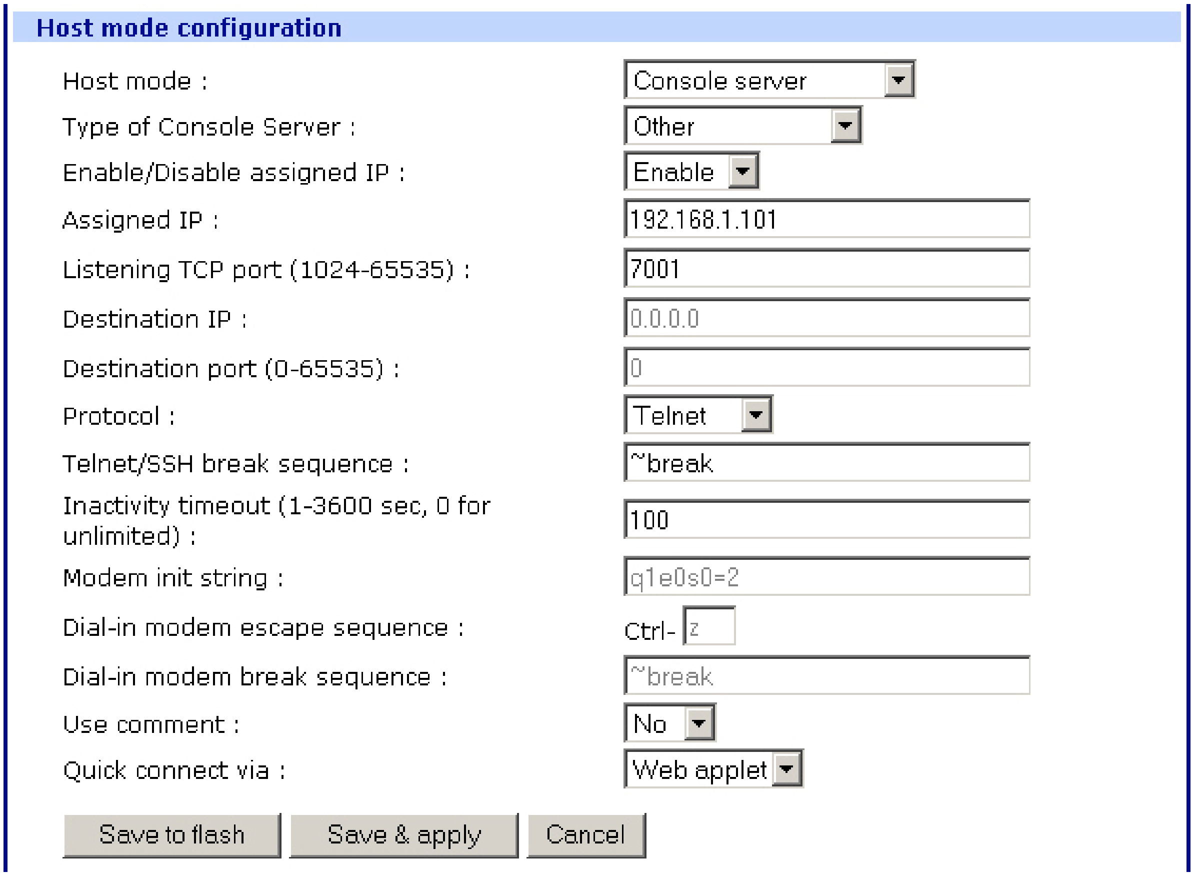
Figure 7- Configure the port access menu for SSH

5. Choose Save & apply.

Configuring a Port for SSH

1. Access the web interface.
2. Log in as root, admin, or a member of the port administration group.
   The default password for root is **dbps**
   The default password for admin is **admin**.
3. Choose Serial port > Configuration.
4. Choose the port or ports to be configured for SSH.
5. Choose Host mode configuration.
6. Specify SSH as the Protocol.
7. Choose Save & Apply.

Note: The SERIMUX supports Blowfish and 3DES encryption methods for SSH.



Host mode configuration

Host mode :	Console server
Type of Console Server :	Other
Enable/Disable assigned IP :	Enable
Assigned IP :	192.168.1.101
Listening TCP port (1024-65535) :	7001
Destination IP :	0.0.0.0
Destination port (0-65535) :	0
Protocol :	Telnet
Telnet/SSH break sequence :	~break
Inactivity timeout (1-3600 sec, 0 for unlimited) :	100
Modem init string :	q1e0s0=2
Dial-in modem escape sequence :	Ctrl- z
Dial-in modem break sequence :	~break
Use comment :	No
Quick connect via :	Web applet

Figure 8- Configure a port for SSH

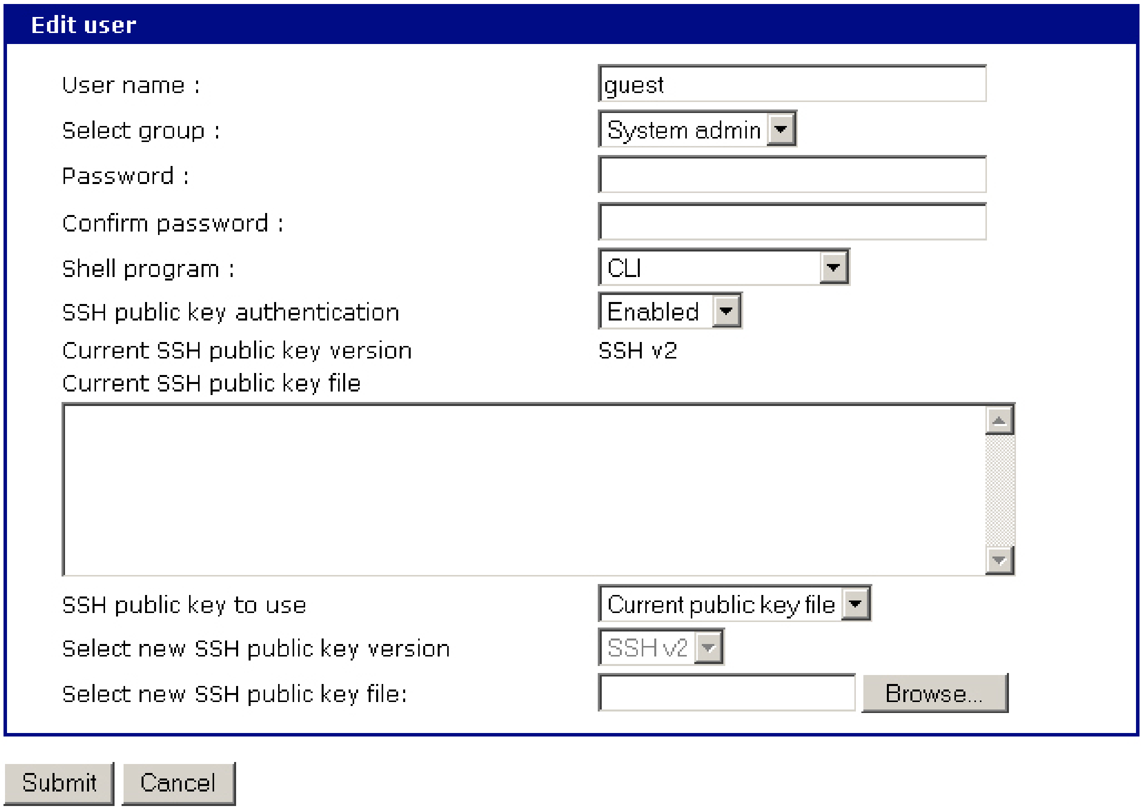
Adding, Editing, and Removing Users

The root user and system administrator can add, remove, or edit users from the web interface.

Procedure

1. Access the web interface.
2. Log in as root or admin.
   The default password for root is **dbps**
   The default password for admin is **admin**.
3. Under the System administration heading choose Users administration.
4. Choose Add User, Edit User, or Remove User.
   - Add a user: Assign a name, user group, password, and shell.
   - Edit user files: Change user group, password, or their shell
   - Remove a user: Remove a user from the system
5. Choose Submit or Cancel.

Note: The root and admin users cannot be removed from the system. The password for root can be changed from the command line only using the command `passwd`.



Edit user

User name :	guest
Select group :	System admin
Password :	
Confirm password :	
Shell program :	CLI
SSH public key authentication	Enabled
Current SSH public key version	SSH v2
Current SSH public key file	
SSH public key to use	Current public key file
Select new SSH public key version	SSH v2
Select new SSH public key file:	

Figure 9- The Edit user menu

About Shell Options

The shell program selection determines the interface the user sees when establishing a Telnet or SSH session with the SERIMUX.

User Group	Shell Program Options
root	Command line
system admin	Command line, configuration menu, port access menu, custom menus
port admin	Configuration menu, port access menu, custom menus
user	Port access menu, custom menus

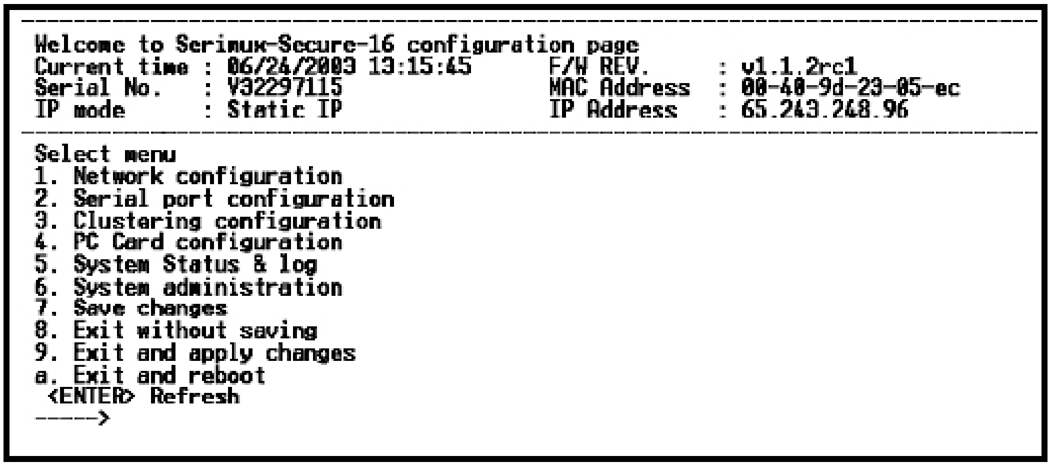
Using the Configuration Menu

The configuration menu presents the same functionality in configuring the SERIMUX as does the web interface, excluding the creation of custom menus. The configuration menu is navigated by using the number representing the menu item and the ESC key to return to earlier menus.

Configuring SSH

1. Telnet to the SERIMUX.
2. Log in as root or admin.
   The default password for root is **dbps**
   The default password for admin is **admin**.
3. Do one of the following:
   - If the user is logged in as admin, the configuration menu will automatically appear, so go to the next step.
   - If the user is logged in as root, enter the `configmenu` command.

Note: The Save changes option saves changes to flash memory only.



```
--------------------------------------------------------------------------------
 Welcome to Serimux-Secure-16 configuration page
 Current time : 06/24/2003 13:15:45       F/W REV.      : v1.1.2rc1
 Serial No.   : V32297115                 MAC Address   : 00-40-9d-23-05-ec
 IP mode      : Static IP                 IP Address    : 65.243.248.96
--------------------------------------------------------------------------------
 Select menu
 1. Network configuration
 2. Serial port configuration
 3. Clustering configuration
 4. PC Card configuration
 5. System Status & log
 6. System administration
 7. Save changes
 8. Exit without saving
 9. Exit and apply changes
 a. Exit and reboot
  <ENTER> Refresh
 ----->
```

Figure 10- Using configuration menu to configure SSH

4. Choose 2 (Serial port configuration) and then an individual port number or 0 (zero) for all ports.
5. Choose 3 (Host mode configuration) and then 4 (Protocol) and 2 (for SSH).
6. Use the ESC key to return to the main configuration menu.
7. Choose 9 (Exit and apply changes).

Adding, Editing, and Removing Users

1. Telnet to the SERIMUX.
2. Log in as root or admin.
   The default password for root is **dbps**,
   The default password for admin is **admin**.
3. Do one of the following:
   - If the user is logged in as admin, the configuration menu will automatically appear, so go to the next step.
   - If the user is logged in as root, enter the `configmenu` command.
4. Choose 6 (System administration) > 1 (User administration) and then choose an operation to perform (Add, Remove, or Edit).
5. Configure the user as required.
6. Use the ESC key to return to the main configuration menu.
7. Choose 9 (Exit and apply changes).

Note: Choose Exit and apply changes when all of the changes have been made.

Installing and Configuring PC Cards

Introduction

This chapter includes information on adding and configuring PC cards for the SERIMUX. PC devices that can be added to the SERIMUX include a serial modem, compact-flash card, wireless LAN card, and a network LAN card.

Compatible PC Cards

All compact-flash cards work with the SERIMUX, but not all serial modem, wireless LAN, or regular LAN cards do. See the charts below for compatible cards that have been tested with the SERIMUX.

SERIMUX Supported PC Card List

Ethernet LAN Cards:

Manufacturer	Description	Model Name	Specification
3COM	3CXE589ET-AP	3Com Megahertz 589E TP/BNC LAN PC Card	10 Mbps LAN card

Wireless LAN Cards:

Manufacturer	Description	Model Name	Specification
Cisco Systems	AIR-PCM340/Aironet 340	Cisco Systems 340 Series Wireless LAN Adapter	11 Mbps Wireless LAN Adapter

Modem Cards:

Manufacturer	Description	Model Name	Specification
Billionton Systems Inc.	FM56C series	PCMCIA CARD 56KFaxModem FM56C-NFS 5.41	Ambient (Intel) V.90 FAX/MODEM PC Card
Viking	PC Card Modem 56K	Viking V.90 K56flex 021 A	MODEM PC Card
Multitech	MultiMobile PC Card Modem	MT5634ZLXI	V.90 Data/Fax World Modem
Actiontec	Datalink	FM560LK	V.90 Data/Fax Modem
Star Logic	Platinum	FM56C-NFS	V.92 56K PC Card Modem
Zoom	Zoom/Modem	3075-00-00L	V.90/V.92 56K PCMCIA Fax/Modem

Adding a Compact-flash Card

A PC card slot is located on the front panel of the SERIMUX. (See Fig. 11)   To install and configure the compact-flash card on the SERIMUX, do the following.

1. Insert the card into the PC card slot.
2. Access the web interface.
3. Under the PC card heading choose Configuration.
4. Choose Discover a new card.

The SERIMUX searches for a PC card and displays a configuration menu.

5. Enter the appropriate parameters in the configuration menu.

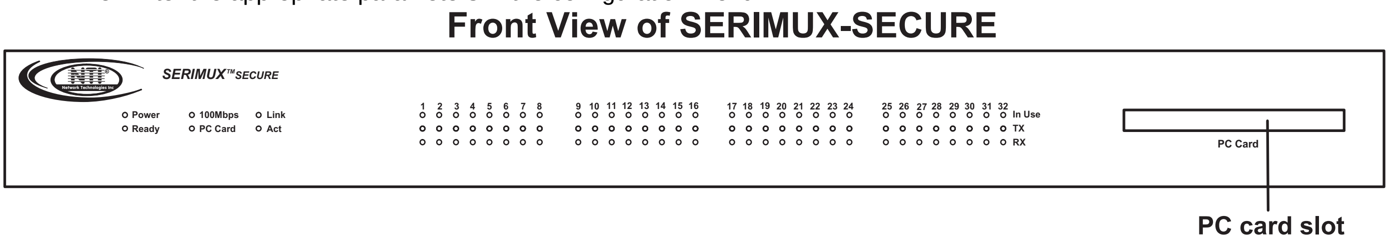
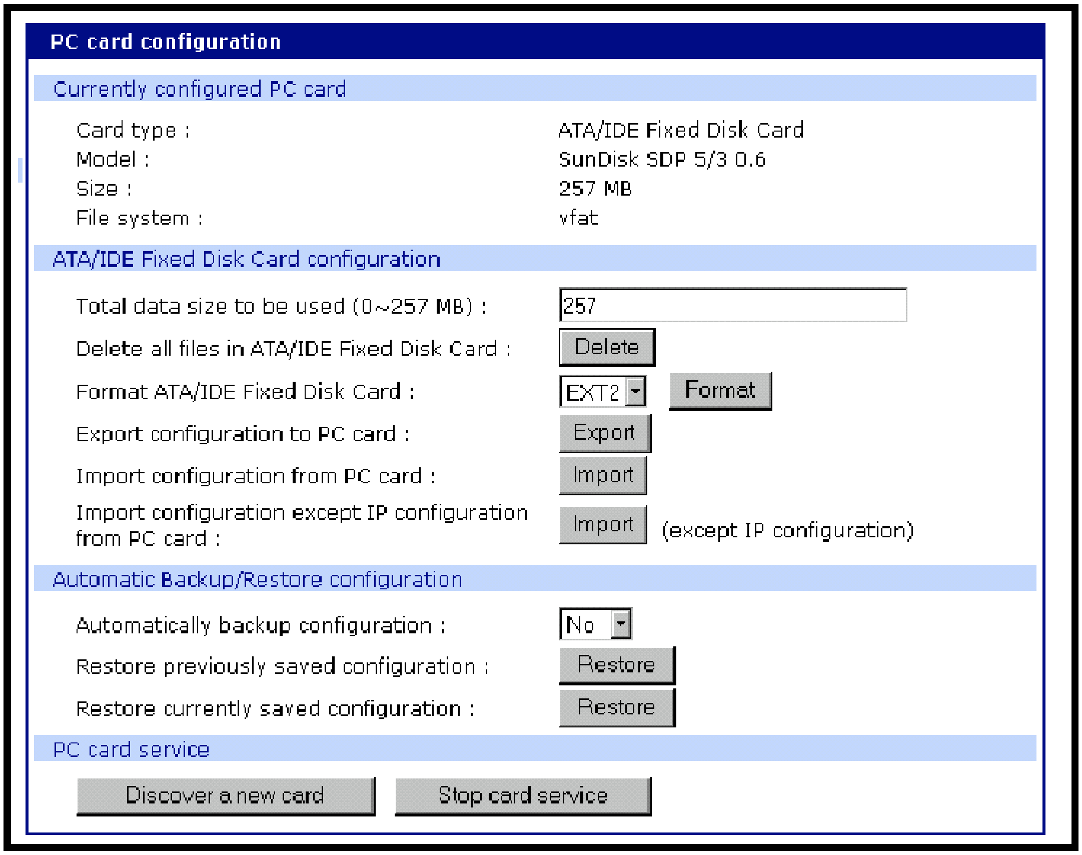


Figure 11- Location of PC card slot



PC card configuration

Currently configured PC card

Card type : ATA/IDE Fixed Disk Card
Model : SunDisk SDP 5/3 0.6
Size : 257 MB
File system : vfat

ATA/IDE Fixed Disk Card configuration

Total data size to be used (0~257 MB) : 257
Delete all files in ATA/IDE Fixed Disk Card : Delete
Format ATA/IDE Fixed Disk Card : EXT2 Format
Export configuration to PC card : Export
Import configuration from PC card : Import
Import configuration except IP configuration from PC card : Import (except IP configuration)

Automatic Backup/Restore configuration

Automatically backup configuration : No
Restore previously saved configuration : Restore
Restore currently saved configuration : Restore

PC card service

Discover a new card   Stop card service

Figure 12- PC card configuration menu

Note: Always select the Stop card service button before removing a PC card.

Configuring the Compact-flash Card

- **Total data size to be used**: Enter the amount of memory to be assigned to the compact-flash card for configuration files.
- **Delete all files in ATA/IDE Fixed Disk Card:** Select this button to clear the compact-flash card of all files.
- **Format ATA/IDE Fixed Disk Card**: The options are EXT2 or FAT formats. Select the format option and then select the Format button.
- **Export configuration to PC card:** Exports the current configuration to the compact-flash card.
- **Import configuration from PC card**: Imports the last saved configuration file from the compact-flash card.
- **Import configuration except IP configuration**: Imports the last saved configuration file from the compact-flash card, excluding the IP settings.

Automatic Configuration File Backup

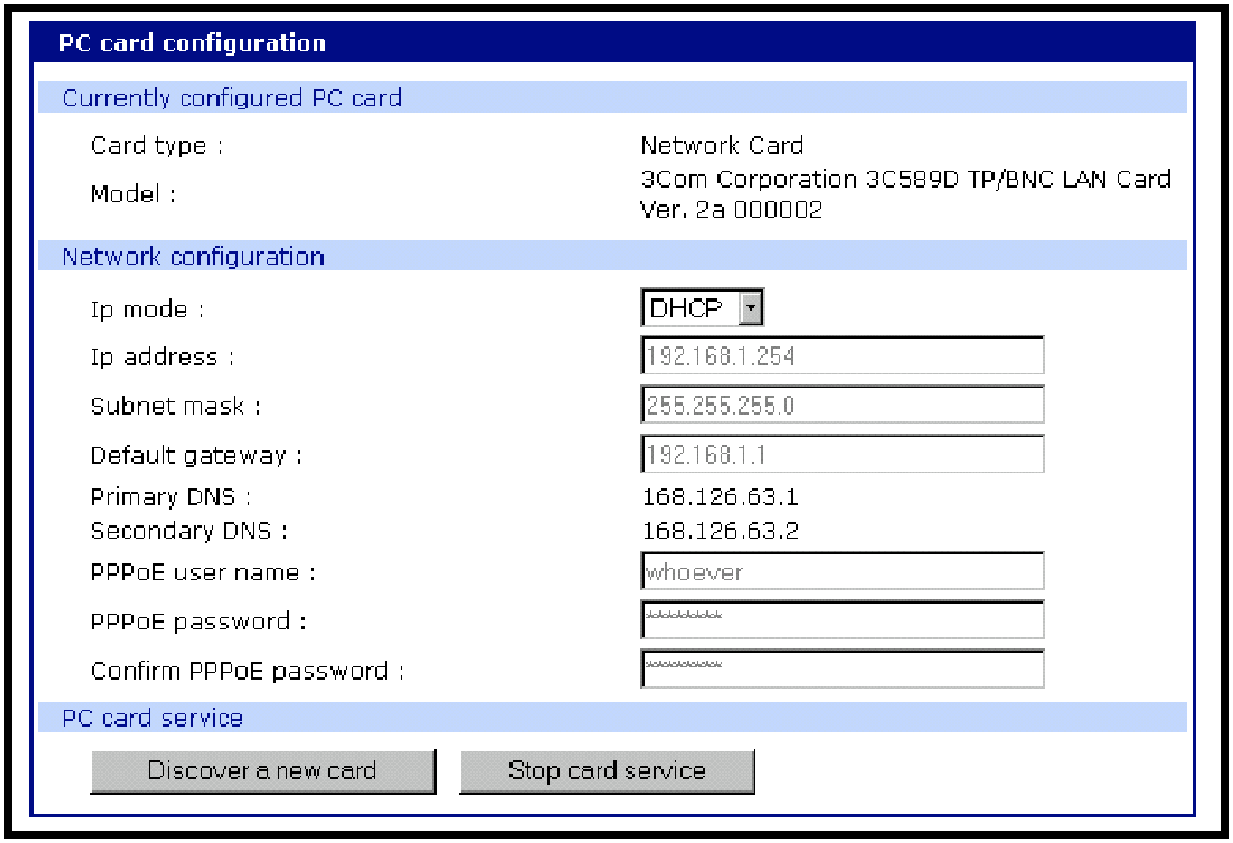
The SERIMUX provides for automatic configuration backup and restoration. The following describes fields related to this function.

- **Automatically backup configuration**: Choose Yes to enable and No to disable automatic backup.
- **Restore previously saved configuration**: Click Restore to import the previously saved configuration.
- **Restore currently saved configuration**: Click Restore to import the most recently saved configuration.

Adding a Network Card

To install and configure a network card on the SERIMUX, do the following.

1. Insert the card into the PC slot.
2. Access the web interface.
3. Under the PC card heading, choose Configuration.
4. Choose Discover a new card.
   The SERIMUX searches for the PC card and displays a configuration menu. (See Fig. 13)
5. Enter the appropriate parameters in the configuration menu.
6. Choose Save & Apply.



PC card configuration

Currently configured PC card

Card type : Network Card

Model : 3Com Corporation 3C589D TP/BNC LAN Card Ver. 2a 000002

Network configuration

Ip mode : DHCP

Ip address : 192.168.1.254

Subnet mask : 255.255.255.0

Default gateway : 192.168.1.1

Primary DNS : 168.126.63.1

Secondary DNS : 168.126.63.2

PPPoE user name : whoever

PPPoE password : ************

Confirm PPPoE password : ************

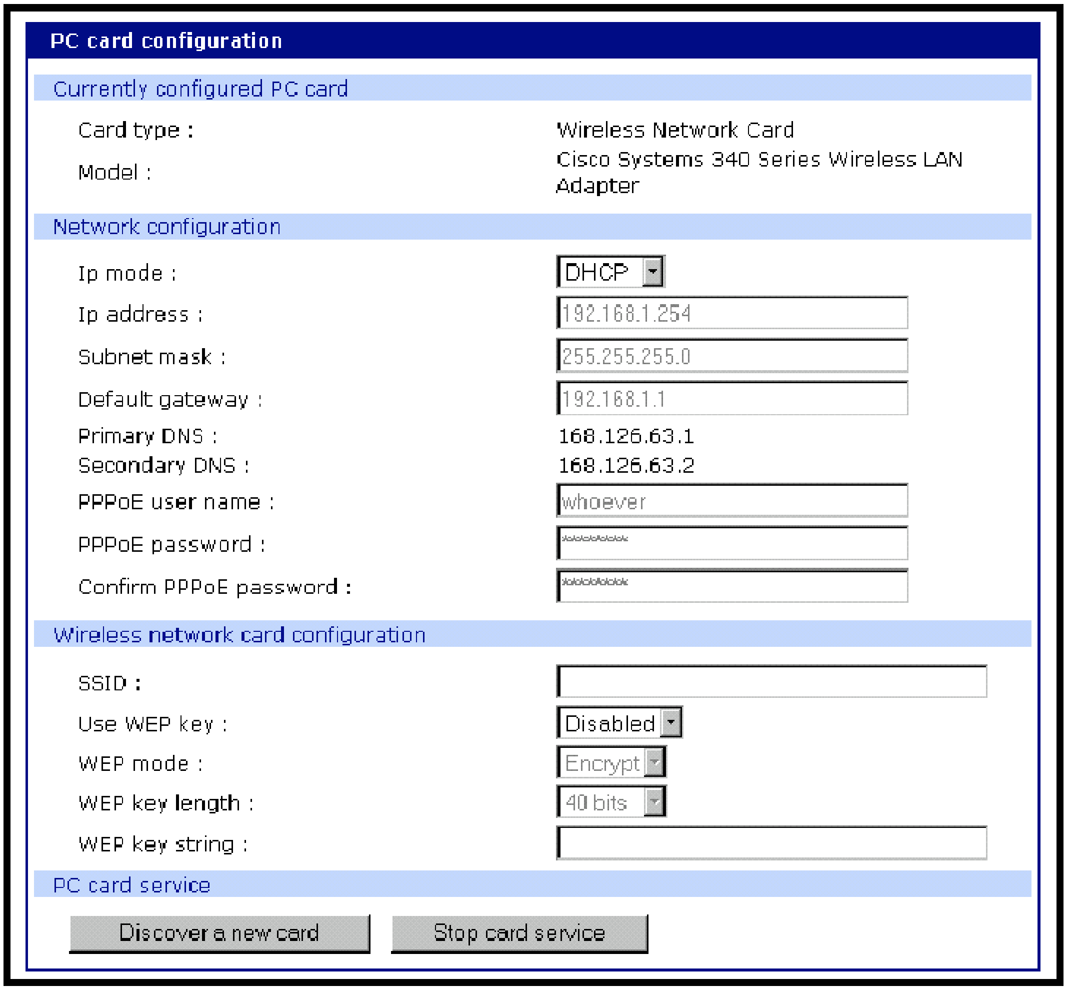
PC card service

Figure 13- Network PC card configuration menu

Adding a Wireless LAN Card

To install and configure a wireless LAN card on the SERIMUX, do the following.
1. Insert the card into the PC slot.
2. Access the web interface.
3. Under the PC card heading, choose Configuration.
4. Choose Discover a new card.
   The SERIMUX searches for the PC card and displays a configuration menu.
5. Enter the appropriate parameters in the configuration menu.

   WEP is the acronym for Wired Equivalent Privacy and is a security protocol for wireless LANs using encryption to protect data transfers. If you are unsure of the settings for the wireless card, see your network administrator.
   - **SSID**: Stands for Set Service Identifier and is the name of the wireless LAN network
   - **Use WEP key**: The options are to enable or disable the WEP key
   - **WEP mode**: Select the mode, either encrypted or unencrypted
   - **WEP key length**: The options are 40 or 128 bits if the WEP key is enabled
   - **WEP key string**: Refer to the wireless network administrator for the wireless encryption key string
6. Choose Save & apply.



PC card configuration

Currently configured PC card

Card type :	Wireless Network Card
Model :	Cisco Systems 340 Series Wireless LAN Adapter

Network configuration

Ip mode :	DHCP
Ip address :	192.168.1.254
Subnet mask :	255.255.255.0
Default gateway :	192.168.1.1
Primary DNS :	168.126.63.1
Secondary DNS :	168.126.63.2
PPPoE user name :	whoever
PPPoE password :	********
Confirm PPPoE password :	********

Wireless network card configuration

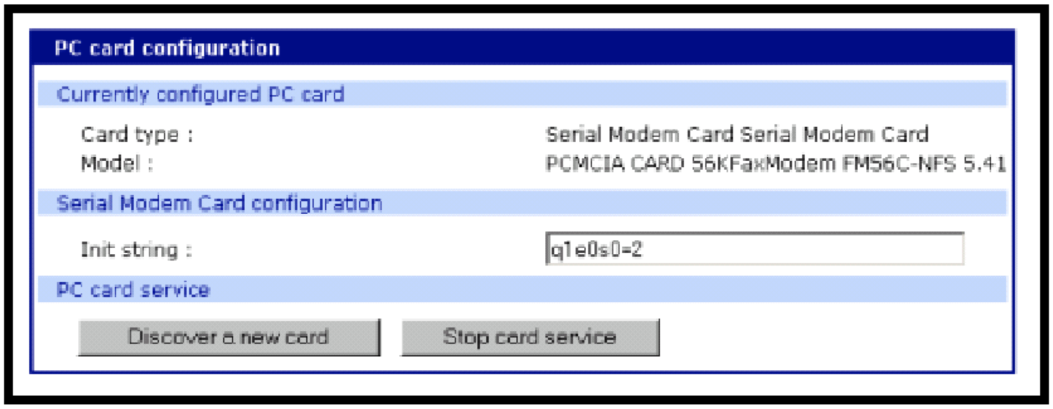
SSID :	
Use WEP key :	Disabled
WEP mode :	Encrypt
WEP key length :	40 bits
WEP key string :	

PC card service

Figure 14- Configure a Wireless Network PC card

Adding A Serial Modem

The modem must first be inserted and installed on the system before it can be used. To configure the modem do the following:
1. Access the web interface.
2. From the menu choose Configuration under the PC card heading.
3. Choose Discover a new card.
   The SERIMUX searches for a PC card and displays a configuration menu.
4. Modify or accept the default Init string.
5. Choose Save & apply.



