DS Series Manual

BayTech®

DATA SWITCH

DS62 Host Ethernet Module

&

DS62-MD4 Host Ethernet-Modem Module

DS62-Network, DS62-MD4 Network/Modem Host Module

DS62-Network, DS62-MD4 Network/Modem Host Module

ABOUT THIS OWNER'S MANUAL

This document is applicable to the **DS62 Network Module and the DS62-MD4 Network/Modem Module** _EXCEPT_ **those paragraphs specifically mentioning the DS62-MD4 do not apply to the DS62**. This document provides information required for installing and operating your Bay Tech equipment. It should allow the user to connect to, power up, and access an applications menu where peripheral equipment can be controlled. We recommend reading this manual carefully, while placing special emphasis on correct cabling and configuration. If you have any problems with your installation, please contact a BayTech Applications Engineer at **228-563-7334**, or toll free from anywhere in the United States using **1-800-523-2702** or contact us at our Web Site, www.baytech.net.

BayTech manufactures many remote site management products, data switches, and remote power controllers. If you would like information on any of these products, please contact BayTech Customer Service at the above numbers or visit our web site.

Conventions used in this manual include:

> **CAUTION:** This term is used to denote any condition that could possibly result in physical harm to personnel or damage to equipment.
> **IMPORTANT:** This term is used to denote conditions that could result in the loss of communications or to highlight the proper functioning of equipment.
> **NOTE:** This term is used to denote items of interest to the user.
> **<cr>:** Carriage Return or ENTER

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Technical Associates, Inc.

In the interest of improving internal design, operational function, and/or reliability, Bay Technical Associates, Inc reserves the right to make changes to the products described in this document without notice.

Bay Technical Associates, Inc does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

BayTech units are in accordance with the general requirements of _Standard for Information Technology Equipment_ (ETL listed, conforms to ANSI/UL STD 60950-1-2003 CERTIFIED CAN/CSA C22.2 NO. 60950-1-03, UL STD 231 8TH EDITION, UL STD 1950 3RD EDITION CERTIFIED CAN/CSA 22.2 NO. 950-95, CE conforms to IEC 60950-1).

We welcome any comments you may have about our products, and we hope that you will continue to look to BayTech for your remote management needs.

DS62-Network, DS62-MD4 Network/Modem Host Module

Connection Description

BayTech's host communication module provides an interface that controls user access to the DS Series data switch and other DS Series connected modules.

EIA-232 SERIAL CONNECTION

The DS-Series host communications modules have an RJ-45 port which uses an 8-pin crossed modular cable to connect to a local EIA-232 device such as a computer terminal or external modem. Most serial computers do not have RJ-45 connections; therefore an adapter is provided with this unit to convert from a DE-9 connector to an RJ-45 connector (Bay Tech Part No. 9FRJ45PC-4). An adapter to convert from a DB-25 connector to an RJ-45 connector is also available from Bay Tech, upon request (Bay Tech Part No. 25FRJ45PC-4). The 8-pin crossed modular cable is configured to operate with these adapters.

Internal MODEM CONNECTION

A Flash upgradeable 56 Kbps (V.90bis) modem allows standard dial-up telephone lines to be used between the Data Switch installation and the user's location.

IMPORTANT: The DS62-MD4 modem option has priority over the EIA-232 serial port. If a serial port user is in configuration mode or connected to a DS74 I/O port when a modem connection is established, the serial port user will be "booted" off, allowing the remote user to communicate with the DS unit. Using the RJ04X007 (RJ-11) modular cable, connect to "LINE" on the DS62-MD4 module to the Telco wall jack. Using communications software, dial the modem using the ATDT command.

10/100 BASE-T NETWORK PORT CONNECTION

Using a straight 10/100 Base-T cable, connect the RJ-45 port labeled ETHERNET on the HOST module to an RJ-45 port on the network hub. The LINK (link integrity) LED, located on the front panel of the HOST, illuminates when a good connection is established between the HOST and the hub.

Installation

UNPACKING

Compare the unit and serial number of the equipment you received to the packing slip located on the outside of the box. Inspect equipment carefully for damage that may have occurred in shipment. If there is damage to the equipment or if materials are missing, contact BayTech technical support at **228-563-7334** or call toll free inside the United States at **800-523-2702**. At a minimum, you should receive the following:

1. The Host Module and DS74 Modules.
2. Manual insert describing the location of the User's Guide on BayTech's website at www.baytech.net.
3. Power Cords that may be attached to the unit (if order requested detachable cords).
4. 1 ea. DE-9 (9 pin) PC com port adapter -- 9FRJ45PC (with Cisco Interface) or 9FRJ45PC-1.
5. 1 ea. RJ-45 Roll over cable -- RJ08X007.

NOTE: Keep the shipping container and packing material in the event future shipment is required.

PREPARING THE INSTALLATION SITE

The installation area should be clean and free of extreme temperatures and humidity. Allow sufficient space behind the DS unit for cabling and receptacle connections. Access to installation site should be restricted to authorized personnel. Installation of these units should be limited to ITE and Telco server environments.

Power

> **CAUTION:** This unit is intended for indoor use only. Do not install near water or expose this unit to moisture. To prevent heat buildup, do not coil the power cord when in use. Do not use extension cords. Do not attempt to make any internal changes to the power source. Do not attempt to modify any portion or component of a DS-Series Data Switch unless specifically directed to; as in Appendix E of this manual. BayTech must perform any internal changes.

> **CAUTION:** High-voltage surges and spikes can damage this equipment. To protect from such power surges and spikes, this unit must have a good earth ground. A grounding screw connection is located near the power switch on the back of the unit.

> **CAUTION:** Before removing or replacing any modules, turn off main power switch located on the DS-Series Base Unit. Communication to the DS-Series Data Switch will be disrupted while power is off.

> **CAUTION:** For PERMANENTLY CONNECTED EQUIPMENT, a readily accessible disconnect device (Circuit Breaker rated not to exceed the amperage rating of the unit) shall be incorporated in the fixed wiring between the power source and the Baytech unit. For PLUGGABLE EQUIPMENT, the socket-outlet shall be installed near the equipment and easily accessible and shall provide back up protection against over current and short circuit by suitable rated protective devices not to exceed the AC current rating for the selected model

QUICK START: HOST Module

by **Bay Technical Associates**
For those Administrators who have requested the bare minimum for this type of equipment, follow these steps exactly. If this is a new unit shipped directly from Baytech, follow the steps. If this is a previously own unit, perform a factory reset to clear out any users and passwords still in the unit.

Ethernet Controller Configuration:
Before continuing your System Administrator needs to tell you to use DHCP or give you an IP Address, Subnet Address, and Gateway Address.
1. Connect the 9FRJ45PC-4 or 9FRJ45PC-1 adapter to your PC.
2. Connect the supplied rollover flat cable RJ08X007 to the adapter and to the EIA232 serial port on the Baytech HOST Module.
3. Use terminal emulation software to access the unit, (i.e. Microsoft Hyper-terminal). Set the PC serial port configuration to the following: **9600 bps, 8 data bits, 1stop bit and no parity.**
4. If you get only a blinking cursor Press 'Enter'. If still only a blinking cursor, Type 5 semi-colons (;), The Attention Character will not echo on the screen. There is a one second delay before the menu is displayed. You should see a menu similar to (Figure 1).

DS62-Network, DS62-MD4 Network/Modem Host Module

5. Select 'C' for the configuration menu.
6. Select the HOST module. You should see a menu similar to (Figure 2).
7. Select the number for 'Login Setup' option. You should see a menu similar to (Figure 3).
8. Select the number for 'Manage Users' option. You should see a menu similar to (Figure 4).
9. **NOTE: The 'root' user can not be deleted.**
10. Select 'A' to add user. Type the name and password at the prompts.
11. Press 'Enter' until get to the 'Login Setup Menu' (Figure 3).
12. Select option 'Access Control' to enable or disable the Tenet and Serial Login Prompt.
13. Press 'Enter' until you get the Configuration menu (Figure 2).
14. Select 'Network Port Configuration' option. You should see a menu similar to (Figure 5).
15. If your System Administrator requires you to use DHCP, then select 'DHCP Enable/Disable' and type 'Y' to enable DHCP. If you wish to assign a static IP address to this unit, disable the DHCP and go to step 18.
16. Press 'Enter' until you are asked to 'Accept Changes'. Type 'Y' to accept changes or 'N' to decline changes.
17. After Accepting or Declining Changes Pres 'Enter ' until you get the Network Access Menu (Figure 1).
18. Select 'Unit reset' to update the external connections. Once the reset is completed (1 minute) connect the Baytech device to your network using an Ethernet cable.
19. If you disabled the DHCP in step 15, you should see a menu similar to (Figure 5).
20. Select the 'IP Address' option and type the assigned IP address and press 'Enter'.
21. Select the 'Subnet Mask' option and type the assigned subnet mask address and press 'Enter'.
22. Select the 'Gateway Address' option and type the assigned Gateway address and press 'Enter'.
23. Press 'Enter' until you are asked to 'Accept Changes'. Type 'Y' to accept changes.
24. Press 'Enter' until you get the Network Access Menu, (Figure 1).
25. Select 'Unit reset' to update the external connections. Once the reset is completed (1 minute) connect the Baytech device to your network using an Ethernet cable.

At this point you have enough basic configurations needed to operate this Baytech unit.

Serial Setup

- Verify **JMP5** is set to pins **1** and **2** on the DS62 module.
- Connect the *9FRJ45PC-4* adapter to the user's computer
- Connect the Host Module's EIA-232 port to the adapter via the *RJ08X007* rolled flat ribbon cable.
- Use terminal emulation software to access the unit, **9600 bps, 8 data bits, 1stop bit and no parity**.

NOTE: At any time during the session you need to go to another menu, use the **Attention Character = semi-colon (;)**. Press the attention character key 5 consecutive times to get back to the main status menu.

