NetMediator RTD G5 Web Browser
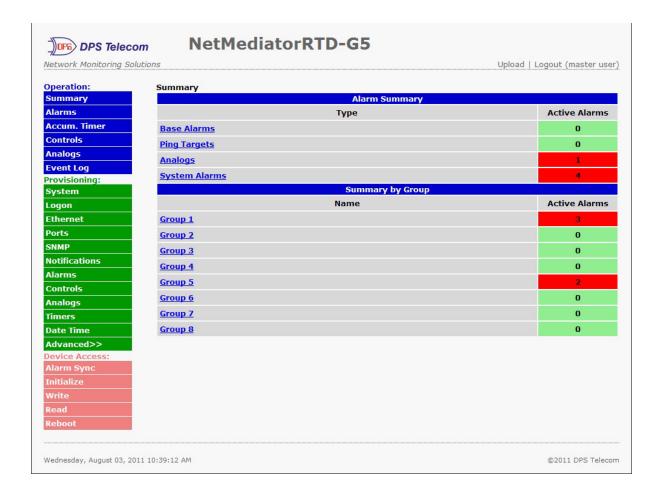
USER MANUAL

Visit our website at www.dpstelecom.com for the latest PDF manual and FAQs.

Revision History

July 15, 2015	Display Mapping Update
September 12, 2011	Added the analog suppression function, new features for login profiles, and other miscellaneous web updates
August 15, 2011	Preliminary Release

Contents

1 Overview

NetMediator RTD G5 monitors alarms, pings network elements, and reports via SNMP, pager, or email

The NetMediator's web interface provides a means to configure and monitor your alarms through the Internet or your Intranet, all without installing 3rd party software.

1.1 Grouped Alarms and Derived Control Logic

Your NetMediator's 8 control relays operate based on derived logic for preconfigured groups of your base discrete, system, and analog threshold alarms (alarm groups 4-8). When configuring your unit's alarms, keep in mind group and relay relationships to ensure proper operation.

For more information about **Groups**, see the **Defining Point Groups** section of this Manual.

Note: While relationships between groups and relays are predetermined, you may edit descriptions, set, and clear messages for your alarm groups from the **Groups** menu in the web interface **without altering group-relay relationships**. For your relays, you can determine whether or not your relays will send SNMP traps when their state changes without affecting relay logic.

Group	Members	Group Name	Set Message	Clear Message	Echoed Relays
4	Base Analogs channels 1, 2, 3, 7	**Analogs 1, 2, 3, 7**	**Alarm**	**Clear**	
5	System Alarms (Display 11) 36, 40, 56, & 57	**All's Well (sys)**	**Alarm**	**Clear**	7, 8
6	Discrete Alarms	**Airflow Sensors**	**Alarm**	**Clear**	8
7	All minor temperature threshold alarms from RTD DX expansion analog channels	**Minor Temp**	**Alarm**	**Clear**	6
8	All major temperature threshold alarms from RTD DX expansion analog channels	**Major Temp**	**Alarm**	**Clear**	1-5

Default alarm groups for the NetMediator and RTD 32 DX Expansions

Relay (display 11)	Logic	Group
1	**_OR G8**	Operates relay when an alarm condition is present in group 8.
2	**_OR G8**	Operates relay when an alarm condition is present in group 8
3	**_OR G8**	Operates relay when an alarm condition is present in group 8.
4	**_OR G8**	Operates relay when an alarm condition is present in group 8.
5	**_OR G8**	Operates relay when an alarm condition is present in group 8.
6	**_OR G7**	Operates relay when an alarm condition is present in group 7
7	**_NO G5**	Relay operates when there are no alarm conditions present in alarm group 5. (All points clear)
8	**_OR G5 G6**	Operates relay when an alarm condition is present in group 5 **or** group 6

Default relay logic for the NetMediator RTD G5

Default Derived Logic:
DPS Telecom does not recommend editing your NetMediator's default alarm groups or relay logic without expressed direction from DPS Telecom Support. However, if you edit your NetMediator's relay logic, you can return your relays to their default logic from the TTY interface. For more information on restoring your NetMediator's default derived logic, see the section of your NetMediator's hardware manual titled: **Restoring Default Derived Logic**.

1.2   Logging in to the NetMediator

To connect to your NetMediator:
1.   Enter the unit's IP address or Hostname in the address bar of your Web browser. It may be helpful to bookmark the logon page to simplify access.

Note: To use your NetMediator's web interface, you must have provisioned the unit with an IP address. For help with initial IP configuration, see your NetMediator Hardware Manual.

2.   Enter your password.

Note: The factory default password is **dpstelecom.** You can change the master password and create up to 16 unique users, each with different access rights to the NetMediator from the **Logon** provisioning menu. See the section entitled "Creating/Editing Logon Profiles" for more information.

Enter your password to enter the NetMediator Web Browser Interface

If you are the master user, "master user" will appear in parenthesis next to the Logout link in the upper-right corner of the web interface.

The NetMediator will inform you if you're logged in as the master user

Up to 4 users can connect to the NetMediator's web interface at a time, and only 1 user can access the Provisioning menus. To prevent rendering the NetMediator inaccessible to some users, you should logout when finished using the web interface.

1.3   Navigating the Web Interface

The Web Interface is split into 3 sections:
• The blue **Operation** menus provide access to monitor alarms, issue controls, and view logs.
• The green **Provisioning** menus are where you'll configure your unit, alarms, controls, and notifications.
• The pink **Device Access** options provide maintenance access to the NetMediator itself, allowing you to read and write configurations, reboot, and initialize the unit.

To navigate to any section of the web interface, simply click the links on left side of the interface.

2   Basic Unit Configuration (Provisioning)

You'll configure your NetMediator from the **Provisioning** menus, the menu options in green on the left-side of the web interface. The following sections in this chapter provide descriptions of available provisioning options and descriptions of the fields within each menu.

Note: Accessing **any** of the Provisioning menus from **any** of the **Operation** menus will execute the **Read** function, ensuring that one user doesn't accidentally overwrite another's changes before they're written to the unit. The unit will display in the top left corner of the web interface as the NetMediator reads the most recent configuration (5-15 seconds). Any configuration changes made before the NetMediator finishes reading the current configuration will not take affect. (The NetMediator will overwrite them with the configuration file read from its own memory.)

Saving Configuration Changes to the NetMediator:
At the bottom of each screen you access from the **Provisioning** Menu, you will see a **Save** button. Clicking Save will cache your changes locally. The web interface will then prompt you to either **Write** your changes to the unit or **Reboot** the unit for changes to take effect in the top-left corner of your browser. The relevant options will be highlighted in the **Device Access** options**.**

Note: If the unit prompts you to both Write changes to the unit **and** Reboot, you will Write your changes first. Rebooting before without writing to the unit (if a Write is required) will cause you to lose your configuration changes.

Please **WRITE** to the unit after you are finished with your changes!
Please **REBOOT** the unit for changes to take effect!

Status messages inform you how to implement your changes

Device Access:
Alarm Sync
Initialize
Write (required)
Read
Reboot (required)

The control menu highlights items that must be completed for your changes to take effect

2.1   Entering System Settings

You can edit system information and DCP settings for your unit from the **System** menu.

Configure the system information by selecting the System screen from the Edit menu

Field	Description
Name	Used to set the Name@Location email address. **Name** is the portion of the address **before the @** character.
Location	Used to set the Name@Location email address. **Location** is the portion of the address **after the @** character, this is a host name or IP address.
Contact	Information for how to contact the person responsible for this NetMediator.
Phone	Contact's telephone number.
Unit ID	User definable ID number for this NetMediator (DCP Address).
DCP Port	Enter the DCP Port for this NetMediator. (1-8 serial otherwise UDP/IP Port)
DCP Protocol	Choose between DCPx, DCPf, or DCPe.
Silence non-reportable system alarms	Check the box to silence alarms not applicable to your configuration. Example: If your NetMediator is not configured to send SNMP traps, you won't receive a failure notification for system alarm 13 (SNMP Trap not sent).
LCD Point Mode	Check this box to place the NetMediator's LCD in "Point Mode". In this mode, the NetMediator's LCD will only display points in alarm, rather than full alarm descriptions. See your hardware manual for details about LCD Point Mode.

System fields

2.2   Editing Logon Information

From the **Logon** menu, you can edit your NetMediator's master password and configure up to 16 independent user profiles, each with their own access rights.

Default Password:
The factory default master password is **dpstelecom**. DPS Telecom strongly recommends that you change the default master password.

Configure the password parameters from the Login screen

2.2.1   Master Password

The **Master Password** provides total access to the NetMediator's editing functions. You can configure individual logon profiles with the same access rights, but the master password prevents the possibility of accidentally blocking particular privilege from all users.

You can **change the master password** from the Login screen by entering a new password and confirming it in the appropriate fields.

Password Options:

Field	Description
Minimum Length	Set the minimum character length of passwords for the NetMediator. The minimum password field cannot be set to less than 3. **Note:** Setting the minimum length field to a value that a current logon password violates will not prevent the user from logging in. However, any attempt to edit that user's profile will require resetting that user's password.
Password/ Confirm Password	Enter and confirm the NetMediator's master password.
Quiet Logon	Check to prevent the password prompt from appearing when logging into the TTY interface. (Users will still enter a password to login to the TTY interface, they simply won't see the prompt.)

Fields available in the Master Password Logon section

2.2.2   Logon Profiles and Access Rights

Creating logon profiles allows you to grant personnel access to certain functions of the NetMediator without allowing access to sensitive or secure areas of the database.

To edit a user profile, click **Edit** in the associated row. By default, all user names are set to **Available**. You can delete a user profile by clicking the **Delete** button associated with that profile.

For each profile, you must enter a **User**name and **Password**. Beyond that, you can enable rights and security call-back for users as you see fit. See the table below for details about access privileges.

When you've finished editing user profiles, or if you access a user profile in error, you can click the **Edit Logon** button to return to the master **Logon** screen.

Logon

Logon Profile 1	
User	dps_support
Password	••••••••••
Confirm Password	••••••••••
Call Back	559-454-1600
Access Privilages	
Admin: Enables the user to add/modify logon profiles and NetMediator password information.	☑
DB Edit: Enables the user to perform database edits in the NetMediator.	☑
Monitor: Enables the user to have Monitor access of the NetMediator.	☑
SDMonitor: Enables the user to view serial port buffers.	☑
Control: Gives the user the ability to issue controls. This also automatically activates Monitor.	☑
Reach-Through: Enables the user to achieve reach-through (Proxy) access.	☑
Modem: Enables the user to call into the unit.	☑
Telnet: Enables the user to have Telnet access to the unit.	☑
PPP: Enables the user to access the NetMediator as a PPP server with the user defined password.	☑

Save

Edit Logon

Configure user profiles and access rights

Note: If you've enabled RADIUS on the NetMediator, the unit will not authenticate passwords locally.

Profile Field	Description
User	Enter a username or a user description. (18 characters maximum)
Password	Enter a unique user password. (4 character minimum) **Note:** This password will be used by the NetMediator to determine whether or not to initiate the "Call-Back" function and also if any limited access applies.
Confirm Password	Re-enter the password.
Call Back	This is the phone number the NetMediator uses to call back to the user's modem.
Access Privileges	
Admin	Enables the user to add/modify logon profiles and NetMediator password information.
DB Edit	Enables the user to perform database edits in the NetMediator.
Monitor	Enables the user to have Monitor access of the NetMediator.
SDMonitor	Enables the user to view serial port buffers.
Control	Gives the user the ability to issue controls. This also automatically activates Monitor.
Reach-Through	Enables the user to achieve reach-through (Proxy) access.
Modem	Enables the user to call into the unit.
Telnet	Enables the user to have Telnet access to the unit.
PPP	Enables the user to access the NetMediator as a PPP server with the user defined password.

Logon profile field descriptions

2.2.3 Security Dial-Back

The Dial-Back feature serves as an additional level of security when accessing the NetMediator from the modem. With Dial Back enabled, your NetMediator will respond to valid access requests from by dialing-back the modem of the expected user.

When accessing your NetMediator with the Security Dial Back feature enabled, users will see a message reading **accepted, Disconnecting** upon entering a valid password. The NetMediator will then hang up and dial back to the users modem using the number entered in the logon profile, granting users access to the NetMediator upon successful connection.

2.3   Ethernet Settings

Click **Ethernet** in the Provisioning menus to set and edit your NetMediator's ethernet settings.

All port configuration is accomplished from the Edit menu > Ethernet screen

Field	Description
Unit Address	IP address of the NetMediator's Net 1 or Net 2 ethernet ports.
Subnet Mask	A road sign to the NetMediator telling it whether your packets should stay on your local network or be forwarded somewhere else on a wide area network. Set individually for Net 1 and Net 2 ethernet ports.
Default Gateway	An important parameter if you are on a network that is connected to a wide area network, telling the NetMediator which machine is the gateway out of your local network. Set for both Net 1 and Net 2 ethernet ports or to 255.255.255.255 if not using.
DNS Address	IP address of the domain name server. Set to 255.255.255.255 if not using.
Proxy Base	Defines the NetMediator TCP ports used by data ports 1-8 (serial ports). Data port 1 receives the port number entered here. Data ports 2-8 receive the next 7 port numbers in ascending order. (i.e. TCP port 3000 through port 3007 at the IP address of the NetMediator).
HTTP Port	Enter 80 for HTTP
DCHP	Toggles the Dynamic Host Connection Protocol On or Off. **NOT recommended.** Enabling DHCP will allow your DHCP server to issue the NetMediator an IP address, overwriting your settings for Net 1 and Net 2. A NetMediator with DHCP enabled will NOT operate in a T/Mon environment.

Fields in the Ethernet Menu

2.4   Configuring Data Ports

From the **Ports** menu, you can edit your unit's serial port, modem, and expansion settings.

2.4.1   Craft Port Baud Rate

Under the **Craft Port** header, use the **Baud** drop-down box to set the rate for your front-side craft port.

Ports	
Craft Port	
Baud	9600 ▼

Configure the craft port baud rate from the Ports screen

2.4.2   Modem Port Settings

Depending on your phone network, you may have to configure the NetMediator's modem to dial out and accept incomming calls. You can edit your NetMediator's modem settings from the **Modem Port** section of the **Ports** menu.

Field	Description
Ring Count	Enter the number of rings your NetMediator will wait before accepting an incomming call (default = 1). **Note:** setting the ring count to 0, will still allow your NetMediator to send out notifications, but will prevent the unit from ever answering an incoming call.
Answer Init	An initialization string allowing the modem to answer incoming calls. See the table below for a list of standard modem commands.
Dial Init	An initialization string allowing the modem to dial-out. See the table below for a list of standard modem commands.