PC card configuration

Currently configured PC card

Card type : Serial Modem Card Serial Modem Card

Model : PCMCIA CARD 56KFaxModem FM56C-NFS 5.41

Serial Modem Card configuration

Init string : q1e0s0=2

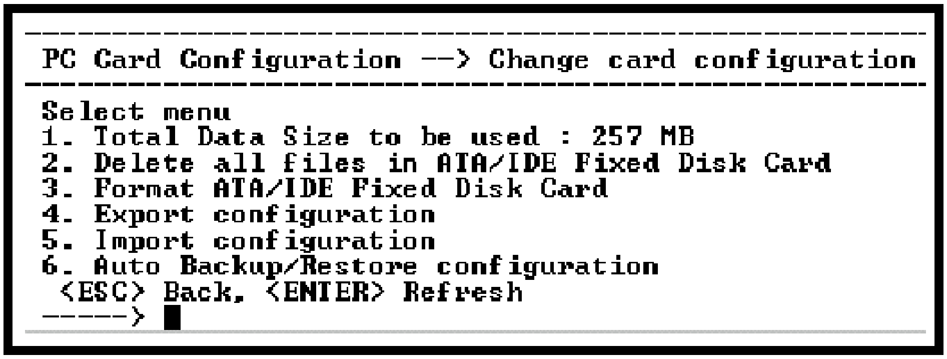
PC card service

Figure 15- Configure a Serial Modem PC card

Using the Configuration Menu

Adding and Configuring a PC Card

To add a modem card, compact-flash card, wireless LAN card, or a network card to the SERIMUX using the configuration menu, do the following:
1. Access the configuration menu.
2. Choose PC Card configuration then Discover a new card.
   The system searches for the card and displays information on the product model number and type of card.
3. Configure the card by choosing Change card configuration.
4. Use the ESC key to back out to the main configuration menu.
5. Choose Save changes.



```
------------------------------------------------------
 PC Card Configuration --> Change card configuration
------------------------------------------------------
 Select menu
 1. Total Data Size to be used : 257 MB
 2. Delete all files in ATA/IDE Fixed Disk Card
 3. Format ATA/IDE Fixed Disk Card
 4. Export configuration
 5. Import configuration
 6. Auto Backup/Restore configuration
  <ESC> Back, <ENTER> Refresh
 ----->
```

Figure 16- Use Configuration menu to add a PC card

Configuring Ports

Introduction

This chapter provides information on configuring serial ports. Key port configuration attributes include the host mode, which defines a type of communication between the port and a remote host, the protocol, authentication, user access restrictions, and serial communication attributes.

Host Mode Configuration

The SERIMUX provides four modes of communication between serial devices and remote hosts. Console server, terminal server, dial-in modem, and dial-in terminal server. These are described in the following sections.

Console Server Mode

Configuring a serial port as a console server creates a TCP socket on the SERIMUX that listens for a Telnet or SSH client connection. Users who connect to the TCP socket have access to the device attached to the serial port as though the device were connected directly to the network. RawTCP is also supported with the Console Server Mode.

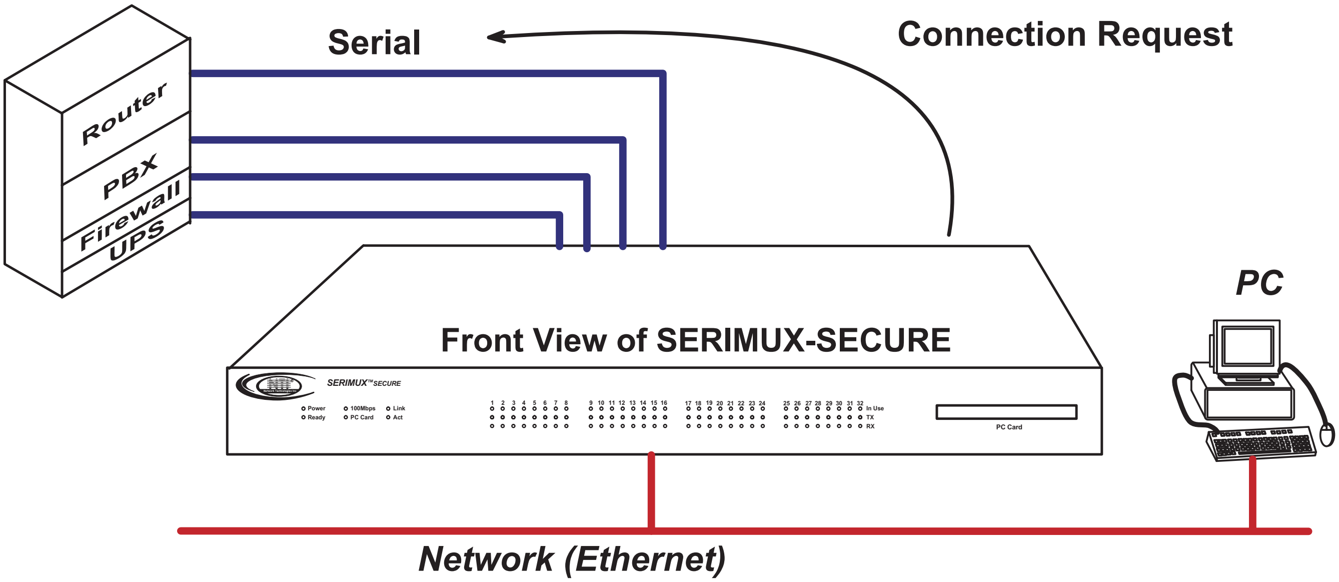


Figure 17- Host Mode Configuration- Console server mode

Terminal Server Mode

In terminal server mode, the SERIMUX serial port is configured to wait for data from the device connected to the port. If data is detected, the SERIMUX starts a TCP session as a Telnet or SSH client to a pre-defined server. The server must be defined by the user before the port can be configured for a Telnet or SSH client. This mode is used when the user wants to access servers on the network from a serial terminal. RawTCP is also supported with the Terminal Server Mode.

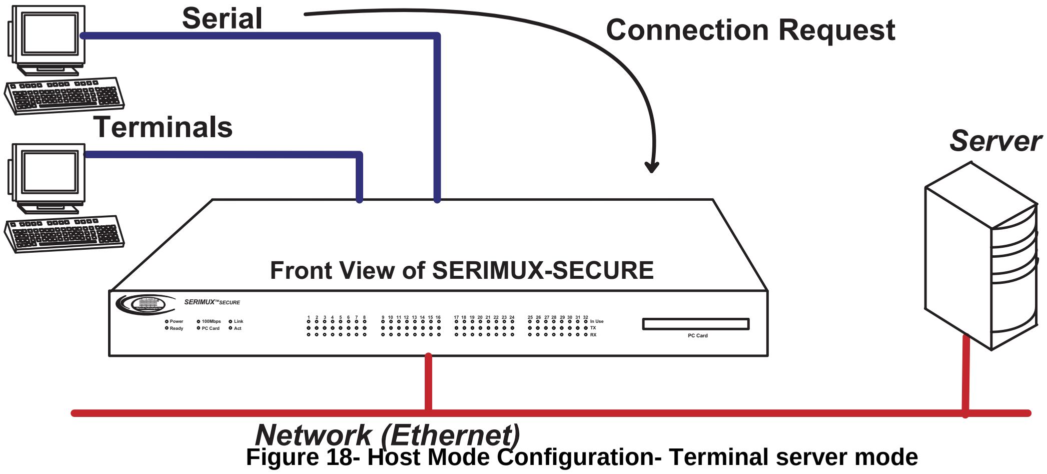


Figure 18- Host Mode Configuration- Terminal server mode

Dial-In Modem Mode

In this mode, the SERIMUX assumes an external modem is attached to the serial port and is waiting for a dial-in connection from a remote site. When a user dials-in using a terminal application, the SERIMUX accepts the connection and displays a menu listing available serial ports. Users can then select a serial port and access the devices attached to the SERIMUX by selecting the serial port number from the menu.

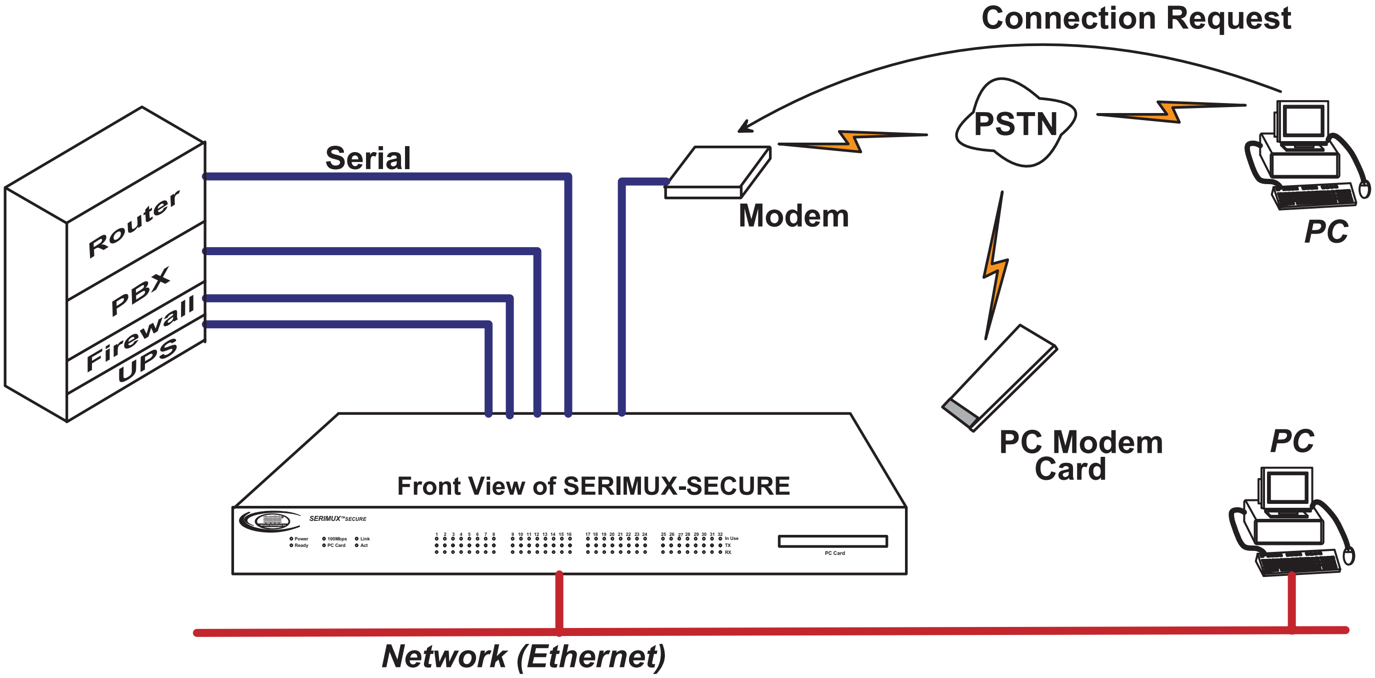


Figure 19- Host Mode Configuration- Dial-In modem mode

Dial-In Terminal Server Mode

Dial-in terminal server mode is a combination of the terminal server mode and the dial-in modem mode. In the dial-in terminal server mode, the SERIMUX assumes the serial port is connected to an external modem and is waiting for a dial-in connection from a remote site. When users dial-in using terminal applications, the SERIMUX accepts the connection as a Telnet or SSH client to a pre-defined server. This mode is most frequently used when users want to use modems to access servers on a network.

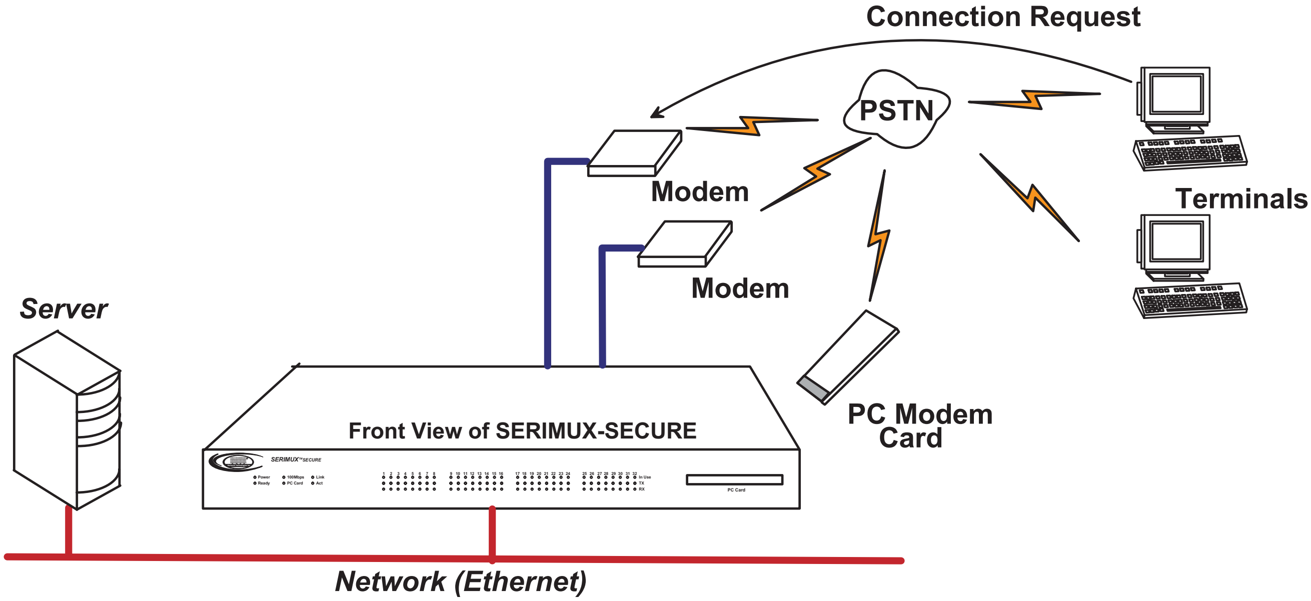


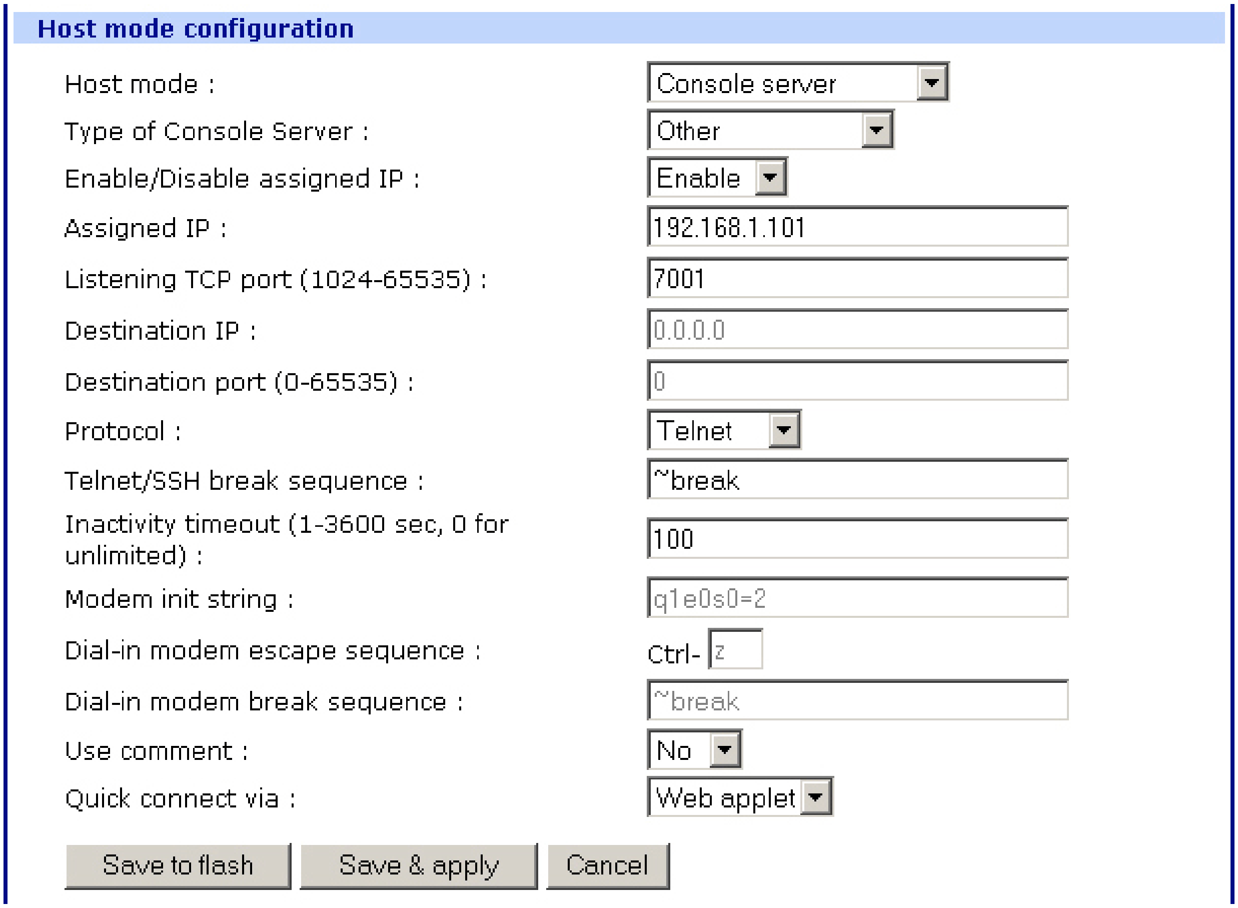
Figure 20- Host Mode Configuration- Dial-In terminal server mode

Configuring Host Mode

To configure a serial port for host mode, enter the values in the applicable fields. To access the Host mode configuration screen, do the following:
1. Access the web interface.
2. Under the Serial Port heading, choose Configuration.
3. Choose All or an Individual port > Host mode configuration.
4. Fill in the highlighted fields as they apply to your configuration.

- Host mode: The options are console server mode, terminal server mode, dial-in modem mode, and dial-in terminal server mode.
- Type of console server: The options are MS SAC console, which you use to provide a graphic user interface to the Windows Server 2003 Special Administration Console (see "Microsoft SAC Support" on page 52) and Other, which you use in all other cases.
- Enable/Disable Assigned IP address. Determines whether an IP address will be assigned to the port. The default is Enable.
- Assigned IP: Also known as alternate IP, this field assigns an IP address to the port, enabling a user to Telnet directly to the serial port using an IP address (without having to specify a TCP port).
- Listening TCP port: This is the TCP port users will specify to access the port when connecting directly to the port using Telnet or SSH.
- Destination IP: Used in terminal server mode, this is the IP address of the system that users will be automatically connected to when they access the port.
- Destination port: Used in terminal server mode, this is the TCP port that will be used when the user who accesses the port is automatically connected to a system on the network.
- Protocol: The options are SSH, RawTCP, and Telnet.
- Telnet/SSH break sequence: The sequence of characters that sends a break character to a device.
- Inactivity timeout: The timeout length ranges from 1 to 3600 seconds. 0 means that there is no timeout.
- Modem init string: Use the default string or enter your own string.
- Dial-in modem escape sequence: The key sequence used to return to the menu in dial-in mode.
- Use comment: Determines whether a port user is prompted to add a comment each time the port is accessed.
- Quick connect via: Determines method for connecting to a port when in console server mode.

5. Choose Save & Apply.



Host mode configuration

Host mode :	Console server
Type of Console Server :	Other
Enable/Disable assigned IP :	Enable
Assigned IP :	192.168.1.101
Listening TCP port (1024-65535) :	7001
Destination IP :	0.0.0.0
Destination port (0-65535) :	0
Protocol :	Telnet
Telnet/SSH break sequence :	~break
Inactivity timeout (1-3600 sec, 0 for unlimited) :	100
Modem init string :	q1e0s0=2
Dial-in modem escape sequence :	Ctrl- z
Dial-in modem break sequence :	~break
Use comment :	No
Quick connect via :	Web applet

Figure 21- Configure serial port for host mode

Supported Protocols

In configuring a serial port, the user has three protocol options. The three protocols available are: RawTCP, SSH, and Telnet.

- Choose SSH as the protocol for users logging in from an SSH client program to access a port.
- Choose RawTCP for users connecting directly to a TCP socket.
- Choose Telnet for users logging in from a Telnet client program and accessing the ports.

Use the Host mode configuration page in the web interface to select the correct protocol.

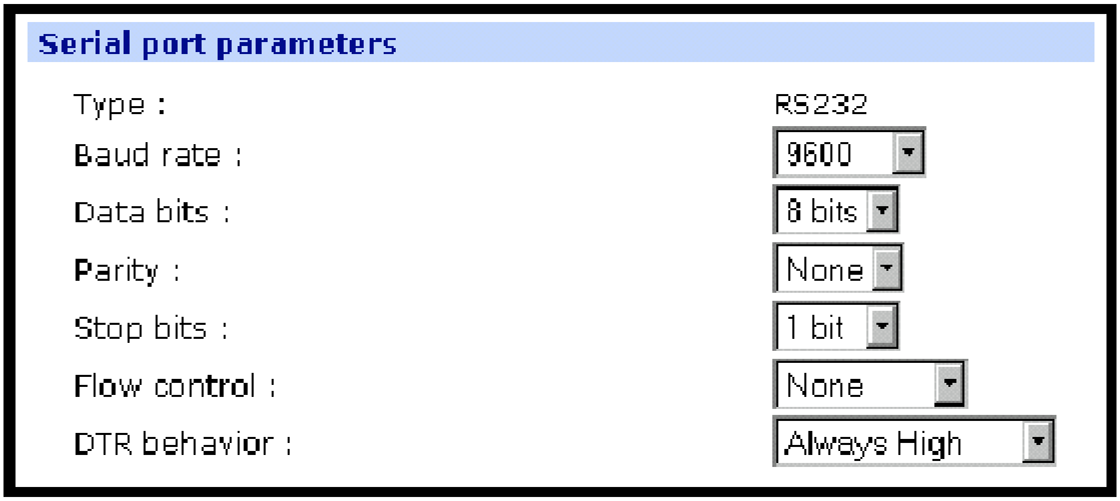
Port Parameters

In attaching a serial device to a SERIMUX serial port, the port parameters must match. The serial ports by default are enabled, meaning users have full access to the port. To configure the port parameters for the SERIMUX, do the following:

1. Access the web interface.
2. Under the Serial Port heading, choose Configuration.
3. Choose All or an Individual port > Port parameters.
4. Fill in the serial port parameters. The following are the defaults:

bps = 9600
data bits = 8
parity = none
stop bits = 1
flow control = none
DTR behavior = always high

5. Choose Save & Apply.



Serial port parameters

Type : RS232
Baud rate : 9600
Data bits : 8 bits
Parity : None
Stop bits : 1 bit
Flow control : None
DTR behavior : Always High

Figure 22- Setup serial port communication parameters

DTR Behavior

DTR can be set on the serial port to one of three settings: always high, always low, or High when open. Setting the DTR to High when open keeps the DTR high if a TCP connection is established. The DTR setting cannot be set by the user when the host mode is configured for dial-in modem or dial-in terminal server mode.

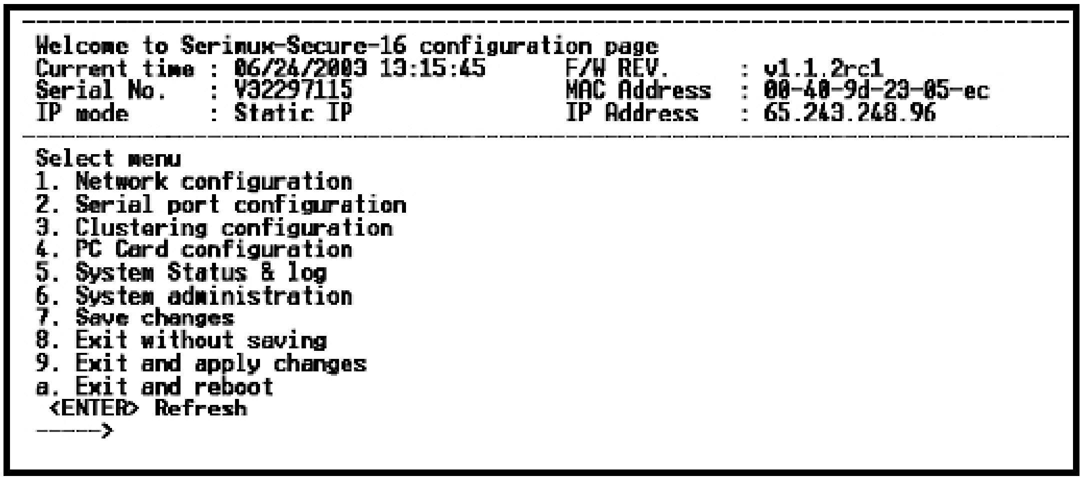
Inter-character Timeout

This setting is only available when the host mode protocol is set for RawTCP. The parameter sets the time value for the SERIMUX to transfer data stored in the buffer. The SERIMUX transfers data when the buffer is full using the TCP/IP protocol. However, if it is not full, the SERIMUX will also transfer data dependent on the timeout value selected.

Using the Configuration Menu

Host Mode Configuration

1. Access the configuration menu.
2. Choose Serial port configuration > an individual port number or 0 (zero) for all ports > Host mode configuration.



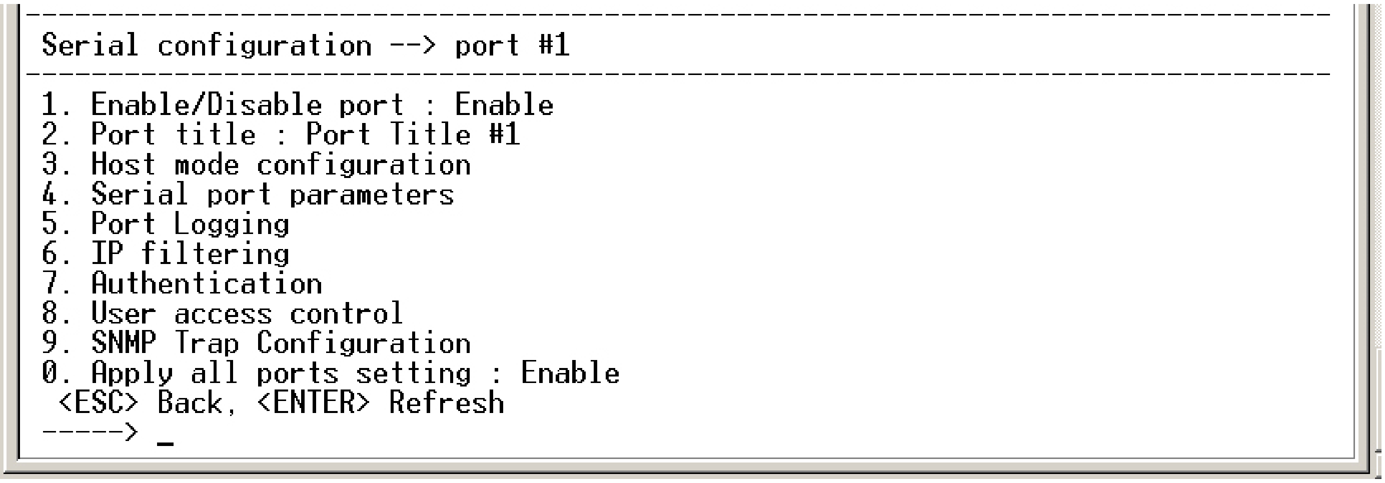
```
--------------------------------------------------------------------------------
 Welcome to Serimux-Secure-16 configuration page
 Current time : 06/24/2003 13:15:45      F/W REV.     : v1.1.2rc1
 Serial No.   : V32297115                MAC Address  : 00-40-9d-23-05-ec
 IP mode      : Static IP                IP Address   : 65.243.248.96
--------------------------------------------------------------------------------
 Select menu
 1. Network configuration
 2. Serial port configuration
 3. Clustering configuration
 4. PC Card configuration
 5. System Status & log
 6. System administration
 7. Save changes
 8. Exit without saving
 9. Exit and apply changes
 a. Exit and reboot
  <ENTER> Refresh
 ----->
```

Figure 23- Configure Host mode via Configuration menu

3. Enter the desired parameters for each menu item.
4. Use the ESC key when all parameters are entered to return to the main menu.
5. Choose Save changes.

