NetGuardian 832A G4

USER MANUAL
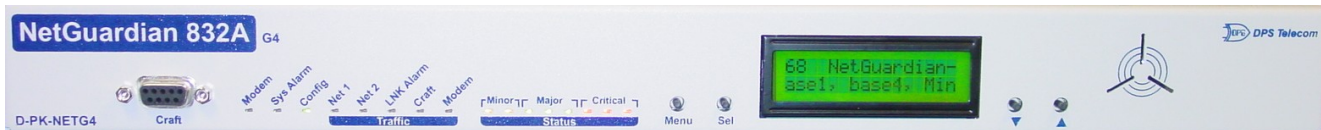
Revision History

February 6, 2018	Updated Display Map for XBEE sensors
August 28, 2012	Updated part number for new RoHS ethernet cables
June 7, 2012	Added 202 modem tune up information
February 6, 2012	Updated shipping list
January 19, 2011	Added analog entries to SNMP Manager Functions
November 10, 2010	Added note describing alarm speaker operation.
March 29, 2010	Added more detail on analog parameters
February 7, 2008	Added GND pins to RS485 and 202 pinouts
March 28, 2008	Added section on anchoring amphenol cables and updated blue LCDs to yellow. Added pictures of sealed hardware kits
July 13, 2009	Revisions to sections on Analog Pinout and LAN connection

Contents

1 NetGuardian 832A Overview

Fig. 1.1. *The NetGuardian has all the tools you need to manage your remote site*

The NetGuardian 832A — The Intelligent RTU for Complete Site Management
The NetGuardian 832A is a RoHS-compliant, LAN-based, SNMP/DCPx remote telemetry unit. The NetGuardian has all the tools you need to manage your remote sites, including built-in alarm monitoring, paging and email capabilities that can eliminate the need for an alarm master.

With the NetGuardian, you can:
- Monitor 32 discrete alarms, 32 ping alarms, and 8 analog alarms
- Control remote site equipment via 8 terminal server ports and 8 control relays
- Monitor your remote site from anywhere using the NetGuardian's built-in Web Browser Interface.
- Automatically send pager and email alarm notifications 24/7.
- Connect multiple concurrent users via Telnet over LAN to telecom switches, servers, radios, PBXs and other equipment.
- Monitor discrete and analog alarms.
- Operate control relays.
- Ping IP network devices and verify that they're online and operating.
- Report alarms to multiple SNMP managers or the T/Mon NOC Alarm Monitoring System.
- Report alarms via LAN or dial-up connection.

New: The NetGuardian G4 supports serial baud rates up to 115,200, the analog readings accurate to within +/- 1% , dual NICs (Private / Public), SNMPv2 and SNMPv2c Inform.

Stand-alone local visibility
You don't need an alarm master unit to monitor your site with the NetGuardian. With the NetGuardian's built-in Web Browser Interface, you can access the NetGuardian, view and acknowledge alarms and control remote site devices from any computer anywhere in your network.

24/7 pager and email alerts - no master needed
Out of the box, the NetGuardian supports 24/7 pager and email reporting. Send alarms directly to maintenance technicians in the field, even when no one's in the office.

Connect via LAN to telecom switches, servers, radios and more
Each of the NetGuardian's eight serial ports can be individually configured to serve as a craft port, a channel port or a TCP or UDP reach-through port, giving you LAN-based terminal server access to up to eight serial devices.

Multiple users can connect to the NetGuardian simultaneously via Telnet over LAN to connect and control telecom switches, servers, radios, PBXs and other remote site equipment.

Reports to multiple SNMP managers and T/Mon NOC simultaneously
The NetGuardian reports to both the T/Mon NOC Alarm Monitoring System and any SNMP manager. You can simultaneously forward alarms from the NetGuardian to T/Mon NOC and multiple SNMP managers at multiple IP

addresses.

2 About This Manual

There are three separate user manuals for the NetGuardian 832A: the Hardware Manual (which you're reading now), the NGEdit4 User Manual, and the NetGuardian 832A Web Interface User Manual.

This Hardware Manual provides instructions for hardware installation and using the TTY interface. The NGEdit4 and Web Interface User Manuals, included on the NetGuardian Resource CD, provide instructions for configuring the NetGuardian using the Windows-based NGEdit4 utility software or the Web Interface.

3 Shipping List

While unpacking the NetGuardian, please make sure that all of the following items are included. If some parts are missing, or if you ever need to order new parts, please refer to the part numbers listed and call DPS Telecom at **(800) 622-3314**.

NetGuardian 832A G4
D-PK-NETG4-12001

NetGuardian 832A G4 Hardware
Manual D-UM-NETG4

NetGuardian 832A G4 Resource CD
(includes manuals, MIBs, and software)

DB9M-DB9F Download Cable 6 ft.
D-PR-045-10-A-04

Two Ethernet Cables 14 ft.
D-PR-923-10B-14

Telephone Cable 6 ft.
D-PR-045-10A-01

23" Rack Ears
D-CS-325-10A-01

19" Rack Ears
D-CS-325-10A-00

Eight 3/8'' Ear Screws
2-000-60375-05

Four Standard Rack Screws
1-000-12500-06

Four Metric Rack Screws
2-000-80750-03

Two 3/4-Amp GMT Main Power Fuses
2-741-00750-00

Two Large Power Connector Plugs for Main Power
2-820-00862-02

Four Cable Ties
(Sixteen with hinged panel)

4 Pin Analog Connector
2-820-00814-02

Pads
2-015-00030-00

Optional Items

Two 1/2-Amp GMT Accessory Fuses Sensor Output
2-741-00500-00

One Small Power Connector Plug for

2-820-00812-02

4   Optional Accessories

You can extend the capabilities of the NetGuardian through accessory units that provide greater discrete alarm capacity, remote audiovisual alarm notification, visual surveillance of remote sites, and other options. If you would like to order any of these accessories, or if you would like more information about them, call DPS Telecom at **(800) 622-3314**.
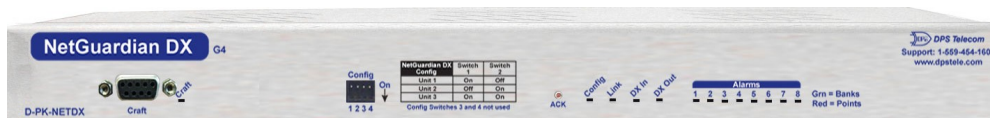
NetGuardian Expansion (NetGuardian DX G4)
D-PK-NETDX-12022.00001
The NetGuardian Expansion G4 provides an additional 48 discrete alarm points. Up to three NetGuardian Expansions can be daisy-chained off one NetGuardian, providing a total of 176 discrete alarm points.

General LCD Display (GLD)
D-PC-820-10A-04
The General LCD Display (GLD) is a small wall-mounted remote terminal for the NetGuardian. The LCD display shows system status and alarm messages, and the built-in speaker gives an audible notice of alarms. Up to 12 GLDs can be daisy-chained off the NetGuardian. (NetGuardian with optional RS-485 port required.)

NetGuardian SiteMON IP   D-PK-CAMRA
The NetGuardian SiteMON provides security surveillance of remote sites. The SiteMON connects to either the NetGuardian's integrated 10/100BaseT switch or a separate 10/100/1000 switch. SiteMON images can be accessed directly from the SiteMON's Web Browser Interface or T/GFX. You can also mount the camera at harsh weather sites with the wide-temp chassis design.

Hinged Wire-Wrap Back Panel
For 19" rack: D-PK-NGPAN-12002
For 23" rack: D-PK-NGPAN-12006
The hinged wire-wrap back panel provides wire-wrap connections for the NetGuardian's alarms and control relays.
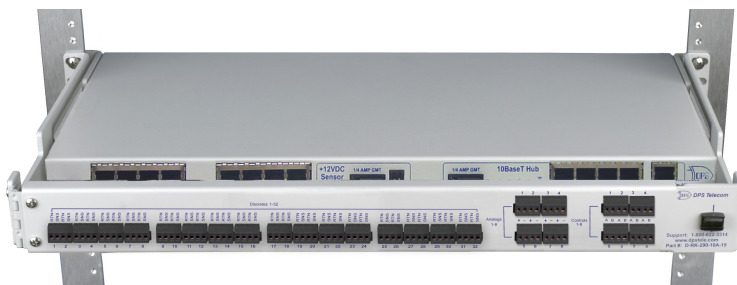
Pluggable Barrier Panel
For 19" rack: D-PK-NGPAN-12003
For 23" rack: D-PK-NGPAN-12007
The pluggable barrier panel provides screw-lug barrier plug connections for the NetGuardian's alarms and control relays.

5 Specifications

Discrete Alarm Inputs: 32 (expandable to 80, 128, or 176)

Analog Alarms: 8
    Analog Input Range: (–94 to 94 VDC or 4 to 20 mA)
    Analog Accuracy: +/- 1%

Control Relays: 8 Form C (expandable to 16, 24, 32)
    Maximum Voltage: 60 VDC/120 VAC
    Maximum Current: 1 Amp, AC/DC

Ping Alarms: 32

Protocols: SNMP, DCPx, TRIP
                  SMTP, TAP

Interfaces: 8 RJ45 Yost RS-232 ports
                  2 RJ45 10BaseT (half-duplex) Ethernet ports
                  1 RJ11 telco jack
                  2 50-pin amphenol connectors (discretes, controls, and analogs)
                  1 4-pin screw connector (analogs)

Dimensions: 1.75"H x 17"W x 12"D (4.5 cm x 43.2 cm x 30.5 cm)

Weight: 4 lbs. 3 oz. (1.9 kg)

Mounting: 19" or 23" rack

Power Input: –48VDC (–40 to –70 VDC)
                  (Optional) –24 VDC (–18 to –36 VDC)
                  (Optional) Wide Range –24/–48 VDC (–18 to –72 VDC)

Power Output: 12 VDC power output for external sensor

Current Draw: 200 mA

Fuse: 3/4 amp GMT for power inputs
                  1/4 amp GMT for external sensor power output and integrated Ethernet hub

Modem: 33.6 K internal

Visual Interface: LCD display
                  18 bicolor LEDs
                  5 unicolor LEDs (11 with Hub Option)

Audible Notification: Alarm speaker

MTBF: 60 years

Windows Compatibility: XP, Vista, 7 32/64 bit

Operating Temperature: 32°–140° F (0°–60° C)

Operating Humidity: 0%–95% noncondensing

RoHS 5 Approved

NEBS3 Compliant

6   Hardware Installation

6.1   Tools Needed

To install the NetGuardian, you'll need the following tools:

Phillips No. 2 Screwdriver   **Small Standard No. 2 Screwdriver**

Wire Strippers/Cutter   **Wire Wrap Gun (if hinged wire wrap panel is used)**

Punch Down Tool (if 66 blocks are used)   **PC with NGEdit4 software**

6.2   Mounting
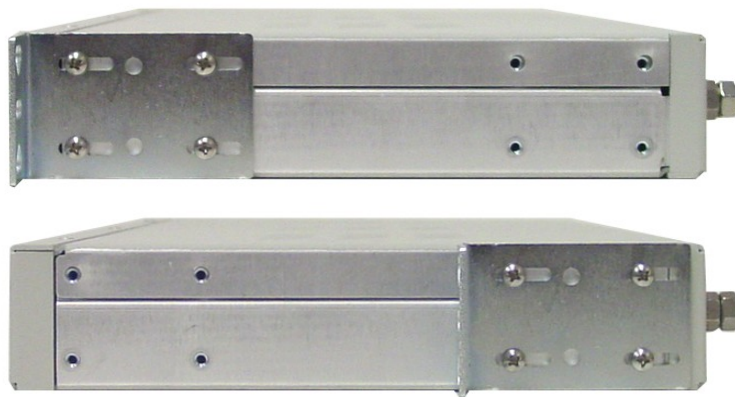
Fig. 6.2.1. The NetGuardian can be flush or rear-mounted

The NetGuardian mounts in a 19" rack or a 23" rack using the provided rack ears for each size. Two rack ear locations are provided. Attach the appropriate rack ears in the flush-mount or rear-mount locations shown in Figure 6.2.1.

