2019

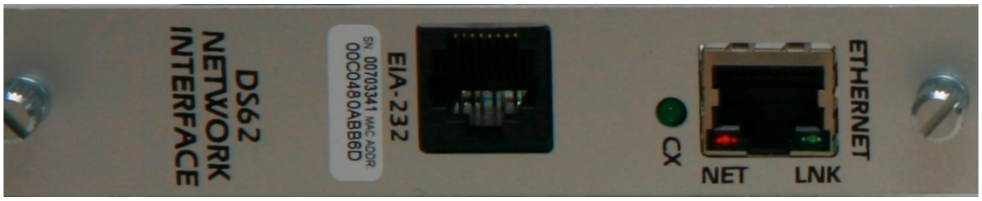
DATA SWITCH DS62/DS62-MD4

BayTech®

Bay Technical Associates, Inc

2/1/2019

DS62 Ethernet Host Module



DS62-MD4 Ethernet & 56K Modem Host Module

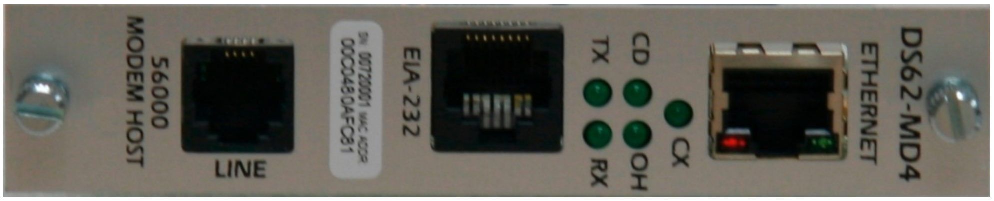


Table of Contents

ABOUT THIS DS62 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 power products and data switches. 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.

COMPLIANCE STANDARD

BayTech units are in accordance with the general requirements of *Standard for Information Technology Equipment* (ETL listed, conforms to ANSI/UL 60950-1 2nd Edition and CAN/CSA C22.2 No. 60950-00. CE conforms to IEC 60950.) *Equipment installations are to be in accordance with the Canadian Electrical Code, Part I, CSA C22.1-02; General Requirements – Canadian Electrical, Part II, CSA C22.2 No 0-M91; the National Electrical Code, NFPA 70-2005; and the National Electrical Safety Code, NFPA, IEEE C2-2002.*

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.

CONNECTION DESCRIPTION

BayTech's Modular Series unit provides a Serial EIA232 interface that controls user access and outlet controls to the power strip.

CAUTION: All power should be removed from the BayTech unit prior to removing or installing cables and /or adapters.

EIA-232 SERIAL CONNECTION

The RPC has 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.

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.

Internal Modem Communications

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. 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.

IMPORTANT: The DS62-MD4 modem option and the Ethernet port have priority over the EIA-232 serial port. If a serial port user is connected to a DS74 I/O port when a modem or Ethernet connection is established, the serial port user will be “booted” off, allowing the remote user to communicate with the DS unit. Whichever port user is the configuration mode cause the message to be sent to the other port user, “Configuration Mode in use”

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 Customer 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 DS Chassis, DS62/DS62-MD4 Host Module and DS74 Modules.
2. Manual insert describing the location of the User's Guide on BayTech's website at http://www.baytech.net/support/ftp_series.php.
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 and **(RJ04X007 if host module has an internal modem).**

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.

PRÉPARATION DE L'EMPLACEMENT D'INSTALLATION

Le secteur d'installation devrait être propre et exempt des températures et de l'humidité extrêmes. Permettez le suffisamment d'espace derrière l'unité de DS pour des raccordements de câblage et de réceptacle. L'accès à l'emplacement d'installation devrait être limité au personnel autorisé. L'installation de ces unités devrait être limitée à ITE et à environnements de serveur de Telco.

POWER

- **208V VAC Model:** Internal 208 VAC 50/60 Hz, 10 Amps Maximum Load.
- **120V VAC Model:** Internal 120 VAC 50/60 Hz, 15, Amps Maximum Load.

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 DS Series Unit unless specifically directed to by BayTech personnel. BayTech must perform any internal operations.

ATTENTION: Cette unité est prévue pour l'usage d'intérieur seulement. N'installez pas près de l'eau ou n'exposez pas cette unité à l'humidité. Pour empêcher l'habillage de la chaleur, ne lovez pas le cordon de secteur en service. N'employez pas les cordes de prolongation. N'essayez pas de n'apporter aucune modification interne à la source d'énergie. N'essayez pas de ne modifier aucune partie ou composant d'une unité de série DS à moins qu'ait spécifiquement dirigé vers par le personnel de BayTech. BayTech doit effectuer toutes les opérations internes.

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 or good power surge protection.
ATTENTION: Les montées subites et les transitoires à haute tension peuvent endommager cet équipement. Pour se protéger contre de telles montées subites et transitoires de puissance, cette unité doit avoir une bonne protection rectifiée ou bonne de la terre de puissance de montée subite.

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. The outlets providing power to the unit shall be protected against over current, short circuit and earth fault by suitable rated protective devices.
ATTENTION: Pour l'ÉQUIPEMENT DE MANIÈRE PERMANENTE RELIÉ, un dispositif aisément accessible de débranchement (disjoncteur évalué pour ne pas dépasser l'estimation d'ampérage de l'unité) sera incorporé dans le câblage fixe entre la source d'énergie et l'unité de Baytech. Pour l'ÉQUIPEMENT QUE L'ON PEUT BRANCHER, la douille-sortie sera installée près de l'équipement et facilement accessible. Les sorties fournissant la puissance à l'unité seront protégées contre le courant, le court-circuit et le défaut de terre finis par les dispositifs protecteurs évalués appropriés.

CABLING

RJ-45 Cable

Control Module RJ-45 pin Signals

Pin	EIA 232 Signal	Signal Direction	Description
1	DTR	Out	+10V when activated by DCD. Toggles on logout for modem disconnect.
2	GND		Signal Ground
3	RTS	Out	+10 V when power is applied. Not used as a handshake line.
4	TX	Out	Transmit (Data Out)
5	RX	In	Receive (Data In)
6	N/C	In	No Connection.
7	GND		Signal Ground
8	DCD	In	DCD into the MRP.

Adapter signals

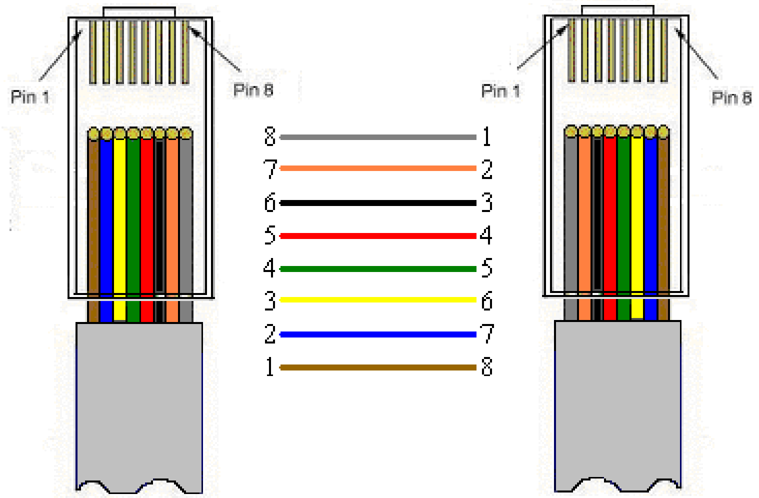
Listed are the pin specifications for the BayTech cable and adapters and the terminal COM ports:

Serial 1: Port Pin out Table

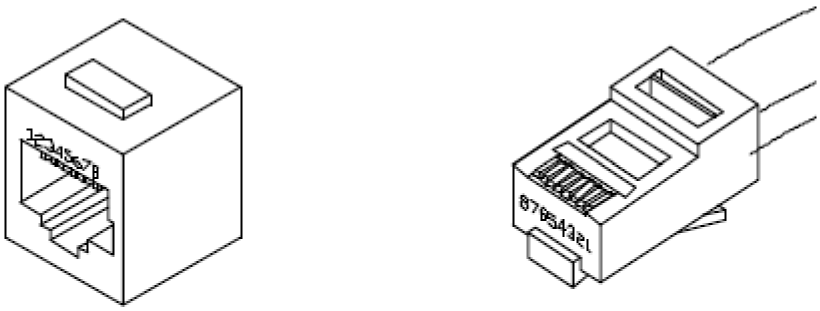
Signal	RS-232 Port (DS)	RS-232 Port (RPC)	COM Port DE-9 Pin	COM Port DB-25 Pin	Signal
DTR	1	1	4	20	DSR
GND	2	2		1	GND
RTS	3	3	7	5	CTS
TXD	4	4	3	2	RXD
RXD	5	5	2	3	TXD
DSR	6	N/C	6	6	DTR
GND	7	7	5	7	GND
CTS	8		8	4	RTS
DTR			4		DCD
DCD		8	1	8	DTR
RI	9			22	