Port Parameters

1. Access the configuration menu.
2. Choose Serial port configuration > an individual port number or 0 (zero) for all ports.
3. Enter the desired parameters for each menu item.



```
--------------------------------------------------------------------------------
 Serial configuration --> port #1
--------------------------------------------------------------------------------
 1. Enable/Disable port : Enable
 2. Port title : Port Title #1
 3. Host mode configuration
 4. Serial port parameters
 5. Port Logging
 6. IP filtering
 7. Authentication
 8. User access control
 9. SNMP Trap Configuration
 0. Apply all ports setting : Enable
  <ESC> Back, <ENTER> Refresh
 -----> _
```

Figure 24- Setup Port communication parameters via Configuration menu

4. Use the ESC key when all parameters are entered to return to the main menu.
5. Choose Save changes.

System and Port Logging

Introduction

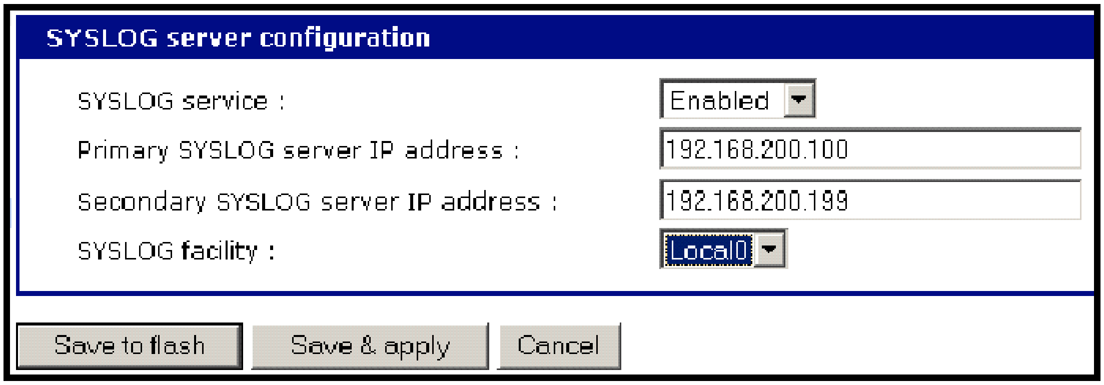
The SERIMUX provides four options for saving system and port logs. The options are: a syslog server, NFS server, compact-flash card, and the SERIMUX memory. When memory is selected as the storage location, log files are saved to volatile memory, meaning files are lost when the power is turned off. To use a syslog server, an NFS server, or a compact-flash card, the user must first enable the devices and enter the required information. Compact-flash cards must be installed before they can be enabled and configured for logging purposes. System logs track events such as logins, authentication failures, system configuration changes, and more. Port logs on the other hand document the data flow through the serial ports. Locations for viewing the system and port logs is outlined in this chapter.

Enabling System Logging Services

Enable Syslog Server

To enable the SERIMUX for system or port logging on a syslog server, do the following:

1. Access the web interface.
2. Under the Network heading, choose SYSLOG server configuration.
3. Choose Enabled.
4. Enter the IP address of the primary and secondary (if applicable) syslog server and select the syslog facility from the drop down menu.
5. Choose Save & apply.



SYSLOG server configuration

SYSLOG service : Enabled

Primary SYSLOG server IP address : 192.168.200.100

Secondary SYSLOG server IP address : 192.168.200.199

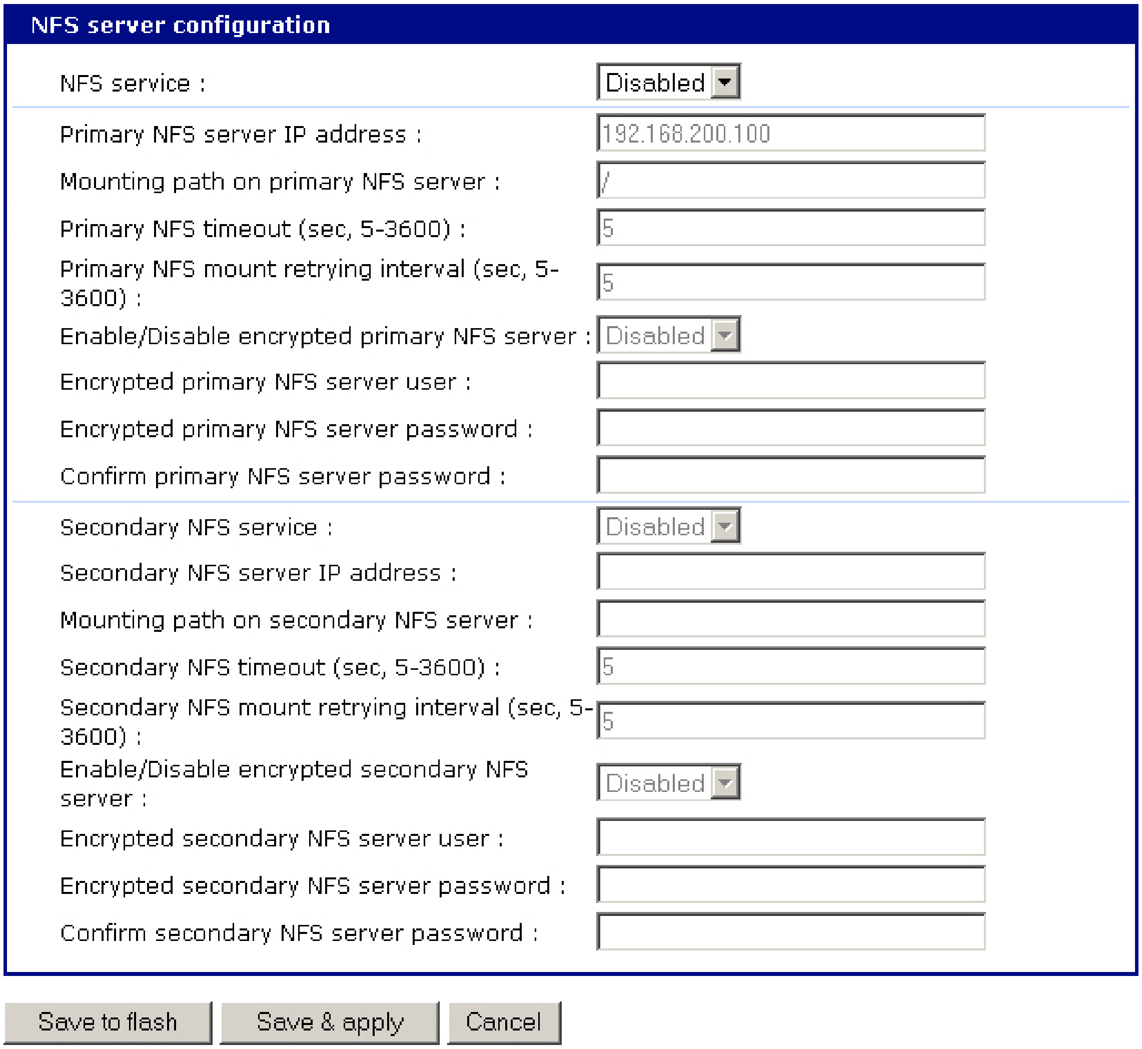
SYSLOG facility : Local0

Figure 25- SYSLOG server configuration menu

Enable NFS Server

Log data can also be saved to an NFS server, but the NFS server must be configured with read and write privileges. To use an NFS server, the user must specify the NFS server's IP address and its mounting path. To enable the NFS server for port or system logging, do the following:

1. Access the web interface.
2. Under the Network heading, choose NFS server configuration.
3. Choose Enabled.
4. Enter the IP address of the primary and secondary (if applicable) NFS server and the mounting path of each.
5. Choose Save & apply.



NFS server configuration

NFS service :	Disabled
Primary NFS server IP address :	192.168.200.100
Mounting path on primary NFS server :	/
Primary NFS timeout (sec, 5-3600) :	5
Primary NFS mount retrying interval (sec, 5-3600) :	5
Enable/Disable encrypted primary NFS server :	Disabled
Encrypted primary NFS server user :	
Encrypted primary NFS server password :	
Confirm primary NFS server password :	
Secondary NFS service :	Disabled
Secondary NFS server IP address :	
Mounting path on secondary NFS server :	
Secondary NFS timeout (sec, 5-3600) :	5
Secondary NFS mount retrying interval (sec, 5-3600) :	5
Enable/Disable encrypted secondary NFS server :	Disabled
Encrypted secondary NFS server user :	
Encrypted secondary NFS server password :	
Confirm secondary NFS server password :	

Figure 26- NFS server configuration menu

Enable A Compact-flash Card

The compact-flash card must be installed and configured on the SERIMUX before it can be used for system logging or storing SERIMUX configuration information. See Adding a Compact-flash Card on page 11.

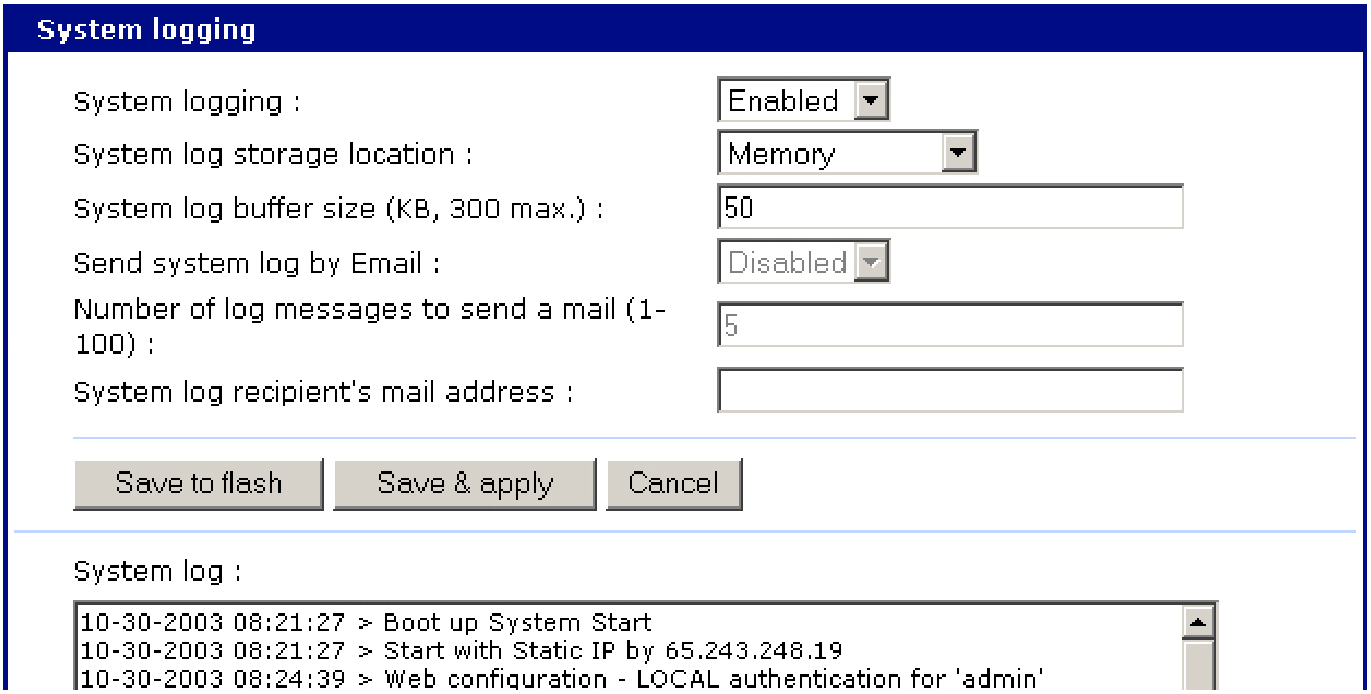
Enable SERIMUX Memory

The SERIMUX memory is already enabled for port logging and only needs to be configured for system or port logging. See Configuring System Logging Services (next section).

Configuring System Logging Services

To configure the SERIMUX for system logging, do the following:

1. Access the web interface.
2. Under System status and log, choose System logging.
3. Choose Enabled for System logging and the log buffer size.
4. From the System log storage location, choose the location you want from the drop down menu. The choices available are dependent on what has been enabled and/or installed. The SERIMUX memory choice is always available.
5. Choose to enable or disable email alerts and the number of log messages to send. The default value is 5 seconds for the delay in log email messages.
6. Enter the contact person's email address.
7. Choose Save & apply.



System logging : Enabled

System log storage location : Memory

System log buffer size (KB, 300 max.) : 50

Send system log by Email : Disabled

Number of log messages to send a mail (1-100) : 5

System log recipient's mail address :

```
10-30-2003 08:21:27 > Boot up System Start
10-30-2003 08:21:27 > Start with Static IP by 65.243.248.19
10-30-2003 08:24:39 > Web configuration - LOCAL authentication for 'admin'
```

Figure 27- Configure system logging services

Viewing System Logs

The system logs can be viewed from the web interface on the System logging page or from the location where they have been saved. The following table lists the file locations of the system logs.

System Logfile	
Log Storage	File Location
Digi memory	/tmp/logs
Compact-flash card	/mnt/flash/logs
Syslog server	must be viewed on the syslog server
NFS server	/mnt/nfs/logs

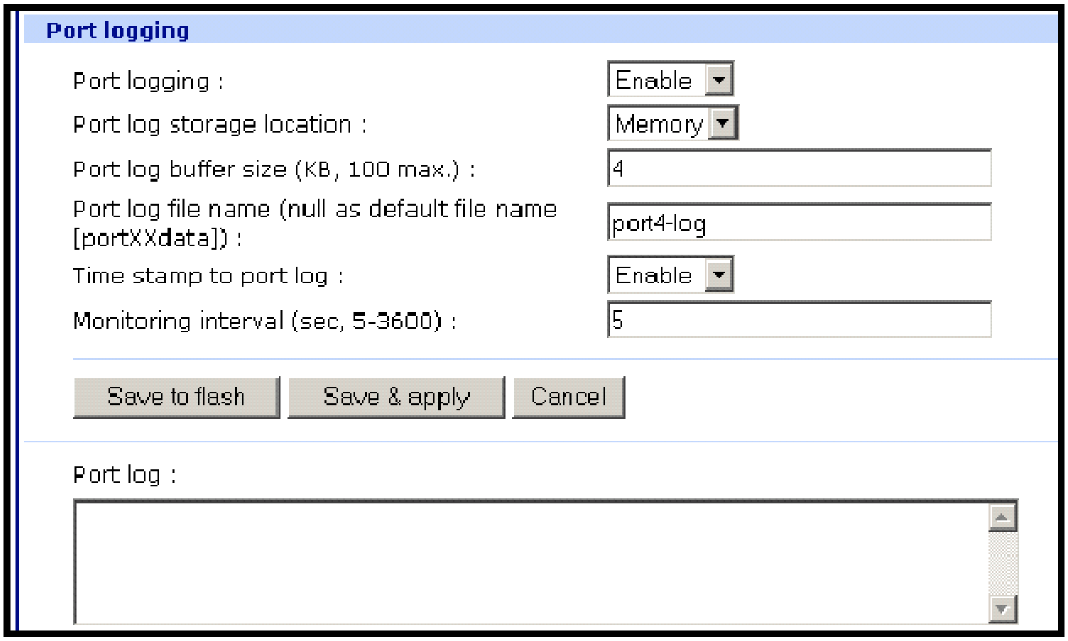
Port Logging

If a serial port is configured for console server mode, the port logging feature can be enabled. Port logging allows the user to save serial data to the memory of the SERIMUX, a compact-flash card, a syslog server, or to an NFS server. If the memory is used for port logging, all data will be cleared when the system's power is turned OFF.

Users can also define alarm keywords for each serial port and send email alerts or SNMP traps to enable unattended serial data monitoring. To configure a serial port for port logging in console server mode, do the following:

1. Access the web interface.
2. Under the Serial Port heading, choose Configuration.
3. Choose All or the Individual port and then Port logging.
4. Configure the settings.
5. Choose Save & apply.

Note: When port logging is enabled, a Port Event Handling page is available to create alarm keywords and send alerts. See Alerts and Notifications on page 24 for more information.



Port logging

Port logging : Enable

Port log storage location : Memory

Port log buffer size (KB, 100 max.) : 4

Port log file name (null as default file name [portXXdata]) : port4-log

Time stamp to port log : Enable

Monitoring interval (sec, 5-3600) : 5

Figure 28- Port logging menu

Viewing Port Logs
The port logs can be viewed from the web interface on the Port logging page or from the location where they have been saved. The following table lists the file locations of the system logs.

System Logfile	
Log Storage	File Location
Digi memory	/tmp/port#data
Compact-flash card	/mnt/flash/port#data
Syslog server	must be viewed from the syslog server
NFS server	/mnt/nfs/port#data

To view the port logs on the NFS server for port number 5, enter the following command:

```
more /mnt/nfs/port5data
```

Partial logfiles can also be viewed on the web interface by going to Serial port > Configuration > select a port you want to view > Port logging.

Using the Configuration Menu

System Logging
System logging is a two part process.

First, the device being used to record the system logs must be configured.

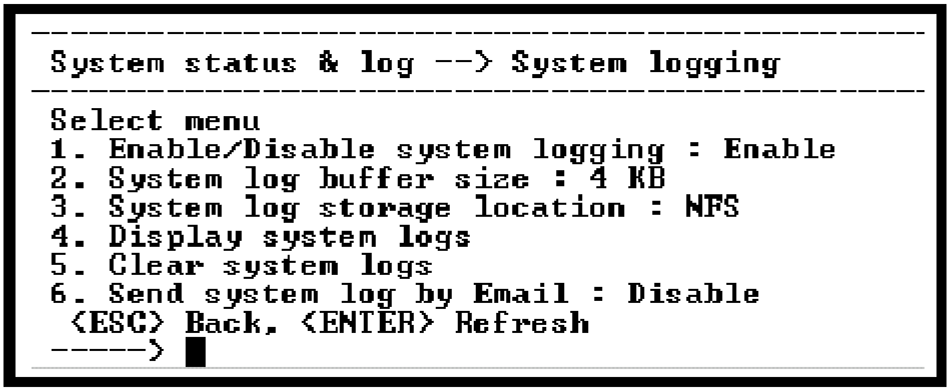
Secondly, system logging must be configured for the system under System status and log.

System logs can be saved to the SERIMUX system memory (there is no need to configure the memory), a compact-flash card, an NFS server, or a Syslog server.

Configure the System Log Device
To configure the compact-flash card for system logging, see Adding a Compact-flash Card on page 11. For an NFS or Syslog server, do the following:

1. Access the configuration menu.
2. Choose Network configuration > NFS or SYSLOG server configuration.
3. Enter the desired parameters for the menu items.
4. Use the ESC key when all parameters are entered to return to the main menu.
5. Choose Save changes.

Configure System Logging
To configure the SERIMUX for system logging, do the following:
1. Access the configuration menu.
2. Choose System Status and log > System logging.



```
---------------------------------------------------------
 System status & log --> System logging
---------------------------------------------------------
 Select menu
 1. Enable/Disable system logging : Enable
 2. System log buffer size : 4 KB
 3. System log storage location : NFS
 4. Display system logs
 5. Clear system logs
 6. Send system log by Email : Disable
  <ESC> Back, <ENTER> Refresh
 -----> █
```

Figure 29- System status logging setup via Configuration menu

3. Enter the desired parameters for the menu items.
4. Use the ESC key when all parameters are entered to return to the main menu.
5. Choose Save changes.

Alerts and Notifications

Introduction

The SERIMUX can be configured for system alerts and notifications. It sends email messages when the number of system log messages reaches a certain value or when an alarm message is detected in the serial port data. The SERIMUX uses SMTP (Simple Mail Transfer Protocol) for sending the notifications. To use SMTP, the system administrator must configure a valid SMTP server for sending the emails. The SERIMUX supports three types of SMTP servers: SMTP server without authentication, SMTP server with authentication, and POP before SMTP.

The SERIMUX also supports SNMP (Simple Network Management Protocol), a protocol used to manage a network and monitor devices on a network. System and port alerts can also be sent using SNMP traps. The SERIMUX supports both versions 1 and 2 of the SNMP protocol. The main function of SNMP on the SERIMUX is to allow a system administrator to query remote devices for information.

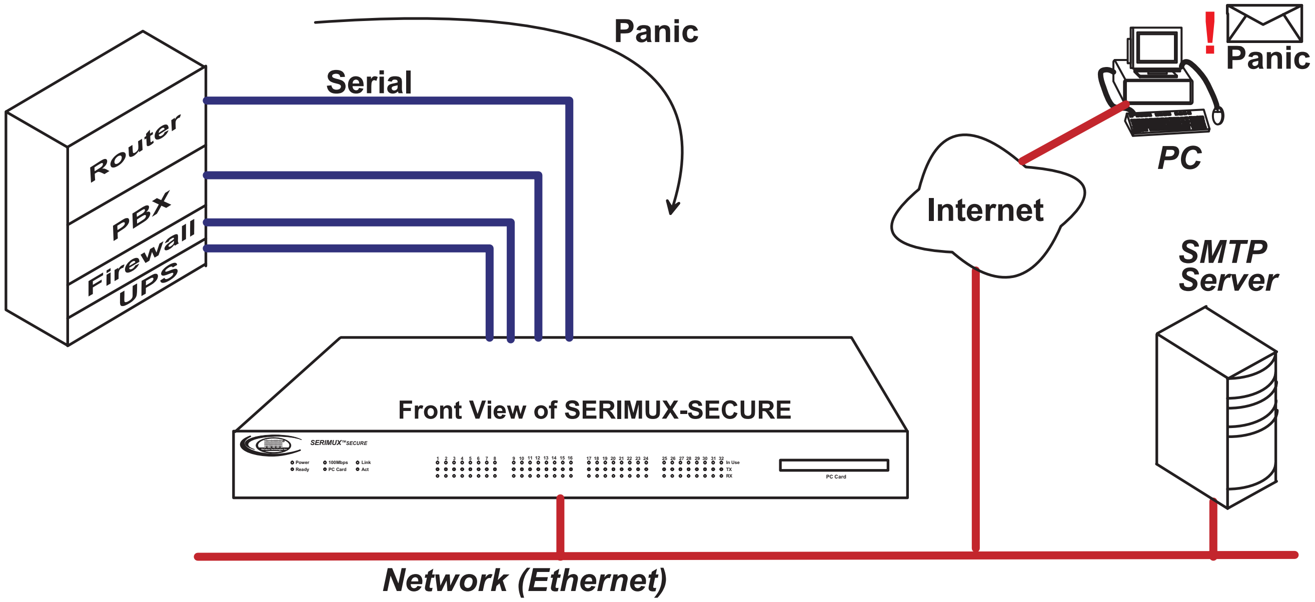


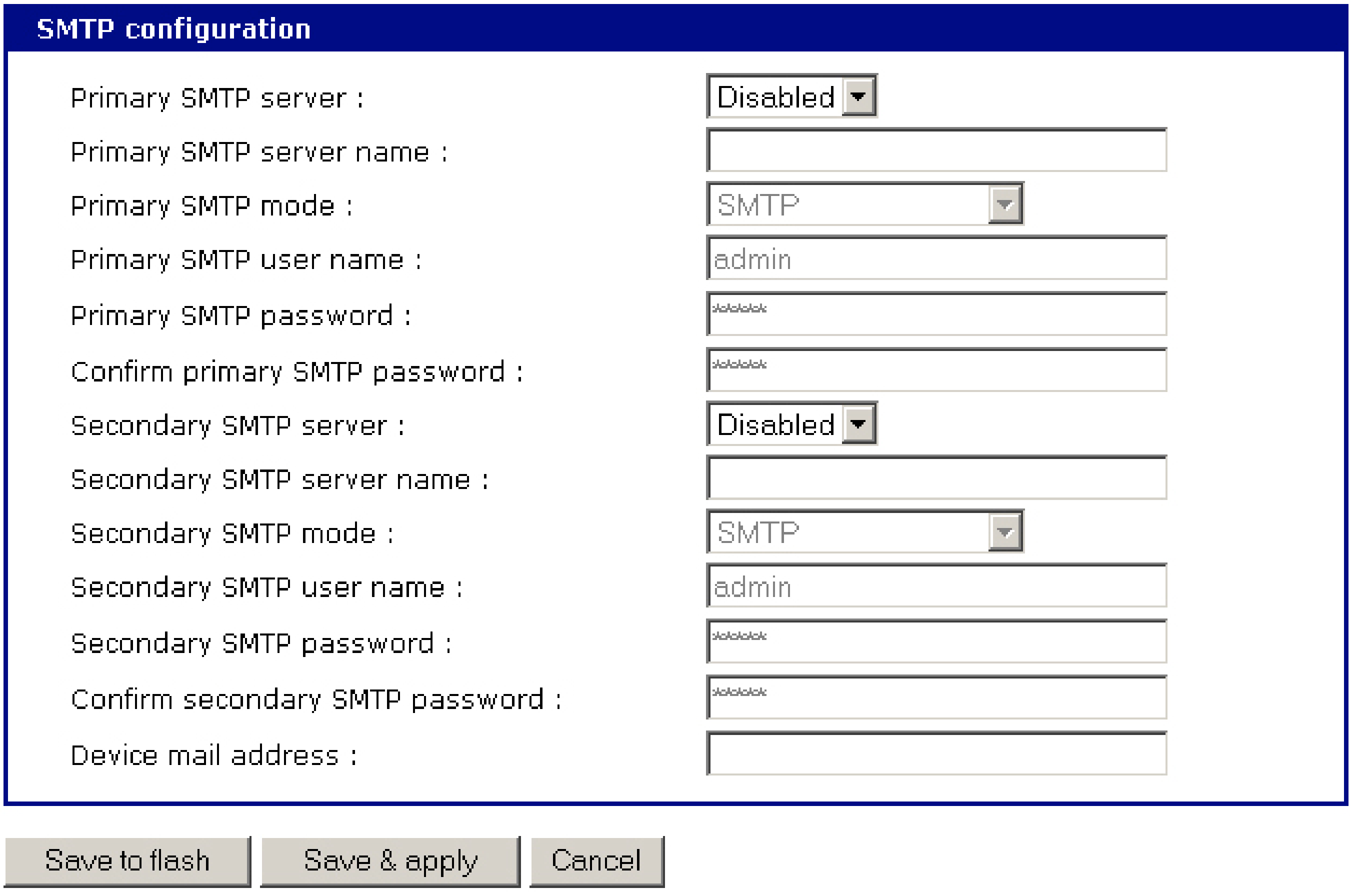
Figure 30- SERIMUX used for system alerts and notifications

Configuring SMTP Alerts

Most SMTP servers check the sender’s email address with the host domain name to verify the address as authentic. Consequently, when assigning an email address for the device email address, any arbitrary username with the registered hostname may be used. An example is username@company.com.
To configure the SERIMUX for SMTP alerts, the following parameters are required:

- **SMTP server**: Use either the hostname or the IP address.
- **Device mail address**: Specify the sender’s email address for the log and alarm delivery.
- **SMTP mode**: Specify the type of SMTP server to use.
- **Username and password**: These fields are required for POP before SMTP and SMTP with authentication servers.

To configure SMTP alerts on the SERIMUX, do the following:
1. Access the web interface.
2. Under the Network heading, choose SMTP configuration.
3. Fill in the required fields. SMTP with authentication and POP before SMTP require usernames and passwords.
4. Choose Save & apply.



SMTP configuration

Primary SMTP server : Disabled
Primary SMTP server name :
Primary SMTP mode : SMTP
Primary SMTP user name : admin
Primary SMTP password : ******
Confirm primary SMTP password : ******
Secondary SMTP server : Disabled
Secondary SMTP server name :
Secondary SMTP mode : SMTP
Secondary SMTP user name : admin
Secondary SMTP password : ******
Confirm secondary SMTP password : ******
Device mail address :

Figure 31- SMTP configuration menu

SNMP Information

Applications such as NMS (Network Management System) or an SNMP browser can exchange information with the SERIMUX and control actions to the unit. The protocol functions defined for SNMP includes GET, SET, GET-Next, GET-Bulk, and TRAP. Below are the definitions of the protocol functions found in SNMP. Authentication, power on, and link up traps are supported.

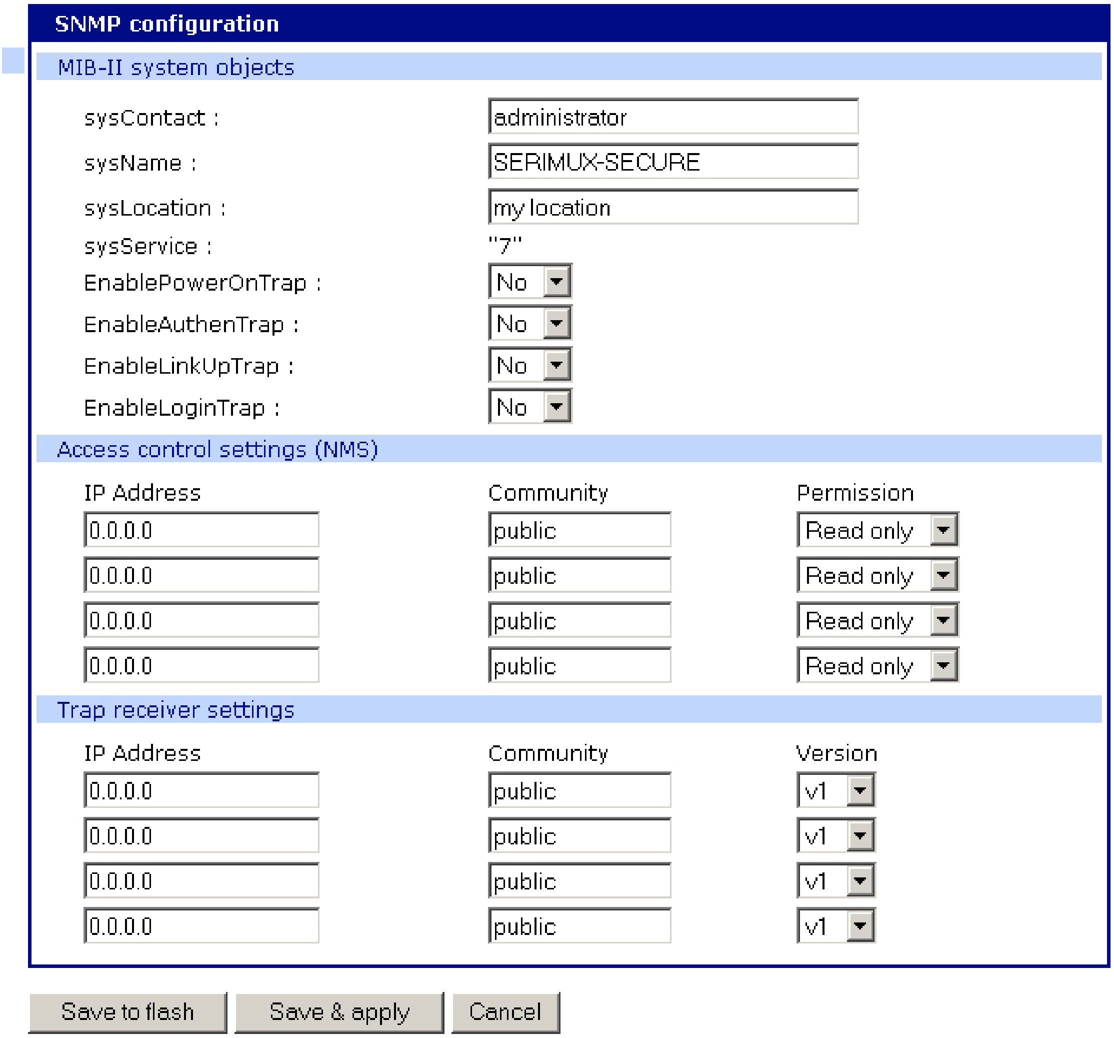
Protocol	Function
GET	Queries a device for more information
SET	Makes changes to a device's state
GET-Next	After an initial GET query, goes to the next value
GET-Bulk	Retrieves tables of information and security functions
TRAP	Notifies a system administrator of a significant event

Configuring SNMP

To configure the SERIMUX for SNMP do the following:
1. Access the SERIMUX web interface.
2. Under the Network heading, choose SNMP configuration.
3. Fill in information for the MIB-II system objects section and choose Yes under EnableAuthenTrap.
   - **sysContact:** Identity of the contact person managing the MIB-II system.
   - **sysName:** The name identifying the system. By convention, this is the fully qualified domain name of the SERIMUX unit.. An example is:SERIMUX@companyname.com.
   - **sysLocation:** The physical location of the unit such as Room 264 or Engineering Lab.
   - **sysService (Read only):** A series of values, separated by commas, indicating the set of services the system provides. By default the SERIMUX only supports Application (7) service level.
   - **EnablePowerOnTrap:** Determines whether the SNMP agent generates a trap each time the SERIMUX is started.
   - **EnableAuthenTrap**: Indicates whether the SNMP agent process is permitted to generate authentication failure traps.
   - **EnableLinkUpTrap**: Determines whether the SNMP agent generates a trap each time the network connection comes up.