Note: Rack ears can be rotated 90° for wall mounting or 180º for other mounting options (not shown).

6.3 Power Connection
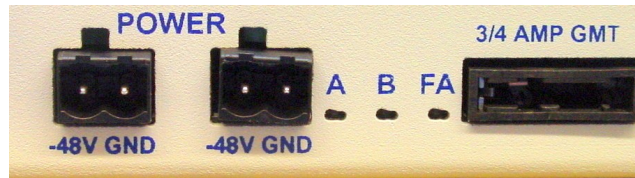
Fig. 6.3.1. *Power connectors and fuse.*

The NetGuardian has two screw terminal barrier plug power connectors, located on the left side of the back panel. (See Figure 6.3.1.)

The Grounding Lug on the back of the unit provides a permanent connection to earth ground when connected. The Grounding Lug must be used in order to comply with **standards.**
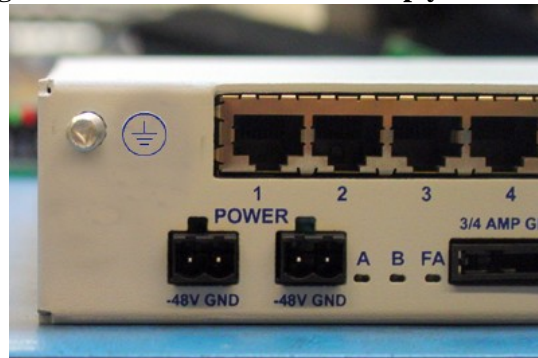
Grounding Lug and Symbol

Before you connect a power supply to the NetGuardian, test the voltage of your power supply:

- Connect the black common lead of a voltmeter to the ground terminal of the battery, and connect the red lead of the voltmeter to the battery's –48 VDC terminal. The voltmeter should read **between –43 and –53 VDC**. If the reading is outside this range, test the power supply.

To connect the NetGuardian to a power supply, follow these steps:

1. Remove the fuse from the back panel of the NetGuardian. **Do not reinsert the fuse until all connections to the unit have been made.**

2. Remove the power connector plug from Power Connector A. Note that the plug can be inserted into the power connector only one way — this ensures that the barrier plug can only be reinserted with the correct polarity. Note that the **–48V terminal is on the left** and the **GND terminal is on the right**.

3. Use the grounding lug to connect the unit to earth ground. The grounding lug is next to the ⏚ symbol.

4. Insert a **battery ground** into the power connector plug's **right terminal** and tighten the screw; then insert a **–48 VDC** line to the plug's **left terminal** and tighten its screw.

5. Push the power connector plug firmly back into the power connector. If the power feed is connected correctly, the LED by the connector will light **GREEN**. If the polarity of the power feed is reversed, the LED will not illuminate.

6. Repeat Steps 2–4 for Power Connector B.

7. Reinsert the fuse to power the NetGuardian. The front panel LEDs will flash **RED** and **GREEN**.

To connect the NetGuardian to a power supply using a WAGO connector, follow these steps:

WARNING!

The Grounding Lug on the back of the unit provides a permanent connection to earth ground when connected. The Grounding Lug must be used in order to comply with C E **standards.**
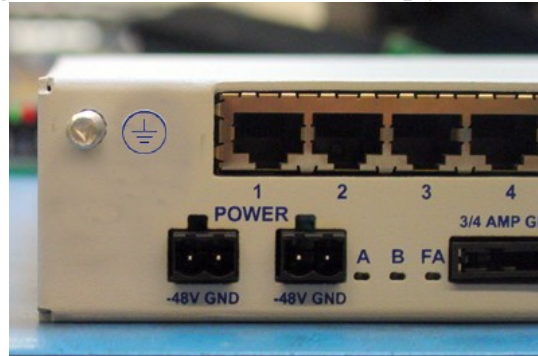
Grounding Lug and Symbol

1. Remove the **2** fuses (**A** & **B**) from the back panel of the NetGuardian. **Do not reinsert the fuses until all connections to the unit have been made.**

2. Remove the WAGO power connector. Note that the plug can be inserted into the power connector only one way — this ensures that the barrier plug can only be reinserted with the correct polarity. Note that the **–48V terminal is on Slots 1 and 3** and the **GND terminal is on Slots 2 and 4**.

3. Use the grounding lug to connect the unit to earth ground. The grounding lug is next to the ⏚ symbol.

4. Insert a **battery ground** into the power connector plug's **slots 2 and 4** by pushing down on top of the appropriate slot of the WAGO connector with a screwdriver and inserting the wire into the slot, then releasing the screwdriver. Insert a **–48 VDC** line to the plug's **slots 1 and 3** using the same method as before.
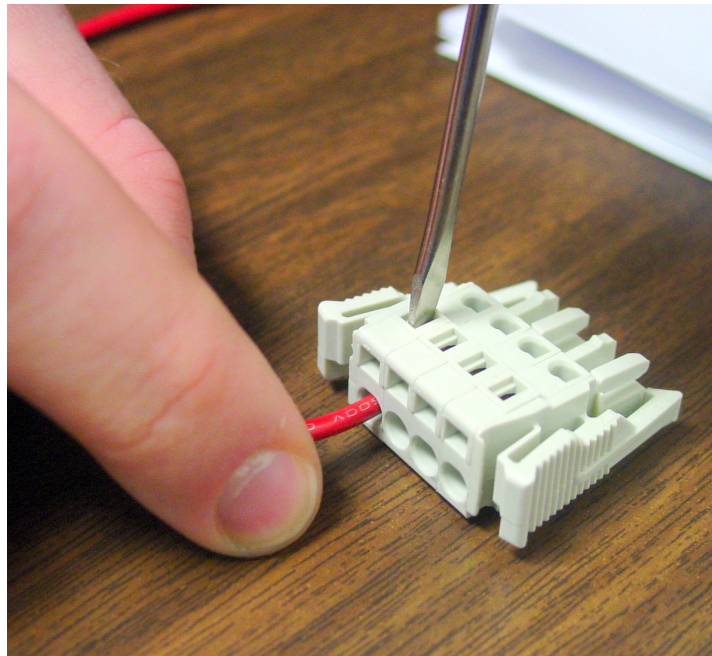
Inserting a -48 VDC Line into Slot 1 of WAGO Connector

5. Push the power connector plug firmly back into the power connector. If the power feed is connected correctly, the LED by the connector will light **GREEN**. If the polarity of the power feed is reversed, the LED will not illuminate.

6. Reinsert the fuses to power the NetGuardian. The front panel LEDs will flash **RED** and **GREEN**.

6.4   LAN Connection
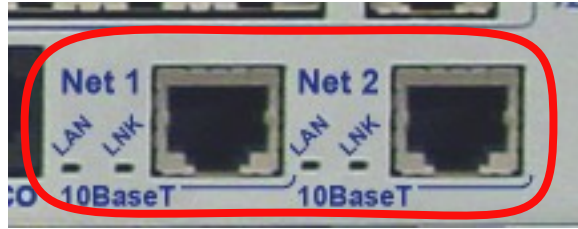
Fig. 6.4.1. *Ethernet ports*

For enhanced security, the NetGuardian 832A has two 10BaseT Ethernet ports. Each port has its own separate IP address and subnet, so you can safely connect one port to your private company LAN and the other to the public Internet.

By default, outbound data traffic from the NetGuardian 832A will be sent over Net 2. Only outbound data that is specifically directed to Net 1, usually the Company's LAN, will be sent to Net 1.

Both ports are standard RJ45 ports that take standard RJ45 Ethernet cables. If the IP connection is OK, the LNK LED will light **SOLID GREEN** when the cable is connected.

RJ45 Ethernet Connection
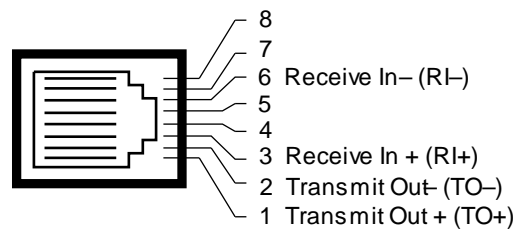
Fig. 6.4.2 *Ethernet port pinout*

The pinout for the Ethernet ports is shown in Figure 6.4.2, above.

NOTE: There is no routing between Net 1 and Net 2, this ensures that both connections are independent of each other.

6.5   Telco Connection
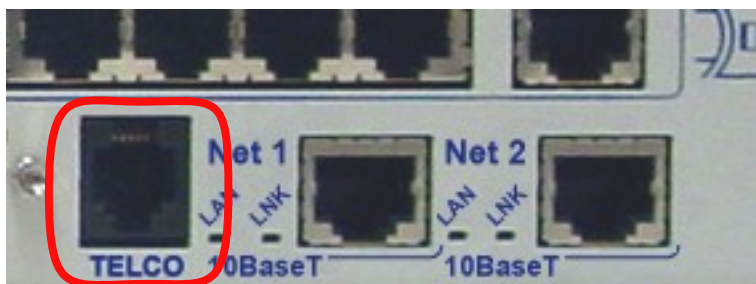
Fig. 6.5.1. *Telco jack*

The rear panel telco jack (see Figure 6.5.1) connects the NetGuardian internal modem to a standard phone line for dial-up access and pager alarm notification.

RJ11 Phone Line Connection
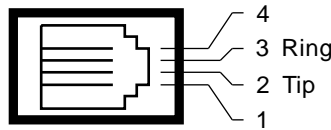
Fig. 6.5.2 *Telco jack pinout*

The pinout for the Telco jack is shown in Figure 6.5.2, above.

6.6   Alarm and Control Relay Connections

Fig. 6.6.1. *Alarm and control relay connectors*

The NetGuardian's discrete alarm inputs, control relay outputs, and first six analog alarm inputs are connected through the two 50-pin connectors labeled "Discretes 1–24" and "Analogs 1–6/Discretes 25–32/Relays 1–8" on the back panel. Analog alarm inputs 7 and 8 are connected through the four-pin connector labeled "Analogs 7–8." (See Figure 6.6.1.)

6.6.1   Alarm and Control Relay Connector Pinout Table

Discretes 1–25							Discretes 25–32				Control Relays 1–8		
	RTN	ALM		RTN	ALM			RTN	ALM			NO/NC	CO
ALM 1	1	26	ALM 13	13	38		ALM 25	1	26		CTRL 1	9	34
ALM 2	2	27	ALM 14	14	39		ALM 26	2	27		CTRL 2	10	35
ALM 3	3	28	ALM 15	15	40		ALM 27	3	28		CTRL 3	11	36
ALM 4	4	29	ALM 16	16	41		ALM 28	4	29		CTRL 4	12	37
ALM 5	5	30	ALM 17	17	42		ALM 29	5	30		CTRL 5	13	38
ALM 6	6	31	ALM 18	18	43		ALM 30	6	31		CTRL 6	14	39
ALM 7	7	32	ALM 19	19	44		ALM 31	7	32		CTRL 7	15	40
ALM 8	8	33	ALM 20	20	45		ALM 32	8	33		CTRL 8	16	41
ALM 9	9	34	ALM 21	21	46						FUSE	17	42
ALM 10	10	35	ALM 22	22	47								
ALM 11	11	36	ALM 23	23	48								
ALM 12	12	37	ALM 24	24	49								
			GND	25	50								

Analogs 1–6		
	+	−

Analogs 7–8		
	+	−

ANA 1	19	44
ANA 2	20	45
ANA 3	21	46
ANA 4	22	47
ANA 5	23	48
ANA 6	24	49
GND	25	50

ANA 7	7+	7-
ANA 8	8+	8-

Analogs 7–8
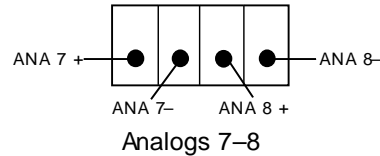
Table 6.6.1.A. *Alarm and control relay connector pinout*

Table 6.6.1.A shows the pinouts for the 50-pin connectors "Discretes 1–24" and "Analogs 1–6/Discretes 25–32/ Relays 1–8," and the pinout for the four-pin connector "Analogs 7–8."