DS62-Network, DS62-MD4 Network/Modem Host Module

Figure 1

```
DS-Series - F 2.10.05      (C) 2005 Bay Technical Associates
    Module Name: DS62


    Module: 1
    Attention Character:  ;
    Device A          (2, 1).........1
    Device B          (2, 2).........2
    Device C          (2, 3).........3
    Device D          (2, 4).........4
    DS-DS             (5, 1).........5
    Status.........................S   Current configuration
    Configure......................C   Make Changes
    Unit Reset....................RU   Resets the DS-Unit, terminates internal &
                                       external modem connections, allow 10
                                       seconds for reset.

    Logout.........................T
  Enter Request :c
```

Select option 'C' for the configuration menu. Select the DS62 module option and the following menu is displayed:

Figure 2

```
Copyright(C) Bay Technical Associates 2006
  DS62 Ethernet Host module
  Revision F 2.10.05        Module 1
  Hardware 1.01             Serial number  509       colilo version 1.05.01

    Status.........................1   Current setting of the module
    Serial Port Configuration......2   Setup the port configuration menu
    Serial Port Device Name........3   Name the port
    Attention Character............4   Pressing the attention character 5
                                       consecutive times will return back to the
                                       main menu.
    Disconnect Timeguard...........5   If more data is received within the delay
                                       period, the DS series treats the
                                       character as data, not an attention
                                       character; thereby preventing unwanted
                                       port disconnection.
    Connect Port ID Echo...........6   Enable port echo by name or module&port#
    Login Setup....................7   Login menu Access/Users/Direct Port
                                       Connection/Radius/TACACS
    Network Port Configuration.....8   Network Setup IP Address
    Module Name....................9   Enter a name for the module
    DS Management.................10   Set up Voltage/Current/Sensor thresholds
    Firmware / Config Download....11   Updates by FTP & Reset to Factory Config
    Exit........................X,CR
  Enter Request :
```

DS62-Network, DS62-MD4 Network/Modem Host Module

Attention Character

If no Baytech power strips are to be controlled through this Data Server, skip this step. Pressing the Attention Character 5 consecutive times will access the network main menu. **The Default is a semi-colon (;)**. Select this option to change the attention character. The DS displays the following:

Attention Character is........... ;

Enter Attention Character :

Login Setup Menu

Figure 3

```
    Access Control..................1   Telnet/Serial Enable/Disable Login prompt
    Manage Users....................2   Change user password or port access,
                                        add/delete user,
    Direct Port Connection..........3   Enable/Disable
    Radius Configuration............4   See below for Radius menu
    TACACS Configuration............5   See below for TACACS menu
    Exit...........................X,CR
  Enter Request :
```

Access Control

This security feature allows the admin to enable or disable usernames and passwords for both network and serial port access.
If either login has been enabled you will get a prompt similar to the following:

```
    Coldfire login: root
    Password:
```

The default user and password is "**root/baytech**", all lower case.

Manage Users

This menu allows the administrator to add/delete users and change their passwords for multiple users. Up to 19 users plus an administrator allowed. Usernames and passwords are case sensitive and alphanumeric. The root user can not be removed. Select Manage User and the DS displays the following:

Figure 4

```
  User Management Menu
  To change user password or port access, enter number of user.
  To add/delete user, select appropriate menu choice.
  SNMP V3 requires passwords that are between 8 and 31 characters long
  Enter request, CR to exit menus.
    A)...Add user
    1)...root
  Enter Request :
```

Radius Configuration

Radius is used to authenticate logins for the serial and the network ports if passwords and user names are enabled on the DS. If the Radius server rejects either the username or password or does not respond, the DS will display "Invalid Password".

TACACS Configuration

TACACS can be used to authenticate logins for the serial port, the network port, and modem. When a telnet / SSH session (or rs232 session) is started the Host module will prompt for the username and password. The Host will communicate with the TACACS server. If the server verifies the username and password, the Host will display the menus. If the server rejects the username and password or does not respond the Host will display the reason why the login failed.

Network Port Configuration

> **IMPORTANT:** For network access, enable Telnet and configure the IP addresses, Subnet Mask, and Gateway Address, or enable the DHCP. The module must be reset for network changes to take effect.

Figure 5

```
Network setup :
Ethernet Address................  00:C0:48:00:01:FD
IP Address......................   70.150.140.89
Subnet Mask.....................   255.255.255.224
Default Gateway.................   70.150.140.65

Connection Inactivity Timeout (mins): Disabled
Carriage Return Translation: Enabled
Break Length (msecs):  350
DHCP is Disabled   Telnet is Enabled    SSH is Enabled
SSH host keys are set to factory default

IP Address........................1
Subnet Mask.......................2
Gateway Address...................3
Inactivity Timeout................4
Carriage Return Translation.......5
Break Length......................6
DHCP Enable/Disable...............7
Telnet Enable/Disable.............8
SSH Enable/Disable................9
SSH Host Key Generation...........10
IP Filter Configuration...........11
SNMP Configuration................12
Web Server Configuration..........13
Exit..............................X,CR
Enter Request :
```

Cabling

RJ-45 Cables and Adapters

DS62 EIA-232 RJ-45 Signal

Pin	EIA 232 Signal	Signal Direction	Description
1	DTR	Out	Handshake, Line Driver Inactive State = High: +12V when power is applied. Used as a handshake line to enable/disable the receiving of characters.
2	GND		Signal Ground
3	RTS	Out	Handshake, Line Driver Inactive State = High: +12 V when power is applied. Not used to enable/disable.
4	TX	Out	Transmit Data Out
5	RX	In	Receive Data In
6	DSR	In	Handshake In. –12V when not used.
7	GND		Signal Ground
8	CTS	In	Used as a handshake line to enable/disable the receiving of characters.

Adapters Signals
Listed are the pin specifications for the BayTech cable and adapters and the terminal COM ports:

Signal	RS-232 Port (DS)	RS-232 Port (RPC)	COM Port DE-9 Pin	COM Port DB-25 Pin	Signal
DTR	1	1	4	20	DSR
GND	2	2		1	GND
RTS	3	3	7	5	CTS
TXD	4	4	3	2	RXD
RXD	5	5	2	3	TXD
DSR	6	N/C	6	6	DTR
GND	7	7	5	7	GND
CTS	8		8	4	RTS
DTR			4		DCD
DCD		8	1	8	DTR
RI	9			22	

DS62-Network, DS62-MD4 Network/Modem Host Module

Adapters

9FRJ45PC **(With Cisco Interface)**   9FRJ45PC-1 **(Without Cisco Interface)**
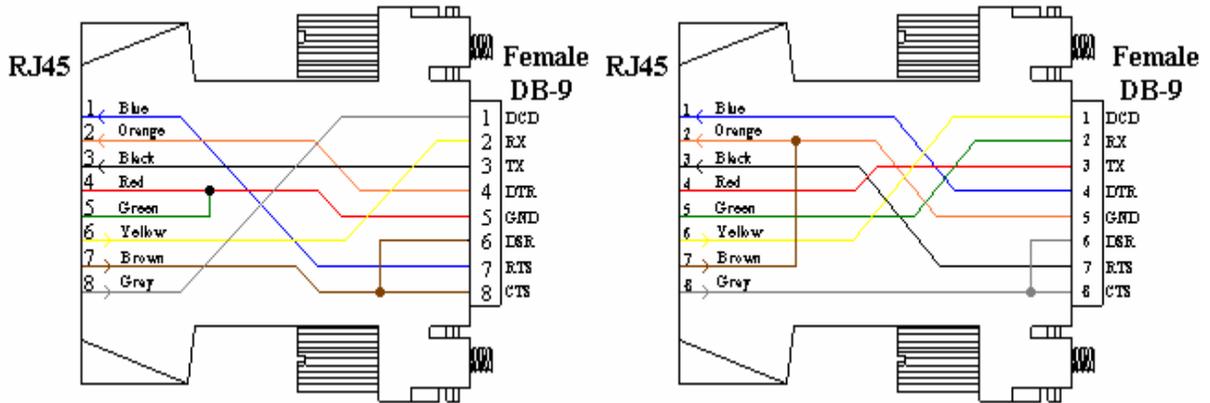
RJ08X007
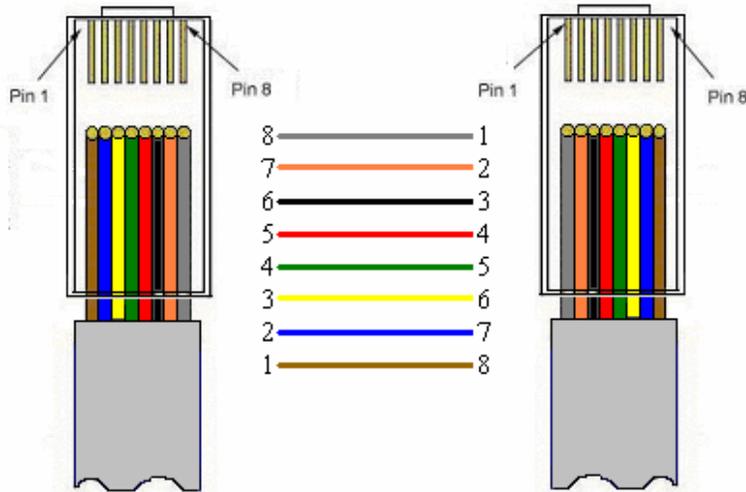
Figures 1 and 2 provide visual representation of an RJ-45 receptacle and plug.
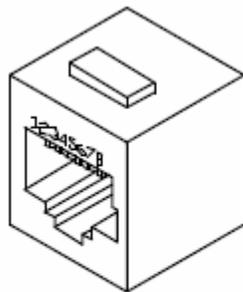
Fig. 1: RJ-45 Receptacle   **Fig. 2: RJ-45 Plug**
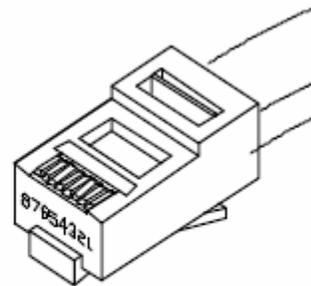
Detail Operations and Configurations

NOTE: Depending on the DS-Series model, the menus may vary according to the number of DS74 modules installed in the unit. If this is not an initial set-up and Password has already been enabled, you are prompted to login. After logging in successfully, invoke the main menu by sending the attention character five times (**;;;;;**).

NOTE: Password feature is case sensitive. Default is **'root/baytech'**.

Main Screen
DS62-MD4

> **IMPORTANT:** The Factory default serial communications parameters are **9600 bps, 8 data bits, 1 stop bit, and no parity.**

With a proper connection to the unit upon power-up or unit reset, the following initialization and Status menu will be displayed except the number of outlets will be dependent on the specific DS unit:

```
DS-Series - F 2.10.05     (C) 2005 Bay Technical Associates
   Module Name: DS62-MD4

   Module: 1
   Attention Character:  ;
   Device A          (2 ,1).........1
   Device B          (2 ,2).........2
   Device C          (2 ,3).........3
   Device D          (2 ,4).........4
   DS-RPC            (5 ,1).........5
   Status........................S  Current configuration
   Configure.....................C  Make Changes
   Unit Reset...................RU  Resets the DS-Unit, terminates internal &
                                    external modem connections, allow 10
                                    seconds for reset.

   Logout........................T
 Enter Request :c
```

> **NOTE:** Only the Administrator user will see the configuration option.