Fields in the Modem Port section of the Ports menu

Change the modem settings from the Edit menu > Ports screen

Command	Description		
A	Answer command		
Bn	Select communications standard		
D	Dial		
	P	Pulse dial
	T	Tone dial
	R	Connect as answering modem
	W	Wait for dial tone
	,	Pause for the duration of S8
	@	Wait for silence
	!	Switch hook flash
	;	Return to the command state
En	Command echo		
Hn	Switch hook control		
In	Modem identification		
Ln	Speaker volume		
Mn	Speaker activity		
On	Online		
Qn	Responses		
Sr?	Interrogate register		
Sr=n	Set register value		
Vn	Result codes		
Xn	Result code set		
Z	Reset		

Modem commands may vary. See your modem user manual for commands specific to your modem.

Standard modem commands (Hayes)

2.4.3 Adding Expansions

If you have RTD expansions or GLD units for your NetMediator, you will database them in the **Expansion Options** section of the **Ports** menu.

RTD 32 DX expansion units increase your NetMediator RTD's analog capacity by 32 inputs per expansion. NetMediator expansions connect on data port 7, and GLD units use the ECU/GLD port. See their respective user manuals for detailed configuration information.

Note; Your NetMediator is preconfigured to support 2 RTD DX expansion units. You **do not** need to edit the NGDdx field to install your two expansions.

Expansion Options	
NGDdx	2-DX units
GLD or BSU	0

Specify the number of RTD DX units in the Expansion Options section of the Ports menu

Field	Description
NGDdx:	Specify the number of RTD expansions connected to your NetMediator. **Default: 2-DX units**
GLD or BSU	Specify the number of GLD or BSU units (up to 13) you have connected to this NetMediator.

2.4.4 Data Ports 1 - 9

Your NetMediator has 9 serial ports (serial ports 1-8 and the ECU/GLD port). You can configure individual settings for each serial port in the **Data Ports** section of the **Ports** provisioning menu.

Data Ports					
Id	Description	Type	Baud	WFmt	
1		OFF	115200	8,N,1	Details<<

CR/LF Mode In	CR/LF Mode Out	RTS Head	RTS Tail		Pool
Ignore	Ignore	0	0		☐

2		OFF	115200	8,N,1	Details>>
3		OFF	115200	8,N,1	Details>>
4		OFF	115200	8,N,1	Details>>
5		OFF	115200	8,N,1	Details>>
6		OFF	115200	8,N,1	Details>>
7	NGDdx Net	OFF	2400	8,N,1	Details>>
8		OFF	115200	8,N,1	Details>>
9	ECU Net	ECU	19200	8,N,1	Details>>

Save

Configure your serial ports in the Data Ports section

For each data port, you can define:

Description:	A description for the port
Type:	Set the data port type. See the section titled **Data Port Types** for more information.
Baud:	Use the drop-down box to define the baud rate for that particular serial port.
WFmt:	Serial word format. Settings listed in the format **Data Bits, Parity, Stop bits**
Details:	Click to reveal additional port options
CR/LF Mode In:	Determines behavior for incoming Carriage Returns/Line Feeds to the Data Port:

- **Ignore: (Default)** Ignores incoming line feeds.
- **Append LF:** Converts Line Feeds to Carriage Returns
- **Remove LF:** Removes Line Feeds

CR/LF Mode Out:	Determines behavior for outgoing Carriage Returns/Line Feeds from the Data Port:

- **Ignore: (Default)** Ignores outgoing line feeds.
- **Append LF:** Converts Line Feeds to Carriage Returns

- **Remove LF:** Removes Line Feeds

RTS Head:	Request to send header - listed in number of bits.
RTS Tail:	Request to send tail - listed in number of bits
Pool:	Check to add ports to the **TCP Port Pool**. Users attempting to reach a TCP port will all connect to the first port in the pool. The NetMediator will then assign users to ports in the order in which they connect.

2.4.4.1   Port Types

Data Port Types available for use with the NetMediator's serial ports:

TCP
Makes reach-through available at TCP ports (Telnet).

RTCP
Raw TCP (negates Telnet negotiation). The RTCP (Raw TCP Data Port) negates Telnet negotiation and will allow all characters (including [FF]) to pass straight through from IP to serial or serial to IP.

HTCP
High speed TCP port (only 1 HTCP port is available). An HTCP, or High-speed TCP data port, which operates in Telnet Raw mode, is essentially the same as a RTCP port except that it offers better performance and is more robust when transferring streaming data. Unlike RTCP ports, the user can only assign one HTCP port.

PTCP
Permanent TCP (proxy connections will never time out).

SPS8
Serial Port Switch 8 (allows eight serial devices to be connected to single port).

UDP
Makes reach-through available at UDP ports (up to 4 UDP ports available).

CHAN
Creates logical bridge to odd/even partner. The odd/even partners are pairs of 1-2, 3-4, 5-6, and 7-8. This allows your NetMediator to view communication traffic in either direction when inserted in the serial communication path between two devices. This is accomplished by going "in" to the NetMediator with one device and "out" to the other device from the odd/even partner port. Data passes directly from one port to its odd/even partner without being altered in any way. This greatly simplifies troubleshooting communication problems by isolating the non-communicating device.

When **CHAN** is selected, Your NetMediator automatically activates the odd/even partner as **CHAN**. You can set Baud rates for the odd/even pairs to any available rate except for any combination of 19200 and 38400 between the two ports. Use "SPO" filter debug to analyze protocol traffic in a terminal.

CRFT
Grants a data port the same functionality as the front panel craft port.

CAP
Allows the user to capture debug information. Debug information is stored in your NetMediator receive queue. This is primarily a troubleshooting feature.

ECU
For use with Entry Control Units (ECUs) (see section "Building Access Controller").

2.4.4.2 Defining SPS8 Ports

Selecting the SPS8 port type

A Serial Port Switch 8 (SPS8) is an external device hub that allows you to connect of up to eight serial devices to a single NetMediator data port.

While you can select the SPS8 **Type** option when configuring data ports using the Web Browser Interface, you may only **edit SPS8 port descriptions using the TTY interface**.

Your NetMediator will negotiate SPS8 connections for you. To break the SPS8 connection and return to the normal TTY interface, type **@@@** and press Enter.

⚠ *Hot Tip!*

SPS8 ports do not support direct proxy. You must navigate them via the TTY menu. If interfacing T/Mon to SPS8 through a NetMediator, set the port type to **TCP**.

2.4.4.3   Direct and Indirect Proxy Connections

Your NetMediator supports both direct and indirect proxy connections. In a **direct proxy** connection, users will enter an IP address and port number to Telnet directly to a TCP serial port. In an **indirect proxy connection**, users will navigate the TTY menu to select a proxy port.

Indirect proxy connections require a password and are therefore **more secure**. You may wish to disable direct proxy access for all connections in order to enforce the password security provided by the TTY interface.

To **discourage direct proxy** access to your NetMediator you can set the proxy port to an uncommon value.

To **disable direct proxy access**, set the data port **Type** to **Off.** When set to **off**, the port is no longer associated with a TCP socket, effectively disabling direct proxy access to the port.

Set proxy connections in Edit menu > Ports screen > Data Ports

2.5   SNMP Settings

From the **SNMP** provisioning link, you can set and edit community names, SNMP v3 users, and information for your trap managers. See the table below for field descriptions within the SNMP menu.

SNMP

Global Settings

Read and Write Access	All
v3 Engine ID	80000a7a03001081006124

Community Names

Get	dps_public
Set	dps_public
Trap / v3-ContextName	dps_public

v3-Users

Id	Username	Access Mode	Auth Pass	Priv Pass
1	Support	Priv Auth-MD5	Call	Support
2		No-Auth,No-Priv		
3		No-Auth,No-Priv		
4		No-Auth,No-Priv		

Global Trap Managers

Id	IPA	Port	Format	Retry	Seconds	v3-User
1	126.010.215.097	162	v2c-Trap	1	1	0
2	126.010.215.198	162	v3-Trap	1	1	1

Save

SNMP Menu

Globals	
Read and Write Access	Defines which SNMP version(s) you can use to acces your NetMediator: • All- Allows you to read or write using any version of SNMP (v1, v2c, v3) • Disabled- Restricts all access to unit via SNMP • v1-Only- Allows SNMPv1 access only • v2c-Only- Allows SNMPv2c access only • v3-Only- Allows SNMPv3 access only
v3 Engine ID	Specifies the v3 Engine ID for your NetMediator. DPS recommends using the default ID for the unit, which the unit automatically generates according to RFC3411 based on its unique MAC address and DPS Telecom's SNMP enterprise number. **Note:** To have your NetMediator generate a unique Engine ID, clear the **v3 Engine ID** field and press the **Save** button.
Community Names	
Get	Community name for SNMP requests.
Set	Community name for SNMP SET requests.
Trap / v3 Context Name	Community name for SNMP TRAP requests. In SNMP v3, defines the context name field of a v3-Trap. **Note:** Make sure that your community strings match those used by the SNMP manager. In v1 and v2c, community strings are security passwords; if the strings do not match, the SNMP manager will not accept Traps from your NetMediator. Community strings are case sensitive.

v3-Users	
ID	The number designated for a v3-user. Your NetMediator supports up to four v3-User profiles.
Username	The name of the user for which an SNMPv3 management operation is performed.
Access Mode	This identifies the security modes available when utilizing SNMPv3. • **No-Auth, No-Priv-** access does not require authentication and does not require encryption. This mode is the least secure and is comparable to v1 and v2c. • **Auth-MD5,No-Priv-** Provides authentication based on the MD5 algorithm and does not require encryption. • **Auth-SHA,No-Priv-** Provides authentication based on the SHA algorithm and does not require encryption. • **Priv Auth-MD5-** Provides authentication based on the MD5 algorithm and provides DES 56-bit encryption based on the CBC-DES standard. • **Priv Auth-SHA-** Provides authentication based on the SHA algorithm and provides DES 56-bit encryption based on the CBC-DES standard.
Auth Pass	Contains the password used with either MD5 or SHA authentication algorithms.
Priv Pass	Contains the password used with privatization encryption.
Global Trap Managers	
IPA	Defines the SNMP trap manager's IP address. Set to 255.255.255.255 if not using.
Port	The UDP port set by the SNMP manager to receive traps, usually 162.
Format	Trap Formats: v1-Trap, v2c-Trap, v2c-Inform, or v3-Trap.
Retry	Number of times the NetMediator G5 will resend SNMP v2c-Informs
Seconds	Time interval in seconds between attempts to resend SNMP v2c-Informs.
v3-Users	Association to the v3-User Table specifies the username, security mode, and passwords used for sending a v3-Trap.

Fields in the Edit > SNMP settings

If using SNMPv3, any changes to the Engine ID or passwords will require you to reboot.
At bootup, you may experience a slight delay while the authorization and privatization keys update.

2.6 Configuring Notifications

Click **Notifications** to set or edit notifications that can be sent from your NetMediator. Your NetMediator can send 11 different types of notifications, listed in the table below.

Setting Notifications for Point Groups:
From the **Notifications** menu, you may associate any of your NetMediator's 8 notification types with a point group (1-8) in the **Groups** column. For more information about point groups, see the **Defining Point Groups** section of this manual. To associate a notification with individual alarms, see the **Defining Alarms** and **Configuring Analog Inputs** sections of this manual.

Note: You'll use the notification **Id** number in the alarm provisioning menu to designate the primary and secondary notifications sent by your NetMediator when an alarm condition occurs or clears.

Multiple notification methods and group assignments are configured from the Notification screen

For instructions configuring individual notification types, see the following subsections.

Notification Format	Description
Alphanumeric	Format recognizes numbers, letters, and symbols. Can receive information including alarm point addresses, alarm descriptions, time of alarms, and alarm state a.k.a TAP.
Numeric	Format recognizes numbers only. Reports messages in the following order: [IP]*[Display] [Address]*[State]. When read on the pager it appears as follows: 192.168.1.100 99.01.01.01
Text	Can receive information including alarm point addresses, alarm descriptions, time of alarms, and alarm state. Terminal accessible.
T/Mon	Your T/Mon may receive alarm information from the NetMediator via dial-up and display alarm description and threshold status. (Only activates if DCP Poller is inactive)
TCP (ASCII)	Alarm status notification via multiple TCP or HTCP ports. Your NetMediator must establish a connection to a higher-level master to make this option available.
Email/SMTP	Provides alarm notification via email, with a description similar to the Alphanumeric pager.
SNMPv1	May send alarm status to multiple SNMP managers, including the SNMP that alarms are reporting to. The SNMP trap format is v1.
SNMPv3	May send alarm status to multiple SNMP managers, including the SNMP that alarms are reporting to. The SNMP trap format is v3.
Num17	Provides alarm notification in a manner similar to that of the Numeric pager. However, Num17 eliminates the (*) symbol from the page. Reports messages in the following order: [IP]

Notification Format	Description
	[Display][Address][State]. When read on the pager it appears as follows: 192.168.1.100 99.01.01.01
SNPP	Sends alarm notifications via Simple Network Paging Protocol.
Echo	Allows an alarm point on the NetMediator G5 to operate a control on another SNMP-enabled, DPS Telecom RTU.

Notification formats

Note: Many cellular carriers offer a TAP gateway to SMS. Check with your carrier to see if you can use a dial-up connection to send SMS messages to your phone. This creates an out-of-band alarm reporting path in the case of a network failure.

2.6.1 Alphanumeric Pager Setup

The alpha numeric pager can receive text messages including alarm descriptions, time of occurrence, and point addresses.

To configure the alpha numeric pager settings:
1. In the **Type** drop-down menu, select **Alpha**.
2. Enter the phone number of the Alpha numeric pager in the **Phone/Domain** field.
3. Enter a personal identification number in the **PIN/Rcpt/Port** field.
4. Set the pager data rate (i.e. 300, 1200, 2400 or 9600). The default baud is 1200.
5. Select a pager word format (Data Bits, Parity, Stop Bits). The default setting is 7,Even,1.

1. Number of pages
2. Unit name
3. Port # and Address (Applicable to T/Mon and IAM only)
4. Display number
5. Alarm point number
6. Alarm status: 1=alarm, 0=clear
7. Date and Time NetGuardian sent page
8. Alarm point description
9. Alarm status

Alpha numeric pager description

2.6.2 SNPP Notification Setup

An alpha numeric pager can receive text messages including alarm descriptions, time of occurrence, and point addresses from your SNPP service.

To Configure SNPP Paging:
1. In the **Type** field, select **SNPP** from the drop-down menu.
2. If a username and password are required, enter them in the **Phone/Domain** field. The username and password must be separated by a colon and be no longer than 29 characters combined. Otherwise, leave this field blank.
3. Enter the numeric pager number in the **PIN/Rcpt/Port** field.
4. In the IPA field, enter the static IP address of the SNPP server. The port number automatically defaults to 444.

2.6.3   Numeric Pager Setup

A **Numeric Pager** can receive point addresses of alarms.

To Configure Numeric Paging:
1.   In the **Type** field, select **Numeric** from the drop-down menu.
2.   Enter the phone number of the numeric pager in the **Phone/Domain** field, followed by 7 commas (e.g. **555-1212,,,,,,,**). Each comma after the phone number initiates a two second pause. This allows enough time for the pager to answer before the NetMediator attempts to send the alarm information.

Note: The Baud/Wfmt and IPA fields are not used from numeric pager types.