RJ08X007 Standard Rollover Cable – RJ45 to RJ45

Serial 2: RJ08X007 Pin out

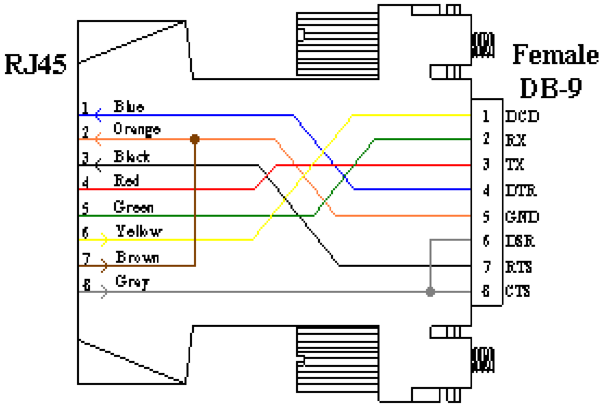


Serial 3: RJ45 Receptacle & Plug

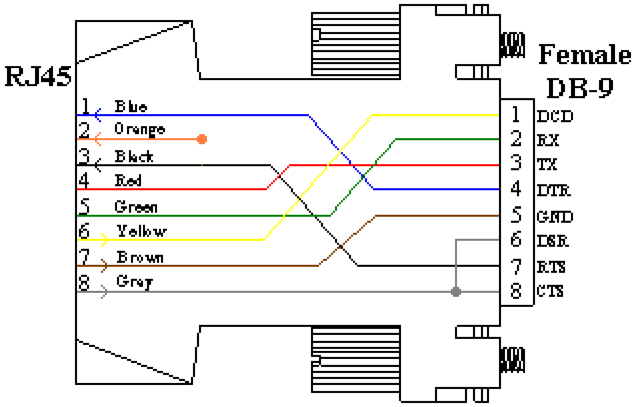


Adapters

Serial 4: 9FRJ45PC-1 Adapter Pin Out



Serial 5: 9FRJ45PC-4 Adapter Pin out



(Use with RJ08X007 Cable and B/C switch in "B")

Serial Setup

- Verify **JMP5** is set to shunt pins 1 and 2 together
- For DS62, Connect the *9FRJ45PC-1* adapter to the user's computer
    - *For DS62-MD4, Connect the 9FRJ45PC-4 adapter to the user's computer*
- Connect the RPC 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, B/C switch set to 'B'**.

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-times to get back to the main status menu.

NOTE: Password feature is case sensitive. (Default is user/password is **root/baytech**)

NOTE: All screen shots are valid for **Firmware** F3.XX and later. Not all options are available for earlier firmware.

QUICK START: DS62/DS62-MD4 SERIES

This is the bare minimum for Ethernet Control. 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. The System Administrator should tell you to use DHCP or provide you an IP Address, Subnet Mask, and Gateway Address. **NOTE: default IP Address is 0.0.0.0**

Ethernet Configuration:

1. Connect to the Serial port (EIA232) using the supplied rollover flat cable and adapter.
2. 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.**
3. If you get only a blinking cursor Press 'Enter'. If still only a blinking cursor, Type 5 Attention Characters, (factory default is the 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).**
4. Select 'C' for the configuration menu. You should see a menu similar to **(Figure 2)**.
5. Select the number for 'Login Setup' option. You should see a menu similar to **(Figure 3)**.
6. Select the number for 'Manage Users' option. You should see a menu similar to **(Figure 6)**.
7. **NOTE: The 'root' user can not be deleted.**
8. Select 'A' to add user. Type the name and password at the prompts.
9. Press 'Enter' until get to the 'Login Setup Menu' **(Figure 3)**.
10. Select 'Access Control' to enable or disable the Tenet and Serial Login Prompt **(Figure 4)**.
11. Press 'Enter' until you get the Configuration menu **(Figure 2)**.
12. Select 'Network Port Configuration' option. You should see a menu similar to **(Figure 7)**.
13. If your System Administrator requires you to use DHCP, then select 'DHCP Enable/Disable' and type **"Y"** to enable DHCP. Continue to next step. ***If you wish to assign a static IP address to this unit, disable the DHCP and go to step 17***.
14. Press 'Enter' until you are asked to 'Accept Changes'. Type **"Y"** to accept changes or **"N"** to decline changes.
15. After Accepting or Declining Changes you should get the Network Access Menu **(Figure 1)**.
16. 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.
17. If you disabled the DHCP in step 13, you should see a menu similar to **(Figure 7)**.
18. Select the 'IP Address' option and type the assigned IP address and press 'Enter'.
19. Select the 'Subnet Mask' option and type the assigned subnet mask address and press 'Enter'.
20. Select the 'Gateway Address' option and type the assigned Gateway address and press 'Enter'.
21. Press 'Enter' until you are asked to 'Accept Changes'. Type **"Y"** to accept changes. You should get the Network Access Menu **(Figure 1)**.
22. 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.
23. You should be prompted for a user name and password, similar to **(Figure 5)**

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

Universal Ethernet Controller Configuration:

Access Menu: The Access Menu screen, allows for Outlet Operations, Network Configuration, or Disconnection. To access the Network Configuration Screen, **type five Attention Characters**.

NOTE: For initial network access, the IP address, subnet mask, and gateway must be configured from the serial port. **Default setting is 0.0.0.0.**

Figure 1: Network Controller

```
     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           (3 ,1).........5
     Status.........................S
     Configure......................C
     Unit Reset.....................RU
     Logout.........................T
   Enter Request :
```

Figure 2: Network Configuration

```
   Copyright(C) Bay Technical Associates 2008
   DS62 Ethernet Host Module
   Revision F 3.10.01      Module 1
   Hardware 1.00         Serial number  22222  colilo version 1.05.01

 Status.........................1       Status of all network options
 Serial Port Configuration.......2       Setup the Serial port EIA232
 Serial Port Device Name.........3       Change the EIA232 port name
 Attention Character.............4       Type 5 times to access Network Main menu.
 Disconnect Timeguard............5       Data received within the delay period,
                                         is data, not attention character; thereby
                                         preventing unwanted port disconnection
 Connect Port ID Echo............6       Echo port name or module# & port#
 Login Setup.....................7       Login Menu Serial/Telnet/Radius/TACACS
                                         access control, manage users
 Network Port Configuration......8       Network Port IP Address
 Module Name.....................9       Change name of module
 RPC Management.................10       Set up Voltage/Current/Sensor threshold
 Firmware / Config Download.....11       Update Firmware, SSL, Configuration files
 Modem Configuration............12       DS62-MD4 Module ONLY
 Exit........................X,CR
 Enter Request :
```

Login Setup Menu

Figure 3: Network Login setup

```
     Access Control..................1
     Manage Users....................2
     Direct Port Connection..........3
     Radius Configuration............4
     TACACS Configuration............5
     Dial Back Configuration.........6     DS62-MD4 ONLY
     Exit............................X,CR
```

Access Control

Enable or disable usernames and passwords for network, serial, and **DS62MD4** modem port access. If any login has been enabled you will get a prompt similar to the following:

Figure 4: Network Access Control

```
Telnet Login Prompt Enable/Disable..1
Serial Login Prompt Enable/Disable..2
Modem Login Prompt Enable/Disable...3     DS62-MD4 only
```

Figure 5: Network Login Prompt

```
DS62 login:
Password:
```

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

Manage Users

Add/delete users and change their passwords. Usernames and passwords are case sensitive and alphanumeric. **The root user can not be removed**.

Figure 6: Network Manage Users

```
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
```

Network Port Configuration

For network access, you must configure the IP addresses, Subnet Mask, and Gateway Address, or enable the DHCP. The Changes must be saved and the module reset for network changes to take effect.

Figure 7: Network Port Configuration

```
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
```

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

NETWORK MENU

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

With a proper serial port connection, upon power-up or unit reset, the following Status menu will be displayed. The number of devices displayed is dependent on the number of DS74 modules installed.

```
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  Displayed for DS-RPC units ONLY
    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.

NOTE: If select the "Configure" option and get the following message (`Configuration mode in use`), the other port has the configuration option selected.

IMPORTANT: Any changes made in the Configuration menu will NOT take effect until changes are accepted. Type "X" and press 'Enter" until the unit displays a prompt: {Accept Changes? (Y/N)}. Type "Y" to accept changes. The unit will display: (Changes Accepted) Press 'Enter" to get out of the configuration menu. If the DS62 does not automatically reset, type "RU" (Unit Reset) at the prompt and press 'Enter' This action will update the configuration in the RAM.

STATUS MENU

Status Menu 1: Network Status

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

Overall System Status.............1     Available memory, System up time
Network Status....................2     IP address, MAC, packets
Logged Users......................3     Active users, admin terminates users
Memory Usage......................4     Memory statuses
Current Routing Cache.............5     Current routing caches
Route Setup.......................6     Routing table
Processes.........................7     Processes in memory
UnitInfo Database.................8     Data collection

Enter Request :
```

Overall System Status

Select 1), 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

Select 2), Network Status contains the MAC address, IP address, Mask, TX/RX packets and their status.

```
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

Select 3), to show the name of the user account, the type of interface (serial or network) and the status of the active sessions

```
C=configuration user   *=current process
Active Users:

 #  USER    FROM          INTERNAL CONN STATUS PID
 1  root    localhost                   Normal   23
C 2  root   70.150.140.69               Normal   490
 * 3  root  70.150.140.66               Normal   492

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

Terminate a session by typing **"T"** at the prompt. The unit will display the following:

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

Memory Usage

Select 4), to see where your memory is being utilized.

```
          total:    used:    free:  shared: buffers:  cached:
Mem:  11735040  4136960  7598080        0   380928   458752
   Press ENTER to continue
```

Current Routing Cache

Select 5), to see the IP Data currently held in cache or none upon power cycle.

```
Kernel IP routing cache
Source            Destination       Gateway         Flags Metric Ref  Use Iface
66.186.36.195     70.150.140.86     70.150.140.86   l      0      0    1   lo
70.150.140.86     66.186.36.195     70.150.140.65          0      0    0   eth0
70.150.140.69     70.150.140.86     70.150.140.86   il     0      0   154  lo
207.206.133.250   70.150.140.86     70.150.140.86   l      0      0   76   lo
           Press ENTER to continue
```

Route Setup

Select 6), 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** defines how closely an address must match the network destination, octet by octet, to use the route.
- **Iface** interface used to reach the network gateway, in this case 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

Select 7), to see a list of Process commands used by the firmware to operate.