Note: Trap values override all other configuration information, meaning all other authentication failure traps can be disabled with this setting.

4. Enter Access control settings.
   - **IP Address**: Defines what applications can access the SERIMUX SNMP agent to exchange information and control actions. If no IP addresses are listed, any application can access the SNMP agent.
   - **Community:** The options are public or private.
   - **Permissions**: The options are Read only or Read/Write.
5. Enter Trap receiver settings.
   - **IP Address**: Enter the IP address of the device receiving the trap alerts.
   - **Community:** The options are public or private.
   - **Version:** Choose the SNMP version, either version 1 or version 2c.
6. Choose Save & apply.



SNMP configuration

MIB-II system objects

sysContact :	administrator
sysName :	SERIMUX-SECURE
sysLocation :	my location
sysService :	"7"
EnablePowerOnTrap :	No
EnableAuthenTrap :	No
EnableLinkUpTrap :	No
EnableLoginTrap :	No

Access control settings (NMS)

IP Address	Community	Permission
0.0.0.0	public	Read only
0.0.0.0	public	Read only
0.0.0.0	public	Read only
0.0.0.0	public	Read only

Trap receiver settings

IP Address	Community	Version
0.0.0.0	public	v1
0.0.0.0	public	v1
0.0.0.0	public	v1
0.0.0.0	public	v1

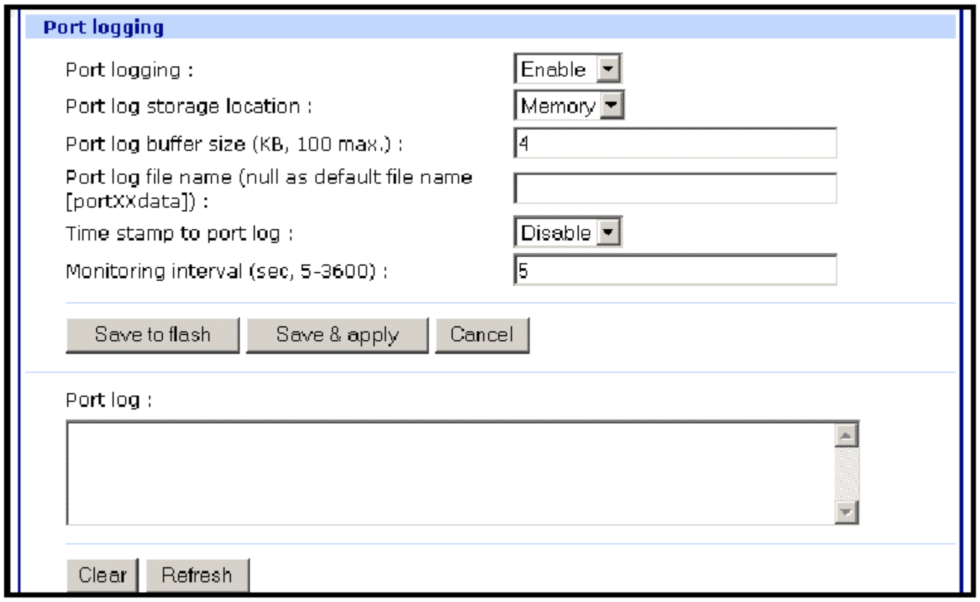
Figure 32- SMNP configuration menu

Managing the SNMP Protocol

The SERIMUX SNMP protocol can be managed using an NMS or SNMP browser. However, before the NMS or SNMP browser can access the data, the Access control settings must list the IP address of the host from which the browser is executed. See the preceding graphic for details.

Configuring Port Event Handling

Once an SMTP or SNMP server has been configured, it can be used to send port-related alerts and notifications. The following describes how to configure a port for port event handling.
1. Access the web interface.
2. Choose Serial port > Configuration.
3. Choose a port to configure and then Port logging.
4. Use the Port logging page to enable logging.



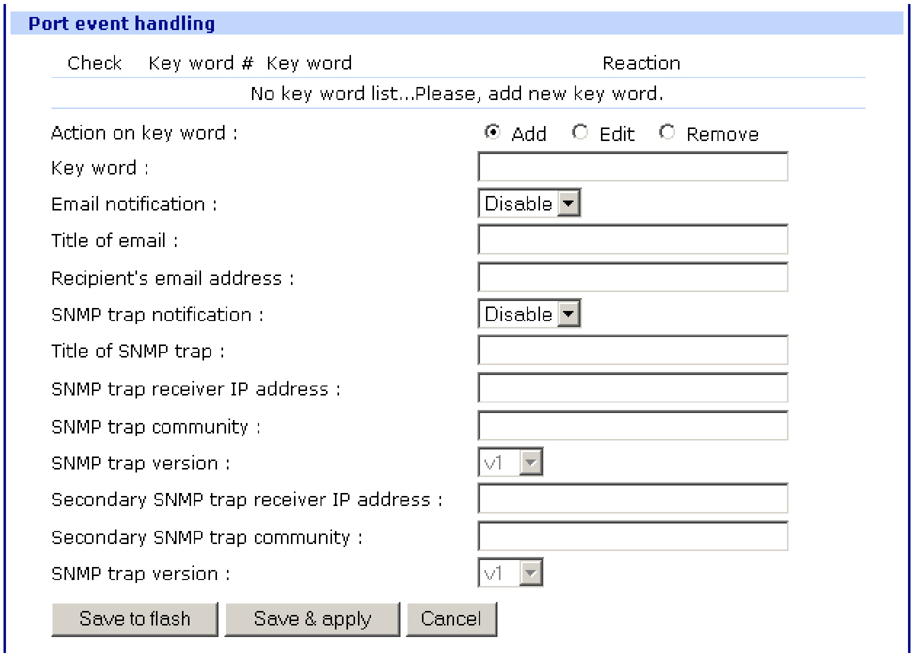
Port logging

Port logging :	Enable
Port log storage location :	Memory
Port log buffer size (KB, 100 max.) :	4
Port log file name (null as default file name [portXXdata]) :	
Time stamp to port log :	Disable
Monitoring interval (sec, 5-3600) :	5

Port log :

Figure 33- Configure a port for to enable logging of port events

5. Choose Save & apply.
6. Choose Port event handling.
The following window appears.



Port event handling

Check	Key word #	Key word	Reaction
No key word list...Please, add new key word.			

Action on key word :	● Add ○ Edit ○ Remove
Key word :	
Email notification :	Disable
Title of email :	
Recipient's email address :	
SNMP trap notification :	Disable
Title of SNMP trap :	
SNMP trap receiver IP address :	
SNMP trap community :	
SNMP trap version :	v1
Secondary SNMP trap receiver IP address :	
Secondary SNMP trap community :	
SNMP trap version :	v1

FYI: "Key word" is any text string that will trigger an alert when it traverses the serial port.

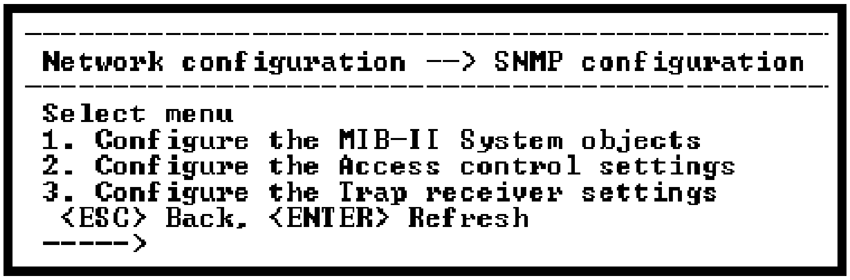
Figure 34- Configure port for event handling

7. Complete configuration and then choose Save & apply.

Using the Configuration Menu

Configuring SNMP

To configure SNMP from the configuration menu, do the following:
1. Access the Configuration menu.
2. Choose Network configuration > SNMP configuration.



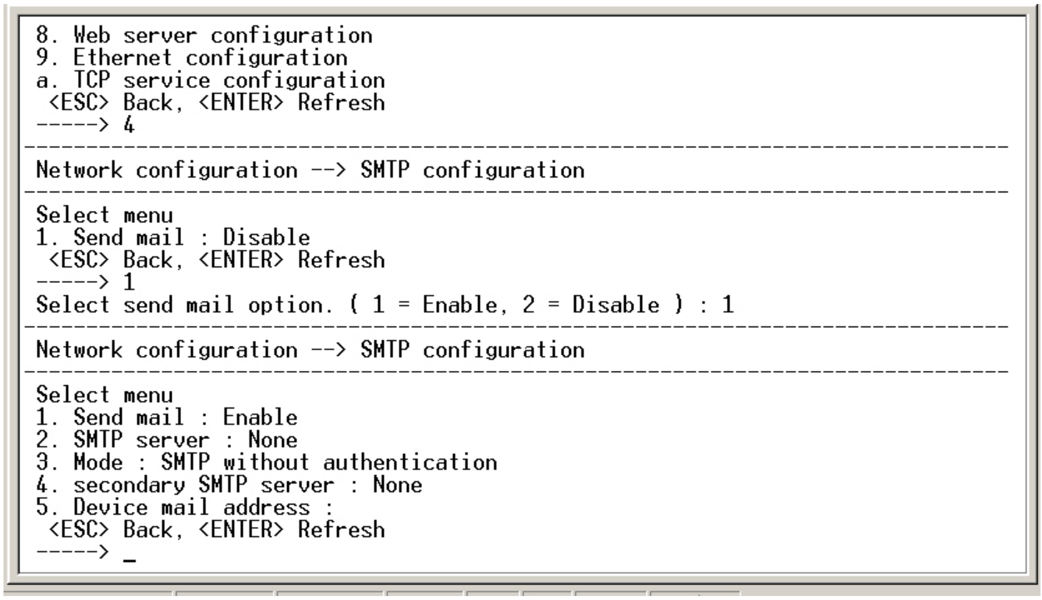
```
--------------------------------------------
 Network configuration --> SNMP configuration
--------------------------------------------
 Select menu
 1. Configure the MIB-II System objects
 2. Configure the Access control settings
 3. Configure the Trap receiver settings
  <ESC> Back, <ENTER> Refresh
 ----->
```

Figure 35- Configure SNMP via Configuration menu

3. Enter the desired parameters for the menu items.
4. Use the ESC key when all parameters are entered to return to the main menu.
5. Choose Save changes.

Configuring SMTP

To configure SMTP from the configuration menu, do the following:
1. Access the Configuration menu.
2. Choose Network configuration > SMTP configuration.



```
 8. Web server configuration
 9. Ethernet configuration
 a. TCP service configuration
  <ESC> Back, <ENTER> Refresh
 -----> 4
--------------------------------------------------------------------------------
 Network configuration --> SMTP configuration
--------------------------------------------------------------------------------
 Select menu
 1. Send mail : Disable
  <ESC> Back, <ENTER> Refresh
 -----> 1
 Select send mail option. ( 1 = Enable, 2 = Disable ) : 1
--------------------------------------------------------------------------------
 Network configuration --> SMTP configuration
--------------------------------------------------------------------------------
 Select menu
 1. Send mail : Enable
 2. SMTP server : None
 3. Mode : SMTP without authentication
 4. secondary SMTP server : None
 5. Device mail address :
  <ESC> Back, <ENTER> Refresh
 -----> _
```

Figure 36- Configure SMTP via Configuration menu

3. If the Send mail option is disabled, you must first enable it to see the rest of the menu.
   Press 1 to bring up the enable/disable option
   press 1 again to enable it.
4. Enter the desired parameters for the menu items.
5. Press Enter to refresh the screen with the configuration changes
6. Use the ESC key when all parameters are entered to return to the main menu.
6. Choose Save changes.

Configuring Security and Authentication

Introduction

The SERIMUX provides several ways to control access to the network and the devices on the network. One method is through IP filtering, which allows or prevents users with specific IP addresses from accessing devices or serial ports on the network. IP filtering can be permitted or restricted for all ports globally or on a per port basis. Another access control method involves restricting or permitting specific users. Users can be easily added or removed from either a restricted or permitted users list. Sniff session access, which allows multiple users to access a single port, is also discussed.

The SERIMUX provides for various authentication methods. They are: Local, RADIUS, TACACS+, LDAP, and Kerberos. Authentication may be configured where a secondary method is attempted if the primary method fails.

Configuring Network IP Filtering

Access to the SERIMUX can be controlled through IP filtering. IP filtering controls access to the SERIMUX from remote hosts either trying to access from a remote console or a web browser. IP filtering can also be used to control access to individual ports.

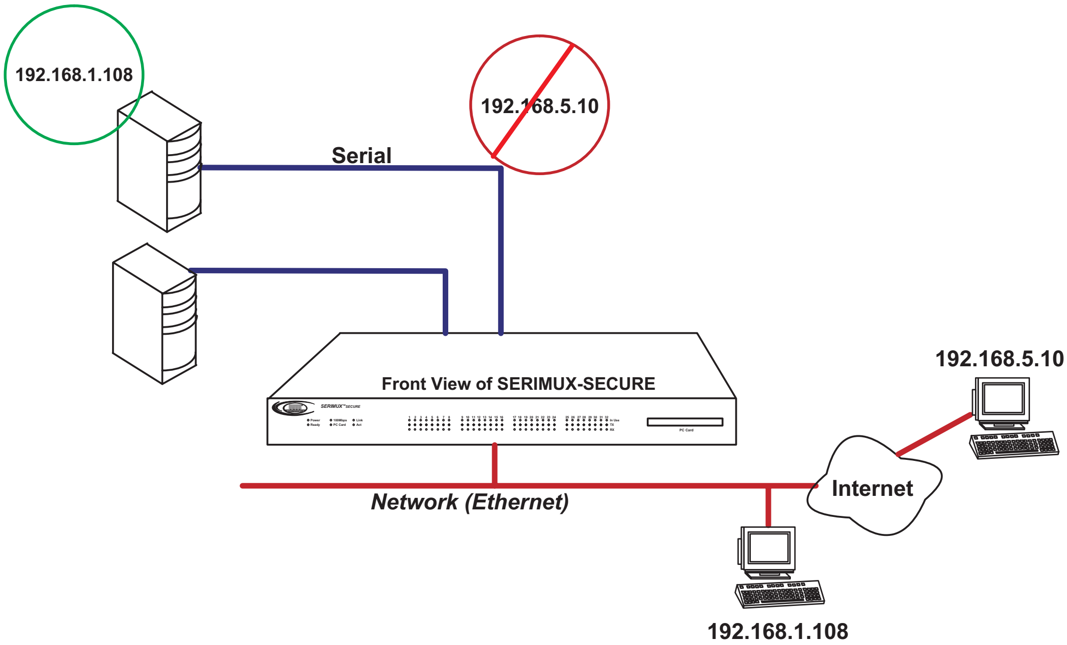
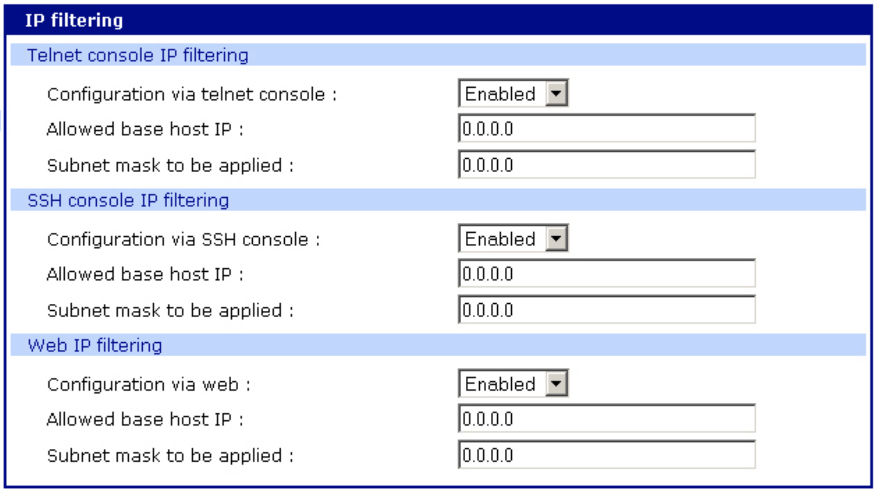


Figure 37- SERIMUX access controlled by IP filtering

Console and Web IP Filtering

IP filtering is a way of controlling access to the SERIMUX from remote hosts. If the administrator wants to allow specific remote hosts access to the SERIMUX, the administrator must provide the host's IP address and subnet mask. To configure the SERIMUX for IP filtering, do the following:

1. Access the web interface.
2. Under the Network heading, choose IP filtering.
3. Choose Enabled for either Telnet console, SSH console, Web IP filtering or all.
4. Enter the IP address and subnet mask for the remote host.
5. Choose Save and apply.



IP filtering

Telnet console IP filtering

Configuration via telnet console :	Enabled
Allowed base host IP :	0.0.0.0
Subnet mask to be applied :	0.0.0.0

SSH console IP filtering

Configuration via SSH console :	Enabled
Allowed base host IP :	0.0.0.0
Subnet mask to be applied :	0.0.0.0

Web IP filtering

Configuration via web :	Enabled
Allowed base host IP :	0.0.0.0
Subnet mask to be applied :	0.0.0.0

Figure 38- IP filtering menu

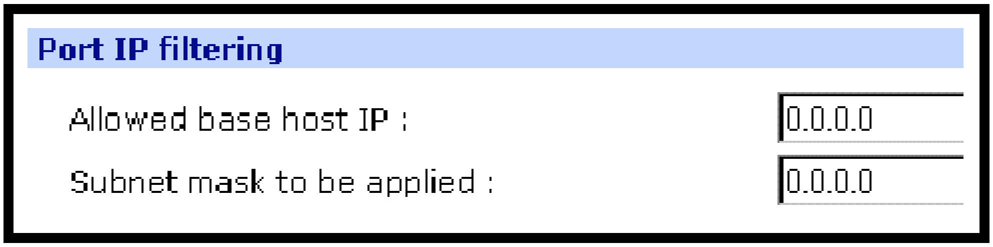
The following table displays examples of allowed remote hosts.

Allowable Hosts	Input format	
	Base Host IP Address	Subnet mask
Any host	0.0.0.0	0.0.0.0
192.168.1.120	192.168.1.120	255.255.255.255
192.168.1.1 - 192.168.1.254	192.168.1.0	255.255.255.0
192.168.0.1 - 192.168.255.254	192.168.0.0	255.255.0.0
192.168.1.1 - 192.168.1.126	192.168.1.0	255.255.255.128
192.168.1.129 - 192.168.1.254	192.168.1.128	255.255.255.128

Serial Port IP Filtering

Each serial port can be configured individually for IP filtering. To configure a serial port for IP filtering, do the following:

1. Access the web interface.
2. Under the Serial Port heading, choose Configuration.
3. Choose All under All port configuration to configure all the ports or a specific port under Individual port configuration > Port IP filtering.
4. Enter the IP address and subnet mask for the remote host that is allowed access.
5. Choose Save & apply.



Port IP filtering

Allowed base host IP : 0.0.0.0

Subnet mask to be applied : 0.0.0.0

Figure 39- Serial Port IP filtering

Using IP Tables

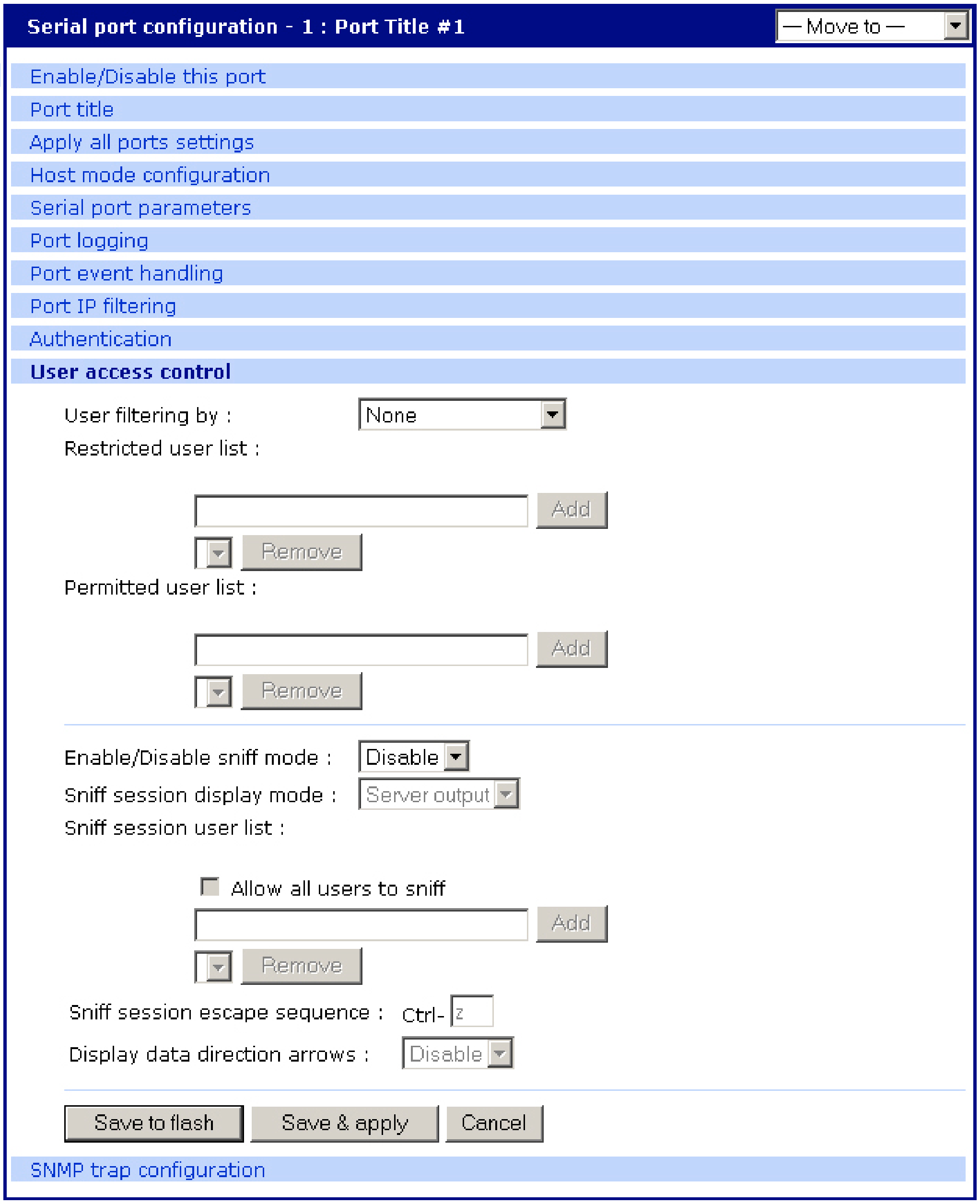
Linux and UNIX systems have an IP filtering program called IPtables. Administrators desiring to add further security by controlling access to the SERIMUX should look at this program. Information about IPtables can be found on most Linux or UNIX systems by viewing the man pages.

Configuring User Access Control

Another method to control access to the serial ports on the SERIMUX is through the User Access Control configuration. This configuration can be done on a per port basis or globally by selecting the All Ports option. There are three options for user access control: None, Restricted user list, and Permitted user list. Users must have already been added to the system before they can be entered on a Restricted or Permitted user list or for a Sniff Session user list.

- When None is selected, any user that is registered on the authentication server can access a serial port.
- When Restricted user list is selected, a user cannot access a serial port even if they are registered on an authentication server.
- When Permitted user list is selected, only this user can access a specific serial port.

Note: Users do not necessarily need to be local, but can be users on any configured authentication server.



User filtering by : None

Restricted user list :

Permitted user list :

Enable/Disable sniff mode : Disable

Sniff session display mode : Server output

Sniff session user list :

□ Allow all users to sniff

Sniff session escape sequence : Ctrl- z

Display data direction arrows : Disable

Figure 40- Configure User access control

Sniff Session

A Sniff Session enables multiple users to access a single serial port for viewing the data stream. Users who are registered for a sniff session can access a specific serial port even if another user is using the port. The SERIMUX supports multiple concurrent sniff sessions.

- **Allow all users to sniff**: When checked, all users with permission to access the port can participate in sniff sessions.
- **Sniff session escape sequence**: Key sequence that ends a sniff session takes the user back to the sniff session menu.

There are two options for Sniff mode:

- **disabled:** The sniff mode is disabled and no user can enter a sniff session
- **enabled**: The sniff mode is enabled and those in the Permitted user list can access the port

If enabled, the sniff session display mode has three options that can be configured on a per-port basis from the Serial port configuration page.

- **user input:** A sniff user can view all data to a serial port from a remote connection
- **server output:** A sniff user can view all data from a serial port to a remote connection
- **both:** A sniff user can see all data transmitted or received through a serial port

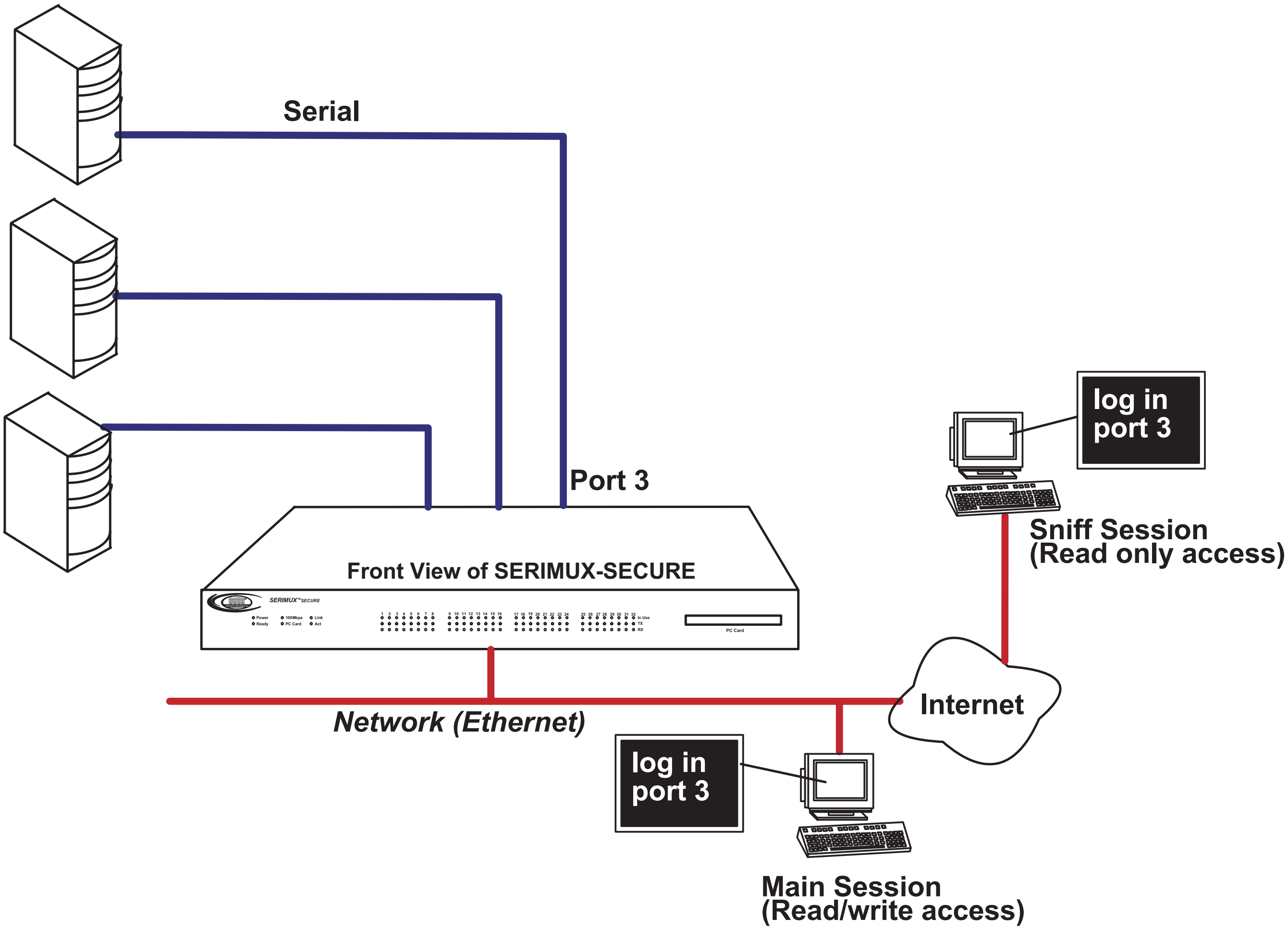
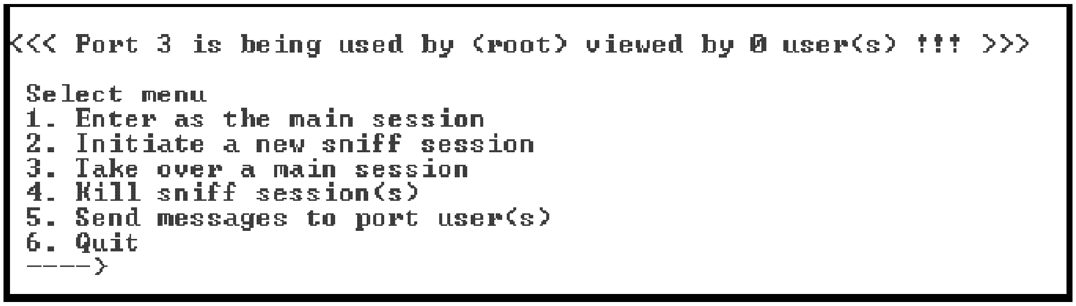


Figure 41- User in a Sniff Session

Viewing A Sniff Session

A sniff user enters a sniff session by starting a Telnet session on a specified port. In the following example, a sniff user Telnets to port 7 of a SERIMUX. From the command prompt enter the following command:

```
telnet 192.168.100.42 7007
```



```
<<< Port 3 is being used by (root) viewed by 0 user(s) !!! >>>

 Select menu
 1. Enter as the main session
 2. Initiate a new sniff session
 3. Take over a main session
 4. Kill sniff session(s)
 5. Send messages to port user(s)
 6. Quit
 ---->
```

Figure 42- Sniff session user menu

When sniff users login to a port from a Telnet session, a sniff session menu is displayed with these options:

- **1 (Enter as the main session):** Disconnects the user of the current main session from the system and allows the new user to take over as the main session.
- **2 (Initiate a new sniff session):** Initiates a new sniff session. Pressing the sniff session escape sequence (the default is Ctrl-Z) returns the user to the sniff session menu.
- **3 (Take over a main session):** Converts the user of the current main session to a sniff session user and enables the new user to take over the current main session.
- **4 (Kill a sniff session):** Kills the sniff session.
- **5 (Send message to port user):** Enables sniff session user to send a message to other port users.
- **6 (Quit):** Closes the Telnet session.