Note that the NetGuardian's control relays can be set for either Normally Open or Normally Closed operation. By factory default, all control relays are set to Normally Open. You can reset all relays for Normally Closed operation at the hardware level by resetting a jumper on the NetGuardian circuit board. You can also configure the control relays individually, using either the Web interface or the NGEdit4 software utility.

For instructions on resetting control relays for Normally Closed operation, see Section 6.12, "Jumper Options."

6.6.2   Discretes 1–24 Connector Pinout Diagram

RTN 1	1		26	ALM 1
RTN 2	2		27	ALM 2
RTN 3	3		28	ALM 3
RTN 4	4		29	ALM 4
RTN 5	5		30	ALM 5
RTN 6	6		31	ALM 6
RTN 7	7		32	ALM 7
RTN 8	8		33	ALM 8
RTN 9	9		34	ALM 9
RTN 10	10		35	ALM 10
RTN 11	11		36	ALM 11
RTN 12	12		37	ALM 12
RTN 13	13		38	ALM 13
RTN 14	14		39	ALM 14
RTN 15	15		40	ALM 15
RTN 16	16		41	ALM 16
RTN 17	17		42	ALM 17
RTN 18	18		43	ALM 18
RTN 19	19		44	ALM 19
RTN 20	20		45	ALM 20
RTN 21	21		46	ALM 21
RTN 22	22		47	ALM 22
RTN 23	23		48	ALM 23
RTN 24	24		49	ALM 24
GND	25		50	GND

Fig. 6.6.2.1. Pinout Diagram for Discretes 1–24 connector

6.6.3 Analogs1–6/Discretes 25–32/Relays 1–8 Connector Pinout Diagram

Left Label	Pin	Pin	Right Label
RTN 25	1	26	ALM 25
RTN 26	2	27	ALM 26
RTN 27	3	28	ALM 27
RTN 28	4	29	ALM 28
RTN 29	5	30	ALM 29
RTN 30	6	31	ALM 30
RTN 31	7	32	ALM 31
RTN 32	8	33	ALM 32
CTRL 1 NO	9	34	CTRL 1 CO
CTRL 2 NO	10	35	CTRL 2 CO
CTRL 3 NO	11	36	CTRL 3 CO
CTRL 4 NO	12	37	CTRL 4 CO
CTRL 5 NO	13	38	CTRL 5 CO
CTRL 6 NO	14	39	CTRL 6 CO
CTRL 7 NO	15	40	CTRL 7 CO
CTRL 8 NO	16	41	CTRL 8 CO
FUSE NO	17	42	FUSE CO
Unused	18	43	Unused
ANA 1 +	19	44	ANA 1 –
ANA 2 +	20	45	ANA 2 –
ANA 3 +	21	46	ANA 3 –
ANA 4 +	22	47	ANA 4 –
ANA 5 +	23	48	ANA 5 –
ANA 6 +	24	49	ANA 6 –
GND	25	50	GND

Fig. 6.6.3.1. *Pinout Diagram for Discretes 25–32/Relays 1–8 connector*

6.6.4   Analogs 7–8 Connector
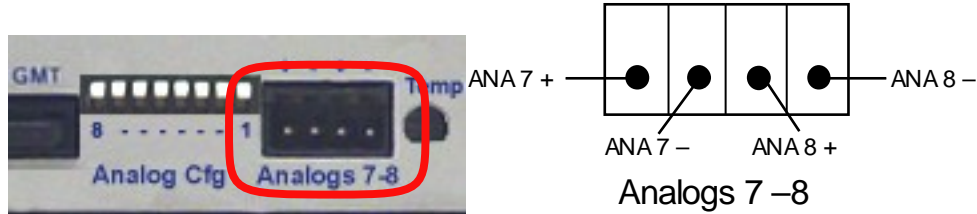
Fig. 6.6.4.1. *Analogs 7–8 4-pin connector and pinout*

Analog alarm inputs 7 and 8 are connected through the back panel four-pin connector labeled "Analogs 7–8." (See Figure 6.6.4.1.)

The four-pin connector is a barrier plug connector similar to the power connector. To connect analog inputs, remove the connector plug, connect the leads to the appropriate terminals and reinsert the barrier plug. Note that the plug can be inserted into its socket only one way — this ensures that the connector plug can only be reinserted with the alarm inputs aligned correctly.

The pinout for the 4 pin analog connector is shown in Figure 6.6.4.1, above.

6.6.5   Analog Dipswitches
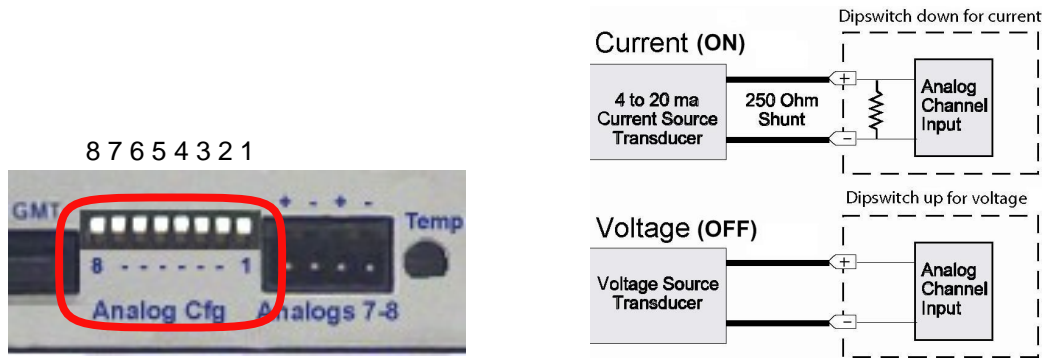
Fig. 6.6.5.1. *Dipswitch location and layout*

The analogs are controlled by the dipswitches to the left of the four-pin connector. For milliamp sensor operation turn the dipswitch on by placing it in the down position. For normal operation place the dipswitch in the up position.

 Hot Tip!   # WARNING

WARNING: Do not put the dipswitches in the downward position unless you are sure of the analog setting. Having the dipswitch on puts a 250 ohm resistor across the input lines. Any voltage beyond 5V or 20 mA will damage components.

6.6.6 Integrated Temperature and Battery Sensor (Optional)

Fig. 6.6.6.1. *The integrated temperature sensor*

The optional integrated temperature and battery sensor monitors the ambient temperature and the NetGuardian's current draw. This option is available only if it was ordered with your NetGuardian. The integrated temperature sensor measures a range of 32° F to 140° F (0° C to 60° C) within an accuracy of ± 1°.

Sensor Function	Analog Input Options
Temperature	Can be used on analog input 4 or 7
Power Feed A	Can be used on analog input 5 or 8
Power Feed B	Can be used on analog input 6

Table 6.6.6.A. *Integrated sensor connection options*

Each integrated sensor takes the place of an analog input, and does not need any external connections. No other analog input can be connected to the input point used for the integrated sensors. Table 6.6.6.A lists the connection options for the integrated temperature sensor. Note that these options are set at the factory, based on the option ordered, and cannot be adjusted by the user.

6.7 Data Ports
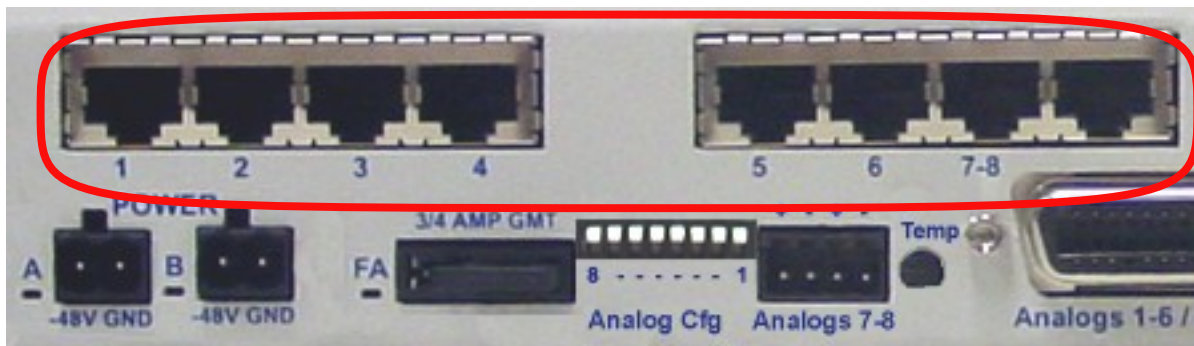
Fig. 6.7.1. *Data ports 1–8*

The NetGuardian's eight data ports provide reach-through terminal server functionality for connecting multiple simultaneous users to external equipment via Telnet over LAN. Each port can function as a proxy connection to an external device, a craft port, a channel port, a TCP or UDP reach-through port. The NetGuardian can support simultaneous proxy connections for up to eight users.

Yost RS-232 RJ45 Connector

8 RTS (Request to Send)
7 DTR (Data Terminal Ready)
6 TXD (Transmit Data)
5 GND (Ground)
4 GND (Ground)
3 RXD (Receive Data)
2 DSR (Data Set Ready)
1 CTS (Clear to Send)

Yost RS-485 RJ45 Connector

8 TX- (Transmit -)
7 N/C (Not Connected)
6 RX- (Receive -)
5 N/C (Not Connected)
4 N/C (Not Connected)
3 RX+ (Receive +)
2 N/C (Not Connected)
1 TX+ (Transmit +)

Yost 4-Wire 202 Connector

8 TX+ (Transmit +)
7 N/C (Not Connected)
6 RX- (Receive -)
5 N/C (Not Connected)
4 N/C (Not Connected)
3 RX+ (Receive +)
2 N/C (Not Connected)
1 TX- (Transmit -)

Fig. 6.7.2 Data port pinouts

NetGuardian data ports can be configured for Yost RS-232, RS-485, and 4-wire 202 RJ45 connects. The pinouts for Data Ports 1–8 are shown in Figure 6.7.2, above.

DB9 RS-232

GND — RX — TX
5 4 3 2 1
9 8 7 6
RTS — CTS

Pin #	Signal	Description
1		Not connected
2	**TX**	**Transmit data**
3	**RX**	**Recieve Data**
4		Not connected
5	**GND**	**Ground**
6		Not connected
7	**CTS**	**Clear to send**
8	**RTS**	**Request to send**
9		Not connected
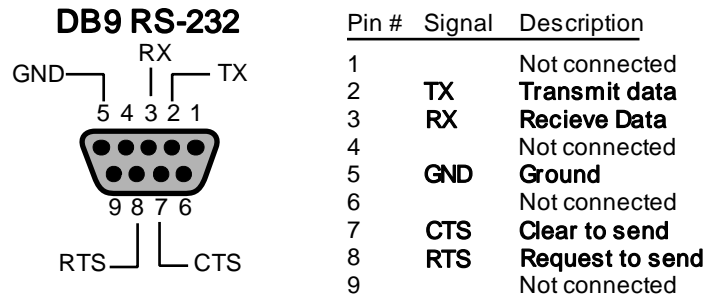
Fig. 6.7.2 DB9 RS-232 Pinouts

6.7.1 Connecting NetGuardian Accessories

Some NetGuardian accessories must be connected to particular data ports. However, if you don't use these accessories, the data ports are available for other uses.