> **IMPORTANT:** If you get the following message after selecting the 'Configure' option, the other port has the configuration option selected.

```
Configuration mode in use.
```

> **IMPORTANT:** Once you make a change to any of the Configuration options, you have to back out of the Configuration menu and will be asked to 'Accept' changes. If you type 'Y' for YES and press <cr>, the changes take effect immediately for the serial port. For the Ethernet port you must do a Unit Reset to get the changes to take effect.

```
Accept changes ? (Y/N) :y
Changes accepted.
```

Unit Configuration Menu

The configuration menu allows the admin user to establish the parameters the DS-Series will operate.

```
Configuration
  DS62            module #1..........1
  DS74            module #2..........2
  DS-RPC          module #5..........3
  Enter Request :
```

Select the number of the host module and the following menu is displayed:

```
Copyright(C) Bay Technical Associates 2006
  DS62-MD4 Ethernet Host module
  Revision F 2.10.05      Module 1
  Hardware 1.01           Serial number  509      colilo version 1.05.01

     Status........................1   Current setting of the module
     Serial Port Configuration.......2   Setup the port configuration menu
     Serial Port Device Name.........3   Name the port
     Attention Character............4   Pressing the attention character 5
                                         consecutive times will return back to the
                                         main menu.
     Disconnect Timeguard...........5   If more data is received within the delay
                                         period, the DS series treats the
                                         character as data, not an attention
                                         character; thereby preventing unwanted
                                         port disconnection.
     Connect Port ID Echo...........6   Enable port echo by name or module&port#
     Login Setup....................7   Login menu Access/Users/Direct Port
                                         Connection/Radius/TACACS
     Network Port Configuration......8   Network Setup IP Address
     Module Name....................9   Enter a name for the module
     DS Management............... ..10   Set up Voltage/Current/Sensor thresholds
     Firmware / Config Download.....11   Updates by FTP & Reset to Factory Config
     Exit.........................X,CR
  Enter Request :
```

Configuration Status

The Status menu displays the modules installed and the current configuration of the host module. The following are the factory default settings:

DS62-Network, DS62-MD4 Network/Modem Host Module

```
Installed Modules :01,02,05
  Attention Character is ......... ;
  Disconnect Time Guard is........ Disabled
  Port ID Echo is................. Disabled
  Module Name is.................. DS62

  Network Connectivity & Login Configuration:
  Ethernet Address................  00:C0:48:00:01:FD
  IP Address...................... 0.0.0.0
  Subnet Mask..................... 0.0.0.0
  Default Gateway................. 0.0.0.0
  Inactivity Timeout (mins)....... Disabled
  Break Length (msecs)........... 350
  Telnet.......................... Enabled
  SSH............................. Enabled
  DHCP............................ Enabled
  Telnet login prompt is.......... Enabled
  Serial login prompt is.......... Disabled
  Direct Port Connection is....... Disabled

SNMP & Web Configuration:
  SNMP Agent is................... Enabled
  SNMPv3 only is.................. Disabled
  SNMP Trap Host 1 Address........ 0.0.0.0
  SNMP Trap Host 2 Address........ 0.0.0.0
  SNMP Trap Host 3 Address........ 0.0.0.0
  SNMP Trap Host 4 Address........ 0.0.0.0
  SNMP Read-Only Community........ public
  SNMP Read-Write Community....... private

  Web Server is................... Enabled
  Web Login is.................... Disabled
  Web Secure Connection is........ Disabled
  Web Activity Timeout is......... Disabled

  Radius Setup:
  Radius Logins are............... Disabled
  Radius Primary Server Address... 0.0.0.0
  Radius Backup Server Address.... 0.0.0.0
  Radius Secret................... HardlyASecret
  Radius Login Timeout............ 5
  DS62 Usernames as Backup is.... Disabled

  TACACS Setup:
  TACACS Logins are............... Disabled
  TACACS Server Address........... 0.0.0.0
  TACACS Server Address........... 0.0.0.0
  TACACS Secret................... HardlyASecret
  TACACS encryption is............ Enabled
  DS62 Usernames as Backup is.... Disabled
  TACACS Server Port is........... 49

  Modem Status:

+----+------+----------------+------+------+------+------+---------+----+----+
|Port|Device|    Device      | Baud | Word | Stop |Parity|Handshake|LineDrive|
|    | Type |    Name        | Rate | Size | Bits |      |         |DTR |RTS |
+----+------+----------------+------+------+------+------+---------+----+----+
| 2  | MODEM| Host V90 Modem |115.2K|  8   |  1   | None | None    | LO | LO |
+----+------+----------------+------+------+------+------+---------+----+----+
  Rings to AutoAnswer: 2
  Modem Connectivity Timeout (mins): 60
  Modem Inactivity Timeout (mins): 60
  Modem Login: Enabled
```

Serial Port Configuration

Handshaking, Baud Rate, Word Size, Stop Bits, and Parity are configured through either the serial or Ethernet ports using the menus. RTS and DTR Line Drivers can only be configured through the phone line via a modem. The **default settings** are **9600bps, 8 data bits, no parity, one stop bit, RTS and DTR High**.

> **IMPORTANT:** Changing the Host module serial port configuration could create a communications lock-out if the terminal computer serial port configuration does not match the host module.

```
+----+------+----------------+------+------+------+------+---------+----+----+
|Port|Device|     Device     | Baud | Word | Stop |Parity|Handshake|LineDrive|
|    | Type |     Name       | Rate | Size | Bits |      |         |DTR |RTS |
+----+------+----------------+------+------+------+------+---------+----+----+
| 1  | RS232| EIA-RS232      | 9600 |  8   |  1   | None | None    | HI | HI |
+----+------+----------------+------+------+------+------+---------+----+----+

   Handshaking.....................1
   Baud Rate.......................2
   Word Size.......................3
   Stop Bits.......................4
   Parity..........................5
   RTS Line Driver Inactive State...6
   DTR Line Driver Inactive State...7

   Enter Request :1
```

Handshaking

For a simple communication between modems three connected lines are needed: TX, Rx, and Ground. For the data to be transmitted, both sides have to be clocking the data at the same baud rate. While this method is sufficient for most applications, it is limited in being able to respond to problems such as the receiver getting overloaded. This is where serial handshaking can help.

Select "Handshaking" and the DS displays with the following:
Default is None

```
        Select handshaking:
         1 For None
         2 For Software Handshaking
         3 For Hardware Handshaking
         Enter Request :
```

1. **Software Handshaking:** This style uses actual data bytes as control characters. The lines necessary are TX, Rx, and ground since the control characters are sent over the transmission line like regular data. The two control characters, XON and XOFF are characters sent by the receiver of the data to halt the transmitter during communication.

   NOTE: A drawback to this method is also the most important fact to keep in mind. In ASCII transmissions these character values are non-character values; however, data being transmitted

via binary, it is very likely that these values could be transmitted as data and the transmission would fail.

2. **Hardware Handshaking:** This style uses actual hardware lines. Like the TX and Rx lines, the RTS/CTS and DTR/DSR lines work together. When a receiver is ready for data, it will assert the RTS (Request to Send) line. This is then read by the sender at the CTS (Clear to Send) input, indicating it is clear to send the data. DTR (Data Terminal Ready) and DSR (Data Set Ready) allow the serial port and the modem to communicate their status. When the modem is ready for data to be sent, it will assert the DTR line indicating that a connection has been made across the phone line. This is read in through the DSR line and the modem can begin to send data. The general rule of thumb is that the DTR/DSR lines are used to indicate that the system is ready for communication where the RTS/CTS lines are used for individual packets of data.

Baud Rate

Select "Baud Rate" to change the rate the modem transfers Data bites per second, the DS displays the following: **Default is 9600**

```
Select baud rate:
 1 For   300
 2 For   600
 3 For  1200
 4 For  2400
 5 For  4800
 6 For  9600
 7 For 19200
 8 For 38400
 9 For 57.6K
 A For 115.2K
 Enter Request :
```

Word Size

The word size is the measurement of the actual data bits in a transmission. Which setting you choose depends on what information you are transferring. For example, standard ASCII has values from 0 to 127 (7 bits). Extended ASCII uses 0 to 255 (8 bits). If the data being transferred is simple text (standard ASCII), sending 7 bits of data per packet is sufficient for communication. A packet refers to a single byte transfer, including start/stop bits, data bits, and parity.

Select "Word Size" and the DS displays the following: **Default is 8**

```
Select word size:
 1 For    5
 2 For    6
 3 For    7
 4 For    8
 Enter Request :
```

DS62-Network, DS62-MD4 Network/Modem Host Module

Stop Bits

The Stop Bits are used to signal the end of communication for a single packet. Since the data is clocked across the lines and each device has its own clock, it is possible for the two devices to become slightly out of sync. Therefore, the stop bits not only indicate the end of transmission but also give the computers some room for error in the clock speeds. The more bits that are used for stop bits, the greater the lenience in synchronizing the different clocks, but the slower the data transmission rate.

Select "Stop Bits" the DS displays the following: **Default is 1.**

```
Select stop bits:
  1 For   1
  2 For   1.5
  3 For   2
  Enter Request :
```

Parity

Parity is a simple form of error checking used in serial communication. For even and odd parity, the serial port will set the parity bit (the last bit after the data bits) to a value to ensure that the transmission has an even or odd number of logic high bits. For example, if the data was 011, then for even parity, the parity bit would be 0 to keep the number of logic high bits even. If the parity was odd, then the parity bit would be 1, resulting in 3 logic high bits. This allows the receiving device to know the state of a bit so as to enable the device to determine if noise is corrupting the data or if the transmitting and receiving devices' clocks are out of sync.

With no parity selected, it's assumed that there are other forms of checking that will detect any errors in transmission. No parity also usually means that the parity bit can be used for data, speeding up transmission. In modem-to-modem communication, the type of parity is coordinated by the sending and receiving modems before the transmission takes place.