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

```
PID PORT STAT SIZE SHARED %CPU COMMAND
  1       S    133K     0K  0.2 init
  2       S      0K     0K  0.0 keventd
  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 rpccmdd
 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 will prompt for a PID number to terminate:

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

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
```

NETWORK CONFIGURATION MENU:

NOTE: The following message, “**Configuration mode in use**”, signifies a user in the other port is in the “Configuration” menu.

1st level of configuration identifies all modules connected to the DS-chassis. The Ds74 has the (4) serial ports. May have more than one DS74 listed. DS-RPC is the chassis (4) power ports

```
Configuration
  DS62     module #1...1
  DS74     module #2...2
  DS-RPC   module #3...3   DS-RPC Chassis ONLY
```

Menu 1: Network Configuration

```
   Copyright(C) Bay Technical Associates 2009
   DS62 Ethernet Host Module
   Revision F 2.25.06      Module 1
   Hardware 1.01         Serial number  25920003  colilo version 1.05.01

 Status..........................1   Status of all network options
 Serial Port Configuration.......2   Setup the Serial port EIA232
 Serial Port Device Name.........3   Change the EIA232 port name
 Attention Character.............4   Type 5 times to access Network Main menu.
 Disconnect Timeguard............5   Data received within the delay period,
                                     is data, not attention character; thereby
                                     preventing unwanted port disconnection
 Connect Port ID Echo............6   Echo port name or module# & port#
 Login Setup.....................7   Login Menu Serial/Telnet/Radius/TACACS
                                     access control, manage users
 Network Port Configuration......8   Network Port IP Address
 Module Name.....................9   Change name of module
 RPC Management.................10   Set up Voltage/Current/Sensor threshold
 Firmware / Config Download....11    Upload FTP firmware, upload and download
                                     unit configuration
 Modem Configuration............12   DS64-MD4 Module ONLY
 Exit.........................X,CR
 Enter Request :
```

Status

Select 1), displays the current configuration of the unit network information.

```
Installed Modules :01
  Attention Character is ......... ;
  Disconnect Time Guard is........ Disabled
  Port ID Echo is................. Disabled
  Module Name is.................. Universal RPC

  Network Connectivity & Login Configuration:
  Ethernet Address................  00:C0:48:35:DD:40
  IP Address...................... 192.168.2.214
  Subnet Mask..................... 255.255.255.0
  Default Gateway................. 192.168.2.1
  Inactivity Timeout (mins)....... Disabled
  Break Length (msecs)............ 350
  Telnet.......................... Enabled
  SSH............................. Enabled
  DHCP............................ Disabled
  Telnet login prompt is.......... Enabled
  Serial login prompt is.......... Disabled
  Direct Port Connection is....... Disabled

SNMP & Web Configuration:
  SNMP Agent is................... Enabled
  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
```

Status
continued.

```
  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
  TACACS DS62 privilege level is..  Disabled
  TACACS DS62 privilege level.....  15

  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 Country Code: B5
  Modem Login: Enabled

  PPP status:
  PPP is disabled
  Dial In IP Address:  0.0.0.0
  CHAP is disabled
  IP Forwarding is disabled
  CHAP Secret: baytech
```

Serial Port Configuration

Select 2), from the Network Configuration Menu configures Handshaking, Baud Rate, Word Size, Stop Bits, and Parity 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: Communications with the terminal computer connected to the port will be lost until the serial port configuration of the terminal computer matches the unit's serial port.

Menu 2: Serial Port Configuration

```
+----+------+----------------+------+------+------+------+---------+----+----+
|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
  Modem DCD Connection Mode....8    DS62-MD4 Module ONLY

  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 1), from the Serial Port Configuration Menu for the Handshaking menu, **Default is None**

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

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.

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 2), from the Serial Port Configuration Menu changes the transfer rate of Data bits per second for the serial port, **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 3), from the Serial Port Configuration Menu changes the Word Size, **Default is 8**

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

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 4), from the Serial Port Configuration Menu changes the Stop Bits, **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 5), from the Serial Port Configuration Menu selects the Parity, **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 DTS **default state is High.**

Select 6), from the Serial Port Configuration Menu changes the RTS driver state, **Default is "High"**

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

Select 7), from the Serial Port Configuration Menu changes the DTR driver state, **Default is "High"**

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

Type **"Y"** for YES or **"N"** for NO and press 'Enter'.

Modem DCD Connection Mode (DS62-MD4 ONLY)

Should a need arise for the use of an external modem. Two steps must be performed before the modem will operate properly with the Ds62 module. 1st step is to enable option (8) of the Serial Port Configuration. 2nd step is to place a shunt on pins 1&2 of JMP4, located next to the serial port on the circuit side of the module.

Select 8), to enable the DS62 module console port to operate with an external modem. Ensure JMP4 has pins 1&2 shunted. **Default is Disabled**

```
Modem DCD Connection Mode is: disabled.

Enabling this feature will allow DS62 EIA-232 console port
to operate
in conjunction with DCD signal from an attached external
modem.
Use BayTech MD6 modem adapter & place shunt block across
JMP 4, pins 1 & 2.

  Enable ? (Y/N), CR for no change) :
```

Serial Port Device Name

Select 3, from the Network Configuration Menu allows the serial port to be renamed. Type the new port name and press ‘Enter’.

```
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. **Select 4, from the Network Configuration Menu,** to change the attention character. The unit displays the following: **The Default is a semi-colon (;).**

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

Enter Attention Character :
```

Disconnect Timeguard

Select 5, from the Network Configuration Menu, ensures reliable binary data transmission by providing a one-second “Timeguard” after the unit receives the attention character. If more data is received within the delay period, the unit treats the character as data, not an attention character; thereby preventing unwanted port disconnection. Select 5, from the network menu. **The Default setting is Disabled.**

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

Connect Port ID Echo

Select 6, from the Network Configuration Menu, sets the port identification. The unit displays the Port ID Echo Menu.

```
Port ID Echo is...................Disabled

Connect Port ID Echo Menu

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

Select 1), to disable the echo. **The Default setting is Disabled**.

The unit displays: (blank)

Select 2), to echo the module and port number.

The unit displays:
```
        BAYTECH

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

02,1
```

Select 3), to echo the device name.

The unit displays:
```
        BAYTECH

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

MSP10
```

Login Setup Menu

Select 7, from the Network Configuration Menu, allows the admin user to enable or disable the Access Control, Manage Users, Radius, and TACACS configuration. Depending on the firmware installed the Login Setup menu may be slightly different than what is shown.

Menu 3: Network Login

```
Access Control..................1
Manage Users....................2
Direct Port Connection..........3
Radius Configuration............4
TACACS Configuration............5
Dial Back Configuration.........6
Exit..........................X,CR
```

Access Control

Select 1, from the Login Setup Menu, 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
```

Select 1), for ***Telnet login***
Type **"Y"** to enable Login Prompt,
Type **"N"** to disable prompt.
Press "Enter" to keep same setting

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

Select 2), for ***Serial login***
Type **"Y"** to enable Login Prompt,
Type **"N"** to disable prompt.
Press "Enter" to keep same setting

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

Select 3), for ***Modem login***
Type **"Y"** to enable Login Prompt,
Type **"N"** to disable prompt.
Press "Enter" to keep same setting

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

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

```
DS62 login: root
Password:
```

The default user and password is **root** and **baytech**, all lower case.
NOTE: Modem hangs up and Pauses for 10 seconds after 3-login failures.

Manage Users

Select 2, from the Login setup Menu, to allow the administrator to add/delete users and change their passwords for multiple users. Usernames and passwords are case sensitive and alphanumeric. The root user can not be removed. Select Manage User and the Unit displays the following:

NOTE: The port access mentioned in the User Management Menu below is not used in the MSP series.

Menu 4: Network Manage User

```
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
```

Type **“A”** and press ‘Enter’ to ***Add user*** and their password, the Unit displays the following:

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

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.

```
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 Unit displays the following menu:

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

Enter Request :1
```

Select 1), to **change a user’s password** The Unit displays the following menu:

```
User name: root
Enter old password (CR if none)>*******
```

If the user does not have a password the DS62 will respond for a new password and a confirmation to re-enter the new password:

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

Select 2), to change the Port Access Rights. In the menu to the right are 5 ports available between two modules. To assign a user to an individual port, type the module number and port number, i.e. (2.4,3.1).