Authentication

The SERIMUX supports multiple methods of user authentication. The following methods are supported: Local, TACACS+, RADIUS, LDAP, and Kerberos. The type of authentication protocol you use is dependent on your environment.

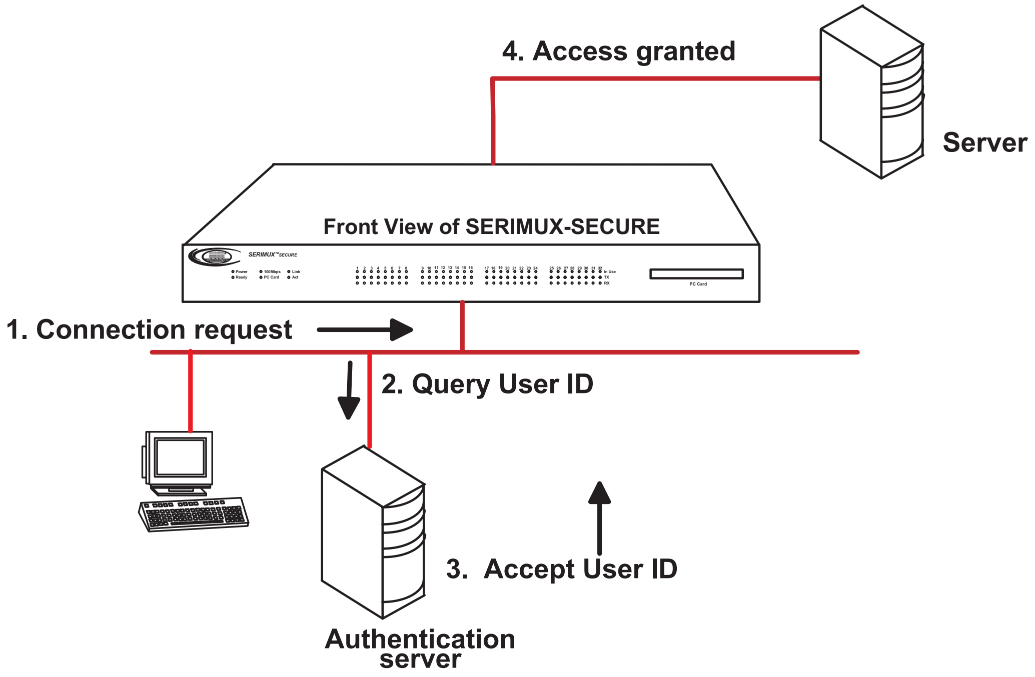
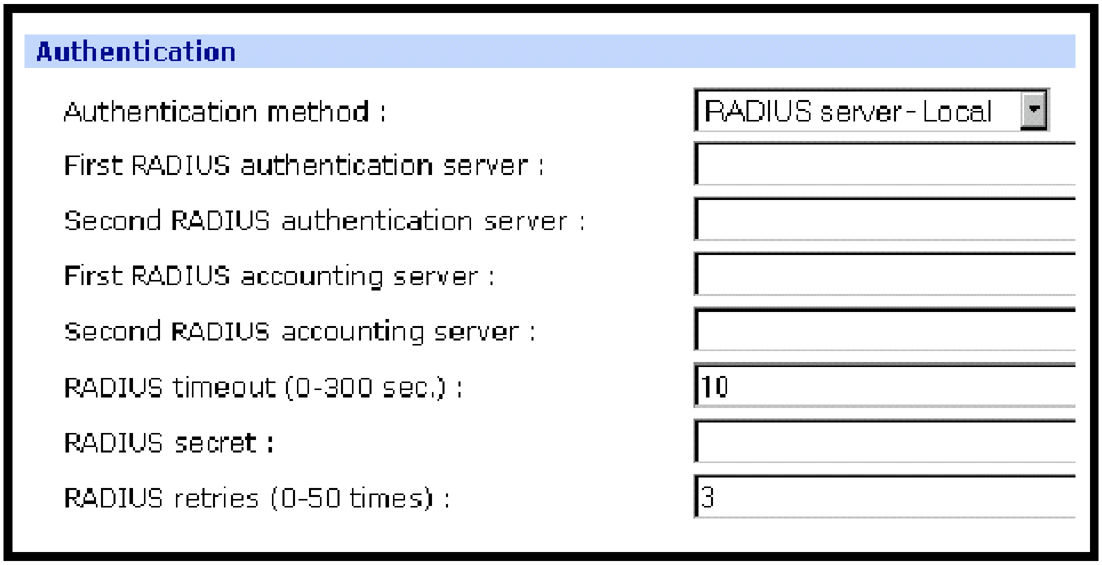


Figure 43- SERIMUX supports user authentication

Configuring Authentication Methods for Port Access

Users can choose between having a single authentication method, such as RADIUS, or an authentication method where a Local authentication service is used in addition to the RADIUS, LDAP, TACACS+ server, or Kerberos. These options are listed when the SERIMUX is configured for authentication. To configure a SERIMUX for authentication, do the following:

1. Access the web interface.
2. Under the Serial Port heading, choose Configuration.
3. Choose All or an Individual port > Authentication.
4. From the drop down menu, choose an authentication method. A configuration screen for that particular authentication method is displayed. The following figure displays the parameters for setting up a RADIUS server as the primary authentication server and Local authentication if the primary authentication method fails.



Authentication

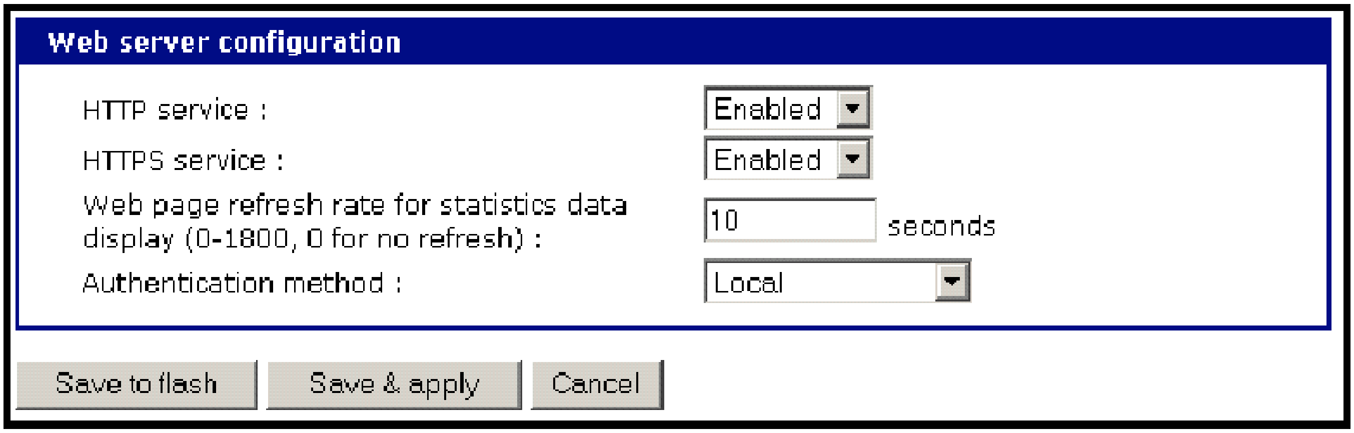
Authentication method :	RADIUS server - Local
First RADIUS authentication server :	
Second RADIUS authentication server :	
First RADIUS accounting server :	
Second RADIUS accounting server :	
RADIUS timeout (0-300 sec.) :	10
RADIUS secret :	
RADIUS retries (0-50 times) :	3

Figure 44- Configure SERIMUX for authentication

5. Fill in the appropriate fields.
6. Choose Save & apply changes.

Configuring Authentication for the Web Server

1. Access the web interface.
2. Choose Network > Web server configuration.
The following screen appears.



Web server configuration

HTTP service : Enabled

HTTPS service : Enabled

Web page refresh rate for statistics data display (0-1800, 0 for no refresh) : 10 seconds

Authentication method : Local

Figure 45- Configure WEB server for authentication

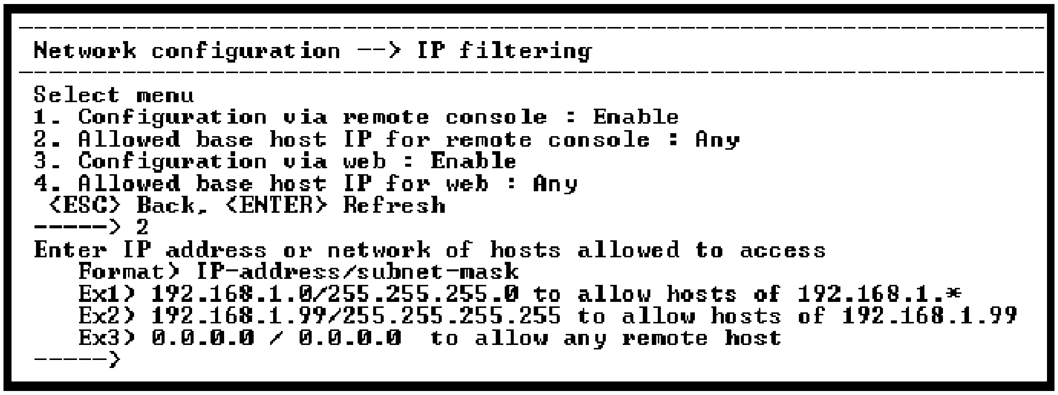
3. Choose an authentication method and then Save & apply.

Note: When using remote authentication for the web server, such as Radius, TACACS+, LDAP or Kerberos, the user must also be added to the local database. See "Adding, Editing, and Removing Users" on page 48 for details. Once the user's password is approved by the authentication server, the SERIMUX uses the local permission rights to provide proper access privileges for the user to ports and the configuration.

Using the Configuration Menu

Network IP Filtering

To configure the SERIMUX for Network IP filtering, do the following:
1. Access the configuration menu.
2. Choose Network configuration > IP filtering.



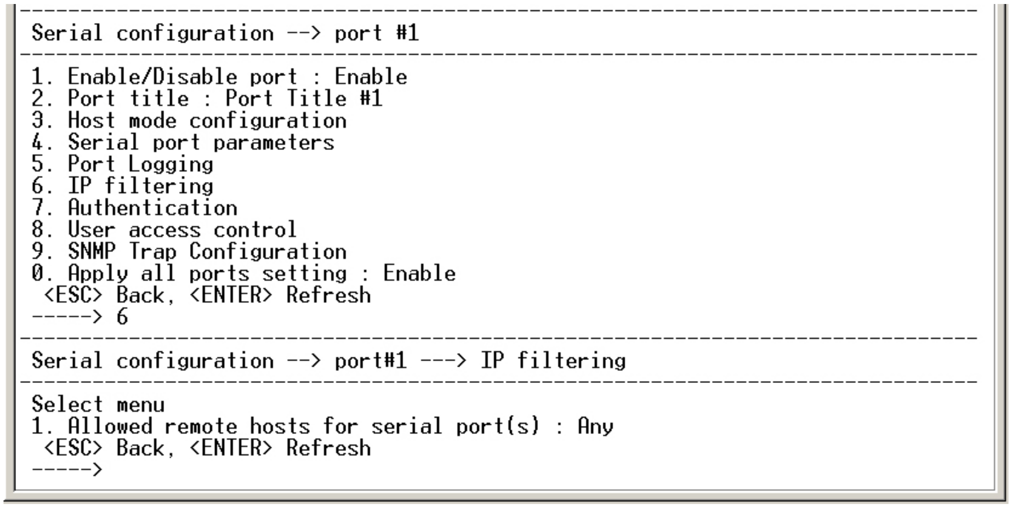
```
-----------------------------------------------------------------------
 Network configuration --> IP filtering
-----------------------------------------------------------------------
 Select menu
 1. Configuration via remote console : Enable
 2. Allowed base host IP for remote console : Any
 3. Configuration via web : Enable
 4. Allowed base host IP for web : Any
  <ESC> Back, <ENTER> Refresh
 -----> 2
 Enter IP address or network of hosts allowed to access
    Format> IP-address/subnet-mask
    Ex1> 192.168.1.0/255.255.255.0 to allow hosts of 192.168.1.*
    Ex2> 192.168.1.99/255.255.255.255 to allow hosts of 192.168.1.99
    Ex3> 0.0.0.0 / 0.0.0.0  to allow any remote host
 ----->
```

Figure 46- Use Configuration menu to setup IP filtering

3. Choose a menu item and enter the desired parameters for the menu items.
4. Use the ESC key to return to the main menu.
5. Choose Save changes.

Port IP Filtering

To configure the SERIMUX for Port IP filtering, do the following:
1. Access the configuration menu.
2. Choose Serial port configuration.
3. Choose an individual port number or 0 (zero) for all ports > IP filtering.



```
-----------------------------------------------------------------------------
 Serial configuration --> port #1
-----------------------------------------------------------------------------
 1. Enable/Disable port : Enable
 2. Port title : Port Title #1
 3. Host mode configuration
 4. Serial port parameters
 5. Port Logging
 6. IP filtering
 7. Authentication
 8. User access control
 9. SNMP Trap Configuration
 0. Apply all ports setting : Enable
  <ESC> Back, <ENTER> Refresh
 -----> 6
-----------------------------------------------------------------------------
 Serial configuration --> port#1 ---> IP filtering
-----------------------------------------------------------------------------
 Select menu
 1. Allowed remote hosts for serial port(s) : Any
  <ESC> Back, <ENTER> Refresh
 ----->
```

Figure 47- Configure Port IP filtering through the Configuration menu

4. Choose a menu item and enter the desired parameters for the menu items.
5. Use the ESC key when all parameters are entered to return to the main menu.
6. Choose Save changes.

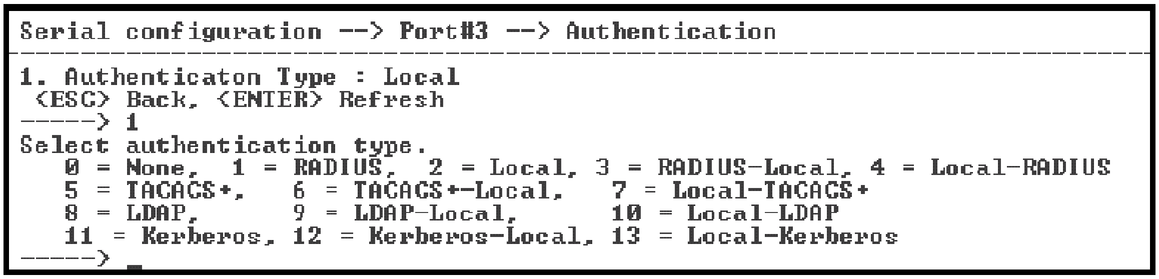
Sniff Sessions

To configure a port or all ports for sniff users, do the following:
1. Access the configuration menu.
2. Choose Serial port configuration.
3. Choose an individual port number or 0 (zero) for all ports > User access control.
4. Choose a menu item and enter the desired parameters for the menu items.
5. Use the ESC key when all parameters are entered to return to the main menu.
6. Choose Save changes.

For information on entering a sniff session, see "Viewing A Sniff Session" on page 32.

Authentication

1. Access the configuration menu.
2. Choose Serial port configuration.
3. Choose an individual port number or 0 (zero) for all ports > Authentication.



```
Serial configuration --> Port#3 --> Authentication
-------------------------------------------------------------------------------
1. Authenticaton Type : Local
 <ESC> Back, <ENTER> Refresh
-----> 1
Select authentication type.
   0 = None,   1 = RADIUS,   2 = Local, 3 = RADIUS-Local, 4 = Local-RADIUS
   5 = TACACS+,   6 = TACACS+-Local,   7 = Local-TACACS+
   8 = LDAP,      9 = LDAP-Local,       10 = Local-LDAP
   11 = Kerberos, 12 = Kerberos-Local, 13 = Local-Kerberos
-----> _
```

Figure 48- Setup user authentication through the Configuration menu

4. Choose an Authentication type.
5. Use the ESC key to return to the main menu.
6. Choose Save changes.

Custom and Default Menus

Introduction

The SERIMUX has several default menus for easy configuration and access by different users. Depending on access privileges, the menus available are the Web Interface, Configuration Menu, and Port Access menu. A custom menu feature for creating menus is also available through the web interface. The custom menu feature enables system administrators to create menus for specific users, which provide each with a customized interface to selected ports.

Making Custom Menus

Before making custom menus, plan the kind of menus and menu items to be made available to the users. A good plan would be to:

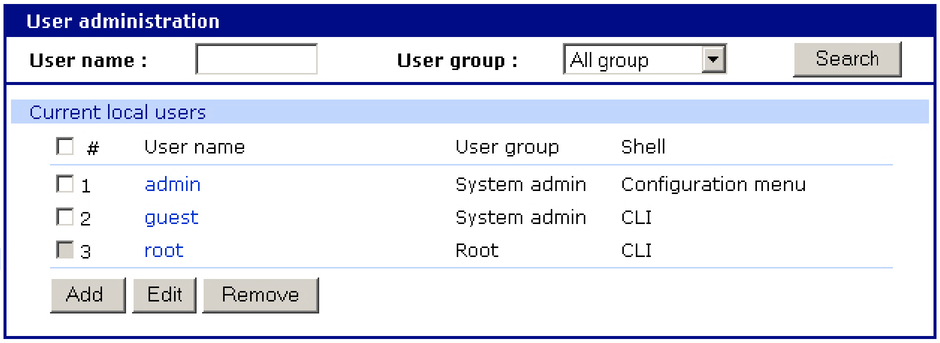
1. Add users to the system.
2. Create a menu name with sort and display features.
3. Add menu items and submenus to the new menu.
4. Assign users to the menus.

Adding Users

Users cannot be assigned to a menu until the users have been added to the system.
To add users, do the following:

1. Access the web interface.
2. Choose Users administration under the System Administration heading.
3. Choose Add User and then fill in settings to assign the user.
4. Choose Custom menu for the Shell program.
5. Choose Add to add the user.
6. Continue to add users as needed.

Note: It is not necessary to Save to flash or Apply changes to add users.



User administration

User name : ______ User group : All group ▾ Search

Current local users

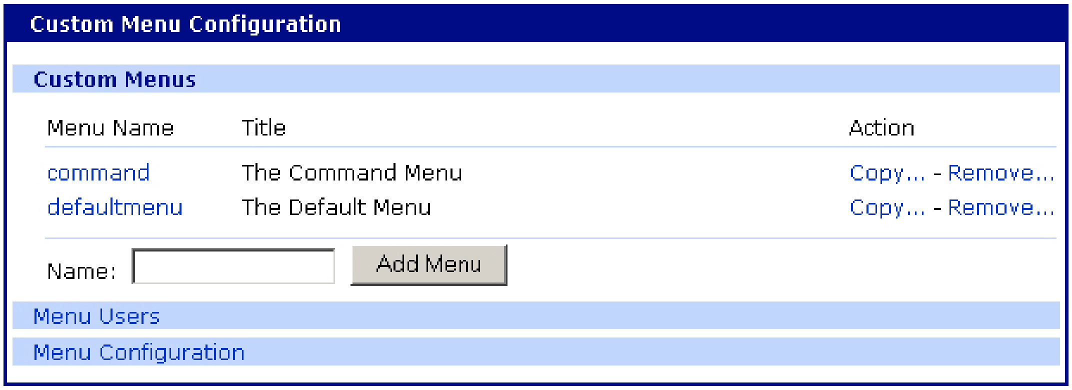
□ #	User name	User group	Shell
□ 1	admin	System admin	Configuration menu
□ 2	guest	System admin	CLI
□ 3	root	Root	CLI

Figure 49- Add users to the system

Creating Menu Names

To make a custom menu, do the following:

1. Access the web interface.
2. Choose Configuration under the Custom Menus heading.
3. Enter the Menu Name to assign and choose the Add Menu button. The menu is added.
4. Choose the hyperlink to the menu you just created.
5. From the drop down menu, select the way to Sort and Display items.



Custom Menu Configuration

Custom Menus

Menu Name	Title	Action
command	The Command Menu	Copy... - Remove...
defaultmenu	The Default Menu	Copy... - Remove...

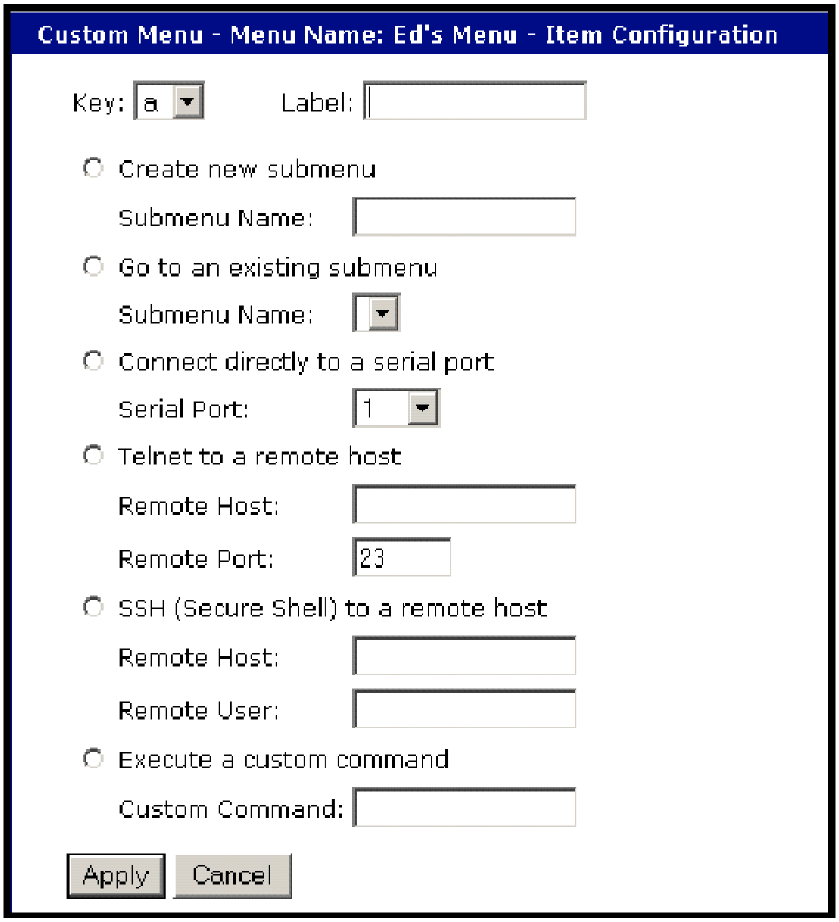
Name: ______ Add Menu

Figure 50- Creating menu names

6. Choose Save & apply.
7. Repeat as required to create additional menus.

Adding Menu Items

Once a menu name is defined and users are added, menu items can then be added. To add menu items, do the following:
1. Choose Configuration under Custom Menus and then the Menu Name hyperlink for the menu to be configured.
2. Choose Menu Items > Add Item.
The following screen appears.



Custom Menu - Menu Name: Ed's Menu - Item Configuration

Key: a Label:

○ Create new submenu

Submenu Name:

○ Go to an existing submenu

Submenu Name:

○ Connect directly to a serial port

Serial Port: 1

○ Telnet to a remote host

Remote Host:

Remote Port: 23

○ SSH (Secure Shell) to a remote host

Remote Host:

Remote User:

○ Execute a custom command

Custom Command:

Figure 51- Adding menu items

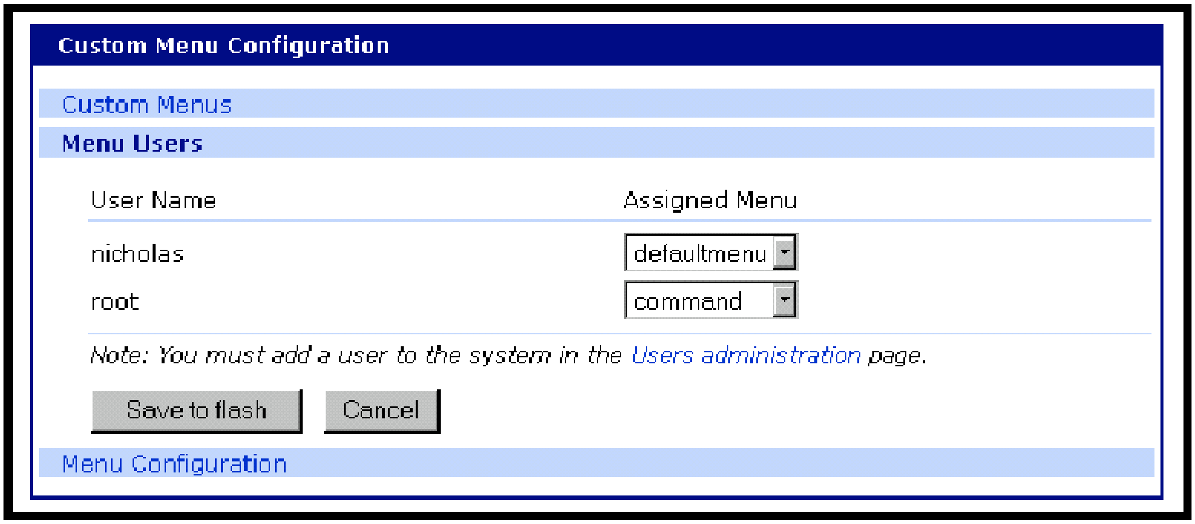
3. Fill in the desired parameters. The parameters are:
   - **Key:** Assign any letter or number except a value already used by another menu item.
   - **Label:** Assign a label or name for the menu item.
   - **Create new submenu:** Assign a name for a new submenu that this menu item will be assigned or linked to.
   - **Go to existing submenu:** Choose an existing submenu from the drop down menu that this menu item will be assigned or linked to.
   - **Connect directly to a serial port:** Connects the user to a specified port.
   - **Telnet to a remote host:** Enter a remote host's IP address or hostname.
   - **SSH to a remote host:** Enter the hostname or IP address of a remote host and the remote username.
   - **Execute a custom command**: Enter a customized command that is any valid command on the command line with acceptable user privileges.
4. Choose Apply.
5. Repeat this procedure to add more menu items.

Note: To add or configure submenus, select the Submenus hyperlink on the Menu Configuration page.

Assigning Users To A Menu

Once a menu has been created, users can be assigned to the menu by doing the following:

1. Access the web interface.
2. Under the Custom Menus heading, choose Configuration > Menu Users.
   A list of available users is displayed.



User Name	Assigned Menu
nicholas	defaultmenu
root	command

Note: You must add a user to the system in the Users administration page.

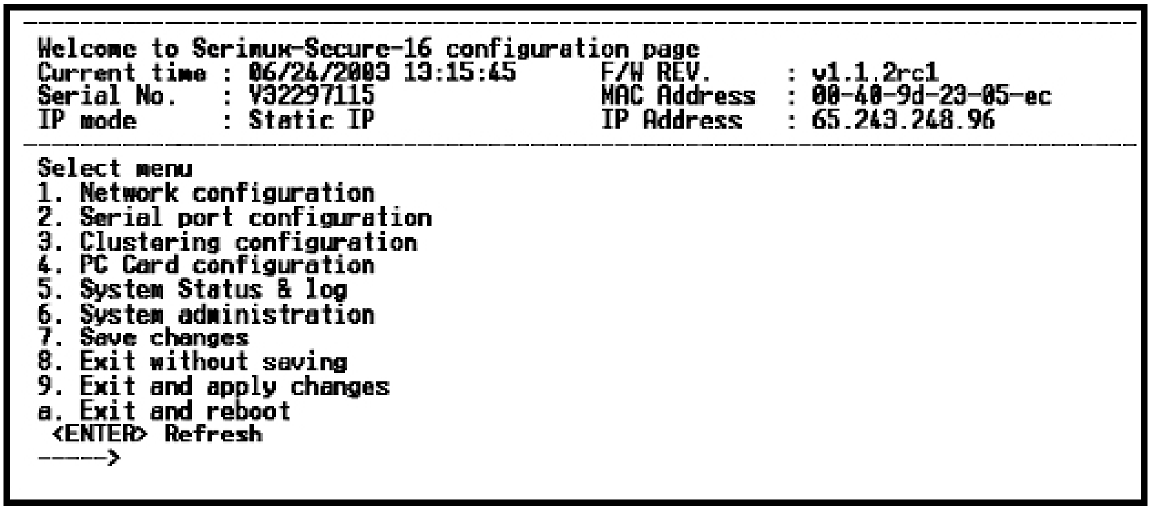
Figure 52- Assign users to a menu

3. Choose a menu for a user by selecting a menu from the drop down Assigned Menu list.
4. Choose Save & apply.

Using the Configuration Menu

The configuration menu is available through a Telnet or SSH session to the root user and system administrator. The configuration menu enables the authorized users to configure the SERIMUX with the same functionality as is available with the web interface. The only functionality missing from the configuration menu is the ability to create custom menus.