Select "Parity" the DS displays the following: **Default is None.**

```
Select parity:
  1 For  None
  2 For  Even
  3 For   Odd
  Enter Request :
```

RTS/DTR Line Driver Inactivity State

RTS (Request to Send)/ DTR (Data Terminal Ready) is normally used in conjunction with an external modem. With no modem the RTS and DTR **default state is High.**

Select "RTS Driver State" the DS displays the following:

```
RTS Line Driver Inactive State is: High
High ? (Y/N, CR for no change):
```

Select "DTR Driver State" the DS displays the following:

```
DTR Line Driver Inactive State is: High
High ? (Y/N, CR for no change):
```

Serial Port Device Name

Select a port and type the new name.

```
Current device name: EIA-RS232
Enter device name for serial port ((1 - 16 char., CR to end) :
```

Attention Character

Pressing the Attention Character 5 consecutive times will access the network main menu. **The Default is a semi-colon (;)**. Select this option to change the attention character. The DS displays the following:

```
Attention Character is........... ;

Enter Attention Character :
```

Disconnect Timeguard

This feature ensures reliable binary data transmission by providing a one-second "Timeguard" after the DS-Series receives the attention character. If more data is received within the delay period, the DS treats the character as data, not an attention character; thereby preventing unwanted port disconnection. **The Default setting is Disabled.**

```
Disconnect Time Guard is.......... Disabled
Enable ? (Y/N), CR for no change) :
```

Connect Port ID Echo

When a user logs into the DS unit the port is identified in the following example:

```
        BAYTECH

For further information check:
http://www.baytech.net/

DS62                    <= Device name Port echo.
  or
02,1                    <= Module and Port Number echo.
```

Select option 1, to disable the echo. **The Default setting is Disabled**.
Select option 2 to echo the module and port number. (i.e. 3, 2)
Select option 3 to echo the device name. (Device A)

DS62-Network, DS62-MD4 Network/Modem Host Module

```
Port ID Echo is...................Disabled
Disable Port ID Echo..............1
Use Module, Port Number...........2
Use Device Name...................3
Exit..............................X,CR
Enter Request :
```

Login Setup Menu

This menu allows the admin user to enable or disable the Access Control, Manage Users, Direct Port Connection, Radius, and TACACS configuration. Depending on what firmware the Host Module has, the Login Setup menu may be different than what is shown in this figure, but are defined below.

```
Access Control..................1   Telnet/Serial Enable/Disable Login prompt
Manage Users....................2   Change user password or port access,
                                    add/delete user,
Direct Port Connection..........3   Enable/Disable
Radius Configuration............4   See below for Radius menu
TACACS Configuration............5   See below for TACACS menu
Exit..........................X,CR
Enter Request :
```

Access Control

This security feature allows the admin to enable or disable usernames and passwords for both network and serial port access.

```
Telnet Login Prompt Enable/Disable..1
Serial Login Prompt Enable/Disable..2
Modem Login Prompt Enable/Disable...3
Enter Request :
```

If either login has been enabled you will get a prompt similar to the following:

```
Coldfire login: root   or Universal DS login: root
Password:                 Password:
```

The default user and password is "**root/baytech**", all lower case.

Manage Users

This menu allows the administrator to add/delete users and change their passwords for multiple users. Up to 19 users plus an administrator allowed. Usernames and passwords are case sensitive and alphanumeric. The root user can not be removed. Select Manage User and the DS displays the following:

```
User Management Menu
To change user password or port access, enter number of user.
To add/delete user, select appropriate menu choice.
SNMP V3 requires passwords that are between 8 and 31 characters long
Enter request, CR to exit menus.
  A)...Add user
  1)...root
Enter Request :
```

ADD User

Select A), and press <cr> to add a user and their password. The DS displays the following:

```
Enter username (<= 31 characters)>user1
Enter new password (<= 31 characters)>******
Confirm by re-entering new password>******
Password change successful.
```

> **NOTE:** Log Out will be the only option available to the user if port access is not assigned.

> **NOTE:** If you forget your password, the administrator has to delete the user then add them back in.

> **IMPORTANT:** You can change the admin password. If you forget, resetting the unit back to factory default is the only way to get the admin password back.

Change User's Port Access and Password

The admin can change a user's port access and password.

```
User Management Menu
To change user password or port access, enter number of user.
To add/delete user, select appropriate menu choice.
SNMP V3 requires passwords that are between 8 and 31 characters long
Enter request, CR to exit menus.
  A)...Add user
  D)...Delete user
  1)...user1
  2)...root
Enter Request :2
```

Select a user number, the DS displays the following menu:

```
        Change Password.............1
        Modify Port Access Rights...2
        Exit........................X
            Enter Request :1
```

DS62-Network, DS62-MD4 Network/Modem Host Module

Select the Change Password option to change the user password, the Host Module displays the following:

```
  User name: root
  Enter old password (CR if none)>*******
  Enter new password (<= 31 characters)>*******
  Confirm by re-entering new password>*******
  Password change successful.
```

Select "Change Port Access Rights" to change the user's assigned ports. If you select the "root user" the Host Module will display the following:

```
root user always has access to all ports and access rights can not be changed
```

Select a non-root user and the DS displays:

```
 Port access for user1
   X = has access
| mod 2 | mod 3 |
| 1234  | 1234  |

Enter port list (mod.port,mod.port), ALL for all ports, NONE for no ports:
all
```

Type 'all' and press <cr>, the DS displays all ports available to 'user1':

```
 Port access for user1
 X = has access
| mod 2 | mod 3 |
| 1234  | 1234  |
  XXXX    XXXX

Enter port list (mod.port,mod.port), ALL for all ports, NONE for no ports:
none
```

Type 'none' and press <cr>, the DS displays the user with no assigned ports:

```
  Port access for user1
  X = has access
| mod 2 | mod 3 |
| 1234  | 1234  |
```

To add specific ports to the user, enter the module/port numbers as shown.

```
Enter port list (mod.port,mod.port), ALL for all ports, NONE for no ports:
2.1,3.2,3.3

 Port access for user1
 X = has access
| mod 2 | mod 3 |
| 1234  | 1234  |
  X        XX
```

Enter an incorrect port the DS displays:

```
Enter port list (mod.port,mod.port), ALL for all ports, NONE for no ports:
1.2

Input Error
```

Delete User

Select D), press <cr>, and type the number of the user to be deleted:

```
From menu above, enter number for user to delete>1
```

> **NOTE:** the 'root' user can not be deleted.

Direct Port Connection

This will allow the user to be connected directly to a DS serial port, as determined by the TCP port, starting at TCP port 50001.

```
Direct Port Connection is.........Disabled
Enable ? (Y/N), CR for no change) :
```

Radius Configuration

Radius is used to authenticate logins for the serial and the network ports if passwords and user names are enabled on the DS. If the Radius server rejects either the username or password or does not respond, the DS will display "Invalid Password".

```
Radius Enable....................1  Enable Radius Login
Radius Server Address............2  Radius server IP address 0.0.0.0 form
Radius Backup Server Address.....3  Backup Radius server IP address
Radius Secret....................4  Radius secret key (16 char max)
Enable DS62 usernames as backup..5  As written
Radius Login Timeout.............6  Enter timeout, in seconds(>=5 and <=30)
Exit.............................X,CR
```

Select "Radius Enable" to turn on or off radius authentication. If enabled, the primary radius server address must be specified.

```
    Radius login is..................Disabled
    Enable ? (Y/N), CR for no change) :
```

Select "Radius Server Address" to assign a specific radius server IP addresses.

```
    Radius Server IP Address is: 0.0.0.0
    Enter radius server address in dotted decimal form :
```

Select "Radius Backup Server Address" to assign a specific backup server IP addresses.

```
    Radius Backup IP Address is: 0.0.0.0
    Enter radius server address in dotted decimal form :
```

Select "Radius Secret" to assign a shared radius secret. A secret can be up to 16 characters and must be exactly the same as the secret stored on the server.

```
Radius secret is: HardlyASecret
Enter radius secret (16 chars max).
:
```

Select "Enable DS62 Usernames as Backup" to allow an unsecured access in case all specified radius servers are unavailable.

```
DS62 usernames as backup login is Disabled
Enable ? (Y/N), CR for no change) :
```

Select "Radius Login Timeout" a specific amount of time the DS will wait for a response from the radius server after sending the login message to the radius server. A timeout on a radius response is treated, per RFC specifications, as a rejection from the radius server.

```
Radius response timeout is         5 seconds
Enter timeout, in seconds ( >=5 and <=30 ) :
```

TACACS Configuration

TACACS can be used to authenticate logins for the serial port, the network port, modem or all three. When a telnet / SSH session (or rs232 session) is started the Host module will prompt for the username. After entering the username the Host will prompt for the password. After the password is entered the Host will communicate with the TACACS server. If the server verifies the username and password, the Host will display the menus. If the server rejects the username and password or does not respond the Host will display the reason why the login failed.

Setting Up TACACS

DS62-Network, DS62-MD4 Network/Modem Host Module

To enable TACACS for logins do the following:

- Enable TACACS from the TACACS configuration menu.
- Enter the IP address of the TACACS server
- Enter the IP address of the backup TACACS server if any.
- Enable local logins as a backup to the TACACS server if needed.
- Secret word must match the secret word in the TACACS server configuration.
- Enable usernames and passwords for the network and serial port via the logins setup access control menu.

Select TACACS Configuration from the Login Setup Menu and the DS displays the following:

```
TACACS Enable....................1   Enable/Disable TACACS
TACACS Server Address............2   TACACS server IP address 0.0.0.0
TACACS Backup Server Address.....3   Backup TACACS server IP address
TACACS Secret....................4   TACACS secret key (16 char max)
Enable DS62 usernames as backup..5   As written
TACACS Encryption Enable.........6   Enable/Disable encryption
TACACS Server Port...............7   Assign secure TCP port, Default = 49
Exit.............................X, CR
```

Select "TACACS Enable" to turn on or off the TACACS authentication on and off. If enabled, the primary TACACS server address must be specified.

```
TACACS login is...................Disabled
Enable ? (Y/N), CR for no change) :
```

Select "TACACS Server Address" to assign a specific TACACS server IP addresses.

```
TACACS Server IP Address is: 0.0.0.0
Enter TACACS server address in dotted decimal form :
```

Select "TACACS Backup Server Address" to assign a specific Backup Server IP addresses.

```
TACACS Backup IP Address is: 0.0.0.0
Enter TACACS server address in dotted decimal form :
```

Select "TACACS Secret" to assign a secret word shared between the TACACS server and this unit. A secret can be up to 16 characters and must be exactly the same as the secret stored on the server.

```
TACACS secret is: HardlyASecret
Enter TACACS secret (16 chars max).
:
```

Select "Enable DS62 Usernames as Backup" to allow an unsecured access in case all specified radius servers are unavailable.