```
Port access for (username)
   X = has access

| mod 2 | mod 3 |
| 1234  | 1     |

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

Type ‘ALL’ in caps to assign all port

```
Port access for JJ
 X = has access

| mod 2 | mod 3 |
| 1234  | 1     |
  XXXX    X
```

Select D), *Delete user*:

The Unit re-displays the “User Menu” minus the deleted user

```
  A)...Add user
  D)...Delete user
  1)...Engineer
  2)...root
 Enter Request :d

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

 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 :
```

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.........Enabled

 Enable ? (Y/N), CR for no change) :
```

Radius Configuration

Select 3, from the Log In Menu, Radius is used to authenticate logins for the serial and the network ports if passwords and user names are enabled in the unit. If the Radius server rejects either the username or password or does not respond, the unit will display “Invalid Password”.

Menu 5: Network Radius Configuration

```
Radius Enable....................1
Radius Server Address............2
Radius Backup Server Address.....3
Radius Secret....................4
Enable DS62 usernames as backup..5
Radius Login Timeout.............6
Radius Server Port...............7
Exit...........................X,CR
```

Select 1, *Radius Enable* enables radius authentication. If enabled, the primary radius server address must be specified

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

Select 2, *Radius Server Address* specifies the radius server IP addresses

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

Select 3, *Radius Backup Server Address* specifies the backup server IP addresses

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

Select 4, *Radius Secret* sets the 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 5, *Enable DS62 usernames as backup* enables DS62 usernames as backup login allows an unsecured access until` the RADIUS server becomes available.

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

Select 6, *Radius Login Timeout* sets the amount of time the unit 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 ) :
```

Select 7, *Radius Server Port* enables the unit to communicate with Radius Server. If you type a port number less than 1024 the Host Module responds with the same screen until a valid entry is typed.

```
RADIUS server port is: 1812
Enter port number (>= 1024, D for default 1812):
```

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 then a password. The Host will send the username and password to 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 the login failed.

Setting up TACACS

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 DS62 Privilege Level and set levels.
- Enable usernames and passwords for the network and serial port via the logins setup access control menu.

Select 4) from the Login Setup Menu displays the TACACS Configuration menu

Menu 6: Network TACACS Configuration

```
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 login Timeout.............7   Sets Time units waits for response
TACACS Server Port...............8   Assign secure TCP port
DS62 Privilege Level Enable......9   Enable/Disable TACACS privilege
DS62 Privilege Level.............10  Set Privilege Level 1-15
Exit.............................X, CR
```

Select 1, ***TACACS Enable*** sends the login information to the TACACS server for authentication. If enabled, the primary TACACS server address' must be specified.

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

Select 2, ***TACACS Server Address*** assigns a specific TACACS server IP addresses.

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

Select 3, ***TACACS Backup Server Address*** assigns a specific Backup Server IP addresses.

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

Select 4, ***TACACS Secret*** assigns 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 5, ***EnableDS62 usernames as backup*** allows 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 6, ***TACACS Encryption Enable*** sets the TACACS+ encryption to 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 7, ***TACACS Login Timeout*** sets the amount of time the unit will wait for a response from the TACACS server.

```
TACACS response timeout is   10 seconds
 Enter timeout, in seconds ( >=0 and <=30 )
 0 = no timeout :
```

Select 8, ***TACACS Server Port*** assigns a more secure port, **default is TCP 49**. If you type a port number less than 1024 the Host Module responds with the same screen until a valid entry is typed.

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

TACACS User Privilege Feature

Important: The TACACS admin user must perform the following before the TACACS Privilege level to operate: Open the tacacs.conf file and add the following entry for each user: (service = exec {priv-lvl = n}). Where "n" is a number from 1 to 15, inclusive. 15 is root privilege level, 1 is lowest level user. "priv-lvl" must be spelled exactly as shown, including case. Restart the daemon after making changes.

Select 9, ***DS62 Privilege Level Enable*** enables the unit to send a privilege level to the TACACS server. **Default is Disabled**

```
TACACS Privilege Level is........Disabled

  Enable ? (Y/N), CR for no change) :
```

Select 10), ***DS62 Privilege Level*** assigns privilege levels. 1 is the minimum user privilege and 15 is the root/admin privilege level.
Default is 15

```
DS62 Privilege Level is: 15
Enter Privilege Level for root access:
```

Example of operation: Privilege Level enabled, set to “10”. In tacacs.conf file on daemon, user1 is configured for exec priv-lvl = 9, user2 is configured for exec priv-lvl = 10, and user3 is configured for exec priv-lvl = 11. In this scenario, user1 will get only user-level access to the power strip, user2 & user3 will get root access.

See APPENDIX: TACACS CONNECTION: for troubleshooting connection problems with TACACS servers.

Login Option Dial-Back Number (*DS62-MD4 ONLY*)

Login Option 6), this feature allows user to dial in, hang up and the unit dials the assigned number back when using a secure phone line.

```
Dial Back User Configuration - Main Menu
Enter User Number to modify.

+----+-----------------------+----------------+------*------+
|User|    Name               |  Phone Number  |Dly(s)|En/Dis|
+----+-----------------------+----------------+------+------+
| 1  |root                   |                | 10   | Dis  |
+----+-----------------------+----------------+------+------+
Enter Request :1
```

Select a user number and the unit displays the following:

```
Dial Back Configuration

+----+-----------------------+----------------+------*------+
|User|    Name               |  Phone Number  |Dly(s)|En/Dis|
+----+-----------------------+----------------+------+------+
| 1  |root                   |                | 10   | Dis  |
+----+-----------------------+----------------+------+------+
Dial Back Option.........................1
Phone Number.............................2
Dial Back Delay..........................3

Enter Request :1
```

Select 1), to enable the Dial Back feature

```
Enable Dial Back for this user? (Y/N): y
```

Select 2), to enter a Dial Back number: Enter only numbers or a Warning is displayed

```
Enter Dial Back number for this unit (<= 20 digits): 228-228-6660
***WARNING: Phone number contains non-numeric characters***
```

Select 3), to how long the unit will wait before calling back. **Default is 10 seconds**

```
Enter Dial Back delay (10 to 60 secs): 30
```

Select 4), to use the Module ID as the username when dialing back

```
Use Module ID as username when dialing
back? (Y/N):
```

Network Port Configuration

Select 8), from the Network Configuration Menu, 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.

Menu 7: Network Port Configuration

```
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 :
```

IMPORTANT: For network access, you must configure the IP addresses, Subnet Mask, and Gateway Address. A unit reset must be performed 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 MSP can be accessible via the network.**

Select 1, to enter the IP Address. Failure to enter the address in the decimal form causes the unit 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 MSP. 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 RPC 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 MSP 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 unit 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 DS62 can be accessed through the network.**

Select 3, to change the Gateway address. Failure to enter the address in the decimal form causes the unit 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

Select 4, from Network Port Configuration Menu to set the amount of time the unit will wait before disconnecting if there is no activity. The enabling input can be from 1 to 120 minutes. **Default is 0 (DISABLED)**

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

Carriage Return Translation

Select 5, from Network Port Configuration Menu to determine what the telnet processor will do with the line-feeds and nulls after a carriage return is sent. **Enable** tells the unit Telnet processor to strip line feeds or nulls 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

Select 6, from Network Port Configuration Menu to adjust the break length feature. Users may configure the RPC for a break length of 1 - 1000 milliseconds. In a Telnet session with the RPC through the serial port of a DS74, send a Telnet break command (0xF3) to the unit, 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) :
```

DHCP Enable/Disable

Select 7, from Network Port Configuration Menu to enable or disable the DHCP feature. 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 ENABLED.

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

Telnet Enable/Disable

Select 8, from Network Port Configuration Menu to enable or disable the Telnet feature. Telnet is a user command and an underlying TCP/IP protocol for accessing remote devices. **Default setting is ENABLED.**

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

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

SSH Enable/Disable

Select 9, from Network Port Configuration Menu to enable or disable the SSH feature. 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**.

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

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

SSH Host Key Generation

Select 10, from Network Port Configuration Menu to allow the user to generate a unique SSH host key for the RPC unit. This key is part of the SSH encryption process. Each RPC 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.

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

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

IP Filter Configuration

Select 11, from Network Port Configuration Menu the IP Filter Management Menu allows the admin user to pass or block certain IP Addresses. If you have no rules defined the unit may display only options (**A, E, C**).

Menu 8: Network IP Filter Configuration

```
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 :a
```

Select A) to ***Add Rule***. Type an IP address, select whether to drop or accept the address.

```
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 :1
```

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

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

Select E), ***Enable IP Filtering*** to enable or disable the filtering function.

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

Select V), ***View Rules*** to see any IP filtering. **NOTE:** At least one rule must be defined for this option to be available.

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

Strike ENTER to continue
```

Select C), ***Set Default Target*** to set ALL IP Addresses to accept or drop all

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

Select F), ***Flush Rules*** to delete all rules. The unit will respond with all filters deleted.

Are you sure you want to delete all filters? (Y/N)

Enter Request :y

All filers have been deleted.