The root user, by default, is connected from a Telnet session to the Linux command line. In order to access the configuration menu, the root user enters `configmenu` at the command prompt. The configuration menu follows the layout of the web interface.



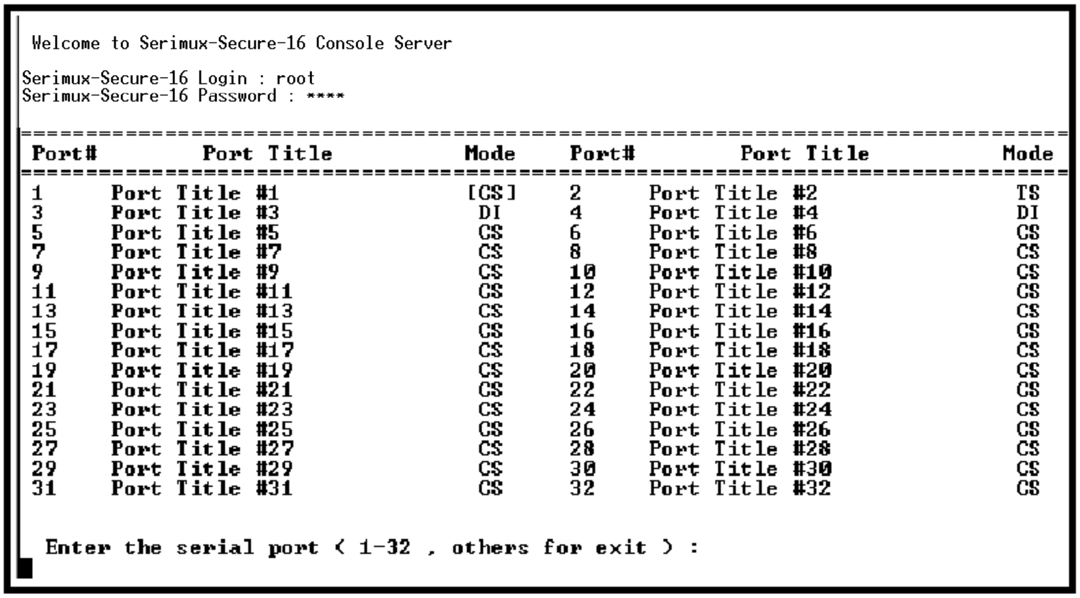
```
--------------------------------------------------------------------------------
 Welcome to Serimux-Secure-16 configuration page
 Current time : 06/24/2003 13:15:45      F/W REV.      : v1.1.2rc1
 Serial No.   : V32297115                MAC Address   : 00-40-9d-23-05-ec
 IP mode      : Static IP                IP Address    : 65.243.248.96
--------------------------------------------------------------------------------
 Select menu
 1. Network configuration
 2. Serial port configuration
 3. Clustering configuration
 4. PC Card configuration
 5. System Status & log
 6. System administration
 7. Save changes
 8. Exit without saving
 9. Exit and apply changes
 a. Exit and reboot
  <ENTER> Refresh
 ----->
```

Figure 53- The Configuration Menu

Choices for the configuration menu are made by selecting the number of a menu item. The ESC key allows the user to move back a menu each time it is selected. Sometimes only one menu item is presented; however, that single menu item has two or more options that have to be configured.

Port Access Menu

Another default menu is the Port Access Menu, which is available to all users. Access to this menu can be established through a Telnet or SSH session or through the web interface by selecting Serial ports > Connection > Port access menu connection.



```
 Welcome to Serimux-Secure-16 Console Server

Serimux-Secure-16 Login : root
Serimux-Secure-16 Password : ****

==============================================================================
 Port#          Port Title              Mode      Port#          Port Title              Mode
==============================================================================
 1      Port Title #1                   [CS]      2      Port Title #2                   TS
 3      Port Title #3                    DI       4      Port Title #4                   DI
 5      Port Title #5                    CS       6      Port Title #6                   CS
 7      Port Title #7                    CS       8      Port Title #8                   CS
 9      Port Title #9                    CS       10     Port Title #10                  CS
 11     Port Title #11                   CS       12     Port Title #12                  CS
 13     Port Title #13                   CS       14     Port Title #14                  CS
 15     Port Title #15                   CS       16     Port Title #16                  CS
 17     Port Title #17                   CS       18     Port Title #18                  CS
 19     Port Title #19                   CS       20     Port Title #20                  CS
 21     Port Title #21                   CS       22     Port Title #22                  CS
 23     Port Title #23                   CS       24     Port Title #24                  CS
 25     Port Title #25                   CS       26     Port Title #26                  CS
 27     Port Title #27                   CS       28     Port Title #28                  CS
 29     Port Title #29                   CS       30     Port Title #30                  CS
 31     Port Title #31                   CS       32     Port Title #32                  CS


  Enter the serial port ( 1-32 , others for exit ) :
```

Figure 54- The Port Access menu through the Configuration menu

Users access this menu through a Telnet or SSH session using the IP address of the SERIMUX followed by the port number 7000. Here is an example:

```
telnet 192.168.100.200 7000
```

By default root is connected to the command line interface and the preceding option allows the root user access to the port access menu.

Configuring Remote Dial-In Access

Introduction

The SERIMUX supports dial-in connections from remote sites for out-of-band access. In this configuration, the SERIMUX has serial ports configured for external modems and waits for dial-in connections from remote sites. If users dial-in using a terminal application, the SERIMUX accepts the connection and displays a menu of available serials ports. In a dial-in terminal server mode, the SERIMUX makes a TCP connection with either a Telnet or SSH client to a pre-defined server. RawTCP is also an option for dial-in users.

For more information on the different types of Host mode configuration, see "Host Mode Configuration" on page 15.

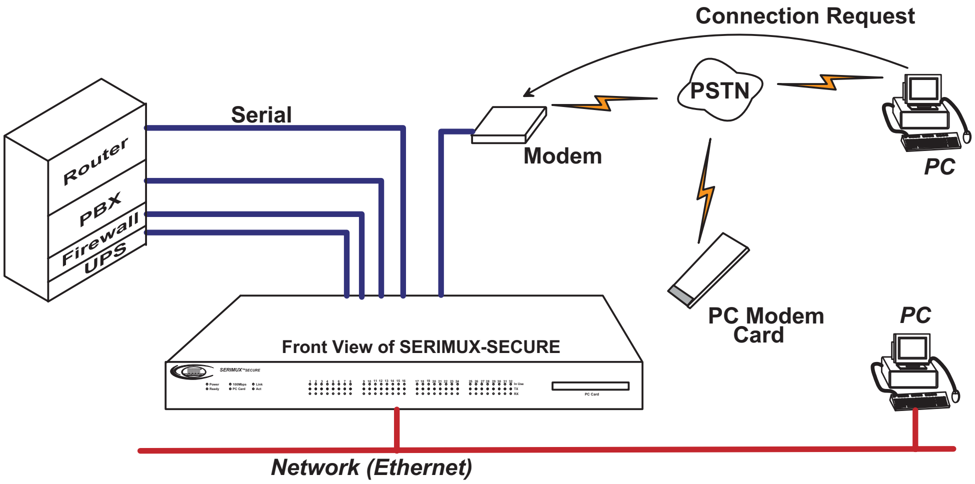
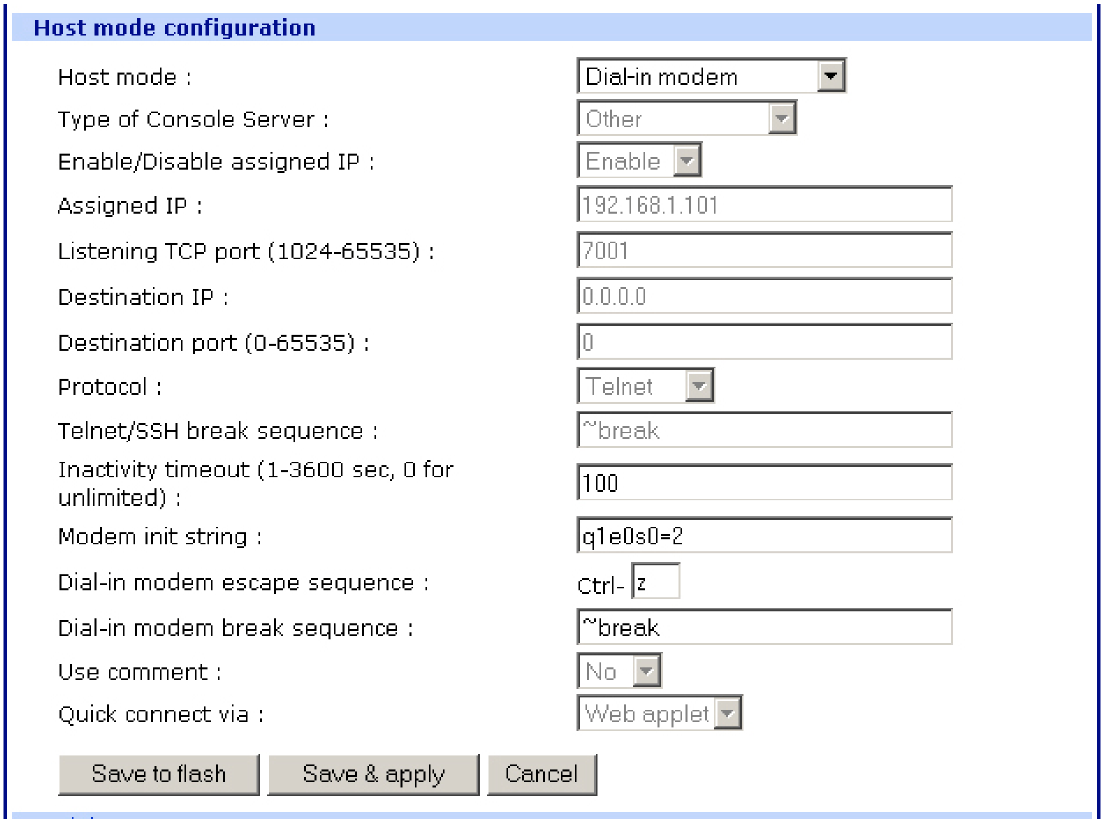


Figure 55- SERIMUX supports remote dial-in access for users

Configuring For Dial-In Modem Access

To configure a serial port for a dial-in modem, enter the values for these fields: Host mode, Modem init string, and Inactivity timeout. To access the Host mode configuration screen, do the following:

1. Access the web interface.
2. Under the Serial Port heading, choose Configuration.
3. Choose a specific port under Individual port configuration and then choose Host mode configuration.
4. Choose Dial-in modem for the Host mode.
5. Enter the information for Inactivity timeout and Modem init string.
   - **Inactivity timeout:** The default value is 100 seconds. You can set the timeout for 1 to 3600 seconds or 0, for unlimited timeout.
   - **Modem init string**: The default modem init string is q1e0s0=2. The init string sets the modem to quiet mode, echo off, and Auto Answer on two rings. The modem init string is used for initializing an external modem attached to a SERIMUX serial port. See your modem user manual for more information.
6. Choose Save & apply.



Host mode configuration

Host mode : Dial-in modem

Type of Console Server : Other

Enable/Disable assigned IP : Enable

Assigned IP : 192.168.1.101

Listening TCP port (1024-65535) : 7001

Destination IP : 0.0.0.0

Destination port (0-65535) : 0

Protocol : Telnet

Telnet/SSH break sequence : ~break

Inactivity timeout (1-3600 sec, 0 for unlimited) : 100

Modem init string : q1e0s0=2

Dial-in modem escape sequence : Ctrl- z

Dial-in modem break sequence : ~break

Use comment : No

Quick connect via : Web applet

Figure 56- Configure port for dial-in modem access

Adding a PC Modem

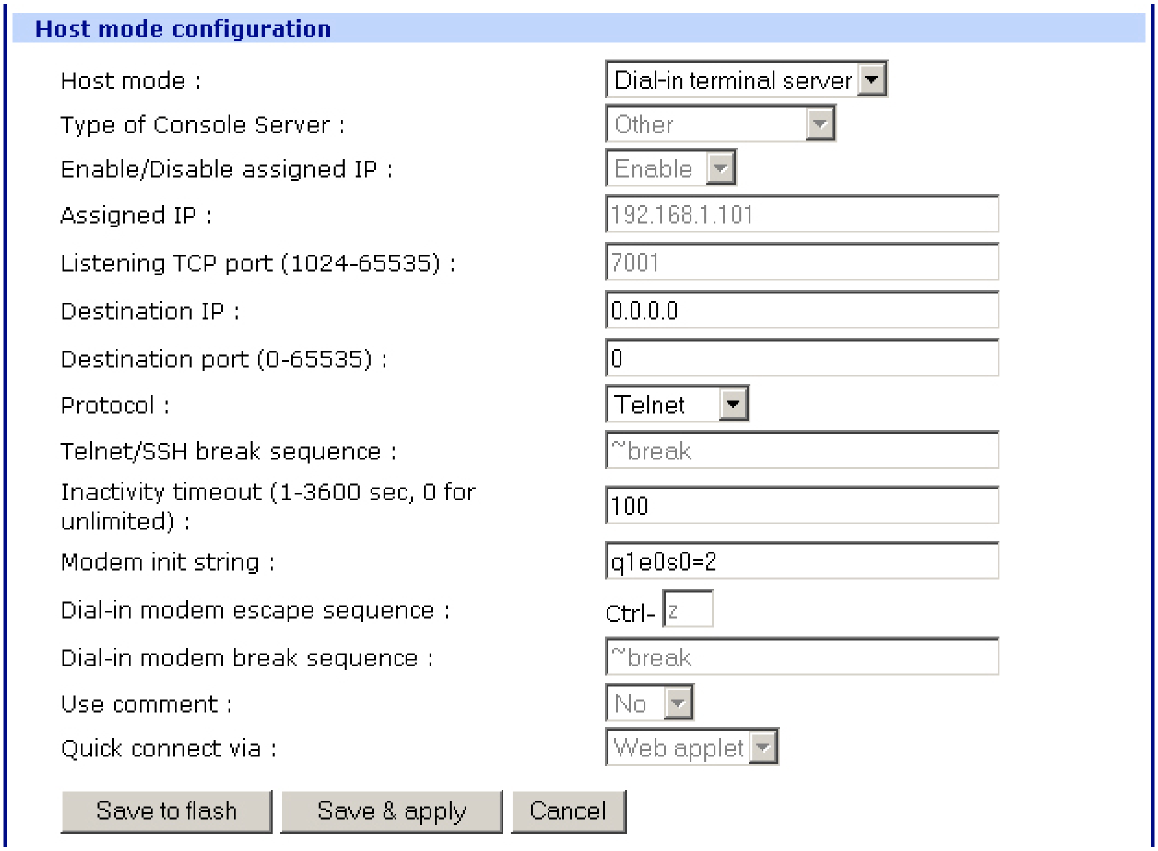
To install and configure the PC modem on the SERIMUX, do the following.

1. Insert the PC modem card into the PC slot.
2. Access the web interface.
3. From the menu, choose Configuration under the PC card heading.
4. Choose Discover a new card.
   The SERIMUX searches for a PC card and displays a configuration menu.
5. Enter the appropriate parameters in the configuration menu.
6. Choose Save & apply.

Configuring For Dial-In Terminal Server Access

To configure a serial port for a dial-in terminal server access, enter the values for these fields: Host mode, Destination IP, Base Port, Protocol, Inactivity timeout, and Modem init string. To access the Host mode configuration screen, do the following:

1. Access the web interface.
2. Under the Serial Port heading, choose Configuration.
3. Choose a specific port under Individual port configuration and then choose Host mode configuration.
4. Choose Dial-in terminal server for the Host mode.



Host mode configuration

Host mode :	Dial-in terminal server
Type of Console Server :	Other
Enable/Disable assigned IP :	Enable
Assigned IP :	192.168.1.101
Listening TCP port (1024-65535) :	7001
Destination IP :	0.0.0.0
Destination port (0-65535) :	0
Protocol :	Telnet
Telnet/SSH break sequence :	~break
Inactivity timeout (1-3600 sec, 0 for unlimited) :	100
Modem init string :	q1e0s0=2
Dial-in modem escape sequence :	Ctrl- z
Dial-in modem break sequence :	~break
Use comment :	No
Quick connect via :	Web applet

Figure 57- Configure port for dial-in terminal server access

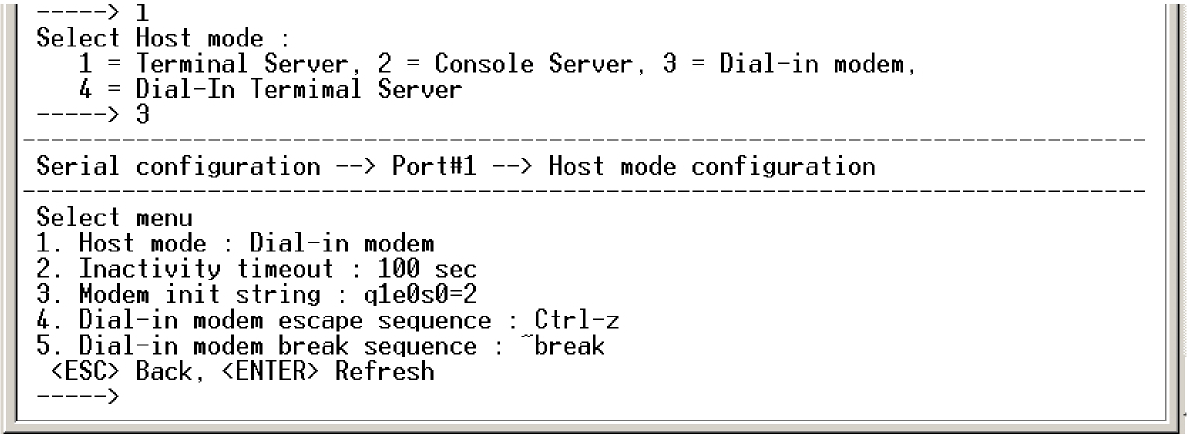
5. Fill in the appropriate fields as they apply to the configuration.
   - **Host mode:** The options are console server mode, terminal server mode, dial-in modem mode, and dial-in terminal server mode.
   - **Type of Console Server:** The options are MS SAC console or Other.
   - **Enable/Disable assigned IP:** Choose one
   - **Assigned IP:** This is also known as alternate IP, where the user can Telnet directly to a serial port using an IP address.
   - **Listening TCP port:** This is also known as reverse Telnet, where a user Telnets to a port using an IP address and a port number.
   - **Destination IP:** In terminal server mode, the user connects directly to a port using an IP address.
   - **Destination port:** In terminal server mode, the user connects directly to a port with an IP address and port number.
   - **Protocol:** The options are SSH, RawTCP, and Telnet.
   - **Telnet/SSH break sequence:** This is a sequence of characters that sends a break character to a device.
   - **Inactivity timeout:** The timeout length ranges from 1 to 3600 seconds; 0 is unlimited timeout.
   - **Modem init string:** Use the default string or enter a different string.
6. Choose Save & apply.

Using the Configuration Menu

Dial-in Modem Access

Individual serial ports on the SERIMUX can be configured for dial-in modem access. To use dial-in modem mode, an external modem is first attached to a serial port and then the serial port is configured for dial-in modem access. In the illustration below, port 7 is configured for a dial-in modem.

To configure a serial port for a dial-in modem, do the following:
1. Access the configuration menu.
2. Choose Serial port configuration.
3. Choose an individual port number and then Host mode configuration.



```
 -----> 1
 Select Host mode :
    1 = Terminal Server, 2 = Console Server, 3 = Dial-in modem,
    4 = Dial-In Termimal Server
 -----> 3
--------------------------------------------------------------------------------
 Serial configuration --> Port#1 --> Host mode configuration
--------------------------------------------------------------------------------
 Select menu
 1. Host mode : Dial-in modem
 2. Inactivity timeout : 100 sec
 3. Modem init string : q1e0s0=2
 4. Dial-in modem escape sequence : Ctrl-z
 5. Dial-in modem break sequence : ~break
  <ESC> Back, <ENTER> Refresh
 ----->
```

Figure 58- Use Configuration menu to configure port for dial-in modem access

4. Choose Dial-in modem and configure the other configuration parameters.
5. Use the ESC key to return to the main menu.
6. Choose Save changes.

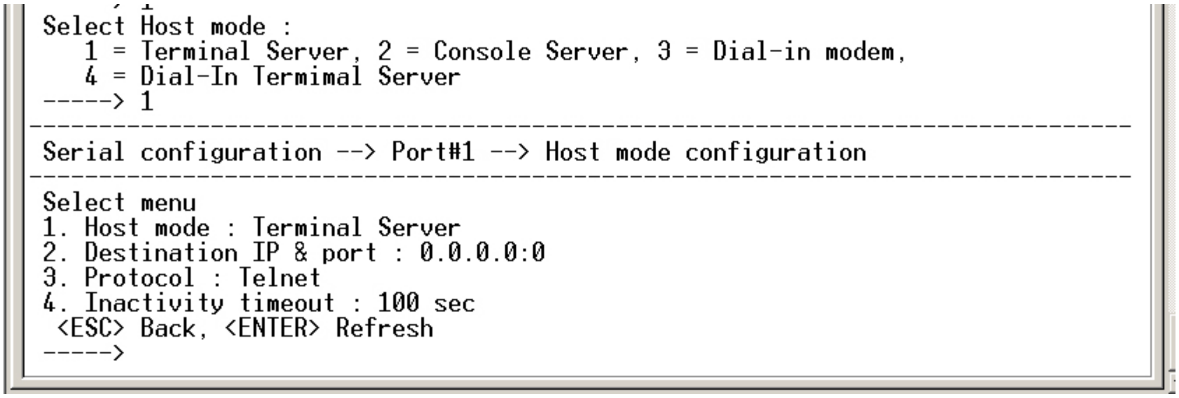
<u>Dial-in Terminal Server Access</u>

Individual serial ports on the SERIMUX can be configured for a dial-in terminal server access. To use dial-in terminal server access, an external modem is first attached to a serial port on the SERIMUX and then the serial port is configured for dial-in terminal server mode. In the illustration below, port 7 is configured for dial-in terminal server mode.

In terminal server mode, the user is connected directly to a server.

To configure a serial port for a dial-in terminal server, do the following:

1. Access the configuration menu.
2. Choose Serial port configuration.
3. Choose an individual port number and then Host mode configuration.



```
 Select Host mode :
    1 = Terminal Server, 2 = Console Server, 3 = Dial-in modem,
    4 = Dial-In Termimal Server
 -----> 1
--------------------------------------------------------------------------------
 Serial configuration --> Port#1 --> Host mode configuration
--------------------------------------------------------------------------------
 Select menu
 1. Host mode : Terminal Server
 2. Destination IP & port : 0.0.0.0:0
 3. Protocol : Telnet
 4. Inactivity timeout : 100 sec
  <ESC> Back, <ENTER> Refresh
 ----->
```

Figure 59- Use Configuration menu to configure port for dial-in terminal server access

4. Choose Terminal Server and configure the other configuration parameters.
5. Use the ESC key to return to the main menu.
6. Choose Save changes.

Port Clustering

Introduction

Port clustering is the ability to manage many serial ports on one or multiple slave devices from one master device using a single IP address. For instance, the SERIMUX can manage up to 16 slave devices or a maximum 544 serial ports with one Master device. Ports can be configured either collectively or individually depending on user preference. Each master and slave device is configured separately; they cannot be configured from one master console.

To set up the SERIMUX for port clustering you will need to:

- Configure all SERIMUX serial ports
- Assign one SERIMUX as the master clustering device; all other SERIMUXs default to slave devices.
- Import slave configuration to the SERIMUX master device

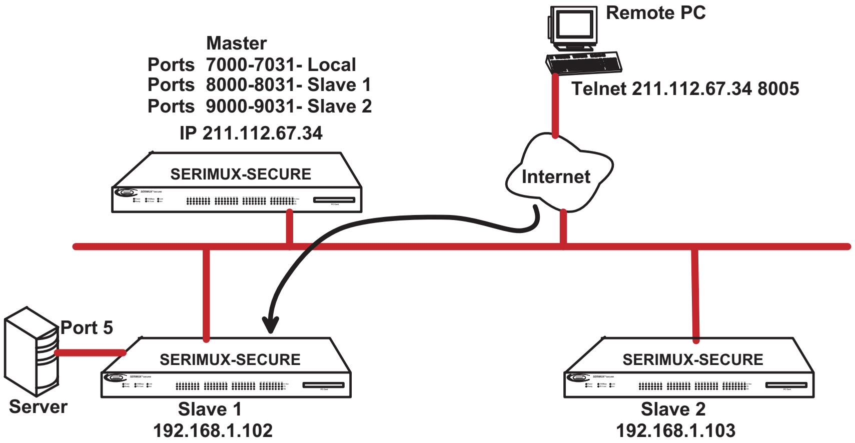


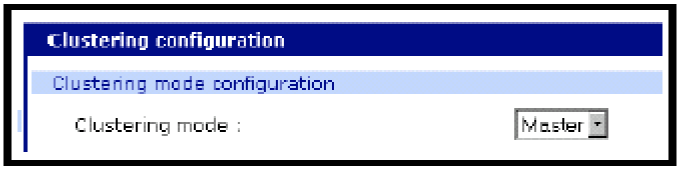
Figure 60- SERIMUX used for port clustering

Configuring Port Clustering

Assigning Master Clustering Mode

To assign a SERIMUX as the master cluster device, do the following:

1. Access the SERIMUX through the web interface. This SERIMUX needs to be the unit to be used as the Master.
2. Under the Clustering heading, choose Configuration.
3. Choose Master from the drop down menu.
   Subsequent units will be configured in Slave mode by default.
4. Choose Save & apply.


Clustering configuration

Clustering mode configuration

Clustering mode : Master

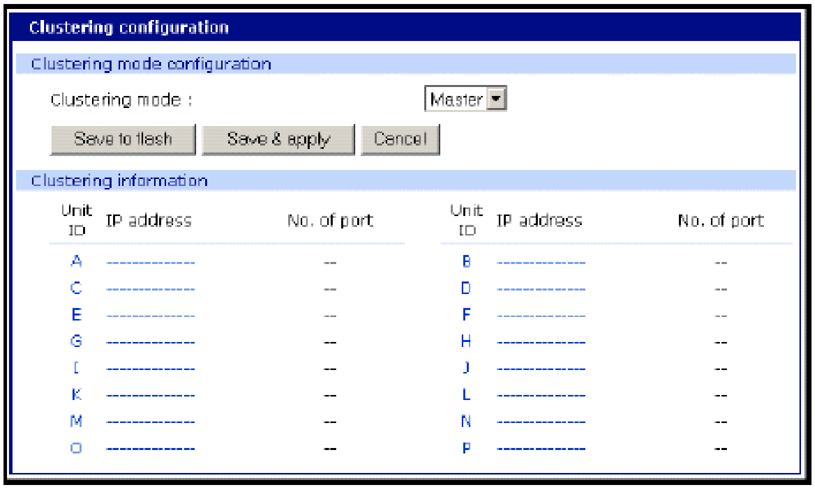
Figure 61- Assign the Master cluster device

Configuring Slave Ports on the Master Unit

Ports on slave units are automatically enabled and set to the Telnet protocol. To disable some or all of the ports or to use a different protocol, make these changes to the slave units before performing the autoconfigure on the slave ports on the master unit.

To configure the slave serial ports on the master unit, do the following:

1. Access the SERIMUX through the web interface.
2. Under the Clustering heading, choose Configuration.
3. Select the hyperlinked number under Unit ID or the dashed line under IP address.



Clustering configuration

Clustering mode configuration

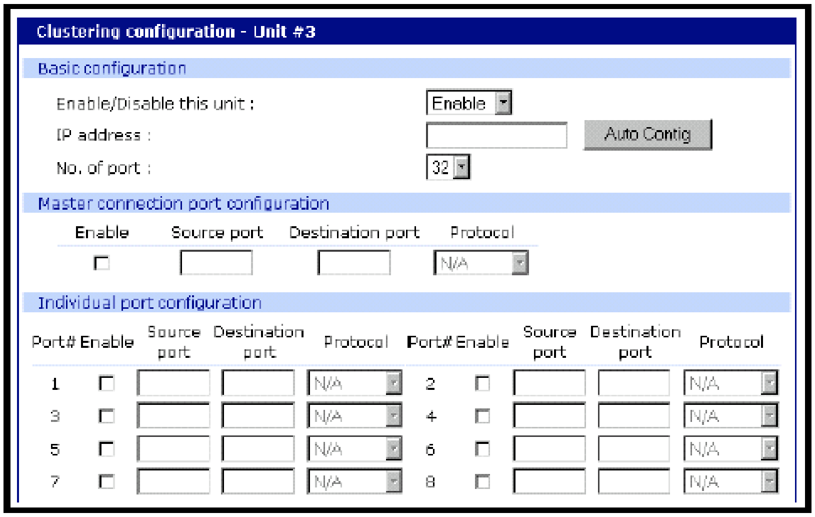
Clustering mode : Master

Clustering information

Unit ID	IP address	No. of port	Unit ID	IP address	No. of port
A	--------------	--	B	--------------	--
C	--------------	--	D	--------------	--
E	--------------	--	F	--------------	--
G	--------------	--	H	--------------	--
I	--------------	--	J	--------------	--
K	--------------	--	L	--------------	--
M	--------------	--	N	--------------	--
O	--------------	--	P	--------------	--

Figure 62- Configure Slave ports on the Master Unit

.4. Select Enable from the "Enable/Disable this unit" drop down menu.
A new configuration screen appears.