DS62-Network, DS62-MD4 Network/Modem Host Module

```
DS62 usernames as backup login is Disabled
Enable ? (Y/N), CR for no change) :
```

Select "TACACS Encryption Enable" to turn TACACS+ encryption off or on. Sending unencrypted TACACS packets is useful for troubleshooting but should not be used under normal operations.

```
TACACS encryption is..............Enabled
Enable ? (Y/N), CR for no change) :
```

Select "TACACS Server Port to assign a more secure port, **default is TCP 49**.

```
TACACS server port is: 49
Enter port number (>= 1024, D for default 49): 12
```

If you type a port number less than 1024 the Host Module responds with the following until a valid entry is typed:

```
TACACS server port is: 49
Enter port number (>= 1024, D for default 49): 1234
```

Network Port Configuration

This menu is used to change the network configuration options such as the IP Address, Subnet Mask, Gateway, DHCP, and Telnet; all of which are necessary during initial startup. The *Connection Inactivity Timeout* allows you to enable/disable whether the firmware will end your session or "times out." The default is 1 hour, but when disabled there is no set time out. Disabling the *Carriage Return Translation* allows you to bypass all unnecessary carriage returns, and it will send you straight to the next "end of line." The *DHCP, Telnet, SSH,* options is to enable or disable these functions. SSH host key Generator allows the user to generate a host key which is used in the SSH encryption process.   *IP Filter* allows or blocks specific IP Addresses, *SNMP* provides a message format for communication between a computer and your devices, and *Web Server* Configuration allows web access and sets up options for each.

DS62-Network, DS62-MD4 Network/Modem Host Module

```
Network setup :
Ethernet Address................   00:C0:48:00:01:FD
IP Address......................    70.150.140.89
Subnet Mask.....................    255.255.255.224
Default Gateway.................    70.150.140.65

Connection Inactivity Timeout (mins): Disabled
Carriage Return Translation: Enabled
Break Length (msecs):  350
DHCP is Disabled   Telnet is Enabled    SSH is Enabled
SSH host keys are set to factory default

IP Address........................1
Subnet Mask.......................2
Gateway Address...................3
Inactivity Timeout................4
Carriage Return Translation.......5
Break Length......................6
DHCP Enable/Disable...............7
Telnet Enable/Disable.............8
SSH Enable/Disable................9
SSH Host Key Generation...........10
IP Filter Configuration...........11
SNMP Configuration................12
Web Server Configuration..........13
Exit..............................X,CR
```

> **IMPORTANT:** For network access, you must configure the IP addresses, Subnet Mask, and Gateway Address. The module must be reset for network changes to take effect.

IP Address

The IP address is the network address assigned by your network manager for your network. The IP Address consists of four bytes, each byte ranging from 0 to 255. This parameter must be programmed before the DS is accessible via the network.

Select 1) to enter the IP Address. Failure to enter the address in the decimal form causes the DS to display the following until it is entered correctly. **Default Module IP Address is 0.0.0.0.**

```
Enter IP address in dotted decimal form :
```

> **NOTE:** There should be no active connections while configuring the DS module. The unit should be reset upon completion of configuration.

Subnet Mask

The Subnet Mask is a bit mask that identifies the network portion of the IP address, allowing the DS to determine whether to send a packet directly to the client or to a gateway. The Subnet Mask consists of four bytes, each byte ranging from 0 to 255. **This parameter must be programmed before the DS-Series can be accessed through the network**.

Select 2) to enter the Subnet Mask followed by <cr>. Failure to enter the address in the decimal form causes the DS to display the following until it is entered correctly. **Default Subnet Mask is 0.0.0.0.**

> **Enter Subnet Mask in dotted decimal form :**

Gateway Address

The Gateway is the address of a router to connect to other parts of a network. The Gateway address consists of four bytes, each byte ranging from 0 to 255. If your network uses gateways, this parameter must be programmed before the DS can be accessed through the network.

Select 3) to enter the Gateway address. Failure to enter the address in the decimal form causes the DS to display the following until it is entered correctly. **Default Gateway address is 0.0.0.0.**

> **Enter Gateway address in dotted decimal form :**

Inactivity Timeout

This option enables the DS to disconnect after the programmed amount of time, if there is no activity. **Default is 0 (DISABLED)**. The enabling input can be from 1 to 120 minutes.

> **Connection Inactivity Timeout is 0 minutes**
> **Enter timeout, in minutes (<=120, 0 to disable) :**
> **Enter 0 to disable or a number between 1 and 120 (inclusive) to set the timeout.**

Carriage Return Translation

This option determines what the telnet processor will do with the line-feeds and nulls after a carriage return is sent. **Enable** tells the DS Telnet processor to strip line feeds or nulls **Translation** after the carriage returns. **Disable** allows the characters to pass through. **Default is "DISABLED"**.

> **Carriage Return Translation is.... Enabled**
> **Enable ? (Y/N), CR for no change) :**

Break Length

Users may configure the DS for a break length of 1 - 1000 milliseconds. In a Telnet session with the DS through the serial port of a DS74, send a Telnet break command (0xF3) to the DS, the serial port will send a break signal of the programmed duration. **Default is 350 milliseconds**.

> **Break Length is (msec)............ 350**
> **Enter break length, in milliseconds (<=10000, 0 to disable) :**

DS62-Network, DS62-MD4 Network/Modem Host Module

DHCP/Telnet/SSH

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. **Default setting is DISABLED.**

```
DHCP is...........................Disabled
Enable ? (Y/N), CR for no change) :
```

Telnet is a user command and an underlying TCP/IP protocol for accessing remote devices. On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. **Default setting is ENABLED.**

> **IMPORTANT:** Changing this setting will logout all SSH and Telnet sessions

```
Telnet is..........................Enabled
Enable ? (Y/N), CR for no change) :
```

Secure Shell (SSH), sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. **Default setting is ENABLED**.

> **IMPORTANT:** changing this setting will logout all SSH and Telnet sessions

```
SSH is............................Enabled
Enable ? (Y/N), CR for no change) :
```

SSH Host Key Generation

Selecting this option allows the user to generate a unique SSH host key for the DS unit. This key is part of the SSH encryption process. Each DS leaving Baytech is shipped with same default SSH host key. It is important that the user generate a new SSH host key if SSH communications will be used.

> **NOTE:** It can take the DS up to 10 minutes to generate a new host key.

```
Generate ? (Y/N)
```

IP Filter Configuration

The IP Filter Management Menu allows the admin user to pass or block certain IP Addresses.
If you have no rules defined the DS may display only options (**A, E, C**).

DS62-Network, DS62-MD4 Network/Modem Host Module

```
Filter Management Menu
Enter request or CR,X to exit menu.
  A)...Add Rule
  E)...Enable IP Filtering
  D)...Delete Rule
  V)...View Rules
  F)...Flush Rules
  C)...Set Default Target
Enter Request :
```

Select A) to add a rule. Type an IP address, select whether to drop or accept the address. The DS will display the following:

```
Please enter a single ip address filter
or an ip address block in ip/<blockmask> notation.
  : 70.150.140.95

Select a target option for this filter:
  DROP the packet..................1
  ACCEPT the packet................2
  Exit.............................X,CR
Enter Request :
```

Selecting either DROP or ACCEPT the packets and the DS will assign filter the next rule number:

```
Filter added as Rule 1.
```

Selecting E), Enable IP Filtering will enable or disable the filtering function. The DS displays:

```
IP Filtering is ENABLED.   Enable? (Y/N): y
```

Select V), View Rules allows the user to see any IP filtering. Note: At least one rule must be defined for this option to be available. The DS displays:

```
Rule Num    Ip Address          Target
1           70.150.140.95       DROP
2           70.150.140.96       ACCEPT
```

Select C), Set Default Target for ALL IP Addresses to accept or drop all. The DS displays:

```
The default target is............ACCEPT
DROP ? (Y/N), CR for no change) :y
```

Select F), Flush Rules to delete all rules. The DS displays:

DS62-Network, DS62-MD4 Network/Modem Host Module

```
Are you sure you want to delete all filters? (Y/N)
Enter Request :y

All filers have been deleted.
```

Select D), Delete Rule to delete a specific rule. The DS displays:

```
Delete Filter Menu
Enter rule number to delete rule, 'M' to view
more rules, or 'X' to exit menu.
Rule Num    Ip Address            Target
1           70.150.140.95         DROP
2           70.150.140.96         ACCEPT
3           70.150.140.99         ACCEPT
Enter Request :2

Filter Rule 2 deleted.
```

SNMP Configuration

Selecting the SNMP Configuration and the Host Module respond:

```
SNMP Trap Host 1 Address..........1
SNMP Trap Host 2 Address..........2
SNMP Trap Host 3 Address..........3
SNMP Trap Host 4 Address..........4
SNMP Read-Only Community..........5
SNMP Read-Write Community........6
SNMP Enable......................7
SNMP v3 Only Enable..............8
SNMP Authentication Traps Enable..9
Exit.............................X,CR
```

Depending on the firmware, SNMP Configuration allows the admin to control whether or not a user has Read/Write access or Read access only. It also allows the admin to control which IP addresses are allowed to receive a host trap, and simply whether to enable or disable the entire SNMP function.

> **IMPORTANT:** You will need some knowledge of SNMP protocols in order to get the Baytech device to work with your SNMP program. Information provided is for the SNMP Agent only. Baytech Support will assist with the Agent part only. For SNMP Manger assistance refer to the vender manual or contact the vender of the SNMP software you are using.

> **NOTE:** There are a number of shareware MIB Browsers that can be downloaded from the internet to make changes and receive traps for a quick verification test.

> **NOTE:** To use the SNMP functions you need to download the MIB from Baytech's web site, www.baytech.net. Look under Tech Support, Docs and Downloads.

> **IMPORTANT:** Changes do not take effect until they are saved when you leave the configuration menu. The DS will display:

DS62-Network, DS62-MD4 Network/Modem Host Module

Accept changes ? (Y/N) :

The SNMP Trap Host is a trap management station that receives and processes traps. Traps are system alerts that the Baytech device generates when certain events occur. By default, no trap manager is defined, and no traps are issued. Up to four SNMP Trap Hosts maybe assigned to receive traps. Select a "SNMP Trap Host", the DS will display the following, **Default address is (0.0.0.0) for all Hosts.**

SNMP Trap Host 1 IP Address: 220.225.36.212
Enter new Trap Host IP Address:

SNMP Trap Host 2 IP Address: 70.154.96.10
Enter new Trap Host IP Address:

SNMP Trap Host 3 IP Address: 192.168.1.102
Enter new Trap Host IP Address:

SNMP Trap Host 4 IP Address: 192.168.2.136
Enter new Trap Host IP Address:

Read/Write Community String:

Community String:

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for your SNMP script/software to access the Baytech SNMP, the community string definitions on your SNMP script/software must match the Baytech SNMP string definitions.