2.6.4   Text Paging Setup

Text Pages can include the point addresses of an alarm, the alarm description, time of the alarm, and the alarm state (alarm or clear). You can view text pages using a terminal emulator, such as HyperTerminal..

To Configure Text Paging:
1.   In the **Type** field, select **Text** from the drop-down menu.
2.   Enter the phone number of the text paging device in the **Phone/Domain** field.
3.   Set the pager data rate (i.e. 300, 1200, 2400 or 9600) using the drop-down box in the **Baud** field. The default baud is 1,200.
4.   Select a pager word format using the drop-down box in the **WFmt** field . The default setting is 7, Even,1.

To set up text paging from T/Mon see the T/Mon user manual.

2.6.5   Email Notification Setup

Email notification from the NetMediator

Email notifications provide full point references and alarm descriptions via email.

To enable email notifications, **you must configure:**
1. The email recipient's address
2. The address from which the NetMediator will send email.

Configuring the "from" address:
1.   In the **Type** field, select **Email** from the drop-down menu.
2.   Enter the email recipient's domain name the **Phone/Domain** field. This is the portion of an email address after the @ symbol in an email address.
3.   Enter the email recipient's user name in the **PIN/Rcpt/Port** field. This is the portion of an email address before the @ symbol in the email address.

Note: Email notification recipients cannot have spaces in their email addresses (in either the **Phone/Domain** or **Pin/Rcpt/Port** fields). **domain name**.

4.   Enter the IP address of your outgoing (SMTP) mail server in the **IPA** field.
5.   Click **Save** to save your email notification settings.

<u>**Configuring the "to" address:**</u>
1. Click on the **System** link to configure the address from which the NetMediator will send notifications.
2. Enter the notification sender's **username** (the portion of the email address before the @ symbol) in the **Name** field
3. Enter the notification sender's **domain name** (the portion of the address after the @ symbol) in the **Location** field.
4. Click **Save**

Note: Your NetMediator will send email notifications from an address in the format **name@location.** Some SMTP servers will **not forward mail** from senders with an **invalid email address or domain**. You may need need to add a domain suffix (.com, .net, etc.) to your NetMediator's Location or set the location to a valid domain name in order for your SMTP server to forward email notifications. Check with your IT department for specifics about your SMTP server.

The "from" email address is for identification purposes. It is not necessarily a real email address to which the user can reply.

2.6.5.1   SMTP POP3 Authentication Support

To send authenticated email notifications:
1.   In the **Pin/Rcpt** field enter the password for the email account notifications will be sent from.
2.   In the **Phone/Domain** field, input the address email will be sent from, in the format "from@fromdomain.com".
3.   Click **Save**.
4.   Click on the **System** link.
5.   In the **Name** field, enter the name of the address you want to receive notifications from the NetMediator (the part of the email address before the @ symbol - **user**@yourdomain.com).
6.   In the **Location** field, enter the domain of the address you want to receive notifications from the NetMediator (this is the part of the address after the @ symbol - user@**yourdomain.com**).
7.   Click **Submit Data** to save the new system information settings.

2.6.6   SNMPv1 Paging Setup

The SNMPv1 paging feature allows you to view alarm status from SNMP managers in addition to the two global managers, configured in the SNMP menu.

To Configure SNMPv1 Paging:
1.   In the **Type** field, select **SNMPv1** from the drop-down menu.
2.   Set the SNMP port in the **PIN/Rcpt/Port** field, usually 162.
3.   Enter the IP address of the SNMP manager in the **IPA** field.

2.6.7   SNMPv3 Paging Setup

The SNMPv3 paging feature allows you to view alarm status from SNMP managers in addition to the two global managers, configured in the SNMP menu.

To Configure SNMPv3 Paging:

1. Select **SNMPv3** from the drop-down menu in the **Type** field.
2. Enter the ID number of one of the v3-User ID's configured in the **SNMP** menu in the **Phone/Domain** field.
3. Set the SNMP port in the **PIN/Rcpt/Port** field, usually 162.
4.. Enter the IP address of the SNMP manager in the **IPA** field.

2.6.8   TCP Paging Setup

<MSG_BEG 00001>
VID : DPS Telecom
FID : NetMediator SNMP v5.0B.3206
SITE: Yale Office
PNT : 99.01.01.01
DESC: RECTIFIER 1
STAT: CLEAR
DATE: 01/01/2001
TIME: 12:17:02
<MSG_END 00001>

Example TCP message

Heading	Description
MSG_BEG MSG_END	Sequential message number used to group the message and detect missing messages (e.g. 00001, 00002, etc...).
VID	Vendor ID
FID	NetMediator Firmware ID.
SITE	NetMediator system name.
PNT	Point ID (port.address.display.point). See Appendix A for display mapping.
DESC	Description set forth in the Alarm parameters.
STAT	Status of the alarm (Clear or Alarm).
DATE	Date the alarm occurred.
TIME	Time the alarm occurred.

TCP alarm message field descriptions

The NetMediator offers alarm status notification via multiple TCP ports. When an alarm condition occurs, an alarm condition formatted according to Figure 2.17 will be sent to the specified TCP points for use by a higher level master. This connection must be established by the master. Any applicable alarm activity occurring prior to an established connection will be discarded.

To Configure TCP Paging:
1. Select **TCP** from the drop-down menu in the **Type** field.
2. In the **Pin/Rcpt/Port** field enter the NetMediator TCP port number where alarm messages will be sent (from 1 to 65,536).
3. The TCP message can be viewed by a Telnet session by connecting to the NetMediator's IP address and the TCP port entered in this screen. For example, Telnet to **126.10.220.199 5000** if port 5000 is selected and 126.10.220.199 is the unit's IP address. See Figure 2.17 for an example message and Table 2.H for TCP message format information.

2.6.9 Num17 Pager Setup

The Num17 Pager can receive point addresses of alarms. It is quite similar to the Numeric Paging format in the way it receives and reports alarms. However, on certain pager systems the symbol ∗ will cause a freeze or other undesirable situations. Num17 eliminates the ∗ symbol from the pages it receives and reports alarms as a 17-digit series of numbers.

User the following steps to configure Num17 Pager settings:
1. From the **Edit** menu > **Notification** screen select an ID number to use, refer to Figure 2.14.
    Note: Pager IDs are used in the alarm provisioning screen to designate the primary and secondary person/ device being paged when an alarm condition occurs or clears.

2. Under the **Type** column select **Num17** from the drop-down menu, see Figure 2.14.

3. Enter the phone number of the numeric pager under the `Phone` heading, followed by commas (for example **555-1212,,,,,,,**). Placing a comma after the phone number initiates a two second pause per comma. This allows enough time for the pager to answer before the NetMediator sends the alarm information. The **Baud/ Wfmt** and **IPA** fields are not used from Num17 pager types.

4. Click **Submit Data** to save the configuration settings.

2.6.10 Echo Notification Setup

⚠ *New Feature!*

As of firmware 5.0K and above. An Echo notification type enables an alarm point on the NetMediator G5 to operate a control on another SNMP remote from DPS.

1. From the **Notification** devices tab, choose **Echo** as the notification **Type**.
2. Enter the Community Set Name in the **Phone/Domain** field.
3. Enter the Relay Point Reference in the **Pin/Pcpt/Port** field. This is entered as:[Port].[Address].[Display]. [Relay Point] **NOTE**: The Port will always be 99, and the address is always 1. Therefore, your entries will always begin with 99.1.
4. The **Baud/WFmt** and **Group** fields will not be used.
5. Under **IPA**, enter in the IP address of the SNMP-enabled, DPS remote you are setting up to operate its relay.

NOTE: If more than one point is mapped to Echo notification, the OR'ed logic is applied.

2.7 Setting System Timers

From the **Timers** option in the Provisioning menus, you can control the interval between certain NetMediator specific events.

Note: Plan settings carefully to ensure that there is no conflict among your timers.

To change the rate of NetMediator activities using **Timers**:
- Change the **Value** for a timer
- Set the unit of time in the **Units** drop-down box (if applicable).

See the table below for timer descriptions and available time values.

Set intervals for system events in the Timers menu

Field	Description	Values
Cycle	This determines how often the NetMediator will attempt to ping its list of **Ping Targets**.	0-120, sec/min
Wait	How long the NetMediator will wait for a response after issuing a ping request to a target before determining that a target is unreachable	0-12, sec/min
Fail	The period of time in which, if a unit has not responded, it is considered failed	0-120 sec/min
Sound	How long the NetMediator's speaker will sound when an alarm sets or clears. **Note:** The speaker shutting off does **not** indicate that an alarm has cleared. This timer only affects the duration of audible alarm annunciation.	0-120 sec/min
Channel	The period of inactivity which will dictate a failure of devices connected to the "channel" port	0-120 sec/min
Craft	The period of inactivity which will dictate a failure of a device connected to the NetMediator's craft port.	0-120 sec/min
DCP	The maximum length of time the NetMediator can go without receiving a DCP poll before setting an alarm.	0-120 sec/min
Timed Tick	For alarm masters that don't perform integrity checks. The timed tick is a "keep-alive" or "heartbeat" communication the NetMediator will issue to an alarm master or other monitoring to device to indicate that it is still online and functioning	0-60 min
PPP	The length of time an OnDemand PPP session will remain connected without activity.	0-120 min
NTP Sync	The period in which the NetMediator will attempt to resynchronize its Date/Time settings with the NTP server.	0-120 sec/min
Proxy	Determines the timeout period for inactive indirect proxy connections.	0-120 sec/min
Web Timeout	A period of inactivity after which a user will be logged out of the NetMediator's web interface	0-120 min
Web Refresh	The period between browser updates in the web interface.	5-120 sec

Field descriptions in the System Timers menu

⚠ *Hot Tip!*

The smaller the CYCLE time, the sooner you will find out about failures; however, you will increase traffic on your LAN.

2.8   Setting the System Date and Time

From the **Date Time** menu option, you can manually set your NetMediator's date and time, or designate a network time server.

The current date and time can be entered from the Date and Time screen or from an SNMP manager

The date is entered in the **month/date/year** format and the time is entered in the **hour:minute:seconds** format.

 Hot Tip!

The date and time can also be set from an SNMP manager.

Resetting the Date and Time following a system restart:
If your NetMediator is not equipped with the real-time clock option and network time is not enabled, you will have to reset your NetMediator's date and time following each restart. See the following section for information about **Network Time Configuration**.

2.8.1   Network Time Protocol Support

A **Network Time Server** provides your NetMediator with accurate date and time information following a restart, so you don't have to manually restore date and time information every time you make changes to your NetMediator's database.

To Setup a Network Time Server:
1. Enter the IP Address of your Network Time Server in the **Time Server IPA** field.
2. Enter the port for the time server in the **Time Server Port** field.
3. Select your **Timezone** from the appropriate drop-down box.
4. Check the **Observe DST** box if you observe daylight savings.

3   Defining Alarms

From the **Alarms** link in the **Provisioning** menus, you can configure and edit your unit's **Base**, **System**, and **Ping** alarms. Click on the tabs at the top of the alarms menu to navigate between the three types of alarms.

Alarms

| Base | System | Ping |

Edit your alarms form the Alarms option in the Provisioning menus

Important!: Some of your NetMedaitor's discrete and system alarms are preconfigured to belong to certain point groups. **Do not edit the Group** field for base alarms **1-8 and 10**, or system alarms **36, 40, 56, or 57 without expressed direction from DPS Telecom Support**.

3.1   Base Alarms

Your NetMediator comes equipped with 32 discrete alarm inputs. From the **Base** tab in the **Alarms** provisioning menu, you can set and edit alarm descriptions, notifications, point groups, and more. See the table below for field descriptions in the Base Alarms Provisioning menu.

Alarms ([Display Map])

| Base | System | Ping |

Pnt	Description	Rev	Trap	Primary	Secondary	Group	Qual
1	INTRUSION - BREACHED DOOR	☑	☐	1	0	6	A
2	BEACON	☐	☐	0	0	6	None
3	SIDE LIGHT	☐	☐	0	0	6	None
4	HUMIDITY	☐	☐	0	0	6	None
5	H20 LEAK	☐	☐	0	0	6	None
6	FIRE	☐	☐	0	0	6	None
7	EQUIPMENT CRITICAL	☐	☐	0	0	7	None
8	EQUIPMENT MAJOR	☐	☐	0	0	8	None
9	EQUIPMENT MINOR	☐	☐	0	0	1	None
10	TX A ACTIVE	☐	☐	0	0	5	None
11	TX B ACTIVE	☐	☐	0	0	1	None

Edit your alarms from the Base tab

Field	Description
ID	The point reference, 1-32, of each alarm.
Description	A description of the alarm.
Rev	Reverses the polarity of an alarm. By default, alarms set when a discrete contact closes. If **Rev** is checked, a contact closure will clear an alarm.
Trap	Indicates whether or not you would like to send SNMP traps for each point.
Primary	Enter the Notification ID, 1-8, of the primary notification you would like the NetMediator to send for each point. The NetMediator will send notifications for both set and cleared alarms. For more information on configuring notifications, see the section titled **Setting Notifications**.
Secondary	Enter the notification ID, 1-8 of the secondary notification you would like the NetMediator to send for each point. The NetMediator will send notifications for both set and cleared alarms.
Group	**Note:** Discrete alarms default to group 6. Changing these group numbers will affect control logic for your NetMediator. **Do not** change the group associations for these points unless you intend to alter control logic for these points or told to do so by DPS Support. Indicate the point group, 1-8, to which each point will belong. Point groups will define custom alarm and clear messages for each point. For more information on Point Groups, see the section titled **Defining Point Groups**.
Qual	Refers to the **Event Qualification Timer.** If an event qualification timer is associated with an alarm, the qualification type (**A** for alarms, **C** for clears, or **B** for both alarms and clears) will appear in the **Qual** column. If a qualification timer is not configured for an alarm, the field will simply read **None**. Clicking a hyperlink in the qualification timer field will either take you to the associated page where the qualification timer is configured, or, if a qualification timer is not yet configured, the link will take you to the next open qualification timer. For more information, see the **Event Qualification Timers** section of this manual.

Fields in the base alarm configuration screen

3.2 System Alarms

Your NetMediator's **System Alarms** are a set of predefined internal housekeeping alarms designed to alert the user of problems with the NetMediator itself. Click the **System** tab from within the **Alarms** provisioning menu to edit system alarm settings.

Available fields in the **System** alarm tab are identical to Base Alarm options. See the table in the previous section for descriptions of the fields in the System Alarms tab.

Note: System alarms **36, 40, 56, & 57** belong to point group 5. Do not edit these groups unless you intend to alter relay logic or told to do so by DPS Support.