If you are using a NetGuardian Expansion, connect it to Port 7. If you are using a General LCD Display (GLD) unit, connect it to Port 8.

6.8   Integrated 10BaseT Ethernet Hub (Optional)
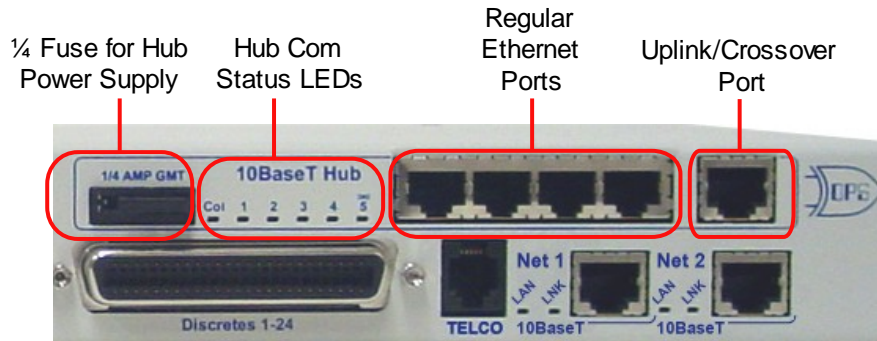
Fig. 6.8.1. NetGuardian integrated Ethernet Hub

You can order your NetGuardian 832A with an optional integrated Ethernet hub, which provides four regular Ethernet ports and one uplink or crossover Ethernet port. (See Figure 6.8.1.). The integrated Ethernet hub is powered by the same –48 VDC power as the NetGuardian, which provides more secure, more robust operation than hubs that run off commercial power. The integrated hub also frees valuable rack space by eliminating an unnecessary extra unit.

To power and activate the integrated Ethernet hub, insert the provided 1/4 amp fuse in the hub's fuse socket. (See Figure 6.8.1.) If you ever want to turn off power to the integrated hub, just remove the fuse.

RJ45 Ethernet Connection

8
7
6 Trasmit Out – (TO–)
5
4
3 Transmit Out + (TO+)
2 Receive In – (RI–)
1 Receive In + (RI+)
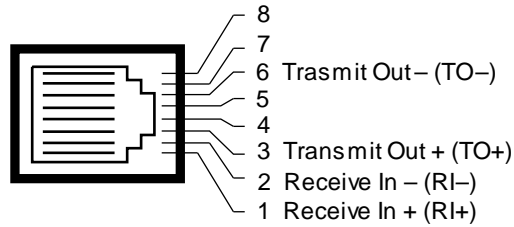
Fig. 6.8.2. Regular Ethernet port pinout

The four Ethernet ports grouped to the left of the hub are regular straight-through Ethernet ports. (See Figure 6.8.1.) The pinout for the regular Ethernet ports is shown in Figure 6.8.2, above.

RJ45 Ethernet Connection

8
7
6 Receive In– (RI–)
5
4
3 Receive In + (RI+)
2 Transmit Out– (TO–)
1 Transmit Out + (TO+)
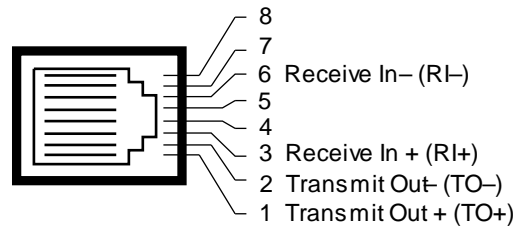
Fig. 6.8.3. Uplink/crossover Ethernet port pinout

The fifth Ethernet port, which is placed separately from the other four on the right, is an uplink/crossover Ethernet port. (See Figure 6.8.1.) This port allows you to connect the NetGuardian integrated hub to other Ethernet hubs without using a crossover cable. The pinout for the uplink/crossover port is shown in Figure 6.8.3, above.

6.9   +12 VDC Sensor Power Supply

***Fig. 6.9.1.** +12 VDC sensor power supply*

You can order your NetGuardian 832A with an optional +12 VDC sensor power supply. (See Figure 6.9.1.) This provides a convenient way to connect an auxiliary sensor to a robust battery power supply.

The two-pin connector for the sensor power supply is a barrier plug connector similar to the main power connector.

To power an external sensor, follow these steps:

1. Remove the 1/4 amp fuse from the sensor power supply on the back panel of the NetGuardian. (See Figure 6.9.1.) **Do not reinsert the fuse until all power connections to the external sensor have been made.**

2. Remove the power connector plug from the sensor power supply. Note that the plug can be inserted into the power connector only one way — this ensures that the barrier plug can only be reinserted with the correct polarity. Note that the **positive terminal is on the left** and the **negative terminal is on the right**.

3. Connect the appropriate leads to each of the plug's screw terminals and tighten the screws.

4. Push the power connector plug firmly back into the sensor power supply connector.

5. Reinsert the fuse to power the external sensor.

6.10 Optional 66 Block Connector

Both of the 50-pin connectors on the back panel of the NetGuardian can be connected to the optional 25-pair 66 Block Connector (part number D-PR-966-10A-00). For 66 block pinout and color code information, see Figure 6.10.1 for Discretes 1–24 and Figure 6.10.2. for Analogs 1–6/Discretes 25–32/Relays 1–8.

Note: If connecting to a 50-pair split block, all connections should be made on the two pin columns closest to the right-hand side of the block or bridge clips should be installed.

Wire color (wire/stripe)	Connection	66 Block Pair #	Corresponding 50-Pin Connector Pin #
WHT/BLU	ALM 1	1	26
BLU/WHT	RTN 1		1
WHT/ORG	ALM 2	2	27
ORG/WHT	RTN 2		2
WHT/GRN	ALM 3	3	28
GRN/WHT	RTN 3		3
WHT/BRN	ALM 4	4	29
BRN/WHT	RTN 4		4
WHT/GRY	ALM 5	5	30
GRY/WHT	RTN 5		5
RED/BLU	ALM 6	6	31
BLU/RED	RTN 6		6
RED/ORG	ALM 7	7	32
ORG/RED	RTN 7		7
RED/GRN	ALM 8	8	33
GRN/RED	RTN 8		8
RED/BRN	ALM 9	9	34
BRN/RED	RTN 9		9
RED/GRY	ALM 10	10	35
GRY/RED	RTN 10		10
BLK/BLU	ALM 11	11	36
BLU/BLK	RTN 11		11
BLK/ORG	ALM 12	12	37
ORG/BLK	RTN 12		12
BLK/GRN	ALM 13	13	38
GRN/BLK	RTN 13		13
BLK/BRN	ALM 14	14	39
BRN/BLK	RTN 14		14
BLK/GRY	ALM 15	15	40
GRY/BLK	RTN 15		15
YEL/BLU	ALM 16	16	41
BLU/YEL	RTN 16		16
YEL/ORG	ALM 17	17	42
ORG/YEL	RTN 17		17
YEL/GRN	ALM 18	18	43
GRN/YEL	RTN 18		18
YEL/BRN	ALM 19	19	44
BRN/YEL	RTN 19		19
YEL/GRY	ALM 20	20	45
GRY/YEL	RTN 20		20
VIO/BLU	ALM 21	21	46
BLU/VIO	RTN 21		21
VIO/ORG	ALM 22	22	47
ORG/VIO	RTN 22		22
VIO/GRN	ALM 23	23	48
GRN/VIO	RTN 23		23
VIO/BRN	ALM 24	24	49
BRN/VIO	RTN 24		24
VIO/GRY	GND	25	50
GRY/VIO	GND		25

Fig 6.10.1. Optional 66 block pinout for Discretes 1–24

Wire color (wire/stripe)	Connection	66 Block Pair #	Corresponding 50-Pin Connector Pin #
WHT/BLU	ALM 25	1	26
BLU/WHT	RTN 25		1
WHT/ORG	ALM 26	2	27
ORG/WHT	RTN 26		2
WHT/GRN	ALM 27	3	28
GRN/WHT	RTN 27		3
WHT/BRN	ALM 28	4	29
BRN/WHT	RTN 28		4
WHT/GRY	ALM 29	5	30
GRY/WHT	RTN 29		5
RED/BLU	ALM 30	6	31
BLU/RED	RTN 30		6
RED/ORG	ALM 31	7	32
ORG/RED	RTN 31		7
RED/GRN	ALM 32	8	33
GRN/RED	RTN 32		8
RED/BRN	CTRL 1 NO	9	34
BRN/RED	CTRL 1 CO		9
RED/GRY	CTRL 2 NO	10	35
GRY/RED	CTRL 2 CO		10
BLK/BLU	CTRL 3 NO	11	36
BLU/BLK	CTRL 3 CO		11
BLK/ORG	CTRL 4 NO	12	37
ORG/BLK	CTRL 4 CO		12
BLK/GRN	CTRL 5 NO	13	38
GRN/BLK	CTRL 5 CO		13
BLK/BRN	CTRL 6 NO	14	39
BRN/BLK	CTRL 6 CO		14
BLK/GRY	CTRL 7 NO	15	40
GRY/BLK	CTRL 7 CO		15
YEL/BLU	CTRL 8 NO	16	41
BLU/YEL	CTRL 8 CO		16
YEL/ORG	FA NO	17	42
ORG/YEL	FA CO		17
YEL/GRN	Unused	18	43
GRN/YEL	Unused		18
YEL/BRN	ANA 1 –	19	44
BRN/YEL	ANA 1 +		19
YEL/GRY	ANA 2 –	20	45
GRY/YEL	ANA 2 +		20
VIO/BLU	ANA 3 –	21	46
BLU/VIO	ANA 3 +		21
VIO/ORG	ANA 4 –	22	47
ORG/VIO	ANA 4 +		22
VIO/GRN	ANA 5 –	23	48
GRN/VIO	ANA 5 +		23
VIO/BRN	ANA 6 –	24	49
BRN/VIO	ANA 6 +		24
VIO/GRY	GND	25	50
GRY/VIO	GND		25

Fig. 6.10.2. Optional 66 block pinout for Analogs 1–8/Discretes 25–32/Relays 1–8

6.11 Optional Hinged Wire-Wrap Back Panel

Turn the plastic sw ivel
to the vertical position
to lock in place

Fig. 6.11.1. *The hinged wire-wrap back panel is mounted on the mounting rack of the NetGuardian*

The optional hinged wire-wrap back panel provides wire-wrap connections for the NetGuardian's alarms and control relays. To connect alarms and control relays to the wire-wrap panel, follow these steps:

1. Mount the hinged wire-wrap back panel on the mounting rack of the NetGuardian. (See Figure 6.11.1.)

2. Close the hinged back panel and lock in place by turning the black plastic locking swivel to the vertical position.

3. Connect discrete alarms, analog alarms, and control relays to the two pin blocks. Figures 6.11.2 and Figure 6.11.3 show the pinouts for the wire-wrap back panel.
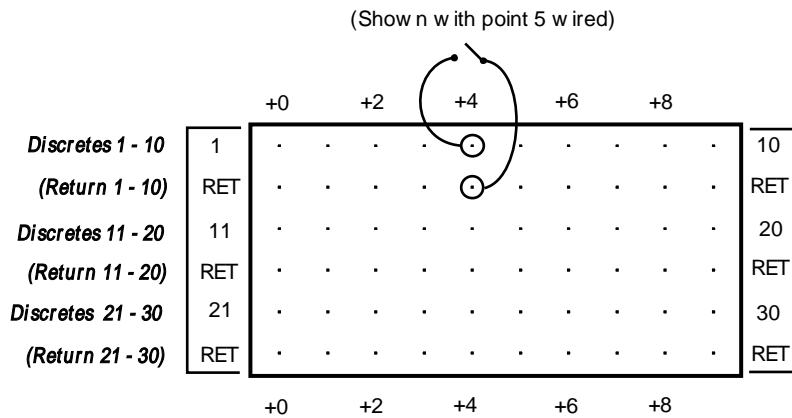
Fig. 6.11.2. *Wire-wrap pinouts for Discretes 1–30*
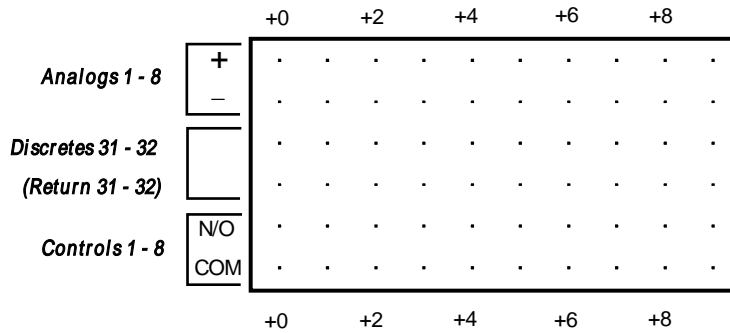
Fig. 6.11.3. *Wire-wrap pinouts for Discretes 31–32, Analogs 1–8, and Controls 1–8*