'**Read**'—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access.

'**Write**'—Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings

Select 'SNMP Read Only Community' option to enter a Read Community string, the DS displays the current setting, **Default is public**.

SNMP Read Community name: public
Enter Read Community Name:

Select 'SNMP Read-Write Community' option to enter a Write Community string, the DS displays the current setting, **Default is private**.

SNMP Write Community name: private
Enter Write Community Name:

Select the 'SNMP Enable' option to enable the SNMP function, the DS displays, **Default is Enabled**.

SNMP is ENABLED. Enable? (Y/N):

DS62-Network, DS62-MD4 Network/Modem Host Module

If you have SNMPv3 software, only the newer firmware will have this option. Selecting this option the DS displays, **Default is Disabled.**

```
SNMPv3 only is DISABLED.  Enable? (Y/N):
```

Select this option to enable a SNMP trap to be sent if an authentication attempt failed, the DS displays, **Default is Disabled.**

```
SNMP Authentication traps are DISABLED.  Enable? (Y/N):
```

Web Server Configuration

Selecting the Web Server Configuration option and the DS displays the following:

```
Web Enable.........................1
Web Login Enable...................2
Web Secure Login Enable............3
Web Login Activity Timeout.........4
Exit...............................X
```

> **NOTE:** For this feature to operate the network port must have an IP Address assigned.

Depending on the firmware in your DS unit, the newest firmware will have the Web Server Configuration menu. To get to the unit web page, type the unit IP address, i.e. http://70.150.140.95.

> **NOTE:** The web page is a quick test to see if SNMP protocol is working in the unit, if SNMP has been enabled.

> **IMPORTANCE:** Currently, all users who access the DS through the web page have administrator privilege.

Select 1), Web Enable to enable or disable the web page feature, the DS displays, **Default is Enabled:**

```
Web is ENABLED.  Enable? (Y/N):
```

Select 2), Web Login Enable to enable or disable the login window to the web page, the DS displays, **Default is Enabled:**

```
Web Login is DISABLED.  Enable? (Y/N):
```

Select 3), Web Secure Login Enable to enable or disable a secure web connection to the web page, the DS display, **Default is Disabled:**

```
Web secure SSL connection is DISABLED.  Enable? (Y/N):
```

Select 4), Web Login Inactivity Timeout to set the Inactivity timeout to the web page, the DS displays, **Default is zero minutes:**

```
Web Connection Inactivity Timeout is  0 minutes
Enter timeout, in minutes (<=120, 0 to disable) :
```

Module Name

This option allows the admin users to change the modules name.

```
Module Name is:  DS62-MD4
Enter Module Name (32 chars max).
:
```

DS Management

These options are independent of the power strip's Alarm Thresholds. It is through these settings that the DS62 SNMP agent will send a (trap) to the designated SNMP Manager.

Use this option to set the temperature, voltage, and current alarm threshold for the DS as shown.

```
Host-controlled DS Feature Configuration
   Temperature Alarm Threshold........1
   Under Voltage Alarm Threshold......2
   Over Voltage Alarm Threshold.......3
   Low Current Alarm Threshold........4
   Environmental Sensors..............5
   Outlet Groups......................6
```

Internal Alarm Threshold

Select any alarm threshold option and the DS will display the following:

Temperature Alarm Threshold:

Sel	M/P	Identifier	Tmp Lvl
1	2/1	DS3ADE	500

Under Voltage Alarm Threshold:

Sel	M/P	Identifier	Lo V Lvl
1	2/1	DS3ADE	900

Over Voltage Alarm Threshold:

Sel	M/P	Identifier	Hi V Lvl
1	2/1	DS3ADE	1300

Low Current Alarm Threshold

DS62-Network, DS62-MD4 Network/Modem Host Module

```
Sel  M/P    Identifier    Low Curr
 1   2/1    DS3ADE           0
```

Enter the Selection number and the unit will display one of the following dependent on the alarm:

Enter threshold value in tenths of unit measurement (degrees,%,etc.):

Enter voltage threshold value in tenths of a volt:

Enter low current threshold value in tenths of an amp:

NOTE: M/P = Module number and Port number; Identifier = this unit's model number; Tmp Lvl = temperature level, Lo V Lvl = low voltage level, Hi V Lvl = High voltage level, low Curr = Low Current. The unit's firmware determines whether the degrees are Celsius or Fahrenheit. Currently there is no option to change the degrees.

External Alarm Threshold

Selecting the Environmental Sensors with no probes attached the DS will display the following:

None of the installed devices support this option (no temperature probes installed).

Strike ENTER to continue

Selecting the Environmental Sensor with a probe attached the DS will display the following:

```
Environmental Sensor Configuration Menu
  Sel  M/P     Identifier
  1    2/1     DS3ADE
  2    All Sensors
```

Select 1), the DS displays:

```
Sel  Type        Name          Hi/En  Lo/En  St/En
 1  Contact     External Sensor1 N/A   N/A    Ds
 2  Temperature External Sensor2 0/Ds  0/Ds   N/A
    Enter Request :2
```

Selecting probe 2 displays a recognized temperature probe:

DS/RPS External Environmental Sensor Configuration Menu
Sensor Number: 2   Name: External Sensor2 Type: Temperature

1...High Threshold (tenths of meas. unit): 0
2...High Threshold Trap Enable: Disabled
3...Low Threshold (tenths of meas. unit): 0
4...Low Threshold Trap Enable: Disabled

Enter Request :1

DS62-Network, DS62-MD4 Network/Modem Host Module

Option 1 and 3 sets the temperature levels to the tenth of a degree. Option 2 and 4 enable the SNMP traps to be sent if the corresponding threshold had been exceeded.

Sel	Type	Name	Hi/En	Lo/En	St/En
1	Contact	External Sensor1	N/A	N/A	En
2	Temperature	External Sensor2	999/En	320/En	N/A

Select 2), 'All Sensors' option allows the administrator to set parameters for the different probe types. This feature is useful for standardization and the probe type is not known due to its final location is not known. The DS displays:

```
For configuration of all sensors of selected type in system with a
single user-supplied value.

1...Contact
2...Temperature
3...Humidity
4...Air Flow
Enter Request :1
```

NOTE: The type 'Contact' signifies the unit does not recognize or detect a probe, but still be able to send SNMP Traps.

Select the specific option to set the High and Low alarm ranges and their corresponding SNMP traps.

```
DS/RPS External Environmental Sensor Configuration Menu
Sensor Number: All Name: all DSs/RPSs     Type: Temperature/Humidity/Air Flow

  1...High Threshold (tenths of meas. unit): NP
  2...High Threshold Trap Enable: NP
  3...Low Threshold (tenths of meas. unit): NP
  4...Low Threshold Trap Enable: NP

Enter Request :

Enter threshold value in tenths of unit measurement (degrees,%%,etc.):
```

Outlet Groups

This is a future option not currently used. This option sets up the outlets into groups.

```
Outlet Group Configuration:

List Outlet Groups...............1
Add Group........................2
Delete Group.....................3
Rename Group.....................4
Modify Outlets in a Group........5
Delete All Outlet Groups.........6

Enter Request :1
```

DS62-Network, DS62-MD4 Network/Modem Host Module

Select 1), List Outlet Groups to list any outlet groups, the DS display:

```
# Group Name              Outlets
1 Router GP-A             2.1.1,2.1.2,2.1.3,2.1.4
2 Server Row              2.1.5,2.1.6,2.1.7,2.1.8
3 Radius                  2.1.9,2.1.10,2.1.11,2.1.12
4 Server backup           2.1.13,2.1.14,2.1.15,2.1.16
```

Select 2), Add Group to add a specific outlet group, the DS display:

```
List up to four outlets in the following form mod.port.outlet,mod.port.outlet
2.1.1,2.1.2,2.1.3,2.1.4
```

The DS displays the following and asks for a name for the new Group:

```
Outlet group is currently defined as:
 #  Group Name              Outlets
 1                          2.1.1,2.1.2,2.1.3,2.1.4

Enter name for outlet group (max 23 characters): Router GP-A
```

Select 3), Delete Group to delete a specific outlet group, the DS displays the following:

```
Enter group number to be deleted: 3
Group deleted
```

Select 4), Rename Group to rename an outlet group's name, the DS displays the selected group:

```
Enter number of group to be renamed: 3

Outlet group is currently defined as:
 #  Group Name              Outlets
 3                          2.1.9,2.1.10,2.1.11,2.1.12

Enter name for outlet group (max 23 characters): Radius
```

Select 5), Modify Outlets in the Group and the DS displays:

```
Enter number of group to be modified: 4

Outlet group is currently defined as:
 #  Group Name              Outlets
 4 Server backup            2.1.13,2.1.14,2.1.15,2.1.16

List up to four outlets in the following form mod.port.outlet,mod.port.outlet
```

Example of an outlet change by retyping the group with the new outlets:

```
2.1.13,2.1.14,2.1.17,2.1.18
```

Select 6), Delete All Outlet Groups and the DS displays:

```
Delete ALL outlet groups? (Y/N): y
```

Note: There will be no confirmation the groups have been deleted. Select option 1 from the Outlet Group Configuration to verify all outlet groups were deleted.

```
#  Group Name              Outlets

Strike ENTER to continue
```

Firmware / Config Download

This option allows the admin to flash upgrade the firmware to the Host module through an FTP client. The admin can upload the configuration file, make changes, and download back to the unit. This feature ensures multiple units will have the same configuration without having to manually configure each unit separately.

```
Enable Firmware Upgrade...........1
Enable SSL Cert Upload............2
Enable Configuration File Upload..3
Restore Configuration Defaults....4
Get Current Configuration File....5
Display Configuration Error Log...6
Exit..............................X,CR

Enter Request :
```

NOTE: Contact Baytech Support for the instruction sheet and firmware upgrade file.

Enable Firmware Upgrade

This option must be enabled to upgrade the firmware via FTP. The DS unit will display the following, **Default is Disabled**:

```
Enabling this will allow the firmware to be updated via ftp
Enable Firmware Upgrade ? (Y/N)
```

IMPORTANT: Do not type 'Y' unless you have received the instructions and firmware from Baytech's Technical Support. If you typed 'Y' and see the following below, turn power off than back on to the unit to close the firmware upgrade.

```
Waiting to receive compressed image file
----------------------------------------------------------------------------
----------------------------------------------------------------------------
--------------------------------------------
```

At this point follow the instruction to FTP the firmware into the unit.