Alarms

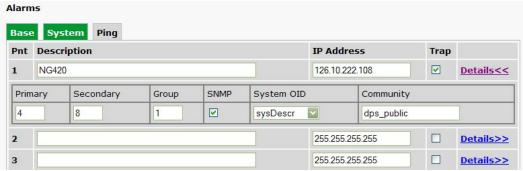| Pnt	Description	Trap	Primary	Secondary	Group
17	Timed Tick	☐	0	0	1
18	Exp.Module Callout	☐	0	0	1
19	Network Time Server	☑	0	0	1
20	Accumulation Event	☑	0	0	1
21	Duplicate IP Address	☑	0	0	1

System Alarms

3.3 Ping Alarms

In the **Ping** tab of the **Alarms** provisioning menu, you can configure and edit up to 32 ping targets.

A **Ping Target** is the IP address of a device that the NetMediator will ping at a regular interval, to ensure connectivity and uptime of equipment over a network. If the NetMediator does not recieve a response to the ping, it will set an alarm, alerting you to a problem.

The NetMediator can also send SNMP GET requests as a next-level-higher option to a ping. While some equipment will still respond to a ping while in a standby or sleep mode, SNMP requests generally require higher-level functionality. The SNMP request ping therefore provides an even more secure way to verify to connectivity and uptime of your equipment.

The interval between pings issued to ping targets is set in the **Timers** menu. For more information about your NetMediator's timers, see the **Editing System Timers** section of this manual.

Alarms

Pnt	Description			IP Address	Trap	
1	NG420			126.10.222.108	☑	Details<<

Primary	Secondary	Group	SNMP	System OID	Community
4	8	1	☑	sysDescr	dps_public

Pnt	Description	IP Address	Trap	
2		255.255.255.255	☐	Details>>
3		255.255.255.255	☐	Details>>

Configuring ping targets to verify connectivity between your equipment and verify uptime

To configure Ping Targets simply enter the **IP Address** of the device the NetMediator is to ping in the IP Address field. For information on other fields available in the **Ping** tab, see the table below.

Field	Description
Pnt	The point reference, 1-32, of each alarm.
Description	A description of the ping target
Trap	Indicates whether or not you would like to send SNMP traps for each point.
Details	**Click to reveal Notification and SNMP options**
Primary	Enter the Notification ID, 1-8, of the primary notification you would like the NetMediator to send for each ping target. The NetMediator will send notifications for both set and cleared alarms. For more information on configuring notifications, see the section titled **Setting Notifications**.
Secondary	Enter the notification ID, 1-8 of the secondary notification you would like the NetMediator to send for each ping target. The NetMediator will send notifications for both set and cleared alarms. For more information on configuring notifications, see the section titled **Setting Notifications**.
Group	Indicate the point group, 1-8, to which each ping target will belong. Point groups can be used to define alarm and clear messages for each alarm point, and define specialized behaviors for members of the group. For more information on Point Groups, see the section titled **Defining Point Groups**.
SNMP	Click to indicate that you would like to send an SNMP_GET request to the ping target.
System OID	Choose the Get request you would like to send to the ping target • sysDescr - requests the ping target's system description • sysObjectID - requests the the ping target's OID • sysUpTime - requests the ping target's uptime
Community	Enter the community name for SNMP Get requests, as defined in the **SNMP** menu.

Available fields in the Ping Target menu
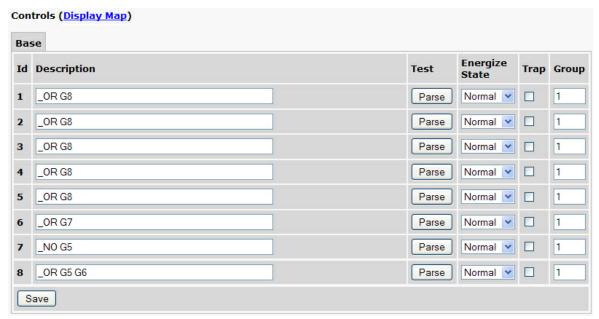
4 Configuring Control Relays

Read This Before Attempting to Configure Your Control Relays:

Your NetMediator's control relays are preconfigured with derived logic to operate when specific sets of discrete, system, or analog threshold alarms occur. **Do not reconfigure relays without expressed direction from DPS Telecom.** For more information on relay logic for your NetMediator, see the **Grouped Alarms and Derived Controls** section of this manual.

You will configure your NetMediator's 8 control relays from the **Control** option in the Provisioning menu.

The NetMediator's relays are normally open (N/O) by default. Jumper settings allow you to configure relays for normally closed operation. Refer to your NetMediator hardware manual for instructions and jumper settings to change your relay's normal state.

See the field descriptions below for help configuring your control relays.

Controls (Display Map)

Base

Id	Description	Test	Energize State	Trap	Group
1	_OR G8	Parse	Normal	☐	1
2	_OR G8	Parse	Normal	☐	1
3	_OR G8	Parse	Normal	☐	1
4	_OR G8	Parse	Normal	☐	1
5	_OR G8	Parse	Normal	☐	1
6	_OR G7	Parse	Normal	☐	1
7	_NO G5	Parse	Normal	☐	1
8	_OR G5 G6	Parse	Normal	☐	1

Save

Configure controls in the Edit menu > Controls screen

Field	Description
ID	The point reference, 1-8, of your control relays.
Description	A description of the relay.
Energize State	Allows you to change the normal electrical state of the relay. • **Normal** sets the relay's normal electrical state to **De-Energized** (default). • **Inverted** sets the relay's normal electrical state to **Energized**.
Trap	Indicates whether or not you would like to send SNMP when a control changes state (operate to release, release to operate, or, in the event of a momentary command, a notification for both operate and release commands).
Group	Indicate the point group, 1-8, to which each point will belong. Point groups can be used to define alarm and clear messages for each point, and define specialized behaviors for members of the group. For more information on Point Groups, see the section titled **Defining Point Groups**.

⚠️ *Hot Tip!*

The Energize State is different than the normal state of the physical contact closure position of each relay, which is determined by circuit board jumpers. This gives you the added benefit of being able to monitor the wire. In the event of a power failure, the relay would de-energize back to it's normal physical contact closure set by the circuit board jumper for that relay. Check your jumper settings and relay connections before setting to Normal or Inverted. Refer to the hardware manual for jumper settings and relay connection options.

4.1 Derived Control Relays and Virtual Alarming

You can derive control relay operations from alarm conditions, providing an automatic response to NetMediator alarms. (i.e. Your primary generator fail alarm can activate the relay to turn on a secondary generator.) Simply enter the formula for the logic you want the relay to follow in the **Description** field.

All logic will follow the syntax:

_OP D#.P

Where **OP** is the operational logic, **D#** indicates the **Display** or **Group** number, followed by the **Point** reference. You can configure multiple operations for each relay, however, your NetMediator will process operations in order, left to right.

Symbols and Notation used for configuring derived control logic:
- **_OR** : Operates the relay if **any** of the referenced points go into an alarm state.
- **_AN** : Operates the relay only if **all** referenced points go into an alarm state
- **_XR** : Set the current operation to XOR. Operates the relay if **any** of the referenced points go into an alarm state, but will not operate the relay if multiple referenced points go into an alarm state.
- **D** : Tag to change the active display number.
- **G** : Tag to change the active group number (used in place of the display number).
- **.** : (**Period**) Used like a comma to delimit numbers.
- **–** : (**Underscore**) Used to specify a range of points.

⚠️ *Hot Tip!*

- Your NetMediator processes operations in order, left to right.
- All number references can either be one or two digits.

Examples:
_OR D1.3-5 is logically equivalent to (1.3 || 1.4 || 1.5)
_AN D 1.3-5 D2.6 _OR D3.7 is logically equivalent to ((1.3 && 1.4 && 1.5 && 2.6) || 3.7)
_OR D01.03-05 D02.06 _AN D02.07 D03.10.-12 is logically equivalent to ((1.3 || 1.4 || 1.5 || 2.6&& (2.7 && 3.10 && 3.12))
_AN D1.3-5D2.6_OR.7D3.10.12 is logically equivalent to ((1.3 && 1.4 && 1.5 && 2.6) || 2.7 || 3.10 || 3.12))
o will not parse
_AN D1-2 : Control will not parse
_OR G1 will latch if any alarm in group 1 is active

4.2 Override Default Relay Momentary Time Using Event Qualification

A momentary (MOM) control command operates (OPR) a relay and subsequently releases it. The **momentary time** is the time between operate and release operations when issuing a momentary command. **By default, the momentary time is 5 seconds**. You can override the momentary time for each relay using an event qualification timer.

Using Event Qualification to override default relay momentary time

To override default relay momentary time:
1. Click **Advanced<<** under in the provisioning menus to reveal the **Event Qual** option. Click **Event Qual**.
2. In the **Display** text box, type 11.
3. In the **Point** text box, type the number of the relay you would like to change, 1-8.
4. In the **Value** box, type the amount of time. You may not select more than 127 units.
5. In the **Units** box, select the appropriate units (seconds, minutes, or hours).
6. In the **Type** box, select **Alm**.
7. Click **Save**.

For more information, see the section of this manual titled **Setting Event Qualification Timers.**

5   Configuring Analog Inputs

With RTD 32 DX expansions, your NetMediator can monitor up to 72 analog inputs. You'll configure and edit your analog inputs from the **Analogs** option in the **Provisioning** menu.

You will set four alarm thresholds (trip points) for each analog input: (listed in ascending order) major under, minor under, minor over, and major over. Under thresholds will cause the NetMediator to set an alarm when the input measures a value below the threshold; over thresholds will cause the NetMediator to set an alarm when the input measures a value above the threshold.

Your NetMediator's analog inputs support an input range of –70 to +94 VDC. The NetMediator will convert voltage readings to other units of measurement (temperature, humidity, wind-speed, etc.) based on user defined reference values.

For example, if attempting to monitor temperature using a sensor with a measurable range between –4° to 167° Fahrenheit and voltage output range between 1 and 5 VDC, you would configure the analog input references such that 1 volt represents –4° Fahrenheit and 5 volts represents 167° Fahrenheit.

By default, your NetMediator's analogs are set to measure voltage. To measure current instead, you must flip a dipswitch. Refer to the NetMediator hardware user manual for details on dipswitch locations and settings. The jumper inserts a 250 ohm shunt resistor across the input to convert the sensors current output to volts. Use ohms law to find the voltage drop across the 250 ohm shunt resistor (multiply the current by the 250 ohm resistance). Please refer to the operation manual for your sensor to determine any other conversion factors.

The Analog Parameters can be viewed and changed from the Analogs screen

To configure your analog inputs:
1. In the **Description** field enter a description for the analog channel.
2. Click **Details<<** to reveal scaling, threshold, and group settings
3. In the **Display Units** field of the **Scaling** section, enter the unit of measurement to which you want to convert (e.g RH for relative humidity, F for degrees Fahrenheit, etc.).
4. In the **Low Reference** row:
   · In the **Actual** column, enter the minimum sensor output value in VDC
   · In the **Display** column, enter the minimum sensor measurement value in Display Units. (Example: For a temperature sensor capable of measuring between 4 and 167 degrees, you would enter 4 here.)
5. In the **High Reference** row:
   · In the **Actual** column, enter the maximum sensor output value in VDC
   · In the **Display** column, enter the maximum sensor measurement value in Display Units. (Example: For a temperature sensor capable of measuring between 4 and 167 degrees, you would enter 167 here.)
6. Set your **Thresholds** in the boxes labeled **MjU**, **MnU**, **MnO**, and **MjO**.

For more information on available fields and options within the analog configuration screen, see the table below.

Field	Description
Chan	The channel reference, 1-8 for base analogs, 1-32 for each of the NetMediator RTD G5's expansion units.
Description	A description of the analog input.
Rev	Reverses the polarity of an alarm. By default, threshold alarms set when the analog sensor measures a value outside the normal range. Checking the **Rev** box causes the unit to set alarms when the analog sensor monitors a value within the boundaries defined by your threshold values.
Trap	Indicates whether or not you would like to send SNMP traps for threshold alarms on any particular analog channel.
Primary	Enter the Notification ID, 1-8, of the primary notification you would like the NetMediator to send for threshold alarms on any given channel. The NetMediator will send notifications for both set and cleared alarms. For more information on configuring notifications, see the section titled **Setting Notifications**.
Secondary	Enter the notification ID, 1-8 of the secondary notification you would like the NetMediator to send for threshold alarms. The NetMediator will send notifications for both set and cleared alarms. For more information on configuring notifications, see the section titled **Setting Notifications**.
Details	Shows/hides Scaling, Threshold, and Group fields.
Scaling	Values that pertain to the sensor's voltage (or current) output
Actual Units	VDC - Analog inputs monitor incoming voltage (or current via Ohm's law) in Volts
Actual Low Ref:	The minimum voltage (or current) output for the sensor connected to a channel.
Actual High Ref:	The maximum voltage (or current) output for the sensor connected to a channel.
Display Units:	Unit of measurement that the analog channel is to display, i.e. F for Fahrenheit, VDC for Volts DC, RH for relative humidity.
Display Low Ref:	The minimum measurable native value for the sensor connected to a channel.
Display High Ref:	The maximum measurable native value for the sensor connected to a channel.
Thresholds	Values that when crossed (below for under, above for over) will cause an alarm. • **MjU:** Major Under - the lowest threshold, indicating a major or critical alarm • **MnU:** Minor Under - a low threshold, indicating a minor alarm • **MnO:** Minor Over - a high threshold, indicating a minor alarm • **MjO:** Major Over - the highest threshold, indicating a major or critical alarm
Group Num.	**Note: Analog thresholds for both RTD DX Expansion units belong to groups 7 and 8 by default.** Changing group associations for expansion analog thresholds will affect relay logic for the NetMediator. **Do not change these group associations without expressed direction from DPS Support.** Indicate the point group, 1-8, to which each threshold will belong. Groups define alarm set and clear messages. You can also use groups to derive actions based on the alarm state of member points. For more information on Point Groups, see the section titled **Defining Point Groups**.

Available fields in the Analog provisioning menu

5.1 Integrated Temperature and Battery Sensor (Optional)

The NetMediator G5 product line is available with integrated sensors to monitor internal temperature, external temperature, and current draw at the NetMediator's power input.

Note: Integrated sensors are an option available when you order the NetMediator. They cannot be added or removed from the final product.

Each sensor option consumes one of the NetMediator's analog channels.

Sensor Function	Analog Input
Internal Temperature	analog input 4
Power Feed A	analog input 5
Power Feed B	analog input 6
External Temperature	analog input 8

Integrated sensor analog channels

CAUTION: Ambient room temperature will be cooler than the NetMediator integrated temperature.

To configure your integrated sensors:

Temperature Sensor:
1. Enter a **description** for the analog channel. Remember: channel 4=internal and channel 8=external.
2. In the **Scaling Display Units** field, enter **iF**
3. Set your desired thresholds.

Battery Sensor
1. Enter a description for the analog channel. Remember; channel 5= Battery A and channel 6= Battery B.
2. Set your desired thresholds. Be sure to set thresholds in reference to your NetMediator's power input (e.g. –24 VDC, –48 VDC, or wide range).