6.11.1 Lexan Wire-Wrap Cover
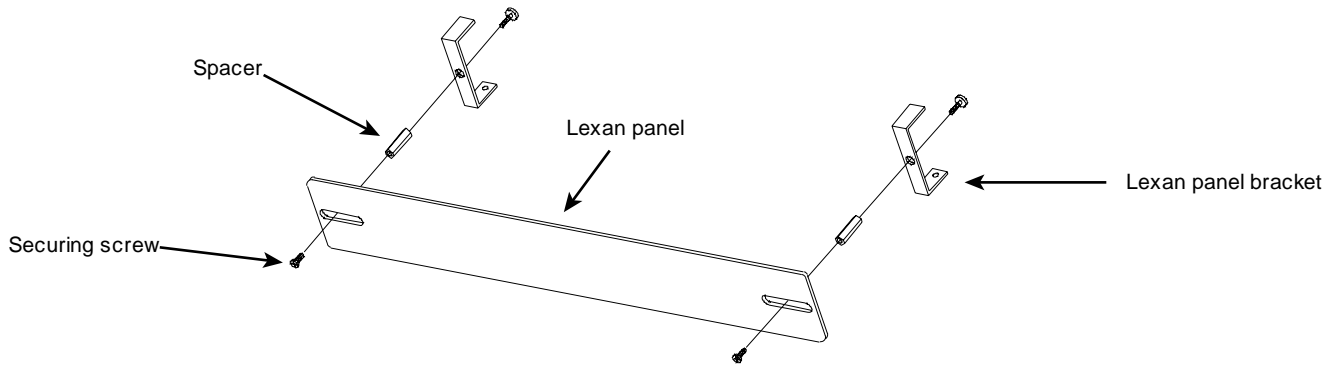
Fig. 6.11.1.1. Lexan panel assembly

To attach the Lexan cover to the hinged wire-wrap panel, follow these steps:

1. Attach communication lines to the wire-wrap pins before connecting the Lexan cover

2. Attach the Lexan cover to the mounting clips and connect to the hinged panel. (See Figure 6.11.1.1.)

6.12 Jumper Options
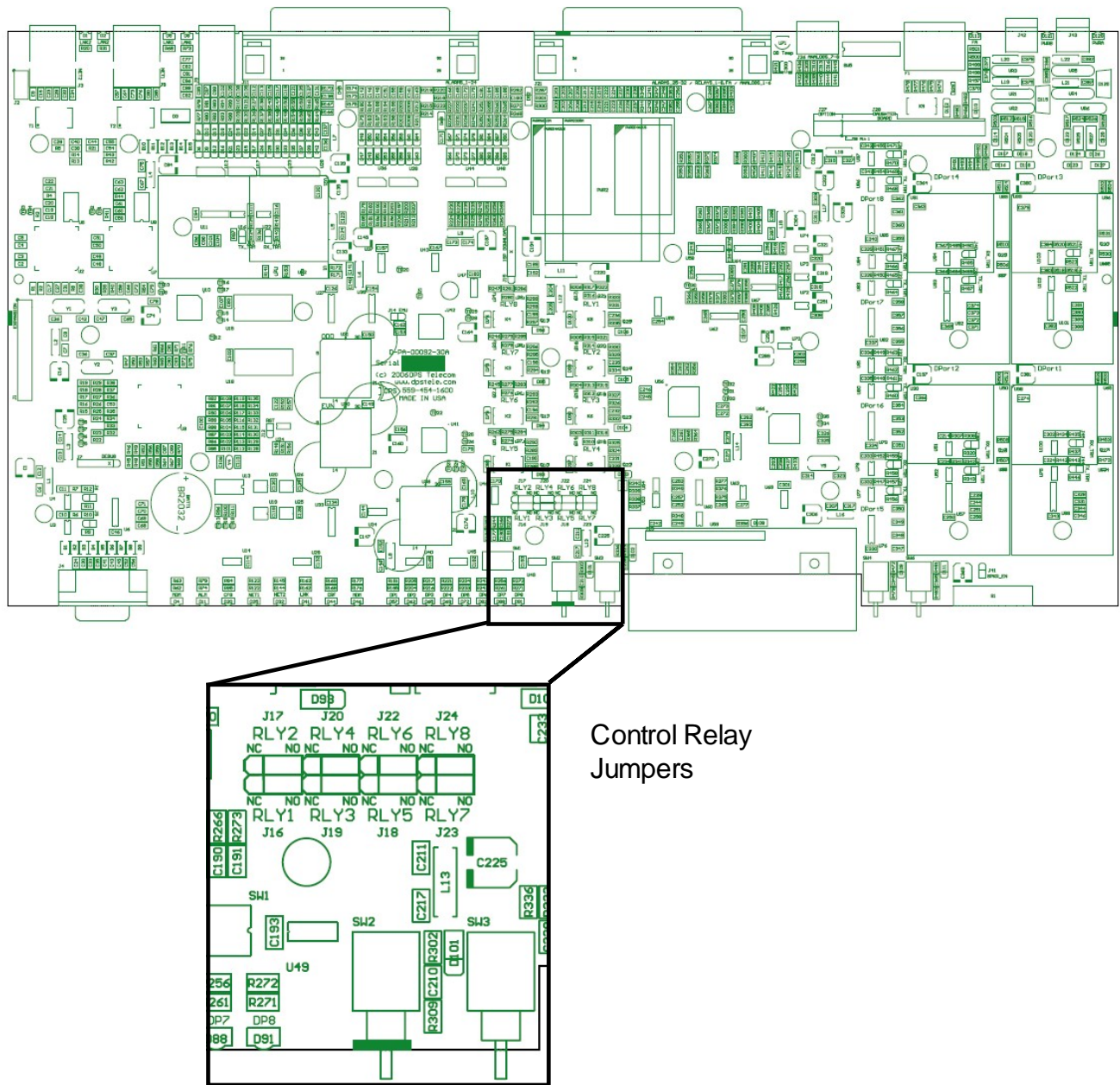
Fig. 6.12.1. *Adjustable jumpers on the NetGuardian circuit board*

The following options are adjusted by resetting jumpers on the NetGuardian's circuit board:

- Control relays can be switched from normally open (N/O) to normally closed (N/C)

To open the unit and expose the circuit board, remove the screws from the top of the NetGuardian and lift the top cover off. Figure 6.12.1 shows the circuit board and the location of the adjustable jumpers.

WARNING: Always observe anti-static precautions whenever opening the unit.

Control Point Detail
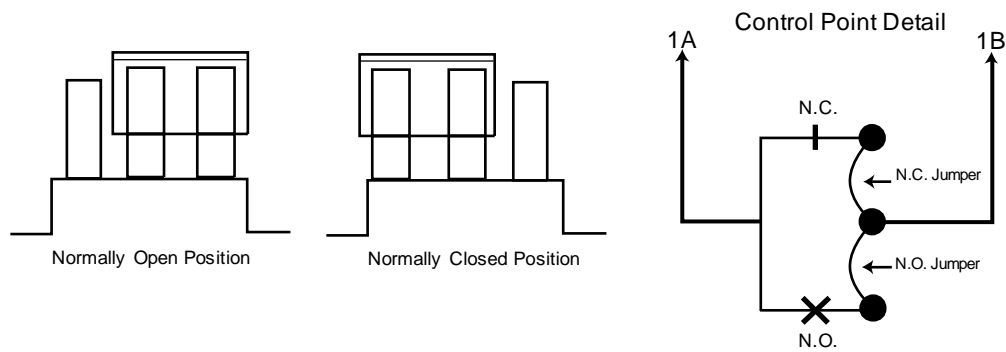
Fig. 6.12.2. Jumper settings for analog alarm inputs and control relays

By default, all the adjustable jumpers are open, except for the speaker jumper. For control relay jumpers, the open position corresponds to normally open operation, and the closed position corresponds to normally closed operation. See Figure 6.12.2. and Refer to Table 6.12.A for default jumper settings and descriptions.

Note: Default settings may be different if you ordered a special configuration NetGuardian.

Jumper	Description
J16 / RLY1	Control Relay 1
J17 / RLY2	Control Relay 2
J19 / RLY3	Control Relay 3
J20 / RLY4	Control Relay 4
J18 / RLY5	Control Relay 5
J22 / RLY6	Control Relay 6
J23 / RLY7	Control Relay 7
J24 / RLY8	Control Relay 8

Table 6.12.A. Jumper descriptions and settings

7 LCD Display

Fig. 7.1. NetGuardian LCD showing the Standard Prompt

The front panel LCD displays the current alarm and control status and provides a command menu for controlling the NetGuardian's basic functions.

Using the LCD command menu
The four buttons surrounding the front panel LCD are used to access the LCD Command Menu. To access the menu, press the Menu button. To scroll the menu, use the q and p buttons. To select a menu command, press the Sel (Select) button.

Standard Prompt

When no Command Menu item is selected and no alarms or relays are active, the LCD displays the firmware version and the standard prompt, Press MENU for front panel options.

Controlling Display Speed
The scroll speed can be temporarily increased by pressing and holding the p button while the message is active.

7.1   Alarm and Control Status Messages

If an alarm or control relay is active, the LCD will display the following messages to indicate alarm and control status:

The LCD panel will display the following messages to indicate alarm and control status:

Discrete Alarms:	If there are any standing discrete alarms, the display will read "Discrete Alarms:", followed by the user-defined descriptions of the standing alarm points.
Relays:	If there are any latched relays, the display will read "Relays:", followed by the user-defined descriptions of the latched relays.
Ping Alarms:	If any ping targets have failed to respond within the specified time, the display will read "Ping Alarms:", followed by the user-defined descriptions of the ping targets.
Analogs:	If any analog channels have crossed a threshold value, the display will read "Analogs", followed by the user-defined description of the analog channel, the channel's last voltage reading, and a letter indicating which threshold the channel has crossed.

Analog thresholds are represented by the following characters:

Major Over: a capital O
Minor Over: a lower-case o
Minor Under: a lower-case u
Major Under: a capital U

7.2   LCD Command Menu
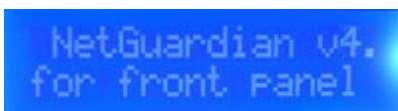
Fig. 7.3.1. LCD display, showing the Standard Prompt

The LCD Command Menu provides commands for controlling some of the NetGuardian's basic functions: temporarily silencing the alarm speaker, rebooting the unit, and running the TTY configuration utility.

When no Command Menu item is selected and no alarms or relays are active, the LCD displays the firmware version and the Standard Prompt, Press MENU for front panel options. (See Figure 7.3.1, above.)

To access the Command Menu, press the Menu button.