Select D), ***Delete Rule*** to a delete a specific rule. The unit will respond with the Filter Rule number deleted.

```
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
```

SNMP Configuration

Select 12 from the Network Port Configuration Menu. This 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.

Menu 9: Network SNMP Configuration

```
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
```

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 Unit will display:

Accept changes ? (Y/N) :

SNMP Trap Host IP Address 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 1, 2, 3, 4**, the unit 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:
```

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 5), ‘***SNMP Read Only Community***’ option to enter a Read Community string, the Unit displays the current setting, **Default is public**.

```
SNMP Read Community name: public
Enter Read Community Name:
```

Select 6), ‘***SNMP Read-Write Community***’ option to enter a Write Community string, the Unit displays the current setting, **Default is private**.

```
SNMP Write Community name: private
Enter Write Community Name:
```

Select 7), ‘***SNMP Enable***’ option to enable the SNMP function, the Unit displays, **Default is Enabled**.

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

Select 8), *SNMPv3 only Enable,* option if you have SNMPv3 software, only the newer firmware will have this option. **Default is Disabled.**

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

IMPORTANCE: The user password has to be 8-31 characters, including the “root” user. The client software will need the same password.

Select 9), *SNMP Authentication Traps Enabled,* option to enable a SNMP trap to be sent if an authentication attempt failed, the Unit displays,
Default is Disabled.

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

IMPORTANCE: If user is serial or telnet into the unit and make changes to cause a trap to be sent, the trap will not leave the unit until the user logs out or types the Attention Character 5-times. This will lease the controller and the SNMP trap is sent.

Web Server Configuration

Select 13 from the Network Port Configuration Menu for the Web Server Configuration menu:

Menu 10: Web Server Configuration

```
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. Type the unit's IP Address on a web browser to get the unit web page, 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 unit through the web page have administrator privilege, unless a TACACS server and privilege levels are used for authentication.

Select 1, ***Web Enable,*** to enable or disable the web page feature, **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, **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, **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, **Default is zero minutes:**

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

IMPORTANCE: If a user is still connected to the outlet controller menu, or the user does not properly release the controller, the Web page will not update.

Module Name

Select 9, from the Network Configuration menu to change the unit name.

```
Module Name is:  RPC
Enter Module Name (32 chars max):
```

RPC Management

Select 10, from the Network Configuration Menu, to establish SNMP outlet traps used by a remote SNMP Manager by creating outlet groups and alarm thresholds.

Menu 11: Network RPC Management

```
Host-controlled RPC 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
 Temperature units (degrees C/F)....7
 Power Factor Threshold.............8
```

Temperature Alarm Threshold

Select 1), to change the alarm for Internal Temperature: Enter the Selection (Sel) Number and press Enter. Type a value in tenths of a degree, *i.e.500 = 50.0º C*

```
Sel  M/P    Identifier     Tmp Lvl
 1    2/1    MSP10          500

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

Under Voltage Alarm Threshold

Select 2), to change the alarm for Low Voltage: Enter the Selection (Sel) Number and press Enter. Type a value in tenths of a volt, *i.e 900 = 90.0 volts.*

```
Sel  M/P    Identifier     Lo V Lvl
 1    2/1    MSP10          900

Enter voltage threshold value in
tenths of a volt:
```

Over Voltage Alarm Threshold

Select 3), to change the alarm for over voltage: Enter the Selection (Sel) Number and press Enter. Type a value in tenths of a volt, *i.e 1300 =130.0 volts.*

```
Sel  M/P    Identifier     Hi V Lvl
 1    2/1    MSP10         1300

Enter voltage threshold value in
tenths of a volt:
```

Low Current Alarm Threshold

Select 4), to change the alarm for low current: Enter the Selection (Sel) Number and press Enter. Type a value in tenths of a volt, *i.e 100 =10.0 amps*

```
Sel  M/P    Identifier     Low Curr
 1    2/1    MSP10           0

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.

Environmental Sensors

Select 5), to change the alarm limits for the Environmental probes:
If the unit does not have a sensor probe connected, the unit will display the following.

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

Strike ENTER to continue
```

Individual Sensors

Select 1), to change the limits of individual probes

```
Environmental Sensor Configuration Menu
Sel  M/P    Identifier
1    2/1    MSP10
2    All Sensors
Enter Request :1
```

Select either 1 or 2 (Sel) probe. (Hi/En) = Hi limit Enabled, (Lo/En) = Low limit Enabled, (St/En) = Sensor Trap enable

```
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
```

Second line identifies the probe name and type. 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

```
RPC/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
```

All Sensors

Select 2), to set parameters for the different probe types. This feature is useful for standardization and the probe type is known.

```
Environmental Sensor Configuration Menu
Sel  M/P    Identifier
1    2/1    MSP10
2    All Sensors
Enter Request :2
```

NOTE: The type 'Contact' signifies a door switch is open even if the switch is not detected, but still be able to send SNMP Traps.

```
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
```

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.

NOTE: NP = No Probe detected.

```
RPC/RPS External Environmental Sensor Configuration Menu
  Sensor Number: All Name: all RPCs/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

Select 6, from the RPC Management Menu, allows user to combine outlets from different modules and ports. One SNMP command is used to turn off/on or reboot the group

```
   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
```

List Outlet Groups

Select 1), to list any outlet groups:

```
# 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
```

Add Group

Select 2), to add a new outlet group: Each outlet is represented by Mod.Port.Outlet. i.e. Mod 2 dot port dot outlet number 1 =2.1.1

```
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
```

NOTE: Mod 2.Port 1.Outlet.# is for the MASTER unit and Mod 2 .Port 2. Outlet # is for the Slave unit

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

```
Outlet group is currently defineded 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
```

NOTE: Get the Group number from the ***List Outlet Groups***

Delete Group

Select 3), to delete a specific outlet group, select the number of the group to be deleted. The unit will display Group Deleted.

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

NOTE: Get the Group number from the ***List Outlet Groups***

Rename Group

Select 4), to rename an outlet group's name, select the number of the group to be renamed. The unit displays the selected group and prompts for a new name:

```
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
```

NOTE: Get the Group number from the ***List Outlet Groups***

Modify Outlets in a Group

Select 5), to modify outlets in a group, select the number of the group to be modified. The unit displays the selected group and prompts for new group of outlets:

```
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
```

Delete All Outlet Groups

Select 6), to delete all groups

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

Note: There will be no confirmation the groups have been deleted. Select ***List Outlet Groups*** to verify all outlet groups were deleted.

Temperature Units (degrees C/F)

Select 7 from the RPC Management Menu, to allows a user to change the reported degrees in Celsius or Fahrenheit

The unit display either of the following:

```
Current temperature reported in degrees Celsius.
Change to report in degrees Fahrenheit (Y/N): y

Converting temp min/max thresholds...done
```

```
Current temperature reported in degrees Fahrenheit.
Change to report in degrees Celsius (Y/N): y

Converting temp min/max thresholds...done
```

Power Factor Threshold Menu

Select 8 from the RPC Management Menu, to display the unit’s power efficiency on the web page and through SNMP. The user sets a minimum power level that will send an SNMP trap to the SNMP Manager. The smaller the power factor, less than (1), more current is needed (wasted) to do the same amount work

Select 1); to display current Power Factor (PF) and Power Threshold settings for each individual unit circuit.

M/P = Module port,
Identifier = Unit Id,
Circuits = number of circuits on unit.
Outlets = number of unit outlets.

```
Power Factor Threshold Menu

    Parameters to control generation of SNMP traps based on
    circuit Power/VA power factor and minimum power level.

  Sel  M/P  Identifier      In/Ck/Out
   1   3/4  RPC10              0/1/ 1

   2  All Inputs/Circuits/Outlets - Power Factor Threshold
   3  All Inputs/Circuits/Outlets - Power Threshold
```

Select 1), or CKT number to display the Circuit Power Factor and Power Threshold settings

```
Breaker List for device 1, RPC10
Ckt   PF Threshold (%)   Pwr Threshold (W)
  1          0                   50
```

Unit displays the Breaker Circuit Threshold Menu with circuit breaker number and current values.

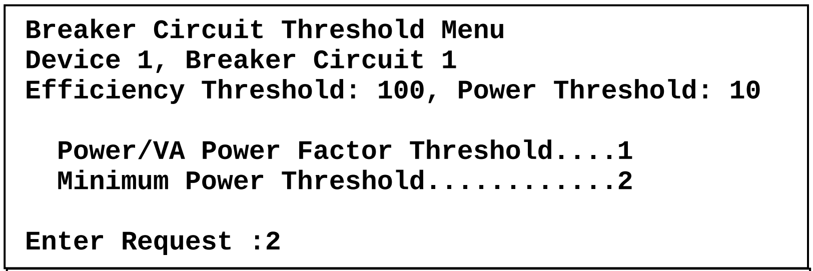
Select 1 to change the Power Factor Threshold level. Enter a per cent value (%). **Factory Default is (0%).**

```
Breaker Circuit Threshold Menu
Device 1, Breaker Circuit 1
Efficiency Threshold: 100, Power Threshold: 10

  Power/VA Power Factor Threshold....1
  Minimum Power Threshold...........2
```

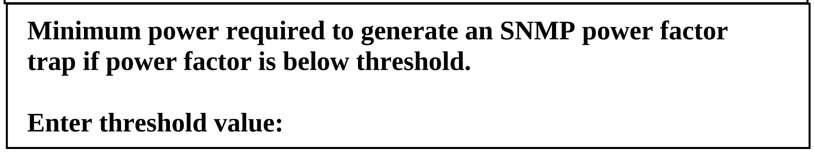
```
Power/VA ratio threshold as a percent, between 0 and 100,
inclusive. Power factors below this value will generate an SNMP
trap, if enabled and power is above minimum power threshold.  A
value of 0 disables threshold.

 Enter threshold value:
```

Unit displays the Breaker Circuit Threshold Menu with current values.