5.2 Analog Polarity Override

To override analog polarity or temperature units, enter the values below in the appropriate analog channel's **scaling display units** field.

iF: Integrated temperature sensor in Fahrenheit
iC: Integrated temperature sensor in Celsius
oV+: Override polarity VDC to positive
oV-: Override polarity VDC to negative

If you have a positive powered NetMediator and the integrated battery sensor, you may wish to override to positive polarity. The Web Browser Interface will display **oV+** and **oV-** units as **VDC,** rather than displaying an uncommon unit tag in monitor mode.

5.3   Analog Step Sizes

Analog Accuracy:
+/- 1% of analog range.

Analog Step Sizes	
Input Voltage Range	**Resolution (Step Size)**
0-5 V	.0015 V
5-14 V	.0038 V
14-30 V	.0081 V
30-70 V	.0182 V
70-90 V	.0231 V

Analog step sizes

6 Advanced System Configuration (Provisioning)

Clicking on the **Advanced>>** option in the Provisioning menus will reveal advanced configuration options for the NetMediator. The following sections in this chapter provide descriptions of the options available in the advanced provisioning menu.

6.1 Using RADIUS Authentication

From the **Radius** option in the **Advanced<<** section of the Provisioning menus, you can configure RADIUS authentication. **RADIUS** (Remote Authentication Dial In User Service) is an industry-standard way to manage logins to many different types of equipment in one central location. With RADIUS enabled, your NetMediator will connect to your RADIUS server to authenticate logon requests.

Note: RADIUS authentication invalidates the NetMediator's local logon profiles.

RADIUS configuration screen

*RADIUS server prompt for Username **and** Password.*

Global Settings	
Retry	Enter the number of times the RADIUS server should retry a logon attempt
Time-out	Enter in the number of seconds before a logon request times-out
Servers 1 / 2	
IPA	Enter the IP address of the RADIUS server
Port	The Port used for RADIUS authentication. Port 1812 is the standard RADIUS port.
Interface	Use the drop-down menu to choose the Net interface that you wish to be RADIUS authenticated
Secret	Enter the RADIUS secret in this field

Fields available in the RADIUS menu

After successfully entering the settings for the RADIUS server, the NetMediator Web Browser will prompt users for both a Username and Password, which it will verify against information and access rights stored in the RADIUS database.

RADIUS logons **are** case-sensitive. If the RADIUS server is unavailable or denies access, the master password will work for craft port access only. You must load the "dictionary.dps" files (included on the Resource Disk) on the RADIUS server for access-right definition.

6.2 Filter IPA Config and Operation

From the **Filter IPA** option in the **Advanced<<** Provisioning menus, you can greatly increase the NetMediator's network security by allowing or deny access to the NetMediator by IP address.

Note: Your NetMediator will **not filter:**
- IP addresses associated with network cameras
- The address of your network time server
- broadcast packets of 255.255.255.255
- ARP requests for the NetMediator IP address.

A warning prompt will appear, when you attempt to access the **Filter IPA** table.
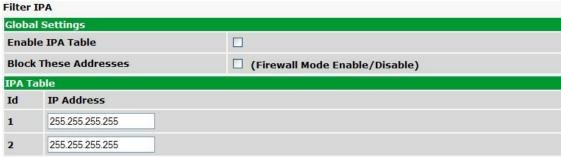

Filter IPA warning prompt

To configure your IPA table:
1. Check the box marked **Enable IPA table**.
2. Determine how you want the table to function by checking/unchecking the box labeled **Block These Addresses**:
   - **Unchecked**: the IP filter functions as a **white-list**. Only the specified IP addresses can connect to the NetMediator
   - **Checked:** the IP filter functions as a **black-list**. Specified IP addresses will not be able to access the NetMediator.
3. Enter the **IP Address**(es) you wish to filter.

⚠ *Hot Tip!*

Entering a zero in any of the octet fields will declare that part of the octet a wildcard.

WARNING: Does not work with networks that assign IP addresses. Use the wildcard field to open an entire subnet.

Select Filter IPA from the Edit menu to configure your Filter IPA table

6.3 Defining Point Groups

Point Groups allow you to group your NetMediator's alarms, configure custom set and clear messages, and dictate derived behaviors for grouped points. You can configure your NetMediator's 8 Point Groups from the **Groups** option in the **Advanced<<** Provisioning menu.

Note: Some of your unit's discrete and system alarms, and all of your RTD DX expansion analog thresholds belong to certain groups by default. Keep in mind alarm-group associations to configure more relevant set and clear messages members of preconfigured groups. Altering group set and clear messages will not affect derived relay behavior for those groups.

Group	Members	Group Name	Set Message	Clear Message	Echoed Relays
4	Base Analogs channels 1, 2, 3, 7	Analogs 1, 2, 3, 7	Alarm	Clear	
5	System Alarms (Display 11) 36, 40, 56, & 57	All's Well (sys)	Alarm	Clear	7, 8
6	Discrete Alarms	Airflow Sensors	Alarm	Clear	8
7	All minor temperature threshold alarms from RTD DX expansion analog channels	Minor Temp	Alarm	Clear	6
8	All major temperature threshold alarms from RTD DX expansion analog channels	Major Temp	Alarm	Clear	1-5

Preconfigured alarm groups for the NetMediator and RTD DX expansions

You can configure your NetMediator's 8 Point Groups from the **Groups** option in the **Advanced<<** Provisioning menu.

Each NetMediator Alarm point can be assigned to one of eight groups, which are identified with a user-defined label. Once the point groups are defined, the Point Group IDs can be used to group base and system alarms, see section "Configuring Base Discrete Alarms."

For each alarm group, you can set:
1. A description for members of the group
2. Messages for members of the group to display **When Set**.
3. Messages for members of the group to display **When Clear**.

Define the Alarm and Clear messages for up to eight different point groups
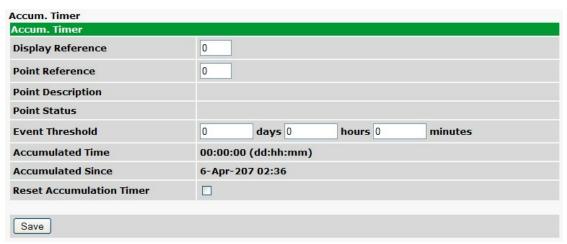
6.4 Setting the Accumulation Timer

You can set an **Accumulation Timer** for one point from the **Accum. Timer** option in the advanced section of the Provisioning menus.

The **Accumulation Timer** keeps a running total of the amount of time a single point records an alarm state and sets an Accumulation Event system alarm once the total time exceeds a defined threshold.

Fill in the appropriate fields to configure the timer. See the table below for descriptions of the fields in the Accum. Timer menu.

Note: The **Point Description, Point Status, Accumulated Time, and Accumulated Since** fields are not configurable. These fields will show the corresponding data of the point for which you configure the accumulation timer.

Define the Accumulation Timer settings to send an Accumulation Event alarm

Field	Description
Display and Point Reference	Indicates which alarm point is to be monitored
Point Description	**Read Only:** The user-defined description of the monitored alarm point.
Point Status	**Read Only:** The current status of the monitored point.
Event Threshold	The amount of time allowed to accumulate before the "Accumulation Event" system alarm is set. Maximum is 45 days.
Accumulated Time	**Read Only:** The total time the monitored point has been in ALARM state.
Accumulated Since	**Read Only:** Indicates the last time the accumulation timer was reset.
Reset Accumulation Timer	Placing a check mark here will reset the timer when the user clicks **Save**.

Fields in the Accumulation Timer screen

6.5   Event Qualification Timers

Event Qualification Timers allow you to qualify an alarm based on the length of time for which it is set, providing a means to reduce or even eliminate nuisance alarms your recorded by your NetMediator. You can also use qualification timers to delay or stagger alarm notifications. You can set event qualification timers from the **Event Qual** option in the **Advanced** section of the Provisioning menus.

The NetMediator supports up to **128 qualification timers**. Timers are grouped in multiples of 16. Navigate between timers using the tabs at the top of the Qual Timer display.

Event Qual

| 1-16 | 17-32 | 33-48 | 49-64 | 65-80 | 81-96 | 97-112 | 113-128 |

Id	Display	Point	Value	Units	Type
1	11	1	5	sec	Alm
2	11	2	5	sec	Alm

Edit the Even Qualification Timer settings from the Edit > Even Qual screen

To configure a qualification timer:
1. Input the **Display** and **Point** reference you wish to qualify.
2. In the **Value** field, enter the length of time that will qualify the specified event.
3. Select the **Units** corresponding to the Value set in the previous step
4. Determine the **Type** of event you wish to qualify, **Alarms (Alm), Primary Notifications (Pri),** or **Secondary notifications (Sec)**.

⚠️ *Hot Tip!*

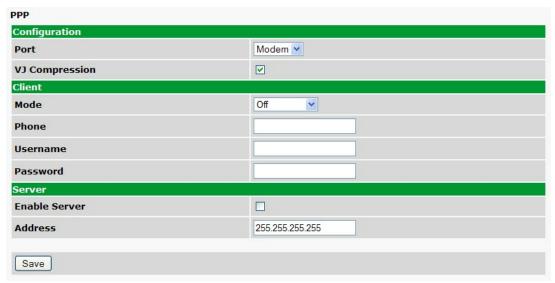To delete the entry, set the **Type** to None.

CAUTION: Alarm Clear conditions are not qualified.

Note: An alarm qualification event becomes a relay momentary time if the display and point reference a control relay. Control relays are mapped to Display 11, Points 1-8. See Reference Information Table A1 and A2 for display descriptions, see Reference Information for Display Mapping Table.

6.6   Configuring PPP Modes

Your NetMediator can connect to, or act as, a PPP (point-to-point protocol) server. Click on the **PPP** option in Advanced section of the Provisioning menu to configure your NetMediator for PPP client or server operation.

Configure the PPP port settings in the Edit menu > PPP screen

To configure the NetMediator as a PPP Server:
1.   In the **Server** section check the **Enable Server** (also known as Hosting Mode) box.
2.   Set the IP address the NetMediator will assign the guest dialing into the unit in the **Address** field. (This must be a valid and available IP address for the subnet on the LAN you will be connecting to, the same one the NetMediator is connected to.)
3.   Click **Save**.

Edit the Modem settings for the PPP server in the Edit menu > Ports screen > Modem section

4.   Select **Ports** from the **Provisioning** menu.
5.   Scroll down to the **Modem** section. Enter a value greater than zero in the **Ring Count** field.
6.   Enter **&Q6 i**n the **Answer Init** field the.
7.   Click **Save**.
8.   Select **Logon** in the **Provisioning** menu.
9.   Click the link for the user you wish to grant PPP and Telnet access privileges.
10. In the **Access Privileges** section check the **PPP** and **Telnet** boxes.
11. Click **Save**.

You will also need to configure your remote terminal modem in order to access your NetMediator via PPP:

Windows 98 users:	Set baud rate to **9600.**
Windows 2000, XP users:	In **Modem Configuration General** tab uncheck **Enable modem error control** and **Enable compression.**
Mac OSX users:	Use standard dial-in.

Field	Description
Configuration	
Port	Choose the port, Modem or data ports 1-8, you wish to use for PPP connections.
VJ Compression	Check to enable VJ Compression (Improves performance over slow serial links)
Client	
Mode	Allows the NetMediator to connect as a client to a PPP server • Off - Disables PPP client access • Permanent - Allows full-time PPP access (Use if the NetMediator's primary connection is through a PPP server) • Backup - Establishes a PPP connection **if Net1 fails**. • On Demand - allows the user to establish PPP connections at will.
Phone	The Phone number of the PPP server the NetMediator will dial.
Username	The Username the NetMediator will use to login to the PPP server
Password	The Password the NetMediator will use to login to the PPP server
Server	
Enable Server	Check to enable your NetMediator's PPP server functionality
Address	The IP address the NetMediator will assign a PPP user. (This must be a valid and available IP address for the subnet on the LAN to which the NetMediator is connected.)

Fields available in the PPP menu

7 Device Access and Maintenance options

The **Device Access** options, listed in pink, provide maintenance options for the NetMediator. From here, you can write changes to the NetMediator, revert to prior settings, and reboot the unit. Click any of the options under **Device Access** to perform the desired action.

The Device Access Menu is located in the bottom left of the web interface

Device Access Option	Description
Alarm Sync	Resynchronizes the NetMediator's alarms, sending new notifications for all standing alarms. Allows the user to turn-up test alarm connections during turnip without rebooting the NetMediator unit. A warning prompt will appear, click **Ok** to continue or **Cancel** to exit without resynchronizing your alarms.
Initialize	Sets the unit's configuration to factory default values.
Write	Commits all changes made in the web interface to the NetMediator's non-volatile memory. **Note:** Changes following a **Write** function frequently require a reboot to take effect.
Read	Reads the units current configuration from the unit's NVRAM. Use the **Read** function to revert to settings currently in the unit's
Reboot	Reboots the NetMediator.

*Options available in the **Device Access** menu*

7.1 Backing Up Your NetMediator's Configuration

DPS Telecom recommends that you backup your NetMediator's configuration, so that you can quickly and easily re-database the unit should you ever have to Initialize NVRAM or transfer settings to a new NetMediator.

To backup your NetMediator's configuration:
1. From a command prompt, type **ftp <your NetMediator's IP Address>**.
2. When prompted, enter your username. (The default username is **dpstelecom**.)
3. Type **bin** to force the unit into binary mode.
4. Enter **get config.bin** to backup your configuration file. (This saves the file to the default drive directory, usually **C:**)
5. Type **bye** to close the ftp session.

To restore your NetMediator's configuration:
6. From a command prompt, type **ftp <your NetMediator's IP Address>**.
7. When prompted, enter your username. (The default username is **dpstelecom**.)
8. Type **bin** to force the unit into binary mode.
9. Enter **put config.bin** to restore your configuration file. (Your config.bin file must be in the default directory, usually **C:**)
10. Type **bye** to close the ftp session.

7.2   Alarm Sync

Clicking on the Alarm Sync link from the Edit menu will re-synchronize all of the NetMediator alarms. This command clears all alarms, so that a new notification is sent for all standing alarms. This option allows you to easily test alarm connections during turn-up without rebooting the NetMediator unit. A warning prompt will appear, click **Ok** to continue or **Cancel** to exit without resynchronizing your alarms.
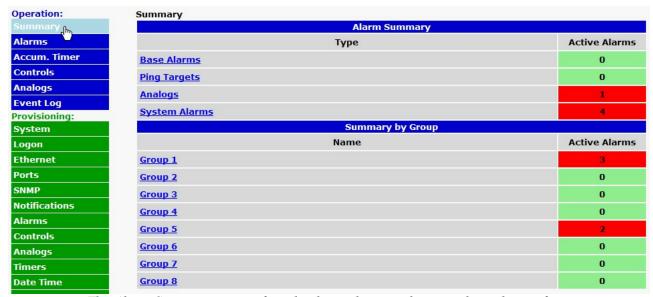

Click Ok to re-synchronize the NetMediator alarms or Cancel to exit

8 Monitoring Alarms and Operating Controls

You can monitor alarms and operate control relays from the **Operation Menus**, the menu options in blue on the left-side of the web interface. The following pages provide descriptions of the options available in each menu option.