DS62-Network, DS62-MD4 Network/Modem Host Module

Enable SSL Cert Upload

Selecting this option allows the admin to upload an SSL Certificate to the DS unit via ftp. The filename of the certificate must be (ssl.pem). An SSL certificate is used by the unit to create secure web connections. The DS unit is shipped with a default SSL certificate. This certificate should be replaced with one that better suits the user's environment. The file format is checked after download to insure that the certificate is valid.

Select this option to Enable SSL Cert Upload, the Host Module will display the following:

> **Enabling this will allow the SSL Certificate to be updated via ftp**
> **Enable SSL Certificate Upload? (Y/N)**

IMPORTANT: If you type 'Y', the DS will display the following. To stop this function power-cycle the unit to close the SSL Certification Upload.

```
Waiting to receive ssl.pem SSL certificate file
--------------
```

At this point FTP the ssl.pem file into the module.

Enable Configuration File Upload

This option allows the admin to upload a configuration file from your computer to the DS.
Select Enable Configuration File and the DS displays the following:

> **Enabling this will allow the system configuration to be updated via ftp**
> **THE UNIT WILL RESET AFTER CONFIGURATION IS COMPLETE**
> **Enable Configuration File Upload? (Y/N)**

IMPORTANT: If you type 'Y', the DS displays the following below. To stop this function power-cycle the unit to close the Configuration File Upload.

```
Waiting to receive configuration file
-------------------------------------------------------------------------
------------------------------------------------------------------
```

At this point FTP the file into the unit. A successful file upload and the DS will display:

```
configuration file valid

updating ds62 configuration
***
ds62 host configuration complete
polling DSs
Found DS at mod 2 port 1
DS polling complete
configuring DSs
```

Unsuccessful file upload and the DS will display:

```
***error in config upload file or transfer operation***
```

> **NOTE:** This part of the program is derived from the DS62 module program, thus the DS62 reference.

Restore Configuration Defaults

This option allows the admin to restore the DS configuration to factory defaults.

> **NOTE:** The network **default** IP Address, Subnet, and Gateway is **0.0.0.0**

Select Restore Configuration Defaults and the DS displays the following:

```
ENABLING THIS WILL ERASE ALL CONFIGURATION BACK TO FACTORY
DEFAULTS AND RESET THE UNIT
Set Configuration to Factory Defaults? (Y/N)
```

A YES response and the DS will display:

```
SETTING DEFAULT CONFIGURATION
set default password file
USING DEFAULT SSL CERTIFICATE

System reset in progress...

This board is a Universal DS Controller
..........Uncompressing...done.
```

Get Current Configuration File

This option allows the admin to get a copy of the current DS configuration file from the unit and FTP's it to your computer. The configuration file to be uploaded is named "confupload". The file maybe opened with any text file editor.

> **NOTE:** Save a copy of the "confupload" file under a different name, just in case a mistake is made that prevents the unit from operating properly. If the unit appears to not respond, power-cycle the unit and type semi-colon five times. If it appears the unit is still not responding, follow the reset procedures to reset the module.

Select Get Current Configuration File and the DS displays:

```
Enabling this will allow the system configuration
file to be retrieved via ftp

Enable Configuration File Retrieval? (Y/N)
```

A YES response and the DS will display the following:

DS62-Network, DS62-MD4 Network/Modem Host Module

```
+----+------+----------------+------+------+------+------+---------+----+----+
|Port|Device|     Device     | Baud | Word | Stop |Parity|Handshake|LineDrive|
|    | Type |     Name       | Rate | Size | Bits |      |         |DTR |RTS |
+----+------+----------------+------+------+------+------+---------+----+----+
| 2  | MODEM| Host V90 Modem | 9600 |  8   |  1   | None | None    | LO | LO |
+----+------+----------------+------+------+------+------+---------+----+----+
   Handshaking......................1
   Baud Rate........................2
   Word Size........................3
   Stop Bits........................4
   Parity...........................5
   Enter Request :
```

Select "Handshaking" and the DS displays with the following:
Default is None

```
Select handshaking:
  1 For None
  2 For Software Handshaking
  3 For Hardware Handshaking
  Enter Request :
```

Select "Baud Rate" to change the rate the modem transfers Data bites per second, the DS displays the following: **Default is 9600**

```
Select baud rate:
  1 For   300
  2 For   600
  3 For  1200
  4 For  2400
  5 For  4800
  6 For  9600
  7 For 19200
  8 For 38400
  9 For 57.6K
  A For 115.2K
  Enter Request :
```

Select "Word Size" and the DS displays the following: **Default is 8**

```
Select word size:
  1 For   7
  2 For   8
  Enter Request :
```

Select "Stop Bits" the DS displays the following: **Default is 1.**

DS62-Network, DS62-MD4 Network/Modem Host Module

```
Select stop bits:
  1 For   1
  2 For   2
  Enter Request :
```

Select "Parity" the DS displays the following: **Default is None.**

```
Select parity:
  1 For  None
  2 For  Even
  3 For   Odd
  Enter Request :
```

Rings to Auto Answer

Select "Rings to Auto Answer" to set the number of rings before the unit answers. The module displays the following: **The default setting is 2**.

```
Rings to Auto Answer: 2
Enter number (1-4):
```

Modem Connectivity Timeout

Select the Modem Connectivity Timeout option to set the continuous connectivity time (1 to 120 minutes) before the modem automatically disconnects. Entering a time of 0 disables the Connectivity Timeout. The timer starts when the modem answers (DCD goes high). The modem will disconnect, regardless of activity, when time runs out. **Default setting is 60 minutes.** The module displays the following:

```
Modem Connectivity Timeout (Minutes): 60
Enter Timeout (1-120 minutes, 0 to disable):
```

Modem Inactivity Timeout

This option sets the time the modem will automatically disconnect, if there is no activity equaling the programmed amount of time (1 to 120 minutes). **Default setting is 0 (disabled)**.
Select Modem Inactivity Timeout and the module display the following:

```
Modem Inactivity Timeout (Minutes): 60
Enter Timeout (1-120 minutes, 0 to disable):
```

Modem Device Name

Select Modem Device Name and the following is displayed:

DS62-Network, DS62-MD4 Network/Modem Host Module

```
Modem Device Name: Host V90 Modem
Enter Device Name (<= 16 characters):
```

Caution: Once you make a change to any of the Configuration options, you have to back out of the Configuration menu and will be asked to Accept changes.

```
Accept changes ? (Y/N) :y
  Changes accepted.
```

Status Menu

```
DS62 Status Menu.
  Enter selection, CR to exit.

  Overall System Status.............1
  Network Status....................2
  Logged Users......................3
  Memory Usage......................4
  Current Routing Cache.............5
  Route Setup.......................6
  Processes.........................7
  UnitInfo Database.................8
```

Overall System Status

System Status provides information about the local memory, how many TCP sockets are in use, and the time the unit has been operating since the last unit reset or power up.

```
System Status:
    Available local memory:  7598080
    TCP sockets in use:            0
    System up time (dd:hh:mm:ss): 0:00:50:10

  Press ENTER to continue
```

Network Status

Network Status contains the MAC address, IP address, Mask, TX/RX packets and their status.

DS62-Network, DS62-MD4 Network/Modem Host Module

```
eth0        Link encap:Ethernet  HWaddr 00:C0:48:00:01:FD
            inet addr:192.168.2.136  Bcast:192.168.2.255  Mask:255.255.255.0
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:100
            Base address:0x840

lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0

  Press ENTER to continue
```

Logged Users

This option shows the number of active sessions. For each session, the name of the user account, the type of interface (serial or network) and the status is provided.

```
C=configuration user    *=current process
Active Users:
  #  USER                              FROM              INTERNAL CONN STATUS PID
* 1  root                              localhost                       Normal  25

  Strike T, CR to terminate a connection/process, CR to continue :
```

Terminate a session by typing "T" at the prompt. The Host Module responds:

```
Enter number of connection to terminate, CR :
```

Memory Usage

```
        total:     used:     free:   shared: buffers:   cached:
Mem:  11735040  4136960  7598080         0   380928    458752
Swap:        0        0        0

  Press ENTER to continue
```

Current Routing Cache

IP Data currently held in cache or none upon power cycle.

```
Kernel IP routing cache
Source           Destination   Gateway         Flags Metric Ref    Use Iface


Press ENTER to continue
```

Route Setup

Every TCP/IP client machine, regardless of operating system, needs to make decisions about where to send a packet after it has been addressed. The route table is the network map that tells your Baytech product how to deliver the packet to its network addressee.

- Destination, is a list of routes. "0" represents any number.
- Gateway, is the network gateway for the route. The connection point to your company network.
- Genmask, It defines how closely an address must match the network destination, octet by octet, to use the route.
- Iface, is the interface used to reach the network gateway, in this case the interface is the Baytech network card.

```
Kernel IP routing table
Destination     Gateway        Genmask         Flags Metric Ref    Use Iface
192.168.2.0     *              255.255.255.0   U     0      0        0 eth0
127.0.0.0       *              255.0.0.0       U     0      0        0 lo
default         192.168.2.1    0.0.0.0         UG    0      0        0 eth0


  Press ENTER to continue
```

Processes

Processes are a list of commands used by the firmware to operate.

```
 PID PORT STAT SIZE SHARED %CPU COMMAND
   1       S    133K    0K  0.2 init
   2       S      0K    0K  0.0 keventd
   3       R      0K    0K  0.0 ksoftirqd_CPU0
   4       S      0K    0K  0.0 kswapd
   5       S      0K    0K  0.0 bdflush
   6       S      0K    0K  0.0 kupdated
  11       R     43K    0K 99.3 baytechd
  12       S     13K    0K  0.1 mdmautologind
  13   S0  S     13K    0K  0.1 /bin/autologind
  14       S     14K    0K  0.0 /bin/inetd
  17       S    133K    0K  0.1 DScmdd
  18       S     13K    0K  0.0 snmppolld
  19       S   1833K    0K  0.0 snmpd
  25   S0  R     71K    0K  1.0 ds62


  Strike T, CR to terminate a connection/process, CR to continue :
```

Type 'T', and the unit responds:

```
Enter PID process to terminate, CR:
```

Enter a PID number and press 'Enter' to terminate the process.

IMPORTANT: If a process is terminated, the functionality of the unit maybe interrupted. To reestablish the unit's functionality, power the unit off than back on.