Select 2 to change the Minimum Power Threshold level. Enter a value. **Factory Default is (50w).**



```
Breaker Circuit Threshold Menu
Device 1, Breaker Circuit 1
Efficiency Threshold: 100, Power Threshold: 10

  Power/VA Power Factor Threshold....1
  Minimum Power Threshold............2

Enter Request :2
```



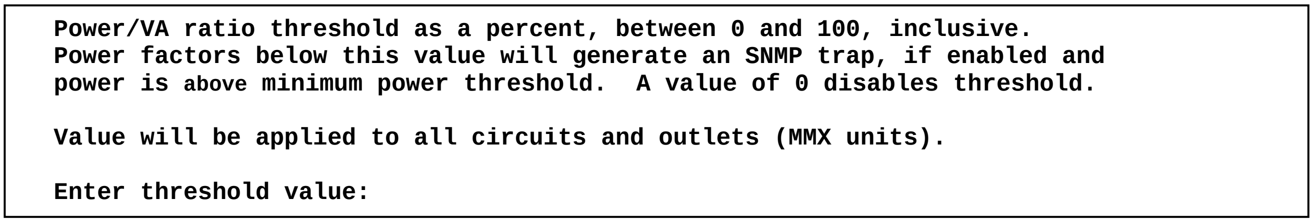
Minimum power required to generate an SNMP power factor trap if power factor is below threshold.

Enter threshold value:

NOTE: The Power Factor Threshold SNMP alarm is sent only if both respective values drop below the Power Factor Threshold and Power Threshold at the same time.

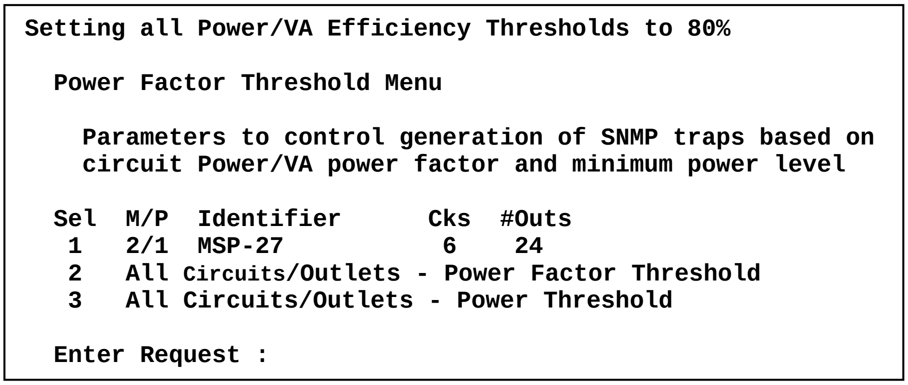
All Inputs/Circuits/Outlets - Power Factor Threshold

Select2) **from the RPC Management Menu** allows user to set all circuits and outlets to the same Power Factor Threshold levels. (MMX) refers to the metered-outlet modular- series. **Default Value = (0%)**



```
Power/VA ratio threshold as a percent, between 0 and 100, inclusive.
Power factors below this value will generate an SNMP trap, if enabled and
power is above minimum power threshold.  A value of 0 disables threshold.

Value will be applied to all circuits and outlets (MMX units).

Enter threshold value:
```

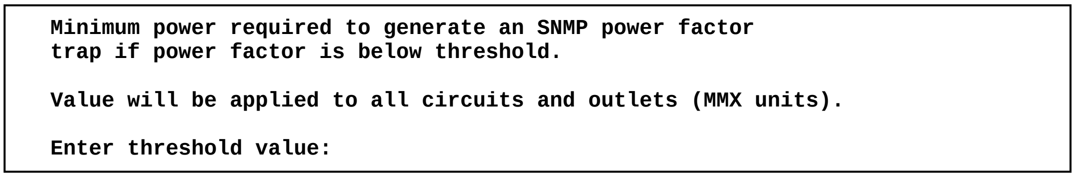
The unit responds with message stating the Thresholds were set to the new value and displays the Menu.



```
Setting all Power/VA Efficiency Thresholds to 80%

  Power Factor Threshold Menu

    Parameters to control generation of SNMP traps based on
    circuit Power/VA power factor and minimum power level

  Sel  M/P  Identifier      Cks  #Outs
   1   2/1  MSP-27           6    24
   2   All Circuits/Outlets - Power Factor Threshold
   3   All Circuits/Outlets - Power Threshold

  Enter Request :
```

All Inputs/Circuits/Outlets - Power Threshold

Select 3), **from the RPC Management Menu** allows user to set all circuits and outlets to the same Power Threshold levels. (MMX) refers to the metered-outlet modular series. **Default Value = (50w)**



```
Minimum power required to generate an SNMP power factor
trap if power factor is below threshold.

Value will be applied to all circuits and outlets (MMX units).

Enter threshold value:
```

The unit responds with message stating the Thresholds were set to the new value and displays the Menu.

```
Setting all minimum Power Threshold levels to 10 Watts

  Power Factor Threshold Menu

    Parameters to control generation of SNMP traps based on
    circuit Power/VA power factor and minimum power level

  Sel  M/P  Identifier      Cks  #Outs
   1   2/1  MSP-27           6    24
   2   All Circuits/Outlets - Power Factor Threshold
   3   All Circuits/Outlets - Power Threshold

  Enter Request :
```

Firmware/Config Download

Select 11), from the Network Configuration Menu, to upgrade the firmware for IP Network, Outlet controller, Uploaded SSL Certificates, and Configuration file.

Menu 12: Network Firmware/Config Download

```
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
Enable Rel Ctl. Firmware Upgrade..7
Exit..............................X,CR
```

Enable Firmware Upgrade

Select 1), to enable the upgrade of the firmware via FTP. The 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.

Selecting **"Y"** for yes the unit will display the following as it waits for the firmware file,

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

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

Enable SSL Cert Upload

Select 2), to allow the admin to upload an SSL Certificate to the 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 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.

The unit 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 unit will display the following. To stop this function power-cycle the unit to close the SSL Certification Upload.

Selecting **“Y”** for yes the unit will display the following as it waits for the certificate.

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

At this point follow the FTP instruction to transfer the ssl.pem file into the module.

Enable Configuration File Upload

Select 3), to allow the admin to upload a configuration file from a computer to the power unit. The unit will display 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 unit 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 unit will display:

```
configuration file valid

updating ds62 configuration
***
ds62 host configuration complete
polling rpcs
Found RPC at mod 2 port 1
rpc polling complete
configuring rpcs
```

Unsuccessful file upload and the unit 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

Select 4), to allow the admin to restore the unit configuration to factory defaults.

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

The unit will display 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 unit will display:

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

System reset in progress...

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

Get Current Configuration File

Select 5), to allow the admin to get a copy of the current unit configuration file from the unit and FTP's it to a computer. The configuration file to be uploaded is named "confupload". The file may be opened with any ASCII or 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 unit will display.

```
Enabling this will allow the system configuration
file to be retrieved via ftp
Enable Configuration File Retrieval? (Y/N)
```

A YES response and the unit will display the following:

```
/var/confupload file created and ready for ftp
retrieval

Waiting to send configuration file
-----------------------------------------------------
-----------------------------------
```

At this point FTP the file to your computer. A Successful file retrieval and the unit displays:

```
get of configuration file complete
```

Unsuccessful file retrieval and the unit displays:

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

Display Configuration Error Log

Select 6), to list any errors in uploading or downloading the configuration file, the unit will display either:

```
no errors
Press CR to continue
or
1. No communication with rpc at mod 3 port 1 (MRP:5)
Press CR to continue
```

Enable Rel Ctl. Firmware Upgrade

Select 7), to upgrade the outlet controller firmware, the unit will display the available controllers:

```
RPC Firmware Upgrade Menu

    RPC10               (2 ,1).........1
    Device B            (2 ,2).........2
    DS-RPC              (3 ,1).........3

Enter Request :
```

Select the controller to be upgraded and the unit will ask if this is the correct controller to enable firmware upgrade. It will also tell you which port you are connected which will determine which method to upload the firmware.

If the unit displays the following, type **"Y"** at the prompt. The unit will wait for the ASCII file to be transfer. An error will occur if the terminal program

```
Upgrading RC firmware on RPC at module 2, port 1.

Enable update of Relay Controller firmware via Console (RS232) port.
Enabling will reset Ethernet Module when Configuration is exited

Enable Firmware Upgrade ? (Y/N) y
```

```
Send RC firmware file using ASCII file transfer option
  on your Terminal program.

Waiting for RC firmware.
-------------------------------
```

CAUTION: The unit may not read the data correctly if the terminal program tries to upload the file as a modem file, i.e. ZModem. Verify the file transfer is ASCII.