8.1 Alarm Summary

The Alarm **Summary** Screen is the first screen you'll see when you login to the web interface. It provides a total number of active alarms, sorted by type and group, including alarms for any connected expansion units.

The Alarm Summary screen first displays when you login to the web interface.

Click **Summary** in the **Operation** menus to return to the alarm summary at any time. Click any of the links in the **Summary** screen for greater detail about the listed alarms.

8.2 Viewing Alarms

Click **Alarms** to view the status of your unit's **Base** discrete, **System**, and **Ping** alarms. Navigate between the three types of alarms using the tabs at the top of the Alarms page.

View the status of the Base Alarms from the Monitor > Base Alarms screen

Alarm State:

The **State** column will display the state of each point, by color and message. If you've configured group messages, the **Alarm State** column will display the appropriate alarm set and clear messages for each group. Regardless of group, the **Alarm State** column will display cleared points with a green background and set points with a red background. For more information about grouping alarms, see the **Defining Point Groups** section of this manual.

8.2.1   Base Discrete Alarms

The **Base** tab displays the state of your NetMediator RTD G5's 32 discrete alarms. Alarms are sorted by point ID, 1-32.

8.2.2   Monitoring System Alarms

The **System Alarms** tab displays the state of the unit's internal "housekeeping" alarms. These alarms report directly on the status of the NetMediator itself.

View the status of the System Alarms

Note: Some of your unit's system alarms (points 36, 40, 56, and 57) are set to **Point Group 5** and tied to one of your NetMediator's Relays.

8.2.3   Monitoring Ping Targets

The **Ping** tab displays the state of your NetMediator's ping targets. If Ping Targets are configured, the NetMediator will issue ping requests to designated IPs. If the NetMediator does not receive a response within the defined time period, it will report an alarm. For more information about designating ping targets, see the **Configuring Ping Targets** section of this manual.

8.3   Monitoring the Accumulation Timer

The **Accumulation Timer** allows you to derive an alarm based on the time any single point spends in an alarm state. Click **Accum. Timer** in the **Operation** menu to display information about the point for which the accumulation timer is configured.
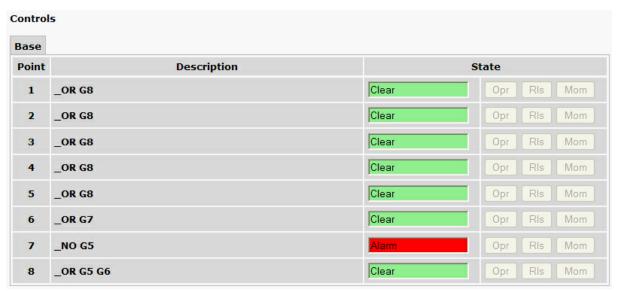

Track the total time a point spends in an alarm state with the accumulation timer

For more information about configuring the accumulation timer, see the **Setting the Accumulation Timer** section of this manual.

8.4 Operating Controls

Your NetMediator's control relays operate based on the status of discrete, system, and analog threshold alarms. **By default, you cannot manually operate your NetMediator's control relays.**

Point	Description	State			
1	_OR G8	Clear	Opr	Rls	Mom
2	_OR G8	Clear	Opr	Rls	Mom
3	_OR G8	Clear	Opr	Rls	Mom
4	_OR G8	Clear	Opr	Rls	Mom
5	_OR G8	Clear	Opr	Rls	Mom
6	_OR G7	Clear	Opr	Rls	Mom
7	_NO G5	Alarm	Opr	Rls	Mom
8	_OR G5 G6	Clear	Opr	Rls	Mom

Issue controls from the Monitor > Controls screen

Removing your NetMediator's derived control logic will allow you to manually operate relays from the **Controls** option in the **Operation** menu.

To operate control relays, click the appropriate command in the **State** column.
- **Opr:** Operates the relay
- **Rls:** Releases the relay
- **Mom:** Issues a momentary command, temporarily operating the relay and then releasing it. You can set the time between operate and release states when issuing a momentary command using a qualification timer.

The **State** column also displays the operational status of your relays, whether they are operating or released. By default, your control relays belong to Point Group 1 and will read **Clear** when **Released** and **Alarm** when **Latched** or **Operational**. You can display custom operate and relay messages by editing the When Set and When Clear fields for your control relays' Point Group in the **Point Groups** menu. For more information, see **Defining Point Groups**.

Note: Assigning relays to different point groups and altering other group behaviors may affect the derived logic driving your relays. Take care when changing any settings affecting control relay operation.

8.5 Monitoring Analogs

You can monitor the status of your analog sensors by clicking **Analogs** from the **Operation** menu.

View Analog sensor readings from the Analogs tab

Your NetMediator RTD G5 supports up to 72 analog sensors via RTD DX expansion units. You will monitor both base and expansion analog channels from the base NetMediator RTD G5's web interface.

Viewing Base or Expansion analogs will show threshold alarms in addition to readings

Navigating your Analogs:
Click the tabs at the top of the **Analogs** page to navigate between your base and expansion analogs.
- **Summary** displays all 72 analog readings, sorted in **Base**, **Expansion 1**, and **Expansion 2** order.
- **Base** displays the 8 analog sensor readings and alarm thresholds on the base RTD G5
- **Exp. 1** displays the 32 analog sensor readings and alarm thresholds from your first RTD DX expansion
- **Exp. 2** displays the 32 analog sensor readings and alarm thresholds from your second RTD DX expansion.

Readings in the NetMediator's Analog monitoring screens are **color coded** to indicate the severity of an alarm.
- **Green:** Indicates cleared status
- **Orange:** Indicates a minor threshold alarm.
- **Red:** Indicates a major threshold alarm.
Arrows will display next to alarm readings, pointing up or down to indicate whether or not the threshold crossed is an over or under alarm.

Note: Your expansion analog thresholds belong to point groups 7 and 8, and are tied to relays on the base NetMediator RTD G5. As such, you can use the status of your control relays to determine whether or not a threshold alarm has been set by the NetMediator.

8.5.1   Suppressing Analog Alarms

Your NetMediator's expansion analog threshold alarms derive control actions for your base NetMediator. In the event of incorrect analog readings or a situation in which you do want NetMediator expansion's threshold alarms on a particular channel to drive your control relays, you may wish to suppress an expansion analog channel's threshold alarms, preventing relay operation.

The **Suppress** feature allows you to manually silence your NetMediator's expansion threshold alarms, preventing relay operation.

Summary	Base	Exp.1	Exp.2						
Point	**Description**		**Suppress**	**Reading**	**MjU**	**MnU**	**MnO**	**MjO**
1	EXP1 CHAN1		Suppress	77.56 iF			x	
2	EXP1 CHAN2		Suppress	Not Detected				

Click the Suppress button to suppress any threshold alarms present on an analog channel

To Suppress expansion threshold alarms:
In the **Exp.1** or **Exp.2** tabs, click the **Suppress** button associated with the analog channel you wish to prevent from setting alarms or operating relays. If an alarm is present on a channel you suppress, the alarm will clear immediately on the NetMediator itself, but it may still appear in the web interface until the interface refreshes. (Your NetMediator's web interface refreshes at a user-defined interval, which you can alter from the **Timers** menu.)

Note: the suppress function will prevent the NetMediator from reporting a threshold alarm on a suppressed channel. However, the channel will continue to display analog readings.

To "UnSuppress" expansion threshold alarms:
Upon suppressing an alarm, the **Suppress** button will become an **UnSuppress** button. Click the UnSuppress button to allow the analog channel to resume setting alarms and driving relay operations.

Summary	Base	Exp.1	Exp.2						
Point	**Description**		**Suppress**	**Reading**	**MjU**	**MnU**	**MnO**	**MjO**
1	EXP1 CHAN1		UnSuppress	77.11 iF				
2	EXP1 CHAN2		Suppress	Not Detected				

Click UnSuppress to allow an analog channel to resume setting alarms and driving relay operations

8.6   Event Logging

Click **Event Log** to display the last 100 events monitored by the NetMediator.

Monitor the last 100 events recorded by the NetMediator in the Event Log window

Event Log Field	Description
Evt	Event number (1-100)
Date	Date the event occurred*
Time	Time the event occurred*
St	State of the event (A=alarm, C=clear)
Pref	Point reference. See Appendix A for display descriptions.
Description	User defined description of the event as entered in the alarm point and relay description fields

Event Log field descriptions

Filtering the Event Log:
- You can filter Event Log entries by Alarm Point Group, to see only the alarms you want.
- You can reset the Event Log, to clear old alarms from the display.
- You can reset the Event Log by Alarm Point Group; for example, clear power alarms while retaining intruder alarms.

All information in the event log will be erased upon reboot or a power failure.

Note: The NetMediator timestamps events based on its real time clock. If the real-time clock is not installed, the NetMediator will base timestamps on its software clock (requires resetting after power failure or power cycle).

9 Appendixes

9.1 Appendix A - Display Mapping

Port	Address	Display	Description	Set	Clear
99	1	1	Discrete Alarms 1-32	8001-8032	9001-9032
99	1	1	E16 DX Controls 1-16	8049-8064	9049-9064
99	1	2	Ping Table	8065-8096	9065-9096
99	1	3	Analog Channel 1	8129-8132	9129-9132
99	1	4	Analog Channel 2	8193-8196	9193-9196
99	1	5	Analog Channel 3	8257-8260	9257-9260
99	1	6	Analog Channel 4	8321-8324	9321-9324
99	1	7	Analog Channel 5	8385-8388	9385-9388
99	1	8	Analog Channel 6	8449-8452	9449-9452
99	1	9	Analog Channel 7	8513-8516	9513-9516
99	1	10	Analog Channel 8	8577-8580	9577-9580
99	1	11	Relays/System Alarms (See table below)	8641-8674	9641-9674

Display descriptions and SNMP Trap numbers for the NetMediator

The TRAP number ranges shown correspond to the point range of each display. For example, the SNMP Trap "Set" number for alarm 1 (in Display 1) is 8001, "Set" for alarm 2 is 8002, "Set" for alarm 3 is 8003, etc.

The TRAP number descriptions for the Analog channels (1-8) are in the following order: minor under, minor over, major under, and major over. For example, for Analog channel 1, the "Set" number for minor under is 8129, minor over is 8130, major under is 8131, and major over is 8132.

9.1.1   NetMediator RTD DX Expansion 1

Your RTD 32 DX Expansion's analog channels are databased on displays 12-27 for expansion 1 and 28-43 for expansion 2.

RTD 32 DX Expansion analog channels consume points 1-5 for the first channel and 33-37 for the second channel in each of their 64 point displays (displays 12-43), with each point corresponding to trap numbers listed below. Analog thresholds on each channel are in the following order (1-4, 33-36): Minor Under, Minor Over, Major Under, and Major Over. The fifth bit for each analog channel (bits 5 and 37) indicates the absence of a sensor on that channel.

Port	Address	Display	Description	Points	Set	Clear
99	1	12	RTD 32 DX 1 Analog Channel 1	1-5	10001-10005	11001-11005
99	1	12	RTD 32 DX 1 Analog Channel 2	33-37	10006-10010	11006-11010
99	1	13	RTD 32 DX 1 Analog Channel 3	1-5	10011-10015	11011-11015
99	1	13	RTD 32 DX 1 Analog Channel 4	33-37	10016-10020	11016-11020
99	1	14	RTD 32 DX 1 Analog Channel 5	1-5	10021-10025	11021-11025
99	1	14	RTD 32 DX 1 Analog Channel 6	33-37	10026-10030	11026-10030
99	1	15	RTD 32 DX 1 Analog Channel 7	1-5	10031-10035	11031-11035
99	1	15	RTD 32 DX 1 Analog Channel 8	33-37	10036-10040	11036-11040
99	1	16	RTD 32 DX 1 Analog Channel 9	1-5	10041-10045	11041-11045
99	1	16	RTD 32 DX 1 Analog Channel 10	33-37	10046-10050	11046-11050
99	1	17	RTD 32 DX 1 Analog Channel 11	1-5	10051-10055	11051-11055
99	1	17	RTD 32 DX 1 Analog Channel 12	33-37	10056-10060	11056-11060
99	1	18	RTD 32 DX 1 Analog Channel 13	1-5	10061-10065	11061-11065
99	1	18	RTD 32 DX 1 Analog Channel 14	33-37	10066-10070	11066-11070
99	1	19	RTD 32 DX 1 Analog Channel 15	1-5	10071-10075	11071-11075
99	1	19	RTD 32 DX 1 Analog Channel 16	33-37	10076-10080	11076-11080
99	1	20	RTD 32 DX 1 Analog Channel 17	1-5	10081-10085	11081-11085
99	1	20	RTD 32 DX 1 Analog Channel 18	33-37	10086-10090	11086-11090
99	1	21	RTD 32 DX 1 Analog Channel 19	1-5	10091-10095	11091-11095
99	1	21	RTD 32 DX 1 Analog Channel 20	33-37	10096-10110	11096-11100
99	1	22	RTD 32 DX 1 Analog Channel 21	1-5	10101-10105	11101-11105
99	1	22	RTD 32 DX 1 Analog Channel 22	33-37	10106-10110	11106-11110
99	1	23	RTD 32 DX 1 Analog Channel 23	1-5	10111-10115	11111-11115
99	1	23	RTD 32 DX 1 Analog Channel 24	33-37	10116-10120	11116-11120
99	1	24	RTD 32 DX 1 Analog Channel 25	1-5	10121-10125	11121-11125
99	1	24	RTD 32 DX 1 Analog Channel 26	33-37	10126-10130	11126-11130
99	1	25	RTD 32 DX 1 Analog Channel 27	1-5	10131-10135	11131-11135
99	1	25	RTD 32 DX 1 Analog Channel 28	33-37	10136-10140	11136-11140
99	1	26	RTD 32 DX 1 Analog Channel 29	1-5	10141-10145	11141-11145
99	1	26	RTD 32 DX 1 Analog Channel 30	33-37	10146-10150	11146-11150
99	1	27	RTD 32 DX 1 Analog Channel 31	1-5	10151-10155	11151-11155
99	1	27	RTD 32 DX 1 Analog Channel 32	33-37	10156-10160	11156-11160