UnitInfo Database

```
unitInfo->portUser 0
unitInfo->cfgUser 0
unitInfo->connState 0
unitInfo->connPid 0
unitInfo->buildUserTableFlag 0
unitInfo->kill_poller 0
unitInfo->background_polling=0
bcTable->connAttempt=0

hit ENTER to continue
```

Unit Reset

NOTE: Resetting the unit does not return user selections to their default settings.

Select RU), to reset the unit to the current configurations, the DS will display:

Reset Unit? (Y/N)

A Unit Reset takes approximately 10 seconds for the unit to reset. It will not affect the state the energized outlets are in. It will not reset the unit to "Factory Default", but it will terminate the external communications.

Logout

Select T), will close the session to the unit, but may not close the terminal emulator session.

Troubleshooting:

Functional Solutions:

1. **No menu serial port:**
    a. DS power is on and cable connected to EIA232 serial port.
    b. Verify the cable and adapter has the correct pin out, RJ08X007 and 9FRJ45PC-1.
    c. Cisco Rollover cables have the same pin out as RJ08X007.
    d. Type 5(;), the Attention Character will not echo to the screen, if it does than it may have been changed to a character other than the semi-colon.
2. **No Menu Ethernet Port:**
    a. Note what the CX LED is doing, refer to Appendix C.
    b. Verify the Ethernet port is connected to your network via an Ethernet cable. The LINK LED is lit for a valid connection.
    c. Type 5(;) semi-colon, the Attention Character will not echo to the screen, if it does print or **Unknown character** than type each character on the keyboard 5-times until you discover the Attention character, else reset unit configuration.
3. **Password not Work:**
    a. Password is case sensitive, check for Caps Lock.
    b. Have the admin user delete the user and add back
        i. Refer to DS Configuration/User Management 'Delete a User' and 'Add a User' section.
        ii. Refer to Network Access Configuration/Login Setup/Manage Users
4. **Network session locks up:**
    a. More than 4 sessions are open, close one session.
5. **No Access to Configuration Menu:**
    a. Only one user at a time can have access. Have the other user back out of the configuration
6. **No DS74 Ports displayed for User:**
    a. DS74 Ports have to be assigned to the user, refer to 'DS Configuration User Management, Change User's Port Access and Password' section.
7. **Not able to PING unit:**
    a. Verify unit connected correctly to network.
    b. Verify unit network configuration is correct.
    c. In the Network Configuration Status Menu, verify the unit has a valid MAC address. The last six digits of the MAC address are the hexadecimal equivalent of the first eight digits of the unit serial number. (i.e. MAC address = 00:C0:48:<u>0A:B6:59</u> equals to decimal 702041)
8. **Verify DS unit is functioning:**
    A rollover cables (pin out 1-8, 2-7, 3-6, 4-5, 5-4, 6-3, 7-2, 8-1) and a 9-pin adapter (9FRJ45PC-1) and Ethernet or Modem cable.

    a. Set up the Host module with modem or Ethernet cables for normal operations.
    b. Connect the rollover cable and adapter from the PC to a DS74 port.
    c. Create a Modem/Ethernet session, (Hyper-terminal). Type semi-colon 5-times (; ; ; ; ;).
    d. The main menu should display the DS74 ports. Select the port connected to the PC from step 2. The cursor will move to next line and wait.

    e. From your PC create a terminal session to the serial port. Default setting is 9600, 8, 1, no parity, no flow.

    f. Type several random characters to see them echoed in the telnet/modem session.

    g. Select the telnet/modem session and type several random characters to see them echoed in the PC serial session.

    h. This verifies the Chassis, Host module, and the I/O port is working.

    i. Move pc cable to next DS74 port and repeat steps (c-h).

If a DS74 module appears not to be working, move the module to a different slot and retest.

DS62 and DS62-MD4 Reset procedure
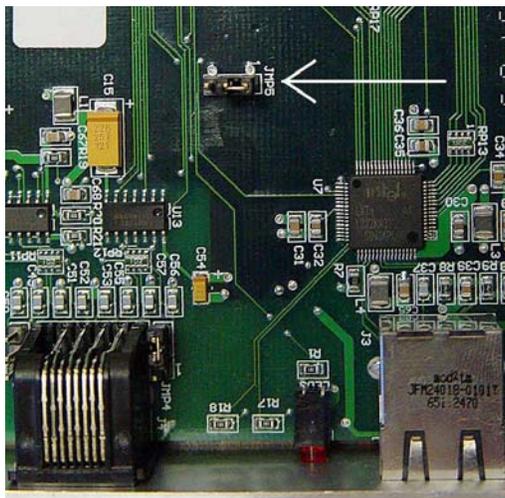
Figure 1
DS62-MD4 similar to DS62

Caution: This procedure will reset configuration to factory default.

DS62/DS62-MD4:

1. Remove the module from the chassis (with the unit powered down).
2. Hold the module with the chip side up and the faceplate towards you.
3. Locate jumper JMP5 approximate center of circuit board.
4. Move the jumper from pins 1 and 2 to pins 2 and 3.
5. Put the module back in the chassis and power up for 15 seconds.
6. Take the module back out and replace the jumper to the original position.

The module is now reset to factory default.

Note: If the module appears not to have reset or opening menu has random characters in it, perform the reset procedure again except increase the reset time from 15 to 30 seconds.

BayTech Product Warranty

Bay Technical Associates (BayTech) warrants that its products will be free from defects in materials and workmanship under normal use for a period of two years from date of purchase (or from date of shipment from BayTech if proof of purchase is not provided).

During this warranty period, BayTech shall, at its discretion, either repair or exchange any defective product at no charge for labor and materials, or refund the amount paid for the product, less shipping and handling charges. Any replacement and/or repaired products are warranted for the remainder of the original warranty.

The customer is responsible for properly packaging the product and for shipping costs for returns. The customer is liable for loss or damage to the product during shipping, as well as any other fees or charges associated with transporting the product back to BayTech. BayTech will pay return costs for delivery within the Continental United States.

All repair and return shipments must be approved by BayTech and must be accompanied by an RA (return authorization) number. Please refer to our Repair and Return Policy below.

For the initial 30 days from the original date of shipment, any unopened product may be returned to BayTech, accompanied by an RA number. Full purchase price will be refunded, provided that the product is in excellent condition. A product may not be returned after 30 days from the original date of shipment unless approved by BayTech management.

Replacements for defective products may be cross-shipped to the customer at no cost if requested within 30 days of date of purchase. At BayTech's discretion, this period may be extended to 90 days. For additional information or more specific warranty issues, contact BayTech's Technical Support Department at **(800) 523-2702** or **(228) 563-7334**.

Exceptions
This warranty does not cover misuse or minor imperfections that fall within design specifications or that do not materially alter functionality. BayTech does not warrant and is not responsible for damages incurred in shipping and handling or caused by disasters (such as fire, flood, wind, earthquake, lightning, power surges or water).

The warranty will be voided regarding products that have been neglected, altered, abused, misused, or used for purposes other than those for which it was designed.

Under no circumstances shall BayTech be liable for any special, incidental, or consequential damages based upon breach of warranty, breach of contract, negligence, strict liability, or any other legal theory. Such damages include (but are not limited to) loss of profits, loss of the product or associated equipment, cost of capital, cost of substitute or replacement equipment, facilities or services, down time, purchaser's time, the claims of third parties, including customers, and injury to property.

BayTech Extended Warranty
Extended warranties and overnight replacements are available for purchase, but only at the time of product purchase. The extended warranty cost will not exceed 7% per year of the product list price unless otherwise stated in the customer contract or approved by BayTech management. Contact BayTech for further details on this.

DS62-Network, DS62-MD4 Network/Modem Host Module

Technical Support

BayTech offers Tech Support for the lifetime of the product. A staff of Applications Engineers is on duty to assist with installation, set up or operation issues. Support is available from **8:00 a.m. to 5 p.m**. (CST or CDT), Monday through Friday at the phone numbers or website provided below.

Please have the following information available to help the Applications Engineers answer questions efficiently:
1. BayTech model type
2. Unit serial number
3. Firmware version (if accessible)
4. A list of devices connected to the BayTech unit
5. A general description of the application being used and the intended outcome
6. Information about cables and adapters being used (type, length, place of purchase)
7. The name of the software emulation program being used
8. Printout of the configuration status (if possible)

Bay Technical Associates, Inc.
5239 A Avenue
Long Beach Industrial Park
Long Beach, MS 39560
Telephone: 800-523-2702 or 228.563.7334
FAX: 228.563.7335
Email: support@baytech.net
Website: www.baytech.net

Repair and Return Policy

(Return policy refers to BayTech products purchased and returned for credit or repair.)
A Return Authorization (RA) number must be obtained in all cases before returning the BayTech product. Have the serial number and reason for the return or description of the problem handy. Customers in the Continental U.S. can call 1-800-523-2702 or international customers can call 228.563.7334 to obtain an RA number.

If a product is being returned for credit (based on BayTech approval), the credit will not include shipping and handling charges. Determination of credit amount will be made after BayTech receives the product.
Returns on BayTech products older than 3 months are subject to a 15% re-stocking fee of the list price of the product and will be evaluated on a case-by-case basis. BayTech does not allow returns on products out of warranty or for any type of custom product.

Before dismantling equipment or returning the unit for any reason, always contact BayTech. Attempting to repair a product without BayTech authorization may result in voiding the warranty.

Follow the instructions below for repackaging and shipping. **NOTE:** *Power should be disconnected from the power source before servicing or dismantling.*

DS62-Network, DS62-MD4 Network/Modem Host Module

Return Authorization Process:

1. Contact BayTech to get a Return Authorization (RA) Number. **IMPORTANT:** *BayTech will not accept any returns without an RA number.*
2. Package the unit carefully in its original packaging or similar packaging. The warranty does not cover damage sustained during shipment. Enclose a letter with name, address, RA number, daytime phone number and description of the problem.
3. Mark the RA number clearly on the outside of the package.

NOTE: If the RA number is not on the outside of the box, the package will be returned back to the sender or will sit in Receiving until the customer calls in regarding status of RA.

4. Ship the unit by insured, prepaid carrier to the following address:

   Bay Technical Associates
   5239 A Avenue
   Long Beach Industrial Park
   Long Beach, MS 39560
   RA #: 140-xxxxx

5. Surround your unit with a minimum of two inches of insulation.

6. Be sure to seal the box securely with strapping or packing tape. We do not recommend masking tape or cellophane tape.