7.2.1 Sound off
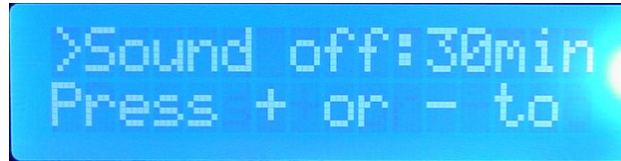
Fig. 7.3.1.1. Sound Off command

Sound off
The Sound off command suppresses sounds from the alarm speaker for a user-defined period of 10, 20, or 30 minutes.

To scroll to the next menu command, press the q button.

To change the Sound off setting, press Sel to select the command. The arrow cursor (>) will move to the right of the colon (:) in Sound off: to indicate that the command submenu is selected. Press the q and p buttons to scroll through the Sound off time period options. Select 0 minutes to allow all sounds. When the time period you want is displayed, press Sel to make your selection.

To exit the Command Menu without changing the Sound off setting, press Menu.

7.2.2 Reboot
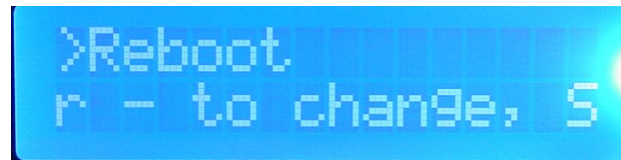
Fig. 7.3.2.1. Reboot command

Reboot
The Reboot command reboots the NetGuardian.

To scroll to the next menu command, press the q button.

To reboot the NetGuardian, press Sel. The LCD will briefly display the message Rebooting ..., and the normal boot sequence will begin.

To exit the Command Menu without rebooting, press Menu.

7.2.3 Run Config

Fig. 7.3.3.1. *Run Config command*

Run Config
The Run Config command forces the TTY configuration interface to run over the craft port at the user defined baud rate (default is 9600 baud).

To scroll to the next menu command, press the q button.

To run the TTY configuration utility, press Sel.

To exit the Command Menu without running the TTY interface, press Menu.

7.2.4 Contrast

Fig. 7.3.4.1. *Contrast command*

Contrast
The **Contrast** command provides controls for adjusting the contrast of the LCD.

To scroll to the next menu command, press the – button.

To adjust the contrast, press Sel to select the command. The arrow cursor (>) will move to the right of the colon (:) in Contrast: to indicate that the command submenu is selected. Press the q or p button until you're satisfied with the contrast setting, then press Sel to make your selection.

To exit the Command Menu and **revert to the default contrast setting**, press Menu.

8 Alarm Speaker

The NetGuardian's alarm speaker emits distinctive tones under two conditions

1. **If there is an Ethernet connection failure,** the speaker will emit a **high-low warbling tone.** Press any front panel button to silence the speaker.

2. **If an alarm occurs,** the speaker will emit an **intermittent beep**. Press any front panel button to silence the speaker. If you do not silence the speaker, the beep will continue for the user defined duration (default is a 6 second duration). Silencing the speaker will allow the next alarm, if any, to sound.

9 Front Panel LEDs
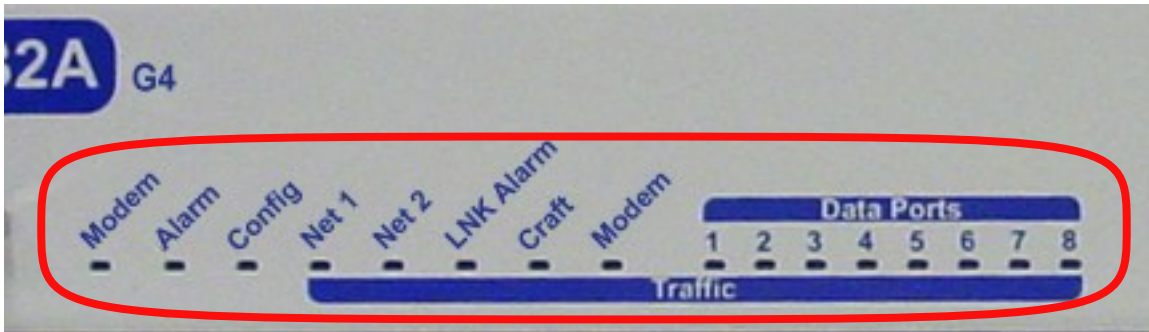
Fig. 9.1. *Front panel LEDs*

The NetGuardian's front panel LEDs indicate communication and alarm reporting status. LED status messages are described below in Table 9.A.

LED	Status	Description
Modem	Solid Red	Modem Initializing or in use
Alarm	Blink Red	New COS alarm*
	Solid Red	One or more standing alarms*
Config	Blink Green	Valid configuration
	Blink Red	Invalid configuration
Net 1	Blink Green	Transmit over Ethernet port 1
	Blink Red	Receive over Ethernet port 1
Net 2	Blink Green	Transmit over Ethernet port 2
	Blink Red	Receive over Ethernet port 2
LNK Alarm	Solid Red	No Ethernet link detected (for configured Net 1 or Net 2)
Craft	Blink Green	Transmit over craft port
	Blink Red	Receive over craft port
Modem	Blink Green	Transmit over Modem port
	Blink Red	Receive over Modem port
Data Ports 1-8	Blink Green	Transmit over indicated data port
	Blink Red	Receive over indicated data port

*NOTE: Alarm must be configured for notification to be reflected in LED

Table 9.A. *Front panel LED Status message descriptions*

10 Back Panel LEDs
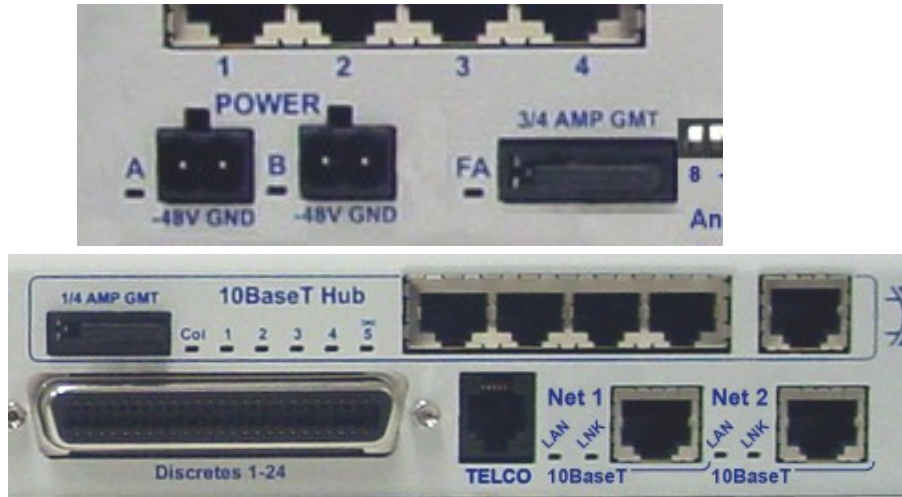
Fig. 10.1. Back panel LEDs for Power (left) and Ethernet connections

The back panel LEDs indicate the status of power and Ethernet connections. LED status messages are described below in Table 10.A.

	LED	Status	Description
Power	Power A	Solid Green	Polarity is correct on power feed A
		Solid Red	Polarity is reversed on power feed A
	Power B	Solid Green	Polarity is correct on power feed B
		Solid Red	Polarity is reversed on power feed B
	FA	Solid Red	Fuse failure
10BaseT Net	LAN	Blink Green	Transmit and receive activity over Ethernet port
	LNK	Solid Green	Ethernet link OK
10BaseT HUB	Col	Blink Green	One or more of the Ethernet Hub ports are active.
	1-5	Blink Green	Transmit over indicated integrated Ethernet Hub port
		Blink Red	Receive over indicated Ethernet Hub port

Table 10.A. Back panel LED Status message descriptions

11 Configuring the NetGuardian

The NetGuardian must be provisioned with log-on passwords, alarm descriptions, port parameters, ping targets, control descriptions, and other system information. You can provision the NetGuardian using either the NGEdit4 software or the Web interface. The NetGuardian also supports a limited TTY interface for configuring some basic options. (For full instructions on configuring the NetGuardian, see the software configuration guides on the NetGuardian Resource CD.)

You can provision the NetGuardian either locally through the craft port or remotely through a LAN connection. However, to access the NetGuardian via LAN you must first make a temporary connection to the NetGuardian and assign it an IP address on your network. For more information, see Section 12, "Connecting to the NetGuardian."

12 Connecting to the NetGuardian

12.1 ... via Craft Port

Fig. 12.1.1. *NetGuardian Craft Port*

The simplest way to connect to the NetGuardian is over a physical cable connection between your PC's COM port and the NetGuardian's craft port.

Note: You must be connected via craft port to use the TTY interface, but you don't have to be connected to a NetGuardian unit to use NGEdit4. You only need a connection to the unit to read or write configuration files to its NVRAM. You can use NGEdit4 on an unconnected PC to create and store NetGuardian configuration files.

Use the DB9M-DB9F download cable provided with your NetGuardian to make a craft port connection.

Select the following COM port options:
• Bits per second: 9600
• Data bits: 8
• Parity: None
• Stop bits: 1
• Flow control: **None**

When a connection is established (sometimes accompanied by receipt of a hex byte), type DPSCFG, then press Enter to activate the configuration menu.

You can perform all configuration tasks via the craft port — but if you like, you can connect via the craft port just to configure the NetGuardian's Private LAN IP address, and then do the rest of your configuration via a LAN connection.

12.2 ... via LAN

Fig. 3.2.1. **Ethernet port 1**

You can also connect to the NetGuardian over a LAN connection. This is a very convenient way to provision multiple NetGuardian units at multiple locations. **Note:** You don't have to be connected to a NetGuardian unit to use NGEdit4. You only need a connection to the unit to read or write configuration files to its NVRAM. You can use NGEdit4 on an unconnected PC to create and store NetGuardian configuration files.

To connect to the NetGuardian via LAN, all you need is the unit's IP address (Default IP address is 192.168.1.100).

If you have physical access to the NetGuardian, the easiest thing to do is connect to the unit through the craft port and then assign it an IP address. Then you can complete the rest of the unit configuration over a remote LAN connection, if you want. For instructions, see Section 12.1, "Connecting to the NetGuardian via Craft Port."

If you DON'T have physical access to the NetGuardian, you can make a LAN connection to the unit by temporarily changing your PC's IP address and subnet mask to match the NetGuardian's factory default IP settings. Follow these steps:

1. Look up your PC's current IP address and subnet mask, and write this information down.

2. Reset your PC's IP address to **192.168.1.200**.

3. Reset your PC's subnet mask to **255.255.0.0**. You may have to reboot your PC to apply your changes.

4. Once the IP address and subnet mask of your computer coincide with the NetGuardian's, you can access the NetGuardian via a Telnet session or via Web browser by using the NetGuardian's default IP address of **192.168.1.100**.

5. Provision the NetGuardian with the appropriate information, then change your computer's IP address and subnet mask back to their original settings.