Display descriptions and Point numbers for the RTD 32 DX Expansion

9.1.2   NetMediator RTD DX Expansion 2

Port	Address	Display	Description	Points	Set	Clear
99	1	28	RTD 32 DX 2 Analog Channel 1	1-5	10161-10165	11161-11165
99	1	28	RTD 32 DX 2 Analog Channel 2	33-37	10166-10170	11166-11170
99	1	29	RTD 32 DX 2 Analog Channel 3	1-5	10171-10175	11171-11175
99	1	29	RTD 32 DX 2 Analog Channel 4	33-37	10176-10180	11176-11180
99	1	30	RTD 32 DX 2 Analog Channel 5	1-5	10181-10185	11181-11185
99	1	30	RTD 32 DX 2 Analog Channel 6	33-37	10186-10190	11186-11190
99	1	31	RTD 32 DX 2 Analog Channel 7	1-5	10191-10195	11191-11195
99	1	31	RTD 32 DX 2 Analog Channel 8	33-37	10196-10200	11196-11200
99	1	32	RTD 32 DX 2 Analog Channel 9	1-5	10201-10205	11201-11205
99	1	32	RTD 32 DX 2 Analog Channel 10	33-37	10206-10210	11206-11210
99	1	33	RTD 32 DX 2 Analog Channel 11	1-5	10211-10215	11211-11215
99	1	33	RTD 32 DX 2 Analog Channel 12	33-37	10216-10220	11216-11220
99	1	34	RTD 32 DX 2 Analog Channel 13	1-5	10221-10225	11221-11225
99	1	34	RTD 32 DX 2 Analog Channel 14	33-37	10226-20230	11226-11230
99	1	35	RTD 32 DX 2 Analog Channel 15	1-5	10231-10235	11231-11235
99	1	35	RTD 32 DX 2 Analog Channel 16	33-37	10236-10240	11236-11240
99	1	36	RTD 32 DX 2 Analog Channel 17	1-5	10241-10245	11241-11245
99	1	36	RTD 32 DX 2 Analog Channel 18	33-37	10246-10250	11246-11250
99	1	37	RTD 32 DX 2 Analog Channel 19	1-5	10251-10255	11251-11255
99	1	37	RTD 32 DX 2 Analog Channel 20	33-37	10256-10260	11256-11260
99	1	38	RTD 32 DX 2 Analog Channel 21	1-5	10261-10265	11261-11265
99	1	38	RTD 32 DX 2 Analog Channel 22	33-37	10266-10270	11266-11270
99	1	39	RTD 32 DX 2 Analog Channel 23	1-5	10271-10275	11271-11275
99	1	39	RTD 32 DX 2 Analog Channel 24	33-37	10276-10280	11276-11280
99	1	40	RTD 32 DX 2 Analog Channel 25	1-5	10281-10285	11281-11285
99	1	40	RTD 32 DX 2 Analog Channel 26	33-37	10286-10290	11286-11290
99	1	41	RTD 32 DX 2 Analog Channel 27	1-5	10291-10295	11291-11295
99	1	41	RTD 32 DX 2 Analog Channel 28	33-37	10296-10300	11296-11300
99	1	42	RTD 32 DX 2 Analog Channel 29	1-5	10301-10305	11301-11305
99	1	42	RTD 32 DX 2 Analog Channel 30	33-37	10306-10310	11306-11310
99	1	43	RTD 32 DX 2 Analog Channel 31	1-5	10311-10315	11311-11315
99	1	43	RTD 32 DX 2 Analog Channel 32	33-37	10316-10320	11316-11320

Display descriptions and Point numbers for your second RTD 32 DX Expansion

9.1.3   System Alarms Display Map

Display	Point	Alarm Point	Description	Solution
11	17	Timed Tick	Toggles state at constant rate as configured by the Timed Tick timer variable. Useful in testing integrity of SNMP trap alarm reporting.	To turn the feature off, set the Timed Tick timer to 0.
	18	Exp. Module Callout	Alarm is triggered whenever an alarm point from an Entry Control Unit (ECU) is collected. A notification event may be associated with the alarm to force a call out or trap.	Disable Building Access Control (BAC) by setting the BAC Unit ID to 0. If Building Access is being used, then investigate the ECU alarm source or don't associate notification with the alarm event.
	19	Network Time Server	Communication with Network Time Server has failed.	Try pinging the Network Time Server's IP Address as it is configured. If the ping test is successful, then check the port setting and verify the port is not being blocked on your network.
	20	Accumulation Event	An alarm has been standing for the time configured under Accum. Timer. The Accumulation timer enables you to monitor how long an alarm has been standing despite system reboots. Only the user may reset the accumulated time, a reboot will not.	To turn off the feature, under Accum. Timer, set the display and point reference to 0.
	21	Duplicate IP Address	The unit has detected another node with the same IP Address.	Unplug the LAN cable and contact your network administrator. Your network and the unit will most likely behave incorrectly. After assigning a correct IP Address, reboot the unit to clear the System alarm.
	33	Power Up	The unit has just come-online. The set alarm condition is followed immediately by a clear alarm condition.	Seeing this alarm is normal if the unit is powering up.
	36	Lost Provisioning	The internal NVRAM may be damaged. The unit is using default configuration settings.	Use Web or latest version of NGEdit4 to configure unit. Power cycle to see if alarm goes away. May require RMA.
	37	DCP Poller Inactive	The unit has not seen a poll from the Master for the time specified by the DCP Timer setting.	If DCP responder is not being used, then set the DCP Unit ID to 0. Otherwise, try increasing the DCP timer setting under timers, or check how long it takes to cycle through the current polling chain on the Master system.
	38	NET1 not active	The Net1 LAN port is down.	Check LAN cable. Ping to and from the unit.
	39	NET2 not active	The Net2 LAN port is down.	
	40	LNK Alarm	No network connection detected	
	41	Modem not responding	An error has been detected during modem initialization. The modem did not respond to the initialization string.	Remove configured modem initialization string, then power cycle the unit. If alarm persists, try resetting the Modem port from the TTY interface, or contact DPS for possible

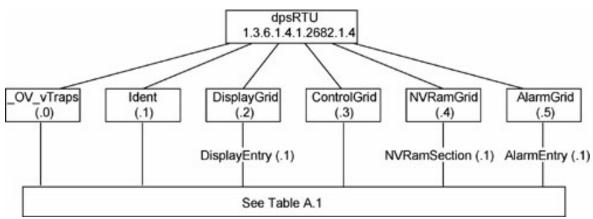| Display	Point	Alarm Point	Description	Solution
				RMA.
	42	No Dial Tone	During dial-out attempt, the unit did not detect a dial tone.	Check the integrity of the phone line and cable.
	43	SNMP Trap not Sent	SNMP trap address is not defined and an SNMP trap event occurred.	Define the IP Address where you would like to send SNMP trap events, or configure the event not to trap.
	44	Pager Queue Overflow	Over 250 events are currently queued in the pager queued and are still trying to report.	Check for failed notification events that may be filling up the pager queue. There may be a configuration or communication problem with the notification events.
	45	Notification failed	A notification event, like a page or email, was unsuccessful.	Use RPT filter debug to help diagnose notification problems.
	46	Craft RcvQ full	The Craft port received more data than it was able to process.	Disconnect whatever device is connected to the craft serial port. This alarm should not occur.
11	47	Modem RcvQ full	The modem port received more data than it was able to process.	Check what is connecting to the NetMediator. This alarm should not occur.
	48	Serial 1 RcvQ full	Serial port 1 (or appropriate serial port number) receiver filled with 8 K of data (4 K if BAC active).	Check proxy connection. The serial port data may not be getting collected as expected.
	49	Serial 2 RcvQ full		
	50	Serial 3 RcvQ full		
	51	Serial 4 RcvQ full		
	52	Serial 5 RcvQ full	Serial port receiver filled with 8K data (4K if BAC Active)	Check proxy connection. Serial port data may not be getting collected as expected.
	53	Serial 6 RcvQ full		
	54	Serial 7 RcvQ full		
	55	Serial 8 RcvQ full		
	11	56	NetMediator DX 1 fail	NGDdx 1 Fail (Expansion shelf 1 communication link failure)
	57	NetMediator DX 2 fail	NGDdx 2 Fail (Expansion shelf 2 communication link failure)	
	58	NetMediator DX 3 fail	NGDdx 3 Fail (Expansion shelf 3 communication link failure)	
	59	GLD 1 fail	GLD address 1 is failed.	Connect just GLD unit 1 and attempt to poll. Verify GLD is connected to data port 8 and the hardware is RS485, not RS232.
	60	GLD 2 fail	GLD address 2 is failed.	Verify the GLD unit addressing, and test GLD units individually on the GLD communication bus.

Display	Point	Alarm Point	Description	Solution
11	61	GLD 3+ fail	One or more GLD units addressed 3 through 12 may be failed.	Reduce the number of connected GLD units to determine which unit may be causing the link to fail.
	62	Chan. Port Timeout	Chan. Port has not forwarded any traffic in the time specified by the Channel Timeout Timer. The channel feature forwards data between two ports so the NG may be used to analyze serial traffic using CHAN filter debug.	Change the data port type to OFF, or set the Channel Timer to a different setting.
	63	Craft Timeout	The Craft Timeout Timer has not been reset in the specified time. This feature is designed so other machines may keep the TTY link active. If the TTY interface becomes unavailable to the machine, then the Craft Timeout alarm is set.	Change the Craft Timeout Timer to 0 to disable the feature.
	64	Event Que Full	The Event Que is filled with more than 500 uncollected events.	Enable DCP timestamp polling on the master so events are collected, or reboot the system to clear the alarm.

Table A.3 *System Alarms Descriptions (continued)*

9.2 Appendix B - SNMP Manager Functions

The SNMP Manager allows the user to view alarm status, set date/time, issue controls, and perform resynchronizations. The display and tables below outline the MIB object identifiers for the NetMediator.

The table below begins with dpsRTU; however, the MIB object identifier tree has several levels above it. The full English name is: **root.iso.org.dod.internet.private.enterprises.dps-Inc.dpsAlarmControl.dpsRTU**. Therefore, dpsRTU's full object identifier is 1.3.6.1.4.1.2682.1.4. Each level beyond dpsRTU adds another object identifying number. For example, the object identifier of the Display portion of the Control Grid is 1.3.6.1.4.1.2682.1.4.3.3 because the object identifier of dpsRTU is 1.3.6.1.4.1.2682.1.4 + the Control Grid (.3) + the Display (.3).

Tbl. B1 (O.)_OV_Traps points
_OV_vTraps **(1.3.6.1.4.1.2682.1.4.0)**
PointSet (.20)
PointClr (.21)
SumPSet (.101)
SumPClr (.102)
ComFailed (.103)
ComRestored (.014)
P0001Set (.10001) through P0064Set (.10064)
P0001Clr (.20001) through P0064Clr (.20064)

Tbl. B2 (.1) Identity points
Ident **(1.3.6.1.4.1.2682.1.4.1)**
Manufacturer (.1)
Model (.2)
Firmware Version (.3)
DateTime (.4)
ResyncReq (.5)*
* Must be set to "1" to perform the resync request which will resend TRAPs for any standing alarm.

Tbl. B3 (.2) DisplayGrid points
DisplayEntry **(1.3.6.1.4.1.2682.1.4.2.1)**
Port (.1)
Address (.2)
Display (.3)
DispDesc (.4)*
PntMap (.5)*

Tbl. B3 (.3) ControlGrid points
ControlGrid **(1.3.6.1.4.1.2682.1.4.3)**
Port (.1)
Address (.2)
Display (.3)
Point (.4)
Action (.5)

Tbl. B5 (.5) AlarmEntry points
AlarmEntry **(1.3.6.4.1.2682.1.4.5.1)**
Aport (.1)
AAddress (.2)
ADisplay (.3)
APoint (.4)
APntDesc (.5)*
AState (.6)
* For specific alarm points, see Table B6

9.3 Appendix C -   SNMP Granular Trap Packets

The tables below provide a list of the information contained in the SNMP Trap packets sent by the NetMediator.

SNMP Trap managers can get alarm information via:
1. Granular traps (not necessary to define your NetMediator's point descriptions.)
OR
2. Reading trap descriptions.

UDP Header	Description
1238	Source port
162	Destination port
303	Length
0xBAB0	Checksum

UDP Headers and descriptions

SNMP Header	Description
0	Version
Public	Request
Trap	Request
1.3.6.1.4.1.2682.1.4	Enterprise
126.10.230.181	Agent address
Enterprise Specific	Generic Trap
8001	Specific Trap
617077	Time stamp
1.3.7.1.2.1.1.1.0	Object
NetMediator 216 v1.0K	Value
1.3.6.1.2.1.1.6.0	Object
1-800-622-3314	Value
1.3.6.1.4.1.2682.1.4.4.1.0	Object
01-02-1995 05:08:27.760	Value
1.3.6.1.4.1.2682.1.4.5.1.1.99.1.1.1	Object
99	Value
1.3.6.1.4.1.2682.1.4.5.1.2.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.4.5.1.3.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.4.5.1.4.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.4.5.1.5.99.1.1.1	Object
Rectifier Failure	Value
1.3.6.1.4.1.2682.1.4.5.1.6.99.1.1.1	Object
Alarm	Value

SNMP Headers and descriptions

9.4 Appendix D - ASCII Conversion

The information contained in Table D.1 is a list of ASCII symbols and their meanings. Refer to the bulleted list below to interpret the ASCII data transmitted or received through the data ports. Port transmit and receive activity can be viewed from the Web Browser Interface.

- Printable ASCII characters will appear as ASCII.
- Non-printable ASCII characters will appear as labels surrounded by { } brackets (e.g. **{NUL}**).
- Non-ASCII characters will appear as hexadecimal surrounded by [ ] brackets (e.g. **[IF]**).
- A received BREAK will appear as <BRK>.

Abbreviation	Description	Abbreviation	Description
NUL	Null	DLE	Data Link Escape
SOH	Start of Heading	DC	Device Control
STX	Start of Text	NAK	Negative Acknowledge
ETX	End of Text	SYN	Synchronous Idle
EOT	End of Transmission	ETB	End of Transmission Block
ENQ	Enquiry	CAN	Cancel
ACK	Acknowledge	EM	End of Medium
BEL	Bell	SUB	Substitute
BS	Backspace	ESC	Escape
HT	Horizontal Tabulation	FS	File Separator
LF	Line Feed	GS	Group Separator
VT	Vertical Tabulation	RS	Record Separator
FF	Form Feed	US	Unit Separator
CR	Carriage Return	SP	Space (blank)
SO	Shift Out	DEL	Delete
SI	Shift In	BRK	Break Received

ASCII symbols

9.5 Appendix E - RADIUS Dictionday File (Available on Resource Disk)

```
# -*- text -*-
#
# dictionary.dps
#
#          DPS Telecom, Inc
#          For assistance or support, please contact support@dpstele.com
#                         v1.0 Released - 1/23/09 (CBH/DPS)


VENDOR            DPS                        2682


#
# Standard attribute for NetMediator RTU.
# All values are integer with 1 = True, 0 = False.
# If attribure does not exist in Access-Accept packet, default value will be 0.
#
BEGIN-VENDOR     DPS


ATTRIBUTE   dps-admin                              1         integer
ATTRIBUTE   dps-edit                               2         integer
ATTRIBUTE   dps-monitor                            3         integer
ATTRIBUTE   dps-SD-monitor                         4         integer
#To allow monitor of data port buffer/activity
ATTRIBUTE   dps-reach-through                      5         integer
#To allow proxy to serial ports via TTY interface
ATTRIBUTE   dps-telnet                             6         integer
#To allow telnet in and out of NetMediator
ATTRIBUTE   dps-control                            7         integer
#To allow manipulation of dry contact relay outputs
ATTRIBUTE   dps-modem                              8         integer
#To allow dial in and out of NetMediator
ATTRIBUTE   dps-ppp                                9         integer
#To allow this user PPP (inbound) access to the NetMediator


END-VENDOR        DPS
```

10 Frequently Asked Questions

Here are answers to some common questions from NetMediator users. The latest FAQs can be found on the NetMediator support web page, **http://www.dpstelecom.com.**

If you have a question about the NetMediator, please call us at **(559) 454-1600** or e-mail us at **support@dpstele.com**

10.1 General FAQs

Q. How do I Telnet to the NetMediator?
A. You can only Telnet to the NetMediator on **port 2002** to the NetMediator. Configure your Telnet client to connect using TCP/IP (**not** Telnet, or any other port options) and enter **telnet <NetMediator IP Address> 2002**.