If the unit displays the following, type **“Y”** at the prompt. The unit will wait for the ASCII file to be transfer via FTP.

```
Upgrading RC firmware on RPC at module 2, port 1.

Enable update of Relay Controller firmware via Console FTP.
Enabling will reset Ethernet Module when Configuration is exited

Enable Firmware Upgrade ? (Y/N) y
```

```
Send file in ASCII file mode.

Waiting for RC firmware.
-------------------------------
```

DS62-MD4 Modem Configuration Menu

Menu 13: Modem Configuration Menu

```
   Modem Port Configuration..................1
   Rings to Auto Answer......................2
   Modem Connectivity Timeout................3
   Modem Inactivity Timeout..................4
   Modem Device Name.........................5
   PPP Configuration.........................6
   Country Code..............................7
   Enter Request :
```

Modem Port Configuration

Select 1), the Modem Port Configuration and the Host Module displays the following menu: The **Default configuration is 9600, 8, 1, none.**

```
+----+------+----------------+------+------+------+------+---------+----+----+
|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 :
```

Handshaking

Select 1), changes “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 :

Baud Rate

Select 2), changes the “Baud Rate” the modem transfers Data bits 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

Select 3), changes the “Word Size” and the DS displays the following: **Default is 8**

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

Stop Bits

Select 4), changes the“Stop Bits” the DS displays the following: **Default is 1.**

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

Parity

Select 5), changes the “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 2), from the Modem Configuration menu, changes the “Rings to Auto Answer” and sets 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 3), from the Modem Configuration Menu, changes 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

Select 4), from the Modem Configuration Menu, 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 Configuration Menu: Option 5), Modem Device Name

Select 5), from the Modem Configuration Menu, changes the Modem Device Name and the following is displayed:

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

Important: Changes are NOT saved until you back out of the Configuration menu. You should be asked to Accept changes.

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

PPP Configuration

Select 6), from the Modem Configuration Menu, the PPP is similar to the dial in modem used by telephone DSL or local cable access. PPP establishes a negotiated connection between two devices. Once connected an assigned IP address is sent to the other device. The logged in user will have network access to the local network. To use this feature, enable PPP & provide the IP address for the dial-in user. Enable CHAP for a stronger security over Password protection. The CHAP (Challenge Handshake Authentication Protocol) feature will disable PAP. The Ip forwarding acts like a router if connected to HTTP. Once connected, the user can access the DS62MD4 or the internet using any network access program (Telnet/SSH/SNMP/HTTP, etc). If CHAP is enabled CHAP Secret is used.

```
PPP Configuration

PPP is disabled
Dial-In IP Address................. 0.0.0.0

Enable PPP..............................1
Dial-In Client IP Address...............2
IP Forward Enable.......................3
CHAP Enable.............................4
CHAP Secret.............................5
```

Select 1), to enable the PPP feature.
Default is Disabled

```
PPP is..........................Disabled

Enable ? (Y/N), CR for no change) :
```

Select 2) to assign an IP Address to the dialed in user. **Default is 0.0.0.0**

```
Enter Dial-In IP Address in dotted decimal
form :
```

Select 3) to enable the IP Foward feature.
Default is Disabled

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

Select 4) to enable the CHAP feature.
Default is Disabled

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

Select 5) to enable the CHAP Secret password feature, minimum of (16) character. **Default is baytech**

```
PPP Secret: baytech
Enter CHAP Secret (16 characters max)
```

Country Code: DS62-MD4 ONLY

Select 7) from the Modem Configuration Menu, this option sets the modem to recognize the countries Telecomm Requirements, i.e. ring tone, dial tone.

```
Typical Country Code:
Argentina.....07 Australia......09 Austria........FD Belgium........FD
Brazil........16 Canada.........B5 Chile..........99 China..........B5
Czech Re......FD Denmark........FD France.........FD Germany........FD
Greece........FD Hong Kong......99 Hungary........FD Iceland........FD
India.........99 Indonesia......99 Israel.........B5 Italy..........FD
Japan.........00 Korea Re.......B5 Lithuania......FD Malaysia.......6C
Mexico........B5 Netherlands....FD New Zealand....7E Norway.........FD
Philippines...B5 Poland.........FD Portugal.......FD Romania........FD
Russian Fe....FD Singapore......9C Slovenia.......FD Spain..........FD
Sweden........FD Switzerland....FD Taiwan.........FE Thailand.......B5
Turkey........FD United Kingdom.FD United States..B5

      Current Country Code is:B5
      Change It ? (Y/N) :y
```

If you type ‘y’ to change the Country Code the module will respond with the following:

```
Enter 2 digits Country Code : b5

      Current Country Code is:B5
```

NOTE: If your country code is not listed select a country code closest to your country.

UNIT RESET

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

Reset Unit? (Y/N)

NOTE: A Unit Reset takes approximately 60 seconds for the unit to reset. It will not reset the unit to “Factory Default”, but it will terminate all external communications.

LOGOUT

Select T), will close the session to the unit, but **<u>may not</u>** close the terminal emulator session.

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.

For additional information or more specific warranty issues, contact BayTech's Technical Support or Customer Service Departments 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 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.

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:

- BayTech model type
- Unit serial number
- Firmware version (if accessible)
  A list of devices connected to the BayTech unit
- A general description of the application being used and the intended outcome
- Information about cables and adapters being used (type, length, place of purchase)
- The name of the software emulation program being used
- 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 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.

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.

Cost and Time:
The cost of repair for units no longer under warranty will be $50.00 per hour plus cost of materials and shipping. Typical turnaround times for repairs are 3 days for domestic requests and 5 days for international.

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

Return Authorization Process:

a. Contact BayTech via Phone, Fax, or Email to get a Return Authorization (RA) Number. *IMPORTANT: BayTech will not accept any returns without an RA number.*

b. 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.

c. Mark the RA number clearly on the outside of the package.

d. 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

APPENDIX: TACACS/RADIUS CONNECTION SCENERIOS

Parameters to determine if user should be able to log in:

- TACACS/RADIUS enabled/disabled
- Good/Bad TACACS/RADIUS connection
- “Enable DS62 usernames as backup” enabled/disabled
- Username/password on TACACS/RADIUS and power strip are same/different

Same username and password in TACACS/RADIUS and DS62

- **Case 1:** TACACS/RADIUS enabled, TACACS/RADIUS contact good, “Enable DS62 usernames as backup” = enabled, user Log in **OK.** Log in is validated by the TACACS/RADIUS server.
- **Case 2:** TACACS/RADIUS enabled, TACACS/RADIUS contact good, “Enable DS62 usernames as backup” = disabled, user Log in **OK.** Log in is validated by the TACACS/RADIUS server.
- **Case 3:** TACACS/RADIUS disabled, or TACACS/RADIUS contact loss, “Enable DS62 usernames as backup” = enabled, user Log in **OK.** DS62 validates the user.
- **Case 4:** TACACS/RADIUS disabled, or TACACS/RADIUS contact loss, “Enable DS62 usernames as backup” = disabled, user Log in **FAIL.** Neither TACACS/RADIUS nor the DS62 can validate the user.

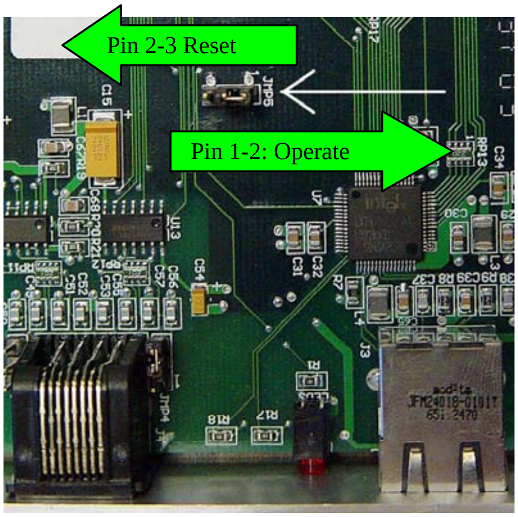
Different username and password in TACACS/RADIUS and power strip: ***TACACS/RADIUS username Login***

- **Case 1:** TACACS/RADIUS enabled, TACACS/RADIUS contact good, “Enable DS62 usernames as backup” = disabled, TACACS/RADIUS username Log in **OK.** Log in validated by the TACACS/RADIUS server.
- **Case 2:** TACACS/RADIUS enabled, TACACS/RADIUS contact good, “Enable DS62 usernames as backup” = enabled, TACACS/RADIUS username Log in **OK.** Log in validated by the TACACS/RADIUS server.
- **Case 3:** TACACS/RADIUS disabled or TACACS/RADIUS contact lost, “Enable DS62 usernames as backup” = disabled, TACACS/RADIUS username Log in **FAIL**. TACACS/RADIUS does not validate the user.
- **Case 4:** TACACS/RADIUS disabled or TACACS/RADIUS contact loss, “Enable DS62 usernames as backup” = enabled, TACACS/RADIUS username Log in **FAIL.** TACACS/RADIUS does not validate the user.