13 TTY Interface
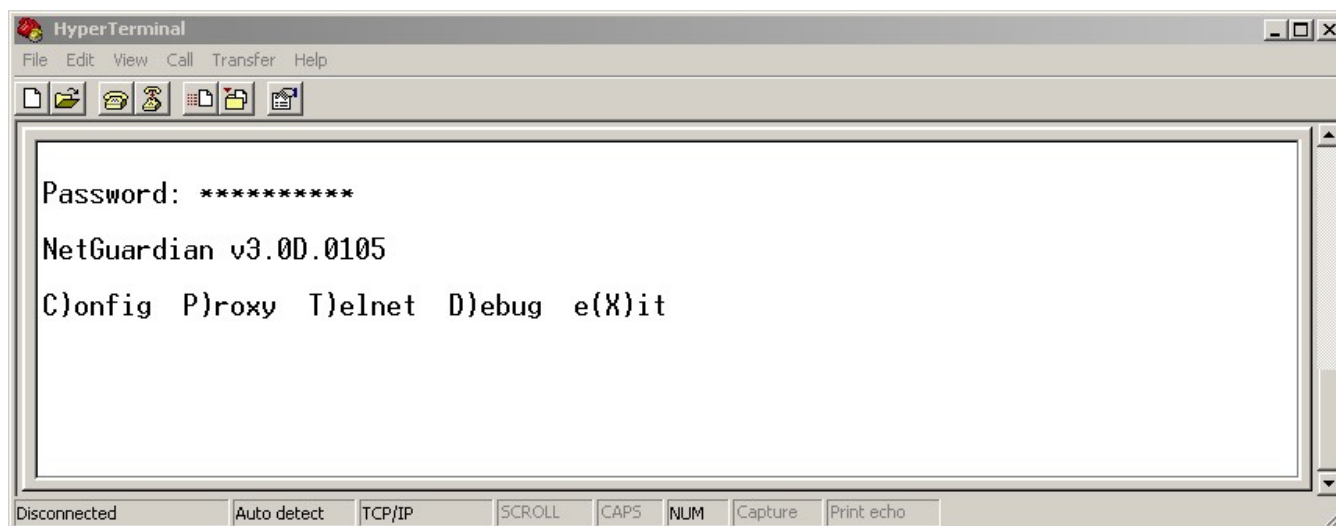
Fig. 13.1. The TTY interface initial configuration screen

The TTY interface is the NetGuardian's built-in provision controls for basic configuration of the NetGuardian. Configure the NetGuardian's ethernet port settings, monitor the status of base and system alarms, operate control relays, view live ping targets , view debug or create proxy connections to other ports. For more advanced configuration tools, please use the Web Browser Interface or the NGEdit4 utility.

To use the TTY interface with the NetGuardian, all you need is any PC with terminal emulation software (i.e. Hyperterminal) and a connection to the NetGuardian. This connection can be a direct connection to the

NetGuardian's front panel craft port or a remote connection via Telnet or dial-up

Some initial software configuration must be performed before you can use a remote connection to the NetGuardian. For Telnet, connect to the Net Guardian's IP address at port 2002 to access the configuration menus after initial LAN/WAN setup. **Telnet sessions are established at port 2002, not the standard Telnet port** as an added security measure.

The TTY interface is primarily used for configuring and provisioning the NetGuardian, but you can also use it to ping IP targets, view system statistics, and data port activity.

NOTE: The TTY default password is "dpstelecom".

13.1 Menu Shortcut Keys

The letters before or enclosed in parentheses ( ) are menu shortcut keys. Press the shortcut key to access that option. Pressing the ESC key will always bring you back to the previous level. Entries are not case sensitive.

13.2 Net Lockdown Mode

The NetGuardian 832A G4 features a new mode called **Net Lockdown**. If this mode is enabled, the NetGuardian will discard any/all LAN packets you choose. (*Ex*. If your NetGuardian is being polled by a T/Mon NOC over UDP, and you would like block access to your NetGuardian web browser, you can enable a Net Lockdown of all HTTP traffic, which will still allow UDP traffic but block all HTTP packets.) This is an option you can implement remotely using NGEdit that will provide instant security.

You can only enable **Net Lockdown** mode from NGEditG4. Once enabled, it will take effect after a reboot. Please refer to the **'Net Lockdown'** section in the NGEditG4 User Manual for instructions on how to enable this feature.

Once enabled, a user will be able to lock down any/all of the following protocols:

- TCP (HTTP, FTP, Telnet, Proxy access)
- UDP (T/Mon, SNMP)
- ICMP (Ping)
- IGMP (Online Video)
- ARP (Address Resolution)

- HTTP (Web)
- SNMP (SNMP Master receiving traps)
- FTP (File Transfer)
- Telnet (Terminal access)
- DCP (over LAN)

Note: Locking down the TCP protocol will effectively block the HTTP, FTP and Telnet protocols

Unchecking the **Enable** box in the Net Lockdown Mode section will put the NetGuardian in a normal state (i.e. no restrictions), and Net Lockdown flags will not be enabled.
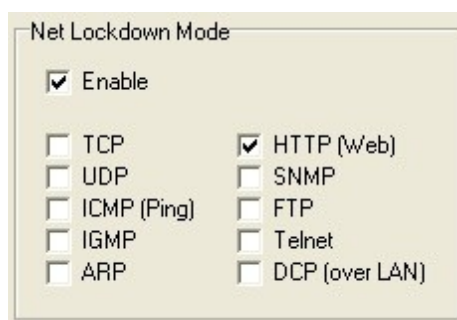
TTY will also allow you to disable the Net Lockdown function.When you select the **N)et Lockdown** option, it will be disabled once you save the changes and reboot. This feature is useful to undo any lockdown changes you might have made through NGEdit that may now prevent you from communicating with the NetGuardian remotely- such as through Telnet, FTP, or the web browser.

Keep in mind that all **Net Lockdown** features will be disabled with this option. If you need to remove certain features and keep existing ones, you will need to re-input the options you want to keep using NGEditG4.

13.3 Tune 202 Modem

Tuning the 202 modem on a NetGuardian G5 can only be done from the TTY interface (using either HyperTerminal through the front craft port or by telnet over LAN on port 2002).
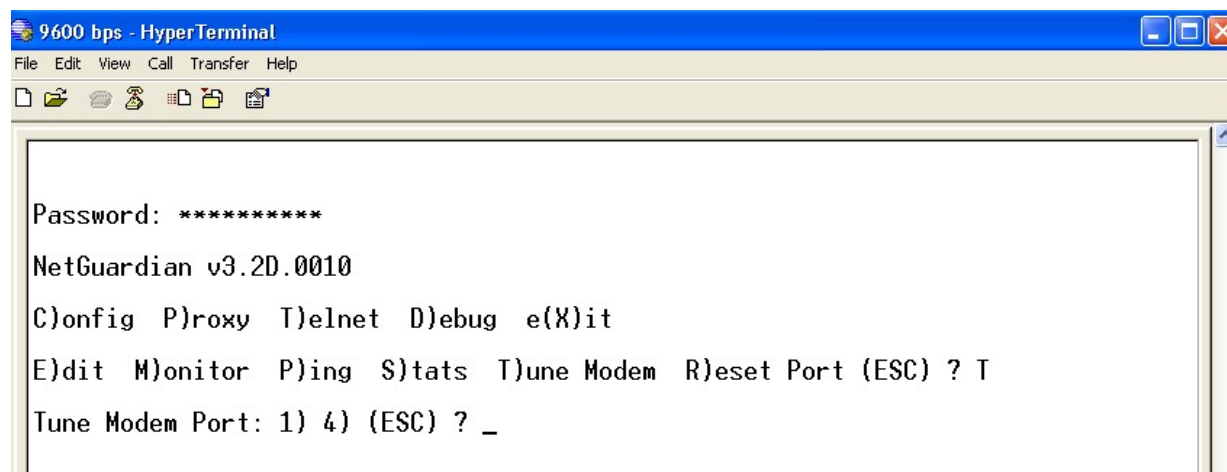
Fig. 13.1.4. *Press 'T' to tune the 202 Modem with the TTY interface*

Though no menu options will appear, use the following commands to tune the 202 modem. Each menu option, when chosen, will output the character "A" on screen:

1) Minor Adjust DB+
2) Minor Adjust DB-
3) High Frequency
4) Low Frequency
5) Off
6) Major Adjust DB-
7) Major Adjust DB+
8) Median Frequency (Average of high and low frequency)

After selecting an option (like #1 in this example) for Minor Adjust the DB+ level, the NetGuardian will return a

'+' command to inform you the task is completed. Each time you hit a number key (1-8), the NetGuardian will a

'+' on your screen.

13.4 Unit Configuration

13.4.1 Ethernet Port Setup

The NetGuardian must be assigned an IP address before you will be able to connect via LAN/WAN using a Telnet client or a Web browser. To connect via LAN, the minimum configuration requires setup of the IP address and subnet mask. Minimum WAN configuration requires that the default gateway be set as well. Follow the instructions below to configure the NetGuardian's IP address, subnet mask, default gateway, trap address, SNMP port number, proxy base, and DCHP option.

```
Password: **********

NetGuardian-G4 v4.1B.0411

C)onfig  P)roxy  T)elnet  D)ebug  e(X)it

E)dit  M)onitor  P)ing  S)tats  T)une Modem  R)eset Port (ESC) ? E

NET(1)  NET(2)  n(U)ram  P)PP  D)ate/time  R)eboot  s(Y)stem (ESC) ? 1

Net 1 Interface

Unit Address    : 126.010.210.192 (126.010.210.192)
Subnet Mask     : 255.255.192.000 (255.255.192.000)
Default Gateway : 126.010.220.254 (126.010.220.254)
IP Filter       : Disabled

MAC Address     : 00.10.81.00.15.AA
Features        : AAA9-25-B995

U)nit Address  S)ubnet Mask  G)ateway  I)P Filter  F)eatures (ESC) ? <--

NET(1)  NET(2)  n(U)ram  P)PP  D)ate/time  R)eboot  s(Y)stem (ESC) ? 2

Net 2 Interface

Unit Address    : 255.255.255.255 (000.000.000.000)
Subnet Mask     : 255.255.000.000 (000.000.000.000)
Default Gateway : 255.255.255.255 (000.000.000.000)
IP Filter       : Disabled

MAC Address     : 00.10.81.00.15.AB

U)nit Address  S)ubnet Mask  G)ateway (ESC) ?
```

Fig. 13.2.1.1. *Configure the Ethernet port parameters*

1. Once a connection is established, the NetGuardian will respond with "Password."

2. Type the default password, "dpstelecom," then press Enter.

    Note: DPS strongly recommends changing the default password.

3. The NetGuardian's main menu will appear.

4. Type C for the C)onfig menu.

5. Type E for E)dit menu.

6. Type E for port settings, 1 for Net 1 and 2 for Net 2.

7. Configure the unit address, subnet mask, and default gateway.

8. ESC to the main menu.

9. When asked if you would like to save changes, type Y (yes).

10. Reboot to save the new configuration to the NetGuardian.

11. Now you can connect to the NetGuardian via LAN and complete the configuration.

13.4.2 Edit PPP Port

Choose P)PP to edit your PPP port in TTY Interface. You can choose a baud rate, depending on what device has been chose for the PPP port.

```
C)onfig  P)roxy  T)elnet  D)ebug  e(X)it

E)dit  M)onitor  P)ing  S)tats  T)une Modem  R)eset Port (ESC) ? E

E)thernet  n(V)ram  P)PP  R)eboot  s(Y)stem (ESC) ? P

Configuration
     Port        : Data1
     Baud        : 9600
     Compression : Yes

Client
     Mode        : onDemand
     Phone       :
     Username    :
     Password    :

Server
     Server      : Disabled
     Address     : 255.255.255.255 (Client Specified)

P)ort  B)aud  mo(D)em  C)ompression  M)ode
  p(H)one  U)sername  pass(W)ord  S)erver  A)ddress  B)aud  mo(D)em (ESC) ?
```

Fig. 13.2.2.1 *Edit your PPP port*

If you are using a modem for the PPP port, then choose mo(D)em for the modem option to define the modem initialization strings (see Figure 10.4).