Q. How can I back up my NetMediator's current configuration?
A. From the NetMediator's web interface or via FTP. You can use FTP to read configuration files from or write files to the NetMediator's NVRAM, but you can't use FTP to edit configuration files.

Q. Can I use my NetMediator as a proxy server to access TTY interfaces on my third-party serial equipment?
A. You can connect RS-232-supporting serial devices to your NetMediator's data ports, 1-8. To establish a proxy connection, you must define the correct TCP port for each serial port. To define TCP ports, you must first connect directly to the NetMediator through its IP address. Once you have connected to the NetMediator, you can define the TCP ports through the NetMediator's TTY or Web Browser Interface.

Q. What do the terms alarm point, display, port, and address mean?
A. These terms define the exact location of a network alarm, from the most specific (an individual alarm point) to the most general (an entire monitored device). An alarm point is a number representing an actual contact closure that is activated when an alarm condition occurs. For example, an alarm point might represent a low oil sensor in a generator or a open/closed sensor in a door. A display is a logical group of 64 alarm points. A port is traditionally the actual physical serial port through which the monitoring device collects data. The address is a number representing the monitored device. The terms port and address have been extended to refer to logical or virtual ports and addresses. For example, the NetMediator reports internal alarms on Port 99, address 1.

Q. What characteristics of an alarm point can I configure through software? For instance, can I configure Point 4 to sense an active-low (normally closed) signal, or Point 5 to sense a level or edge?
A. NetMediator alarm points are level sensed and can be software-configured to generate an alarm on either a high (normally open) or low (normally closed) level.

Q. When I connect to the NetMediator through the craft port on the front panel it either doesn't work correctly or it doesn't work at all. What's going on?
A. Make sure you're using the right COM port settings. The standard settings for the craft port are: 9600 baud, 8 bits, no parity, and 1 stop bit. Flow control **must** be set to **none**. Flow control defaults to hardware in most terminal programs; this will not for the NetMediator.

Q. I just changed the port settings for one of my data ports, but the changes did not seem to take effect even after I wrote the NVRAM.
A. In order for data port and craft port changes (including changes to the baud rate and word format) to take effect, you must reboot the NetMediator. Whenever you make changes, remember to write them to the

NetMediator's NVRAM so they will take effect when you reboot the NetMediator.

Q. How do I get my NetMediator on the network?
A. Before the NetMediator will work on your LAN, you must set the unit address (IP address), the subnet mask, and the default gateway. A sample configuration could look like:

    unit address: 192.168.1.100
    subnet mask: 255.255.255.0
    Default Gateway: 192.168.1.1

Always remember to save your changes by writing to the NVRAM. Any modifications of the NetMediator's IP configuration will also require you to reboot.

Q. Does the PPP allow upload of new firmware over PPP?
A. No.

Q. I'm using HyperTerminal to connect to the NetMediator through the craft port, but the unit won't accept input when I get to the first level menu.
A. Turn off all handshaking in HyperTerminal.

Q. I can't change the craft port baud rate.
A. Once you select a higher baud rate, you must set your terminal emulation to that new baud rate and enter the "DPSCFG and press Enter escape sequence." The craft port interprets a break key as an override to 9600 baud. At slower baud rates, normal keys can appear as a break.

Q. The LAN line LED is green on my NetMediator, but I can't poll it from T/Mon.
A. Some routers will not forward to an IP address until you've registered the MAC address with the router. You need to enter the IP address of your T/Mon system or your gateway in the ping table.

10.2 SNMP FAQs

Q. Which versions of SNMP are supported by the SNMP agent on the NetMediator?
A. SNMP v1, v2c, and v3.

Q. How do I configure the NetMediator to send traps to an SNMP manager? Is there a separate MIB for the NetMediator? How many SNMP managers can the agent send traps to? And how do I set the IP address of the SNMP manager and the community string to be used when sending traps?
A. The NetMediator begins sending traps as soon as you've defined an SNMP manager. The NetMediator MIB is included on the NetMediator Resource CD. You will need to compile the MIB on your SNMP manager. (Note: MIB versions may change.) The unit supports two main SNMP managers, which you'll configure in the SNMP option from the web interface. You can also configure up to eight secondary SNMP managers by designating your SNMP managers as notification recipients. Community strings, however, are configured globally for all SNMP managers.

Q. Does my NetMediator support MIB-2 and/or any other standard MIBs?
A. The NetMediator supports the bulk of MIB-2.

Q. Does my NetMediator SNMP agent support both NetMediator and T/Mon variables?
A. Your NetMediator SNMP agent manages an embedded MIB that only supports the NetMediator's RTU variables. T/Mon variables are included in the distributed MIB only to provide SNMP managers with a single MIB for all DPS Telecom products.

Q. How many traps are triggered when a single point is set or cleared? The MIB defines traps like major alarm set/cleared, RTU point set, and a lot of granular traps, which could imply that more than one trap is sent when a change of state occurs on one point.

A. Generally, a single change of state generates a single trap, but there are two exception to this rule. Exception 1: the first alarm in an all clear condition which generates an additional summary point set trap. Exception 2: the final clear alarm that triggers an all clear condition generates an additional summary point clear trap.

Q. What does point map mean?
A. A point map is a single MIB leaf that presents the current status of a 64-alarm-point display in an ASCII-readable form, where a "." represents a clear and an "x" represents an alarm.

Q. My NetMediator manual talks about eight control relay outputs. How do I control these from my SNMP manager?
A. Your can operate control relays by sending appropriate set commands, contained in the DPS Telecom MIB. For more information about the set commands, see Reference Information, Display Mapping, in any of the NetMediator software configuration guides.

Q. How can I associate descriptive information with a point for the RTU granular traps?
A. Your NetMediator alarm point descriptions are individually defined in the Web Browser or TTY configuration interfaces.

Q. My SNMP traps aren't getting through. What should I try?
A. Try these three steps:
1. Make sure that the trap address (IP address of the SNMP manager) is defined. (If you changed the trap address, make sure you saved the change to NVRAM and rebooted.)
2. Make sure all alarm points are configured to send SNMP traps.
3. Make sure the NetMediator and the SNMP manager are both on the network. Use the NetMediator's ping command to ping the SNMP manager.

10.3 Pager FAQs

Q. Why won't my alpha pager work?
A. To configure your NetMediator to send alarm notifications to an alpha pager, enter the **data** phone number for your pager in the Phone Number field. This phone number should connect to your pager services modem. Then enter the PIN for your pager in the PIN/Rcpt/Port field. You don't need to enter anything in any of the other fields. If you still don't receive pages, try setting the Dial Modem Init string to ATS37=9. This will limit the NetMediator's connection speed.

Q. Numeric pages don't come in or are cut off in the middle of the message. What's wrong?
A. You need to set a delay between the time the NetMediator dials your pager number and the time the NetMediator begins sending the page message. You can set the delay in the Pager Number field, where you enter your pager number. First enter the pager number, then enter some commas directly after the number. Each comma represents a two-second delay. So, for example, if you wanted an eight-second delay, you would enter 555-1212,,,, in the Pager Number field.

Q. How do I set up email notifications?
A. You need to assign the NetMediator an email address and list the addresses of email recipients. An email address consists of two parts, the user name (everything before the @ sign) and the domain (everything after the @ sign). To assign the NetMediator an email address, choose System from the Edit menu. Enter the NetMediator's user name in the Name field (it can't include any spaces) and the domain in the Location field. For example, if the system configuration reads:
    Name: NetMediator
    Location: proactive.com
The NetMediator will then send email notifications from NetMediator@proactive.com. Next, choose Notifications from the Provisioning menu. Enter the domain of each recipient in the Phone/Domain field, and the username of each recipient in the PIN/Rcpt/Port field. Then, Enter the IP address of an SMTP server in

the IPA field.

11 Technical Support

DPS Telecom products are backed by our courteous, friendly Technical Support representatives, who will give you the best in fast and accurate customer service. To help us help you better, please take the following steps before calling Technical Support:

1. Check the DPS Telecom website.
You will find answers to many common questions on the DPS Telecom website, at **http://www.dpstelecom. com/support/**. Look here first for a fast solution to your problem.

2. Prepare relevant information.
Having important information about your DPS Telecom product in hand when you call will greatly reduce the time it takes to answer your questions. If you do not have all of the information when you call, our Technical Support representatives can assist you in gathering it. Please write the information down for easy access. Please have your user manual and hardware serial number ready.

3. Have access to troubled equipment.
Please be at or near your equipment when you call DPS Telecom Technical Support. This will help us solve your problem more efficiently.

4. Call during Customer Support hours. Customer support hours are Monday through Friday, from 7 A.M. to 6 P.M., Pacific time. The DPS Telecom Technical Support phone number is **(559) 454-1600**.

Emergency Assistance: *Emergency assistance is available 24 hours a day, 7 days a week. For emergency assistance after hours, allow the phone to ring until it is answered with a paging message. You will be asked to enter your phone number. An on-call technical support representative will return your call as soon as possible.*

12 End User License Agreement

All Software and firmware used in, for, or in connection with the Product, parts, subsystems, or derivatives thereof, in whatever form, including, without limitation, source code, object code and microcode, including any computer programs and any documentation relating to or describing such Software is furnished to the End User only under a non-exclusive perpetual license solely for End User's use with the Product.

The Software may not be copied or modified, in whole or in part, for any purpose whatsoever. The Software may not be reverse engineered, compiled, or disassembled. No title to or ownership of the Software or any of its parts is transferred to the End User. Title to all patents, copyrights, trade secrets, and any other applicable rights shall remain with the DPS Telecom.

DPS Telecom's warranty and limitation on its liability for the Software is as described in the warranty information provided to End User in the Product Manual.

End User shall indemnify DPS Telecom and hold it harmless for and against any and all claims, damages, losses, costs, expenses, obligations, liabilities, fees and costs and all amounts paid in settlement of any claim, action or suit which may be asserted against DPS Telecom which arise out of or are related to the non-fulfillment of any covenant or obligation of End User in connection with this Agreement.

This Agreement shall be construed and enforced in accordance with the laws of the State of California, without regard to choice of law principles and excluding the provisions of the UN Convention on Contracts for the International Sale of Goods. Any dispute arising out of the Agreement shall be commenced and maintained only in Fresno County, California. In the event suit is brought or an attorney is retained by any party to this Agreement to seek interpretation or construction of any term or provision of this Agreement, to enforce the terms of this Agreement, to collect any money due, or to obtain any money damages or equitable relief for breach, the prevailing party shall be entitled to recover, in addition to any other available remedy, reimbursement for reasonable attorneys' fees, court costs, costs of investigation, and other related expenses.

Warranty

DPS Telecom warrants, to the original purchaser only, that its products a) substantially conform to DPS' published specifications and b) are substantially free from defects in material and workmanship. This warranty expires two years from the date of product delivery with respect to hardware and ninety days from the date of product delivery with respect to software. If the purchaser discovers within these periods a failure of the product to substantially conform to the specifications or that the product is not substantially free from defects in material and workmanship, the purchaser must promply notify DPS. Within reasonable time after notification, DPS will endeavor to correct any substantial non-conformance with the specifications or substantial defects in material and workmanship, with new or used replacement parts. All warranty service will be performed at the company's office in Fresno, California, at no charge to the purchaser, other than the cost of shipping to and from DPS, which shall be the responsiblity of the purchaser. If DPS is unable to repair the product to conform to the warranty, DPS will provide at its option one of the following: a replacement product or a refund of the purchase price for the non-conforming product. These remedies are the purchaser's only remedies for breach of warranty. Prior to initial use the purchaser shall have determined the suitability of the product for its intended use. DPS does not warrant a) any product, components or parts not manufactured by DPS, b) defects caused by the purchaser's failure to provide a suitable installation environment for the product, c) damage caused by use of the product for purposes other than those for which it was designed, d) damage caused by disasters such as fire, flood, wind or lightning unless and to the extent that the product specification provides for resistance to a defined disaster, e) damage caused by unauthorized attachments or modifications, f) damage during shipment from the purchaser to DPS, or g) any abuse or misuse by the purchaser.

THE FOREGOING WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In no event will DPS be liable for any special, incidental, or consequential damages based on breach of warranty, breach of contract, negligence, strict tort, or any other legal theory. Damages that DPS will not be responsible for include but are not limited to, loss of profits; loss of savings or revenue; loss of use of the product or any associated equipment; cost of capital; cost of any substitute equipment, facilities or services; downtime; claims of third parties including customers; and injury to property.

The purchaser shall fill out the requested information on the Product Warranty Card and mail the card to DPS. This card provides information that helps DPS make product improvements and develop new products.

For an additional fee DPS may, at its option, make available by written agreement only an extended warranty providing an additional period of time for the applicability of the standard warranty.

Technical Support

If a purchaser believes that a product is not operating in substantial conformance with DPS' published specifications or there appear to be defects in material and workmanship, the purchaser should contact our technical support representatives. If the problem cannot be corrected over the telephone and the product and problem are covered by the warranty, the technical support representative will authorize the return of the product for service and provide shipping information. If the product is out of warranty, repair charges will be quoted. All non-warranty repairs receive a 90-day warranty.

Free Tech Support is Only a Click Away

Need help with your alarm monitoring? DPS Information Services are ready to serve you … in your email or over the Web!

www.DpsTelecom.com

Free Tech Support in Your Email: The Protocol Alarm Monitoring Ezine

The Protocol Alarm Monitoring Ezine is your free email tech support alert, delivered directly to your in-box every two weeks. Every issue has news you can use right away:

- Expert tips on using your alarm monitoring equipment -   advanced techniques that will save you hours of work

- Educational White Papers deliver fast informal tutorials on SNMP, ASCII processing, TL1 and other alarm monitoring technologies

- New product and upgrade announcements keep you up to date with the latest technology

- Exclusive access to special offers for DPS Telecom Factory Training, product upgrade offers and discounts

To get your free subscription to The Protocol register online at
www.TheProtocol.com/register

Free Tech Support on the Web: MyDPS

MyDPS is your personalized, members-only online resource. Registering for MyDPS is fast, free, and gives you exclusive access to:

- Firmware and software downloads and upgrades
- Product manuals
- Product datasheets
- Exclusive user forms

Register for MyDPS online at
www.DpsTelecom.com/register

(800) 622-3314 • www.DpsTelecom.com • 4955 E. Yale Avenue, Fresno, California 93727