Different username and password in TACACS/RADIUS and power strip: ***Power Strip username Login***

- **Case 1:** TACACS/RADIUS enabled, TACACS/RADIUS contact good, “Enable DS62 usernames as backup” = enabled, Power Strip username Log in **OK.** Power strip validates the user.
- **Case 2:** TACACS/RADIUS disabled or TACACS/RADIUS contact loss, “Enable DS62 usernames as backup” = enabled, Power Strip username Log in **OK.** Power strip validates the user.
- **Case 3:** TACACS/RADIUS enabled, TACACS/RADIUS contact good, “Enable DS62 usernames as backup” = disabled, Power Strip username Log in **FAIL.** Power strip does not validate the user.
- **Case 4:** TACACS/RADIUS disabled or TACACS/RADIUS contact loss, “Enable DS62 usernames as backup” = disabled, Power Strip username Log in **FAIL.** Power strip does not validate the user.

APPENDIX: DS62/DS62-MD4 Reset Procedure



IMPORTANT: This procedure will reset configuration to factory default.

DS62 and DS62-MD4:

1. Remove the module from the chassis (Module is hot swappable).
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 wait 30 seconds.
6. Take the module back out and replace the jumper to the original position, pins 1 & 2.

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 30 to 60 seconds.
DEFAULT username and password = root/baytech (lower case)

APPENDIX: BASIC TROUBLESHOOTING

1. **No menu serial port:**
   a. DS power is on and cable connected to EIA232 serial port.
   b. Verify computer serial port configuration; **9600, 8, none, 1**, **no flow**
   c. Verify the cable and adapter has the correct pin out, RJ08X007 and 9FRJ45PC-1.
   d. Cisco Rollover cables have the same pin out as RJ08X007.
   e. 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.
   f. Test the cables and adapter with a working Baytech device,
   g. Turn power off, reseat the DS62-MD4 module and power on,
   h. Install module in a working DS-series unit and test,
   i. Reset the DS62-MD4 to factory defaults, username/password = root/baytech.

2. **Password not Work:**
   a. Password is case sensitive, check for Caps Lock.
   b. Have the admin user delete the user and add back

3. **No Access to Configuration Menu:**
   a. Only the admin user (root) will see the configure option
   b. Only one user at a time can have access. Have the other user back out of the configuration

4. **No Ports displayed for User:**
   a. Ports have to be assigned to the user, refer to ‘Login Setup: Assign User Ports’

5. **Not able to Connect to Modem.**
   a. Verify you see or hear the modem negotiating
   b. Verify the telecommunications line is a true analog line and not a digital converted to analog
   c. .If the modem negotiates then drops the call, serial into the unit. Verify the Country Code for the modem is set for the local country code.

6. **Verify DS-chassis, Host Module, and DS74 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 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 ‘b”. 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 you have done all of the above steps that are possible and still have problems, contact Baytech Technical Support at 228-563-7334.

APPENDIX: NETWORK MENU OPTION INDEX

Select each menu option, press ‘Enter, then select next option and press ‘Enter’, i.e. {Network Status: (C/1), type ‘C’ (Configure) at prompt and press ‘Enter’, type ‘1’ (Status) at prompt, and press ‘Enter’.

- Network Menu Configure: (**C**)
- Network Status: (**C/1**)
- Serial Port Configuration: (**C/2**)
    - Handshaking: (**C/2/1**)
    - Baud Rate: (**C/2/2**)
    - Word Size: (**C/2/3**)
    - Stop Bits: (**C/2/4**)
    - Parity: (**C/2/5**)
    - RTS/DTR Line Driver Inactive State: (**C/2/6**)
    - Modem DCD Connection Mode (DS62-MD4 ONLY): (**C/2/7**)
- Serial Port Device Name: (**C/3**)
- Attention Character: (**C/4**)
- Disconnect Timeguard: (**C/5**)
- Connect Port ID Echo: (**C/6**)
- Login Setup: (**C/7**)
    - Access Control: (**C/7/1**)
        - Telnet Login Prompt Enable/Disable: (**C/7/1/1**)
        - Serial Login Prompt Enable/Disable: (**C/7/1/2**)
    - Manage Users: (**C/7/2**)
        - Add user: (**C/7/2/A**)
        - Delete user: (**C/7/2/5**)
        - root: (**C/7/2/1**)
    - Direct Port Connection: (**C/7/3**)
    - Radius Configuration: (**C/7/4**)
        - Radius Enable: (**C/7/4/1**)
        - Radius Server Address: (**C/7/4/2**)
        - Radius Backup Server Address: (**C/7/4/3**)
        - Radius Secret: (**C/7/4/4**)
        - Enable DS62 usernames as backup: (**C/7/4/5**)
        - Radius Login Timeout: (**C/7/4/6**)
        - Radius Server Port: (**C/7/4/7**)
    - TACACS Configuration: (**C/7/5**)
        - TACACS Enable: (**C/7/5/1**)
        - TACACS Server Address: (**C/7/5/2**)
        - TACACS Backup Server Address: (**C/7/5/3**)
        - TACACS Secret: (**C/7/5/4**)
        - Enable DS62 usernames as backup: (**C/7/5/5**)
        - TACACS Encryption Enable: (**C/7/5/6**)
        - TACACS Login Timeout: (**C/7/5/7**)
        - TACACS Server Port: (**C/7/5/8**)
        - DS62 Privilege Level Enable: (**C/7/5/9**)
        - DS62 Privilege Level: (**C/7/5/10**)
    - Login Option Dial-Back Number (DS62-MD4 ONLY): (**C/7/6**)
- Network Port Configuration: (**C/8**)
    - IP Address: (**C/8/1**)
    - Subnet Mask: (**C/8/2**)
    - Gateway Address: (**C/8/3**)
    - Inactivity Timeout: (**C/8/4**)
    - Carriage Return Translation: (**C/8/5**)
    - Break Length: (**C/8/6**)
    - DHCP Enable/Disable: (**C/8/7**)
    - Telnet Enable/Disable: (**C/8/8**)
    - SSH Enable/Disable: (**C/8/9**)
    - SSH Host Key Generation: (**C/8/10**)
    - IP Filter Configuration: (**C/8/11**)
    - SNMP Configuration: (**C/8/12**)
        - SNMP Trap Host 1 Address: (**C/8/12/1**)

    - SNMP Trap Host 2 Address: (**C/8/12/2**)
    - SNMP Trap Host 3 Address: (**C/8/12/3**)
    - SNMP Trap Host 4 Address: (**C/8/12/4**)
    - SNMP Read-Only Community: (**C/8/12/5**)
    - SNMP Read-Write Community: (**C/8/12/6**)
    - SNMP Enable: (**C/8/12/7**)
    - SNMP v3 Only Enable: (**C/8/12/8**)
    - SNMP Authentication Traps Enable: (**C/8/12/9**)
  - Web Server Configuration: (**C/8/13**)
    - Web Enable: (**C/8/13/1**)
    - Web Login Enable: (**C/8/13/2**)
    - Web SSL Enable (Secure Comm): (**C/8/13/3**)
    - Web Login Activity Timeout: (**C/8/13/4**)
- Module Name: (**C/9**)
- RPC Management: (**C/10**)
  - Temperature Alarm Threshold: (**C/10/1**)
  - Under Voltage Alarm Threshold: (**C/10/2**)
  - Over Voltage Alarm Threshold: (**C/10/3**)
  - Low Current Alarm Threshold: (**C/10/4**)
  - Environmental Sensors: (**C/10/5**)
  - Outlet Groups: (**C/10/6**)
    - List Outlet Groups: (**C/10/6/1**)
    - Add Group: (**C/10/6/2**)
    - Delete Group: (**C/10/6/3**)
    - Rename Group: (**C/10/6/4**)
    - Modify Outlets in a Group: (**C/10/6/5**)
    - Delete All Outlet Groups: (**C/10/6/6**)
  - Temperature units (degrees C/F): (**C/10/7**)
  - Power Factor Threshold: (**C/10/8**)
    - Individual Unit Power Facter and Power thresholds: (**C/10/8/1**)
    - All Inputs/Circuits/Outlets - Power Factor Threshold: (**C/10/8/2**)
    - All Inputs/Circuits/Outlets - Power Threshold: (**C/10/8/3**)
- Firmware / Config Download: (**C/11**)
  - Enable Firmware Upgrade: (**C/11/1**)
  - Enable SSL Cert Upload: (**C/11/2**)
  - Enable Configuration File Upload: (**C/11/3**)
  - Restore Configuration Defaults: (**C/11/4**)
  - Get Current Configuration File: (**C/11/5**)
  - Display Configuration Error Log: (**C/11/6**)
  - Enable Rel Ctl. Firmware Upgrade: (**C/11/7**)
- Modem Configuration Menu (DS62-MD4 ONLY): (**C/12**)
  - Modem Port Configuration (DS62-MD4 ONLY): (**C/12/1**)
  - Rings to Auto Answer (DS62-MD4 ONLY): (**C/12/2**)
  - Modem Connectivity Timeout (DS62-MD4 ONLY): (**C/12/3**)
  - Modem Inactivity Timeout (DS62-MD4 ONLY): (**C/12/4**)
  - Modem Device Name (DS62-MD4 ONLY): (**C/12/5**)
  - PPP Configuration (DS62-MD4 ONLY): (**C/12/6**)
  - Country Code (DS62-MD4 ONLY): (**C/12/7**)