Clustering configuration - Unit #3

Basic configuration

Enable/Disable this unit : Enable

IP address :

No. of port : 32

Master connection port configuration

Enable	Source port	Destination port	Protocol
□			N/A

Individual port configuration

Port#	Enable	Source port	Destination port	Protocol	Port#	Enable	Source port	Destination port	Protocol
1	□			N/A	2	□			N/A
3	□			N/A	4	□			N/A
5	□			N/A	6	□			N/A
7	□			N/A	8	□			N/A

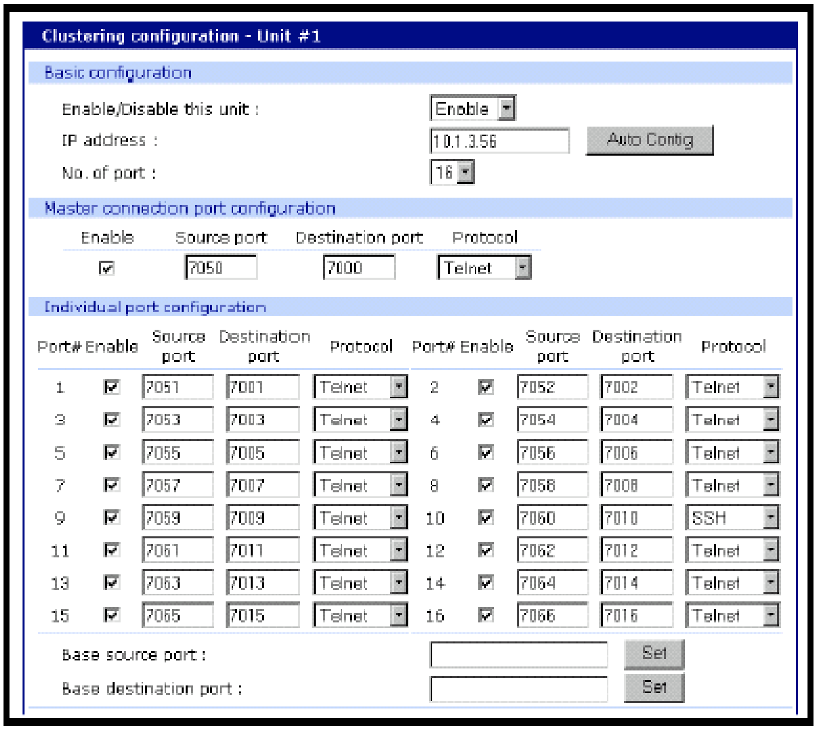
Figure 63- Enable a Slave unit and setup the port information

5. Enter the IP address of the slave unit in the IP address field.
6. Select the Auto Config button and the Master SERIMUX automatically imports the configuration of the Slave serial ports to the Master SERIMUX. The following figure displays serial port configuration imported from a slave unit.
7. Choose Save & apply.

Clustering Parameters

Below is a list and brief description of clustering parameters:

- **Enable:** This shows whether the port is enabled or disabled. All ports are enabled by default.
- **Source port:** This is the port number on the master unit.
- **Destination port:** The destination port is the corresponding port number on the slave unit. On a 32-port slave unit, the destination port numbers range from 7001 to 7032.
- **Protocol**: The four options are N/A (not available), SSH, Telnet, and RawTCP.
- **Base source port:** This sets the first port number on a master unit. By default the base source port on the master unit is 7001. However, the user can change the base source port number to another number and the rest of the ports on the unit will be sequentially numbered from the base source port. For example, starting the base source port number with 7010 results in a 32-port unit being numbered from 7010 to 7041.



Clustering configuration - Unit #1

Basic configuration

Enable/Disable this unit :	Enable	
IP address :	10.1.3.56	Auto Config
No. of port :	16	

Master connection port configuration

Enable	Source port	Destination port	Protocol
☑	7050	7000	Telnet

Individual port configuration

Port#	Enable	Source port	Destination port	Protocol	Port#	Enable	Source port	Destination port	Protocol
1	☑	7051	7001	Telnet	2	☑	7052	7002	Telnet
3	☑	7053	7003	Telnet	4	☑	7054	7004	Telnet
5	☑	7055	7005	Telnet	6	☑	7056	7006	Telnet
7	☑	7057	7007	Telnet	8	☑	7058	7008	Telnet
9	☑	7059	7009	Telnet	10	☑	7060	7010	SSH
11	☑	7061	7011	Telnet	12	☑	7062	7012	Telnet
13	☑	7063	7013	Telnet	14	☑	7064	7014	Telnet
15	☑	7065	7015	Telnet	16	☑	7066	7016	Telnet

Base source port : Set

Base destination port : Set

Figure 64- Setup clustering parameters

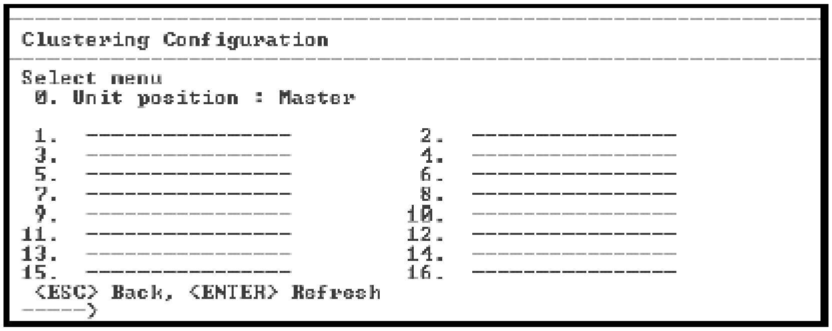
- **Base destination port:** This is the physical port number on a remote slave unit. By default the base destination port on the first slave unit is 7001. However, the user can change the base destination port number to another number and the rest of the ports on the unit will be sequentially numbered from the base destination port. For example, starting the base destination port number with 7010 results in a 32-port unit being numbered from 7010 to 7041.

Using the Configuration Menu

Clustering

By default clustered slave devices are configured using the Telnet protocol and port parameters of the following: bps=9600, data bits=8, parity=none, stop bits=1, flow control=none. When the master device autoconfigures a slave device, it simply imports the information from the slave unit. If other protocols or other port parameters are desired, configure the slave unit first with those parameters before autoconfiguring. Before starting this configuration procedure, the slave units should already be configured unless they are to be set to the default values. To set up the SERIMUX for clustering, do the following:

1. Access the configuration menu.
2. Choose Clustering configuration > Unit position.
3. Assign the unit as the master device.
   A new screen is displayed.



```
------------------------------------------------------------------
Clustering Configuration
------------------------------------------------------------------
Select menu
 0. Unit position : Master

 1.  ----------------          2.  ----------------
 3.  ----------------          4.  ----------------
 5.  ----------------          6.  ----------------
 7.  ----------------          8.  ----------------
 9.  ----------------         10.  ----------------
11.  ----------------         12.  ----------------
13.  ----------------         14.  ----------------
15.  ----------------         16.  ----------------
 <ESC> Back, <ENTER> Refresh
----->
```

Figure 65- Setup clustering using Configuration menu

4. Enter the number 1 for the first slave unit.
5. Choose Enable/Disable unit clustering > Enable.
6. Enter the values for Slave Unit IP, No. of ports, and Port configuration.
7. Choose ESC to return to the main menu.
8. Choose Exit and apply changes.

Command Line Interface

Introduction

The SERIMUX runs the embedded Linux Hard Hat operating system. The command line interface for configuration purposes is accessible only by the root user. The system administrator has read only privileges from the command line. By default the root user is connected to the CLI (command line interface) when Telnetting to the SERIMUX. To gain access to the command prompt, the root user uses the username **root** and the root password. The default root password is **dbps**.

This chapter includes the Linux commands available on the embedded Linux operating system and the location of files useful to the root user for administrative purposes.

Note: The root user should be aware that deleting or corrupting files may prevent the SERIMUX from booting properly. Before editing any files, be sure to back up the configuration files.

Linux Commands

The purpose of this section is to list the various Linux commands available on the SERIMUX. This is simply a listing of commands and does not detail what the commands do or give their particular parameters. If more information is needed, see the man pages on a Linux system.

Two commands that are very important for saving and applying changes to the configuration files are:

- **`saveconf`:** The saveconf command saves the configuration files to flash memory.
- **`applyconf`:** The applyconf command immediately applies the configuration changes.

The configuration files are located in /tmp/cnf directory.

Two system utility menus that are important for configuring the SERIMUX and the serial ports are the `portaccessmenu` and `configmenu.`

- **`portaccessmenu`:** This menu allows the user to configure the serial ports on a SERIMUX.
- **`configmenu`:** This menu enables the system administrator to configure the SERIMUX. It has essentially the same functionality as the web interface for configuring a unit with the exception of the ability to create custom menus.

Shell and Shell Utilities

sh	ash	bash	echo	sed
env	false	grep	more	which
pwd				

File and Disk Utilities

ls	cp	mv	rm	mkdir
rmdir	ln	mknod	chmod	touch
sync	gunzip	gzip	zcat	tar
dd	df	du	find	cat
vi	tail	mkdosfs	mke2fs	e2fsck
fsck	mount	umount	scp	

System Utilities

date	free	hostname	sleep	stty
uname	reset	insmod	rmmod	lsmod
modprobe	kill	killall	ps	half
shutdown	poweroff	reboot	telnet	init
useradd	userdel	usermod	whoami	who
id	su			

Network Utilities

ifconfig	iptables	route	telnet	ftp
ssh	ping			

Important File Locations

The SERIMUX has several files that are important for administrative use. Below is a brief listing of some files that the root user or system administrator might desire to either monitor or edit.

Default Script

The default script file is executed whenever the SERIMUX is booted. The file is /usr/rc.user and can be modified with the vi editor. The modified script becomes effective when the system is rebooted.

Booting Sequence

When the SERIMUX boots, it uncompresses the /cnf/cnf.tar.gz file to /tmp/cnf/* and unmounts the /cnf file. If the configuration files are modified in the /tmp/cnf file and the configuration is saved to flash (saveconf), the unit mounts the /cnf file and compresses the /tmp/cnf/* to /cnf/cnf.tar.gz.

User Storage Space

The SERIMUX comes with 1 megabyte of user storage space. This storage space can be used to store custom scripts. The location is /usr2.

System Administration

Introduction

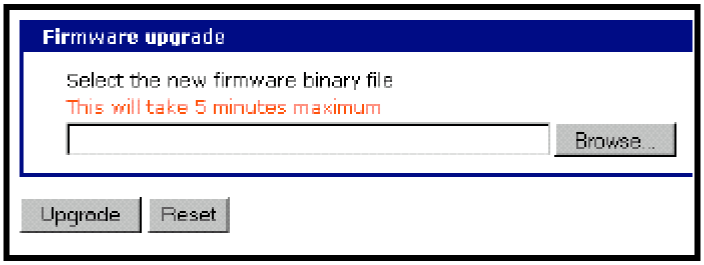
This chapter describes how to perform tasks performed either by root or the system administrator. These tasks fall under the general heading of system administration and include firmware upgrades, resetting the unit to defaults, and disaster recovery procedures.

Upgrading the Firmware

Web Interface

It will be necessary to download the latest firmware version to a system on the same subnet as the SERIMUX. The latest firmware can be downloaded from the SERIMUX support site at: http://www.nti1.com. Do the following to upgrade the firmware:

1. Access the web interface.
2. Under the System administration heading, choose Firmware upgrade.
3. Choose the Browse button and locate the firmware download.
4. Choose Upgrade. The SERIMUX will automatically reboot when the upgrade is complete.



Firmware upgrade

Select the new firmware binary file

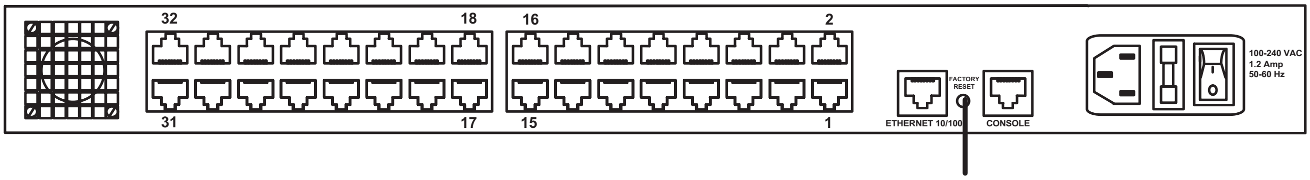
This will take 5 minutes maximum

Figure 66- Locate the firmware upgrade file

Resetting Factory Defaults

There are two ways to reset the unit to the factory defaults. The quickest and simplest method is to push and hold the hardware factory default reset button until the Ready light on the front panel goes out. The reset button is located on the back panel of the unit next to the Ethernet port.

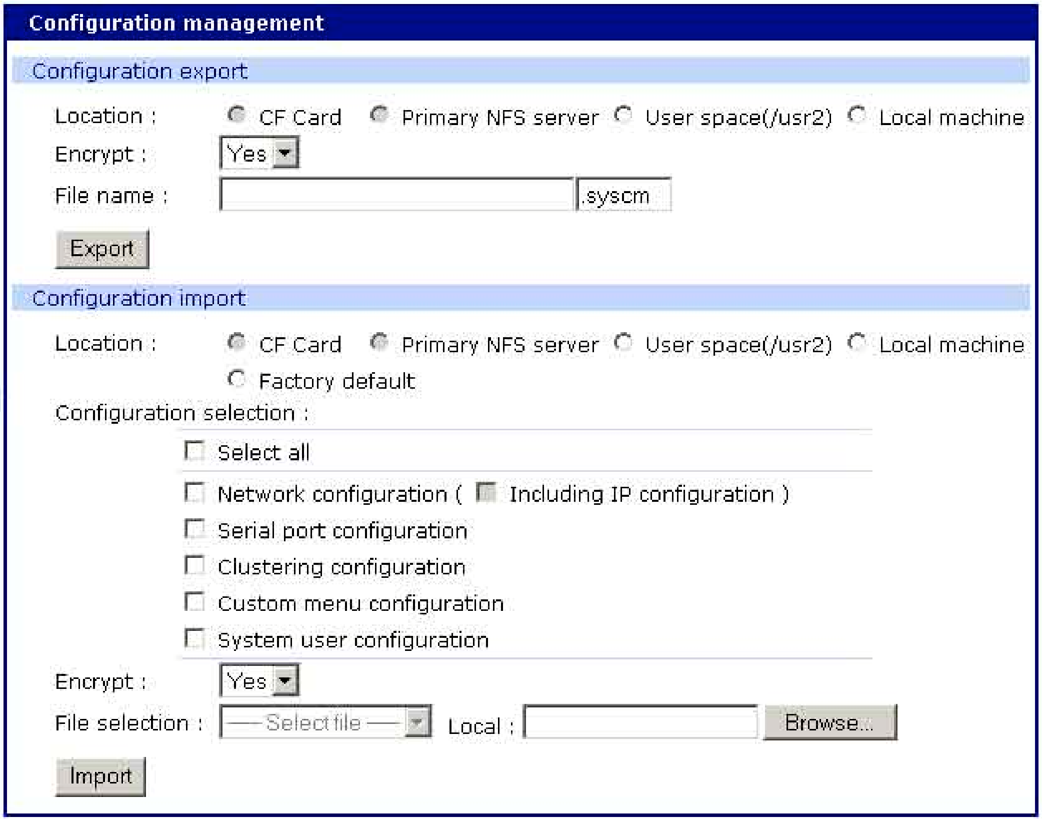
Rear View of SERIMUX-SECURE



Factory reset button

Figure 67- Reset factory defaults

The alternative method to reset the unit is through the web interface. The web interface provides the option of retaining the IP settings. To use the web interface to reset the SERIMUX, do the following:
1. Access the web interface.
2. Under the System administration heading choose Configuration Management.



Configuration management

Configuration export

Location : ○ CF Card ○ Primary NFS server ○ User space(/usr2) ○ Local machine

Encrypt : Yes

File name : .syscm

Configuration import

Location : ○ CF Card ○ Primary NFS server ○ User space(/usr2) ○ Local machine ○ Factory default

Configuration selection :

□ Select all

□ Network configuration (□ Including IP configuration)

□ Serial port configuration

□ Clustering configuration

□ Custom menu configuration

□ System user configuration

Encrypt : Yes

File selection : —— Select file —— Local :

Figure 68- Reset factory defaults through web interface

3. Choose Factory default under Configuration import.   The SERIMUX will automatically reboot.

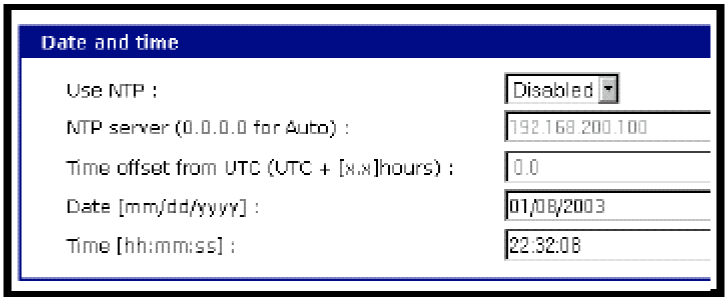
Suggestion: It may be desired to save the current configuration before restoring defaults.   If this is the case, instead of Configuration import, select a desired location to save the configuration file to (i.e. Local machine) under Configuration export, type a desired file name in the block provided, and export the existing configuration to a desired location for future reference.

The following are the default values when the SERIMUX is reset to the factory defaults.

- Static IP Address: 192.168.161.5
- Port Access Menu IP Address: 192.168.1.100
- Port Access Menu TCP Port Number: 7000
- Serial Port IP Address: 192.168.1.101-
- Serial Port TCP Port Number: 7001-

Setting Date and Time

The SERIMUX provides two options for keeping system time. The first is by using an NTP server and the other is through an internal battery backup. To configure the SERIMUX for date and time, do the following:
1. Access the web interface.
2. Under the System administration heading, choose Date and time.



Date and time

Use NTP : Disabled

NTP server (0.0.0.0 for Auto) : 192.168.200.100

Time offset from UTC (UTC + [x.x]hours) : 0.0

Date [mm/dd/yyyy] : 01/08/2003

Time [hh:mm:ss] : 22:32:08

Figure 69- Set the date and time

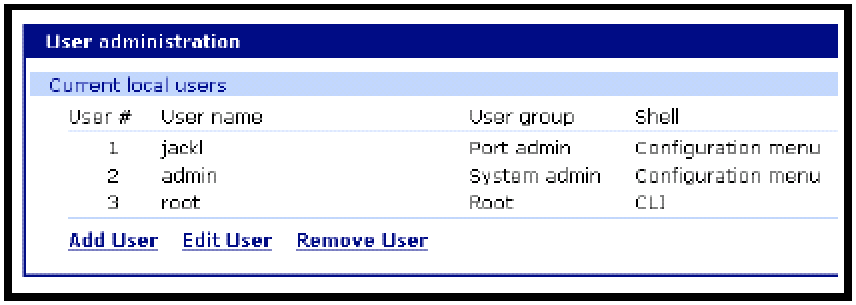
3. To use an NTP server, choose Enable, the NTP server's IP address, the Time offset, and the Date and Time fields.
 or
 To use the internal battery fill in the Date and Time fields only.
4. Choose Save & apply.

Configuring A Device Name

The system administrator can assign a device name to the SERIMUX. This is often helpful for administration purposes to locate a specific SERIMUX on the network. To assign the SERIMUX a device name, do the following:
1. Access the web interface.
2. Under the System administration heading, choose Device name.
3. Enter the name you want to assign the SERIMUX.
4. Choose Save & apply.

Adding, Editing, and Removing Users

The system administrator can add, remove, or edit user files easily from the web interface by doing the following:
1. Access the web interface.
2. Under the System administration heading, choose Users administration.



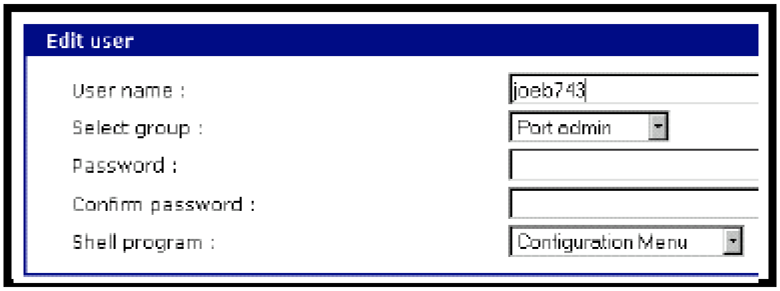
User administration

Current local users

User #	User name	User group	Shell
1	jackl	Port admin	Configuration menu
2	admin	System admin	Configuration menu
3	root	Root	CLI

Figure 70- Administrator's user administration window

3. Choose to Add User, Edit User, or Remove User:
   - **Add a user:** Assign a name, user group, and a password.
   - **Edit user files**: Change user group, password, or their shell.
   - **Remove a user**: Remove a user from the system.



Edit user

User name :	joeb743
Select group :	Port admin
Password :	
Confirm password :	
Shell program :	Configuration Menu

Figure 71- Edit a user

Note: The password for root can be changed from the command line interface only using the command passwd.

4. Choose Save & apply.

Using the Configuration Menu

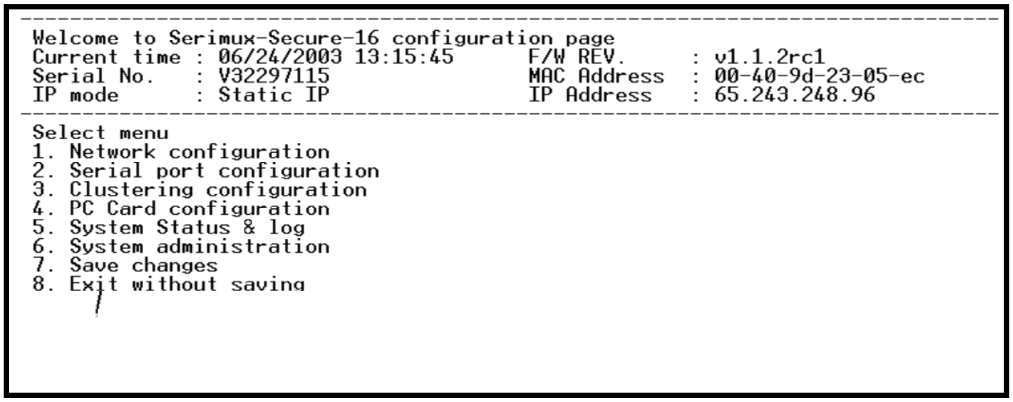
Firmware Upgrade

Before upgrading firmware from the configuration menu it is necessary to:

- Download the firmware to a system on the same subnet
- Set up a terminal emulation program that supports Zmodem transfer protocol

To upgrade the firmware with the configuration menu, do the following:

1. Access the configuration menu.



```
 ------------------------------------------------------------------------------
  Welcome to Serimux-Secure-16 configuration page
  Current time : 06/24/2003 13:15:45       F/W REV.      : v1.1.2rc1
  Serial No.   : V32297115                 MAC Address   : 00-40-9d-23-05-ec
  IP mode      : Static IP                 IP Address    : 65.243.248.96
 ------------------------------------------------------------------------------
  Select menu
  1. Network configuration
  2. Serial port configuration
  3. Clustering configuration
  4. PC Card configuration
  5. System Status & log
  6. System administration
  7. Save changes
  8. Exit without saving
```

Figure 72- Configuration menu

2. Choose System administration.
3. Choose Firmware upgrade. Enter y for Yes when asked if the user wants to upgrade the firmware.

If the firmware upgrade is successful, the SERIMUX will reboot automatically. If a **Firmware upgrade failed!** warning appears, do not reboot the unit but repeat the upgrade process.

Restoring Factory Defaults

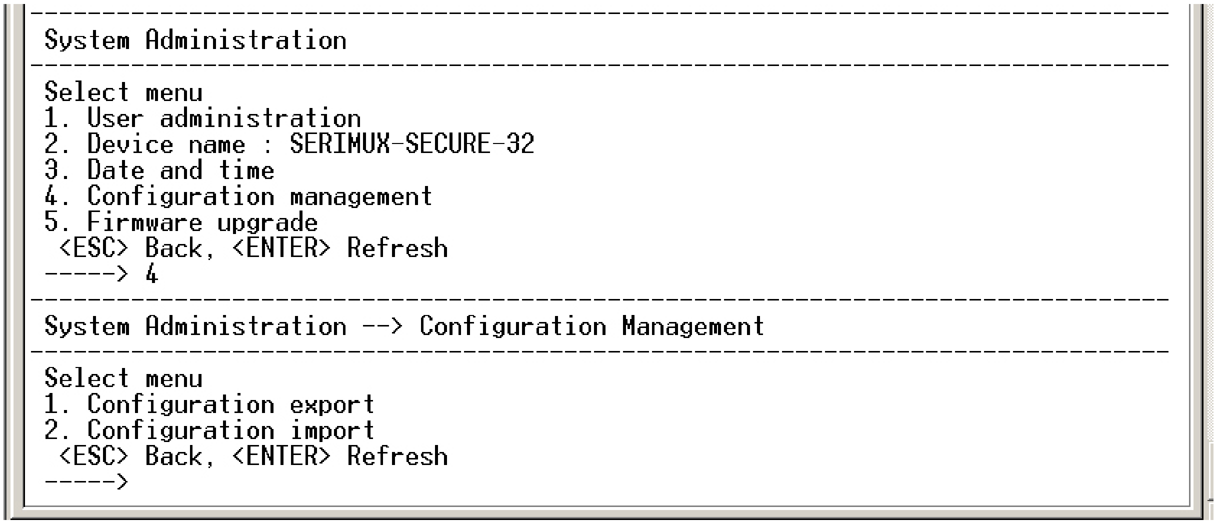
You have 5 choices to restore the unit to its factory defaults. They are to restore:

- Network configuration
- Serial port configuration
- Clustering configuration
- System user configuration
- Custom menu

All of the defaults can be selected, or only those that need to be reset to default while leaving the other settings unchanged.

To restore the unit to the factory defaults, do the following:

1. Access the Configuration menu.
2. Choose System administration.
3. Choose Configuration management.



```
-------------------------------------------------------------------------------
 System Administration
-------------------------------------------------------------------------------
 Select menu
 1. User administration
 2. Device name : SERIMUX-SECURE-32
 3. Date and time
 4. Configuration management
 5. Firmware upgrade
  <ESC> Back, <ENTER> Refresh
 -----> 4
-------------------------------------------------------------------------------
 System Administration --> Configuration Management
-------------------------------------------------------------------------------
 Select menu
 1. Configuration export
 2. Configuration import
  <ESC> Back, <ENTER> Refresh
 ----->
```

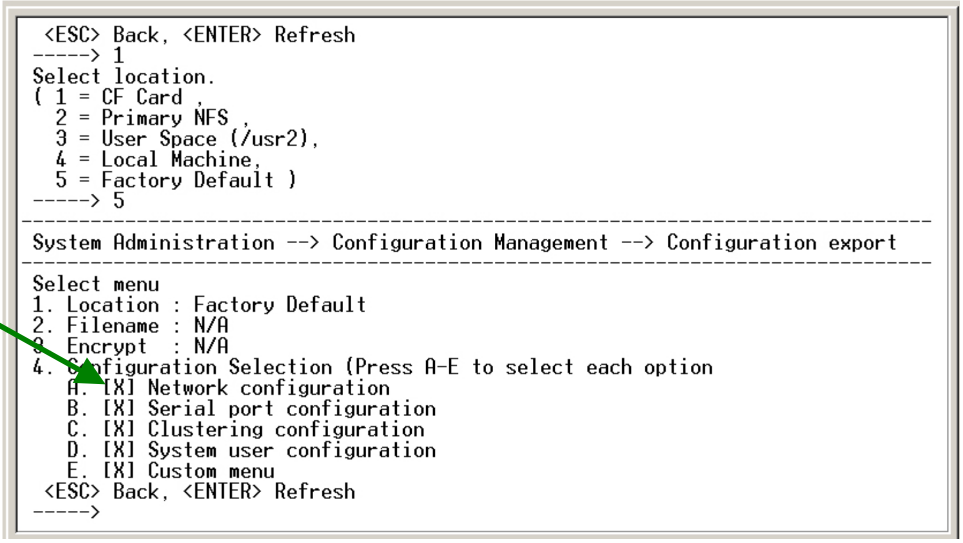
Figure 73- Reset factory defaults through Configuration menu

4. Choose Configuration import.
5. Choose one or more selection to be reset to defaults.

Press A to toggle the Network Configuration to be restored. You will be prompted to import Network configuration with or without the IP configuration, or not to Import the network configuration at all with this function.
Press B to toggle the Serial port to be restored,
Press C to toggle the Clustering configuration to be restored, and so on.

6. When finished selecting defaults to be restored, press 0 to restore chosen defaults. You will be prompted to confirm this action by pressing Y for yes, or N for no.

The system will restore factory defaults, and the unit will automatically reboot.



```
 <ESC> Back, <ENTER> Refresh
-----> 1
Select location.
( 1 = CF Card ,
  2 = Primary NFS ,
  3 = User Space (/usr2),
  4 = Local Machine,
  5 = Factory Default )
-----> 5
-------------------------------------------------------------------------------
System Administration --> Configuration Management --> Configuration export
-------------------------------------------------------------------------------
Select menu
1. Location : Factory Default
2. Filename : N/A
3. Encrypt  : N/A
4. Configuration Selection (Press A-E to select each option
   A. [X] Network configuration
   B. [X] Serial port configuration
   C. [X] Clustering configuration
   D. [X] System user configuration
   E. [X] Custom menu
 <ESC> Back, <ENTER> Refresh
----->
```

An "X" indicates no selection, while an "O" indicates the item is selected for restoration of factory default settings.

Figure 74- Choose which factory defaults to reset

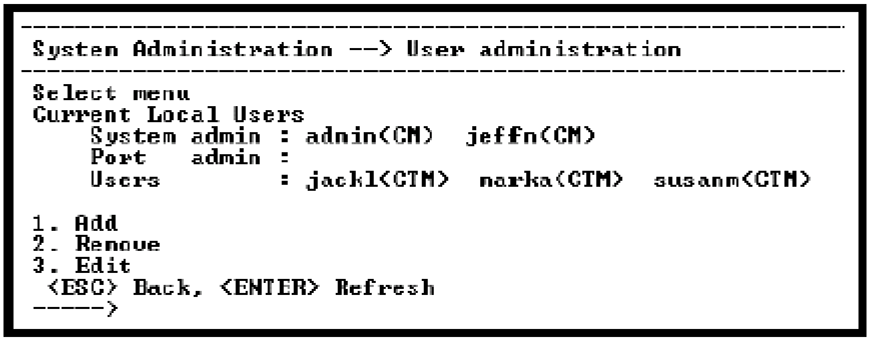
<u>Setting Date and Time</u>

Date and time on the SERIMUX can either be kept internally or by an NFS server. To set the parameters for date and time on the SERIMUX, do the following:
1. Access the configuration menu.
2. Choose System administration.
3. Choose Date and Time.
4. Enter the desired parameters.
5. Choose Save changes.

<u>Adding, Editing, and Removing Users</u>

1. Access the configuration menu.
2. Choose System administration > User Administration.
3. Choose Add, Remove, or Edit.

Users and the user groups are conveniently listed at the top of the configuration screen. The options are:
- **Add a user:** Assign a name, user group, and a password
- **Edit user files:** Change user group, password, or their shell
- **Remove a user:** Remove a user from the system



```
------------------------------------------------------------
System Administration --> User administration
------------------------------------------------------------
Select menu
Current Local Users
     System admin : admin(CM)   jeffn(CM)
     Port   admin :
     Users        : jackl(CTM)   marka(CTM)   susanm(CTM)

1. Add
2. Remove
3. Edit
 <ESC> Back, <ENTER> Refresh
----->
```

Figure 75- Edit users through Configuration menu

4. Choose Save changes.

Accessing the Boot Loader Program

The Boot Loader program can be accessed during the boot process. The main function of the program is to provide a backup means for restoring the firmware if the SERIMUX will no longer boot. It also provides a hardware testing module that detects and tests hardware components on the unit.

To access the Boot Loader program, do the following:

1. Connect the Ethernet cable from the console port on the rear panel of the SERIMUX to a serial port on a workstation. Use the Ethernet cable packaged with the SERIMUX and attach the DB-9 adapter.
2. Set up a terminal emulation program, such as HyperTerminal, using the following port parameters: bps=9600, data bits=8, parity=none, stop bits=1, and flow control=none.
3. Turn the power ON to the unit.
4. Press ESC within 3 seconds of booting the unit to get a command prompt.
5. Enter the username **admin** and the default password **admin** to access the Boot Loader menu.

Hardware Test Menu

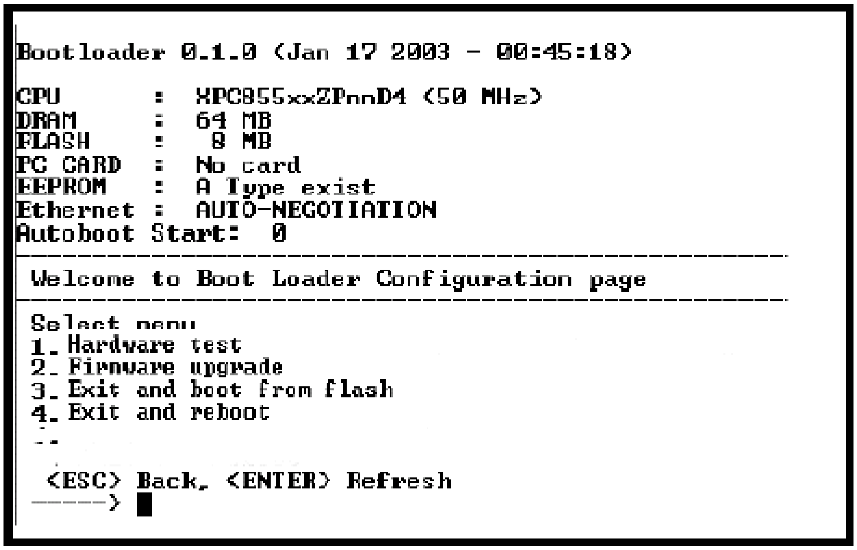
The Boot Loader program provides a hardware test for detecting and testing hardware components on the SERIMUX. From the Boot Loader menu, choose the number 3 to access the Hardware test. Options for several components appear.

Disaster Recovery

The SERIMUX provides a disaster recovery procedure in the event the configuration data is destroyed or corrupted. The SERIMUX automatically restores a corrupted configuration file system to the factory default settings. However, if the SERIMUX fails to boot in spite of being reset to the factory default settings, the firmware can be restored by using the Boot Loader program. To restore the SERIMUX to the factory default configuration settings, the user must use a TFTP or BOOTP server. To use the Boot Loader program to flash new firmware, do the following:

1. Connect the console port on the rear panel of the SERIMUX to a serial port on a workstation. Use an Ethernet cable with a DB-9 adapter.
2. Set up a terminal emulation program such as HyperTerminal. Use the following port parameters: bps=9600, data bits=8, parity=none, stop bits=1, flow control=none
3. Reboot or power ON the SERIMUX.
4. Press the ESC key within three seconds of applying power to the device.

The following screen appears.

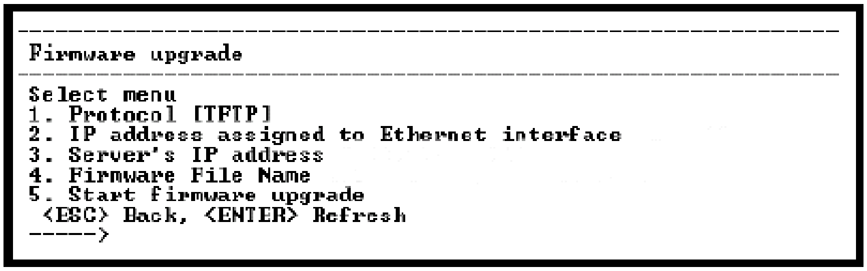


```
Bootloader 0.1.0 (Jan 17 2003 - 00:45:18)

CPU       :  XPC855xxZPnnD4 (50 MHz)
DRAM      :  64 MB
FLASH     :   8 MB
PC CARD   :  No card
EEPROM    :  A Type exist
Ethernet  :  AUTO-NEGOTIATION
Autoboot Start:  0
------------------------------------------------------------
 Welcome to Boot Loader Configuration page
------------------------------------------------------------
 Select menu
 1. Hardware test
 2. Firmware upgrade
 3. Exit and boot from flash
 4. Exit and reboot

  <ESC> Back, <ENTER> Refresh
 -----> 
```

Figure 76- The Boot Loader program

5. Choose Firmware upgrade by entering 2.

The following screen appears.



```
------------------------------------------------------------
 Firmware upgrade
------------------------------------------------------------
 Select menu
 1. Protocol [TFTP]
 2. IP address assigned to Ethernet interface
 3. Server's IP address
 4. Firmware File Name
 5. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 ----->
```

Figure 77- Firmware upgrade via Boot Loader program

Note: Use the ESC key to back up to earlier menu screens.

6. Enter the information for the first menu items.
   - **Protocol:** The choices are BOOTP or TFTP
   - **IP address assigned:** Enter the IP address of the SERIMUX
   - **Server's IP address:** The IP address of the BOOTP or TFTP server
   - **Firmware File Name:** The filename for the firmware

7. Choose Start firmware upgrade.
The firmware upgrade will take several minutes to process.
8. When the upgrade process is complete, choose ESC to return to the main menu.
9. Choose Exit and boot from flash.

Microsoft SAC Support

About SERIMUX Support for Microsoft Windows Server 2003

The SERIMUX provides a browser-based user interface to Microsoft's text-based Special Administration Console (SAC), an integral part of Windows Server 2003 Emergency Management Services (EMS). When a server running Windows Server 2003 is connected to a SERIMUX serial port, key SAC functions--normally accessed from the command line--are available from a graphical user interface (GUI). SAC features accessible from this interface include:

- Reset and shutdown
- Show ID
- Show and configure IP settings per interface
- Show the process list and kill processes

Note: While the EMS port is available at all times using Telnet or SSH, the special GUI is available only while SAC is active.

Set Up Overview

Set up for SERIMUX SAC support is a three-step process:

1. Set up the Windows Server 2003 for SAC support. To do this, ensure that the COM port used for console traffic is properly set up. This includes designating a COM port for console communication and setting the port speed (baud) appropriately. (See the next topic below.)
2. Cable the console port on the Windows Server 2003 to a SERIMUX port. See the cabling information on page 56.
3. Set up the SERIMUX for SAC support. See "Setting Up the SERIMUX for SAC Support" on page 52.

Setting Up the Windows Server 2003 Port

1. Sign on to the Windows Server 2003 as the administrator.
2. Access the command line.
3. Use the bootcfg command to redirect console traffic to the correct COM port. The following is the command syntax and an example. See the Microsoft documentation for additional information on the SAC feature.

Command Syntax

```
bootcfg /ems on /port com# /id # /baud 115200
```

where *com#* is the COM port to which console traffic will be redirected, # is the is the number of the boot entry, and the port speed is set to the SERIMUX recommended rate (although any rate supported by Windows Server 2003 can be used).

Command Example

In this example, console output is redirected to COM 2, the boot entry is specified as 1, and the port speed set to 115200.

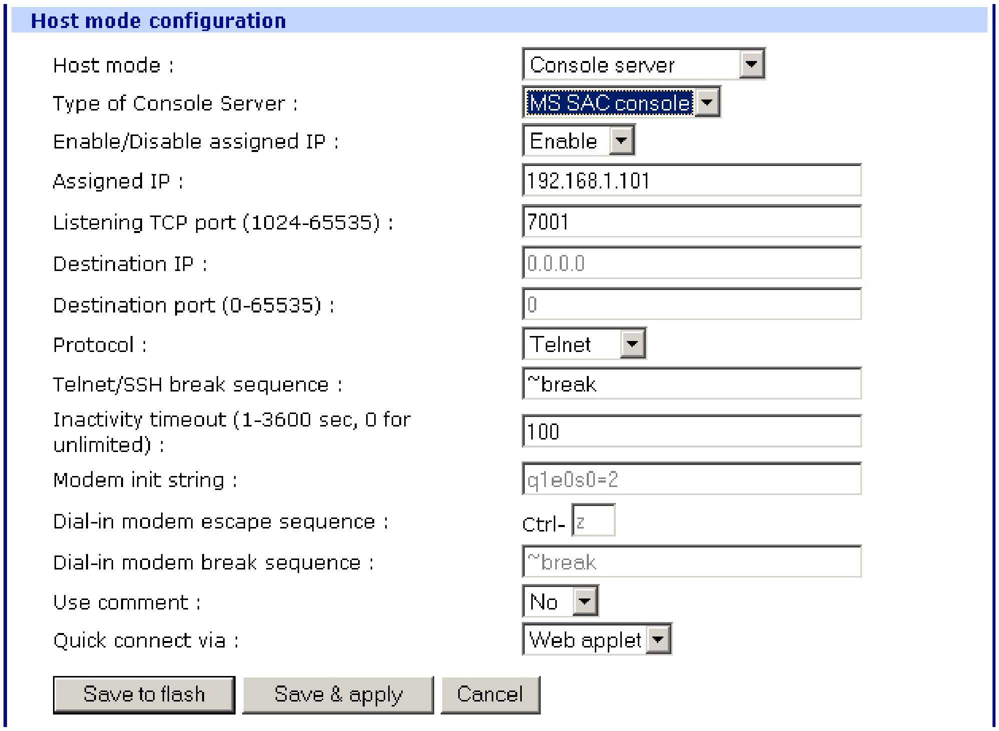
```
bootcfg /ems on /port com2 /id 1 /baud 115200
```

Setting Up the SERIMUX for SAC Support

To set up a serial port to provide access to the Windows Server 2003 console port, do the following:

1. Access the web interface.
2. Choose Serial Port > Configuration.
3. Choose a port .
4. Choose Host mode configuration.
5. The Host mode configuration page appears.

Set the Host mode to Console server and the Type of console server to MS SAC console as shown in the following figure.



Host mode configuration

Host mode :	Console server
Type of Console Server :	MS SAC console
Enable/Disable assigned IP :	Enable
Assigned IP :	192.168.1.101
Listening TCP port (1024-65535) :	7001
Destination IP :	0.0.0.0
Destination port (0-65535) :	0
Protocol :	Telnet
Telnet/SSH break sequence :	~break
Inactivity timeout (1-3600 sec, 0 for unlimited) :	100
Modem init string :	q1e0s0=2
Dial-in modem escape sequence :	Ctrl- z
Dial-in modem break sequence :	~break
Use comment :	No
Quick connect via :	Web applet

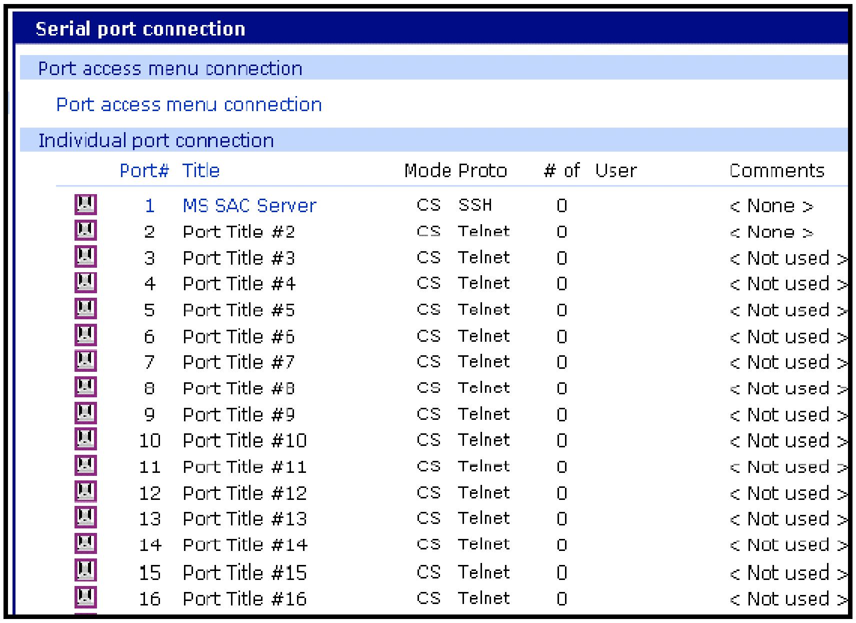
Figure 78- Setup SERIMUX for SAC support

6. Set other fields as appropriate. See "Configuring Host Mode" on page 17 for more information.
7. Choose Save & apply.
8. Configure serial port communication settings, by doing the following:
   a. Choose Serial port parameters from the menu.
   b. Adjust settings as required. This includes ensuring that the Baud rate matches the setting on the Windows Server 2003 serial port and Flow control is set to None. Ignore the DTR behavior field.
   c. Choose Save & apply.

Accessing the Windows Server 2003 Console Port from the SERIMUX GUI

To access the Windows Server 2003 console port, do the following:
1. Access the web interface.
2. Choose Serial Port > Connection.

A screen similar to the following appears.



Serial port connection

Port access menu connection

Port access menu connection

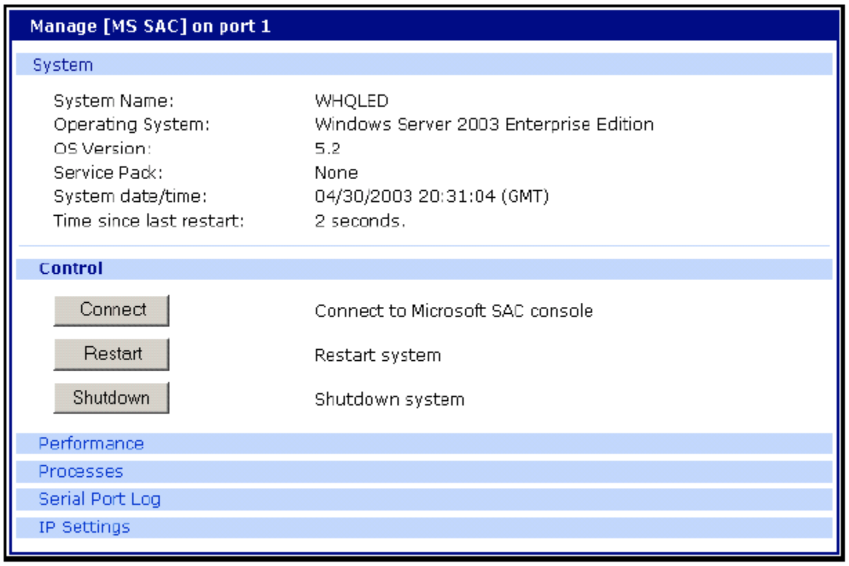
Individual port connection

Port#	Title	Mode	Proto	# of	User	Comments
1	MS SAC Server	CS	SSH	0		< None >
2	Port Title #2	CS	Telnet	0		< None >
3	Port Title #3	CS	Telnet	0		< Not used >
4	Port Title #4	CS	Telnet	0		< Not used >
5	Port Title #5	CS	Telnet	0		< Not used >
6	Port Title #6	CS	Telnet	0		< Not used >
7	Port Title #7	CS	Telnet	0		< Not used >
8	Port Title #8	CS	Telnet	0		< Not used >
9	Port Title #9	CS	Telnet	0		< Not used >
10	Port Title #10	CS	Telnet	0		< Not used >
11	Port Title #11	CS	Telnet	0		< Not used >
12	Port Title #12	CS	Telnet	0		< Not used >
13	Port Title #13	CS	Telnet	0		< Not used >
14	Port Title #14	CS	Telnet	0		< Not used >
15	Port Title #15	CS	Telnet	0		< Not used >
16	Port Title #16	CS	Telnet	0		< Not used >

Figure 79- Access Windows Server 2003 console port from SERIMUX GUI

3. Click on the title of the port to which the Windows Server 2003 console port is connected.

A screen similar to the following appears.



Manage [MS SAC] on port 1

System

System Name: WHQLED
Operating System: Windows Server 2003 Enterprise Edition
OS Version: 5.2
Service Pack: None
System date/time: 04/30/2003 20:31:04 (GMT)
Time since last restart: 2 seconds.

Control

Figure 80- Windows Server 2003 controls

4. Use the SERIMUX GUI to perform SAC functions. The following table describes attributes of the controls on the GUI.

Field	Description
Connect	Connects to the SAC console port via the command line interface.
Restart	Reboots the Microsoft Server 2003.
Shutdown	Shuts down the Microsoft Server 2003.
Performance	Provides access to Microsoft Server 2003 status information.
Process	Provides access to the process list, which allows you to view and kill active processes.
Serial Port Log	Provides access to port logging information.
IP Settings	Provides access to IP settings, enabling you to verify and change settings.

Hardware Information

Introduction

This chapter provides information on SERIMUX hardware. Among the topics covered are the hardware specifications, LED descriptions, pinouts for the Ethernet cable, and pinouts for the cable adapters.

Hardware Specifications: SERIMUX 16 and SERIMUX 32 AC Powered

Attribute	Value
Operating temperature	40°F to 120°F (5°C to 50°C)
Storage temperature	-20°F to 140°F (-29°C to 60°C)
Humidity	10% to 90% non-condensing
Power supply Internal	100 -240VAC, 50/60 Hz, 1.2A (max)
Power consumption	0.1A /120VAC (type), 12W (typical), 40W (max)
Fuse (internal)	FUSE (Type L) AC250V, 2A
Operating system	Linux Hard Hat embedded
SDRAM	64 megabytes
Flash memory	8 megabytes
Size (In.) WxDxH: unpackaged	17 x 8.5 x 1.75
Size (In.) WxDxH: packaged	20.375 x 15.25 x 4.75
Weight: unpackaged	5.8 lbs (2.63 kilograms)
Weight: packaged	8.6 lbs (3.9 kilograms)

Hardware Specifications: SERIMUX 16 and SERIMUX 32 DC Powered

Attribute	Value
Operating temperature	40°F to 120°F (5°C to 50°C)
Storage temperature	-20°F to 140°F (-29°C to 60°C)
Humidity	10% to 90% non-condensing
Power supply Internal	36 - 72 Vdc, 1.2A (max)
Power consumption	0.25A /48Vdc, 12W (typical), 40W (max)
Fuse (internal)	FUSE (Type L) AC250V, 2A
Operating system	Linux Hard Hat embedded
SDRAM	64 megabytes
Flash memory	8 megabytes
Size (In.) WxDxH: unpackaged	17 x 8.5 x 1.75
Size (In.) WxDxH: packaged	20.375 x 15.25 x 4.75
Weight: unpackaged	5.8 lbs (2.63 kilograms)
Weight: packaged	8.6 lbs (3.9 kilograms)

Hardware Specifications: SERIMUX 8 AC Powered

Attribute	Value
Operating temperature	40°F to 120°F (5°C to 50°C)
Storage temperature	-20°F to 140°F (-29°C to 60°C)
Humidity	10% to 90% non-condensing
Power supply External	100 - 240VAC, 50/60 Hz, 1.0A (max)
Power consumption	AC input: 0.05A /120VAC, 6W (typical), 12W (max) DC input: 0.8A/5VAC, 4.5 W (typical), 8W (max)
Operating system	Linux Hard Hat embedded
SDRAM	64 megabytes
Flash memory	8 megabytes
Size (In.) WxDxH	9.5 x 6.25 x 1.25
Weight	2.5 lbs (1.13 kilograms)

LED Indicators

Use the LED indicators to confirm attachment to the network and that the SERIMUX is able to send and receive data.

LED		Function
System	Power	On when power is supplied
	Ready	On when system is ready to run
	PC	On when a PC device is running
Ethernet	100Mbps	On when 100Base-TX connection is detected
	LINK	On when connected to an Ethernet network
	Act	Blinks when there is activity on the Ethernet port
Serial port	In Use	On when the serial port is ready to run
	Rx/Tx	Blinks when there is traffic on the serial port

About Serial Port Cabling

The SERIMUX simplifies cabling. The RJ45 8-pin configuration matches all SUN and Cisco RJ45 console port configurations, enabling CAT 5 cabling without pinout concerns. Three DB-25 and one DB-9 adapters come in the package. A DB-25 male, a DB-25 female, and a DB-9 adapter support console management applications. A DB-25 male adapter provides a modem connection. See the cable adapter information that follows later in this chapter.

Note: The cable length restrictions common to RS-232 cables apply to the SERIMUX serial cable as well.

Serial Port Pinouts

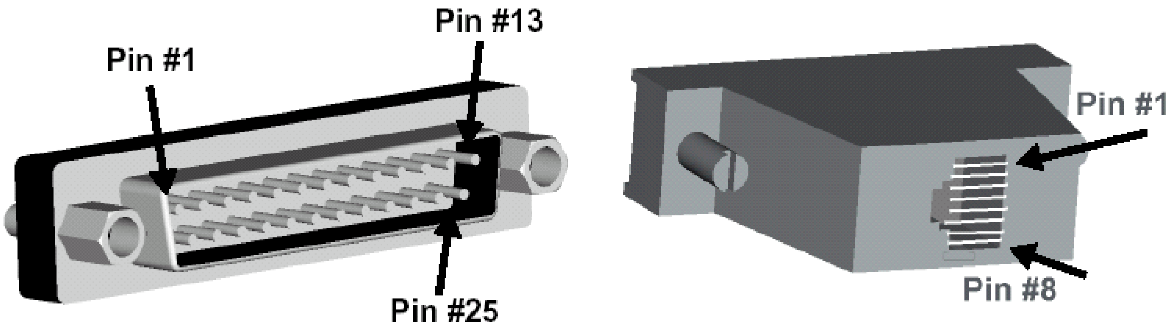
The SERIMUX uses an RJ45 connector for serial ports. Pin assignments are listed in the following table.

Pin	Description
1	CTS
2	DSR
3	RxD
4	GND
5	DCD: Note Inbound signal can also be used as a second ground.
6	TxD
7	DTR
8	RTS

Cable Adapters

The SERIMUX comes with four cable adapters. The following illustrations show cable adapter pin outs. Additional adapters can be purchased from NTI.

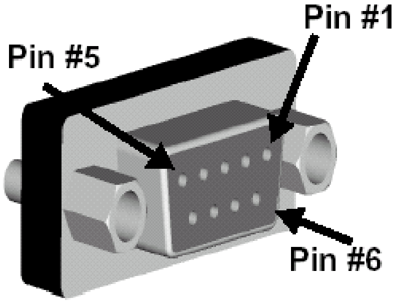
DB-25 Male Console Adapter (NTI P/N DB25M-RJ45F-T)

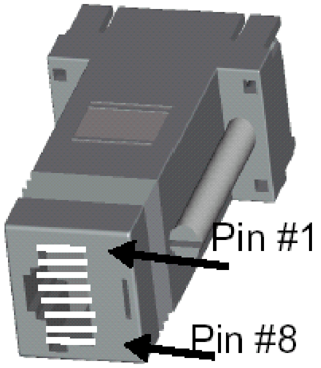


DB-25 Male to RJ45 Connector Pin Assignments

RJ45	Signal		DB-25M	Signal
1	CTS	Connected to	4	RTS
2	DSR	Connected to	20	DTR
5	DCD			
3	RxD	Connected to	2	TxD
4	GND	Connected to	7	GND
6	TxD	Connected to	3	RxD
7	DTR	Connected to	6	DCD
			8	DSR
8	RTS	Connected to	5	CTS

DB-9 Female Console Adapter (NTI P/N DB9F-RJ45F)

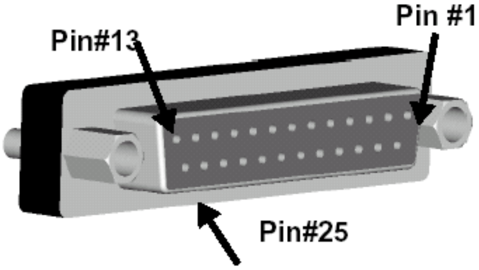


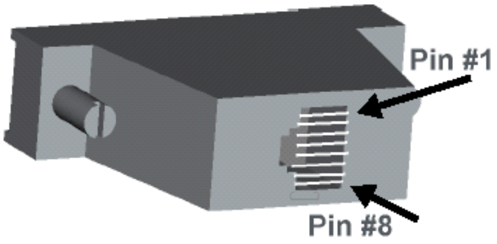


DB-9 Female to RJ45 Pin Assignments

RJ45	Signal		DB-9F	Signal
1	CTS	Connected to	7	RTS
2	DSR	Connected to	4	DTR
5	DCD			
3	RxD	Connected to	3	TxD
4	GND	Connected to	5	GND
6	TxD	Connected to	2	RxD
7	DTR	Connected to	1	DCD
			6	DSR
8	RTS	Connected to	8	CTS

DB-25 Female Console Adapter (NTI P/N DB25F-RJ45F)

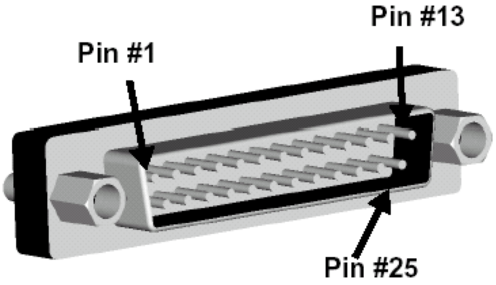


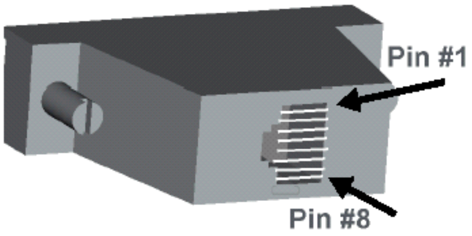


DB-25 Female to RJ45 Pin Assignments

RJ45	Signal		DB-25F	Signal
1	CTS	Connected to	4	RTS
2	DSR	Connected to	20	DTR
5	DCD			
3	RxD	Connected to	2	TxD
4	GND	Connected to	7	GND
6	TxD	Connected to	3	RxD
7	DTR	Connected to	6	DCD
			8	DSR
8	RTS	Connected to	5	CTS

DB-25 Male Modem Adapter (NTI P/N DB25M-RJ45F-C)





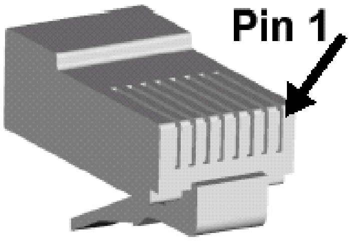
DB-25 Male Modem to RJ45 Pin Assignment

RJ45	Signal		DB-25M	Signal
1	CTS	Connected to	5	CTS
2	DSR	Connected to	6	DSR
3	RxD	Connected to	3	RxD
4	GND	Connected to	7	GND
5	DCD	Connected to	8	DCD
6	TxD	Connected to	2	TxD
7	DTR	Connected to	20	DTR
8	RTS	Connected to	4	RTS

Ethernet Pinouts

The SERIMUX uses a standard Ethernet connector, that is a shielded and compliant with AT&T 258 specifications.

Pin	Description
1	Tx+
2	Tx-
3	Rx+
4	NC
5	NC
6	Rx-
7	NC
8	NC



Certifications

Safety

- US: UL1950
- Canada: CSA 22.2 No. 60950
- Europe: EN60950 (CB Scheme Report)

Working Inside the SERIMUX

NOTICE: Do not attempt to service the SERIMUX except when following the instructions from NTI Technical Support personnel. In such a case, first perform the following actions:

- ***Turn OFF the SERIMUX.***
- ***Ground yourself by touching an unpainted metal surface at the back of the equipment before touching anything inside the equipment.***

Replacing the Battery

A coin-cell battery maintains date and time information. If it is necessary to repeatedly reset time and date information after turning on the SERIMUX, replace the battery.

CAUTION: A new battery can explode if it is incorrectly installed. Replace the 3 Volt CR2032 battery only with the same or equivalent type recommended by the battery manufacturer. Discard used batteries according to the battery manufacturer's instructions.

Safety Instructions

CAUTION: Do not operate the SERIMUX with the cover removed.

- In order to avoid shorting out the SERIMUX when disconnecting the network cable, first unplug the cable from the equipment and then from the network jack. When reconnecting a network cable to the equipment, first plug the cable into the network jack, and then into the equipment.
- To help prevent electric shock, plug the SERIMUX into a properly grounded power source. The cable is equipped with a 3-prong plug to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from the cable. If it is necessary to use an extension cable, use a 3-wire cable with properly grounded plugs.
- To help protect the SERIMUX from transients in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply.
- Be sure that nothing rests on the SERIMUX's cables and that the cables are not located where they can be stepped on or tripped over.
- Do not spill food or liquids on the SERIMUX. If it gets wet, contact NTI Technical Support.
- Do not push any objects into the openings of the SERIMUX. Doing so can cause fire or electric shock by shorting out interior components.
- Keep the SERIMUX away from heat sources. Also, do not block cooling vents.

Emissions

- US: FCC part 15, Class A
- Canada: ICES 003 Class A
- Europe: EN55022, EN61000-3-2, EN61000-3-3
- Japan: VCCI
- Australia: AS3548

Immunity

Europe: EN55024

Index