Choose B)aud to define the baud rate for that port. (See Figure 13.2.2.2.)

```
Client
     Mode        : onDemand
     Phone       :
     Username    :
     Password    :

Server
     Server      : Disabled
     Address     : 255.255.255.255 (Client Specified)

P)ort  B)aud  mo(D)em  C)ompression  M)ode
  p(H)one  U)sername  pass(W)ord  S)erver  A)ddress  B)aud  mo(D)em (ESC) ? B

3)00  6)00  1)200  2)400  4)800  9)600  a)19200  b)38400 (ESC) ?
```

13.5 Monitoring

13.5.1 Monitoring the NetGuardian

Connect a PC running VT100 terminal emulation software to the craft port or connect via LAN using a Telnet client with VT100 emulation to port 2002 to reach the monitor menu selection. This section allows you to do full system monitoring of the NetGuardian including: all alarms, ping information, relays, analogs, and system status.

```
C)onfig  P)roxy  T)elnet  D)ebug  e(X)it

E)dit  M)onitor  P)ing  S)tats  T)une Modem  R)eset Port (ESC) ? M

A)larms  R)elays  a(N)alogs  E)vent log  a(C)cum. Timer
  B)AC  P)ing targets  p(O)rts  S)ystem (ESC) ?
```

Fig. 13.3.1.1. The monitor menu allows status checking on all elements

13.5.1.1 Monitoring Base Alarms

View the status of the device connected to the discrete alarms from the M)onitor menu > A)larms option. Under Status, the word Alarm will appear if an alarm has been activated and Clear will appear if an alarm condition is not present. If groups are used the user defined status will be displayed.

```
A)larms  R)elays  a(N)alogs  E)vent log  a(C)cum. Timer
  B)AC  P)ing targets  p(O)rts  S)ystem (ESC) ? A
B)ase  E)xpansions (ESC) ? B

 ID Description                              Status
  1                                          Clear
  2                                          Clear
  3                                          Clear
  4                                          Clear
  5                                          Clear
  6                                          Clear
  7                                          Clear
  8                                          Clear
  9                                          Clear
 10                                          Clear
 11                                          Clear
 12                                          Clear
 13                                          Clear
 14                                          Clear
 15                                          Clear
 16                                          Clear
ESC to exit  Any key to continue
```

Fig. 13.3.1.1.1. This example shows page two of the discrete alarms

13.5.1.2 Monitoring Ping Targets

View the status of all your ping targets from the M)onitor menu > P)ing targets option. This screen displays the ping target ID, description, and IP address. Under Status the word Alarm will appear if an alarm has been activated and Clear will appear if an alarm condition is not present.

```
B)ase  E)xpansions (ESC) ? <--

A)larms  R)elays  a(N)alogs  E)vent log  a(C)cum. Timer
  B)AC  P)ing targets  p(O)rts  S)ystem (ESC) ? P

 ID Description                                      IP Address      Status
  1                                                  255.255.255.255 Clear
  2                                                  255.255.255.255 Clear
  3                                                  255.255.255.255 Clear
  4                                                  255.255.255.255 Clear
  5                                                  255.255.255.255 Clear
  6                                                  255.255.255.255 Clear
  7                                                  255.255.255.255 Clear
  8                                                  255.255.255.255 Clear
  9                                                  255.255.255.255 Clear
 10                                                  255.255.255.255 Clear
 11                                                  255.255.255.255 Clear
 12                                                  255.255.255.255 Clear
 13                                                  255.255.255.255 Clear
 14                                                  255.255.255.255 Clear
 15                                                  255.255.255.255 Clear
 16                                                  255.255.255.255 Clear
ESC to exit  Any key to continue
```

Fig. 13.3.1.2.1. *The Ping info submenu allows you to change ping targets*

13.5.1.3 Monitoring and Operating Relays (Controls)

The NetGuardian comes equipped with 8 relays that can be used to control external devices. Monitor the status of your relays from the M)onitor menu > R)elays option.

Relays are set to normally open (N/O) as the factory default, but each or all of them can be changed to normally closed (N/C) by changing their respective jumper (see Section 6.12, "Jumper Options").

```
A)larms  R)elays  a(N)alogs  E)vent log  a(C)cum. Timer
  B)AC  P)ing targets  p(O)rts  S)ystem (ESC) ? R

B)ase  E)xpansions (ESC) ? B

Base Relays

 ID Description                                    Mode     Status
  1                                                Normal   Rls
  2                                                Normal   Rls
  3                                                Normal   Rls
  4                                                Normal   Rls
  5                                                Normal   Rls
  6                                                Normal   Rls
  7                                                Normal   Rls
  8                                                Normal   Rls

S)tatus        O)pr  R)ls  M)om (ESC) ?
```

Fig. 13.3.1.3.1 *The eight relays can be operated from this screen*

13.5.1.4 Monitoring Analogs

View the current reading and the alarm status of your analog devices from the M)onitor menu > a(N)logs option. The value shown is a snapshot of the channels measurement, not a real-time reading. Refresh the readings by re-selecting the analogs option. Alarm status indicates that a preset threshold has been crossed and is designated by an X.

The eight analog measuring inputs are set to measure voltage as the factory default. If your sensors output is current, change the appropriate analog dip switch, to the current measuring position. The scaling worksheet in the provisioning section converts all readings shown here into native units, such as degrees Celsius or percent relative humidity.

```
A)larms  R)elays  a(N)alogs  E)vent log  a(C)cum. Timer
  B)AC  P)ing targets  p(O)rts  S)ystem (ESC) ? N

Chn Description                     Reading Units MjU  MnU  MnO  MjO  Err
  1                                 0.0000  VDC   -    -    -    -    -
  2                                 0.0000  VDC   -    -    -    -    -
  3                                 0.0000  VDC   -    -    -    -    -
  4                                 0.0000  VDC   -    -    -    -    -
  5                                 0.0000  VDC   -    -    -    -    -
  6                                 0.0000  VDC   -    -    -    -    -
  7                                 0.0000  VDC   -    -    -    -    -
  8                                 0.0000  VDC   -    -    -    -    -

A)larms  R)elays  a(N)alogs  E)vent log  a(C)cum. Timer
  B)AC  P)ing targets  p(O)rts  S)ystem (ESC) ?
```

Fig. 13.3.1.4.1. *This display allows you to monitor your eight analog inputs*

13.5.1.5 Monitoring System Alarms

View the status of the NetGuardian's system alarms from the M)onitor menu > S)ystem option. Under Status, the word Alarm will appear if an alarm has been activated and Clear will appear if an alarm condition is not present. See Appendix, "System Alarm Descriptions," for more information. If groups are used the user defined status will be displayed.

```
A)larms  R)elays  a(N)alogs  E)vent log  a(C)cum. Timer
  B)AC  P)ing targets  p(O)rts  S)ystem (ESC) ? S
 ID Description          Status
 17 Timed Tick           Clear
 18 Exp.Module Callout    Clear
 19 Network Time Server   Clear
 20 Accumulation Event    Clear
 33 Unit Reset            Clear
 36 Lost Provisioning     Clear
 37 DCP Poller Inactive   Clear
 38 LAN not Active        Clear
 41 Modem not Responding  Clear
 42 No Dialtone           Clear
 43 SNMP Trap not Sent    Clear
 44 Pager Que Overflow    Clear
 45 Notification Failed   Clear
 46 Craft RcvQ Full       Clear
 47 Modem RcvQ Full       Clear
 48 Data 1 RcvQ Full      Clear
ESC to exit  Any key to continue_
```

Fig. 13.3.1.5.1. System Alarms can be viewed from the M)onitor menu > S)ystem option

13.5.1.6 Monitoring Data Port Activity

View the status of the NetGuardian's 8 data ports from the M)onitor menu > p(O)rts option. Enter the number of the port you wish to view and press Enter.

The NetGuardian provides an ASCII description under Transmit and Receive. Choose a) Transmit to view data transmitted to another device. Choose b) Receive to view data received from another device. See Appendix, "ASCII Conversion," for specific ASCII symbol conversion.

```
A)larms  R)elays  a(N)alogs  E)vent log  a(C)cum. Timer
  B)AC  P)ing targets  p(O)rts  S)ystem (ESC) ? O

Data Port ID (1-8): 1

a)Transmit  b)Receive  c)Transmit-HEX  d)Receive-HEX (ESC) ?
```

Fig. 13.3.1.6.1. Data port activity can be viewed from the M)onitor menu > p(O)rts option

13.5.1.7 Monitoring the Accumulation Timer

The Accumulation Timer keeps a running total of the amount of time a point is in an alarm state. An alarm point that exceeds a user defined threshold will trigger a Accumulation Event system alarm. Refer to Figure 13.3.1.7.1. and Table 13.3.1.7.A to define the accumulation timer.

```
C)onfig  P)roxy  T)elnet  D)ebug  e(X)it

E)dit  M)onitor  P)ing  S)tats  T)une Modem  R)eset Port (ESC) ? M

A)larms  R)elays  a(N)alogs  E)vent log  a(C)cum. Timer
  B)AC  P)ing targets  p(O)rts  S)ystem (ESC) ? C

Accumulation Timer: enabled
 Display Reference: 1
   Point Reference: 11
 Point Description:
       Point Status: Clear
   Event Threshold: 00:01:01 (dd:hh:mm)
  Accumulated Time: 00:00:00 (dd:hh:mm)
 Accumulated Since: 22-July-2001 03:16

R)eset AccTmr (ESC) ?
```

Fig. 13.3.1.7.1. *Monitor and reset the Accumulator Timer*

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

Table 13.3.1.7.A. *Field descriptions in the Accumulator Timer Settings*

13.5.2 Viewing Live Target Pings

Choose P)ing to ping any of the NetGuardian's user defined IP addresses. Then enter the ID number (1-32) of the IP address or enter any IP address to ping.

```
E)dit  M)onitor  P)ing  S)tats  T)une Modem  R)eset Port (ESC) ? P

Ping Address / ID (1-32) :
```

Fig. 13.3.2.1. *Continuously ping an IP address that has been defined in the NetGuardian's ping table*

13.5.3 Proxy Menu

You can create proxy connections to reach-through to the craft port, modem port or any of the other eight serial ports from the P)roxy menu. You'll be able to monitor and control additional devices via proxy connection to the NetGuardian. Data presented and handshaking will be specified by the connected device.

To cancel the proxy connection wait a half second, then quickly type @@@ and press ENTER.

```
C)onfig  P)roxy  T)elnet  D)ebug  e(X)it

Available Data Ports:

C) Craft                    (In use)
M) Modem
1)
2)
3)
4)
5)
6)
7)
8) 8

Proxy to : M)odem 1) 2) 3) 4) 5) 6) 7) 8) (ESC) ?
```

Fig. 13.3.3.1. *Access devices connected to the eight data ports on the back panel through M)onitor menu > P)roxy option*

13.5.4 Event Logging

Choose E)vent log to view the up to 100 events posted to the NetGuardian; including power up, base and system alarms, ping alarms, analog alarms, and controls. Posted events for the various alarms include both alarm and clear status. Refer to Table 13.3.4.A for event log field descriptions.

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

```
Password: **********

NetGuardian-G4 v4.1B.0411

C)onfig  P)roxy  T)elnet  D)ebug  e(X)it

E)dit  M)onitor  P)ing  S)tats  T)une Modem  R)eset Port (ESC) ? M

A)larms  R)elays  a(N)alogs  E)vent log  a(C)cum. Timer
   B)AC  P)ing targets  p(O)rts  S)ystem (ESC) ? E

Evt Date        Time      Grp State     PRef  Description

  1 04-20-2006  10:02:10  1   setgrp1   11.59 GLD/BSU 1 Fail
  2 01-01-2045  12:00:00  1   clrgrp1   11.33 Unit Reset
  3 01-01-2045  12:00:00  1   setgrp1   11.33 Unit Reset
  4 01-01-2001  12:00:06  1   setgrp1   9.3   MjU:7
  5 01-01-2001  12:00:06  1   setgrp1   9.1   MnU:7
  6 01-01-2001  12:00:04  1   setgrp1   11.39 NET 2 is not Active

Would you like to Reset the Event Log? (y/N)
```

Fig. 13.3.4.1. *Monitor the last 100 events recorded by the NetGuardian from the M)onitor menu > E)vent log option*

Event Log Field	Description
Evt	Event number (1–100)
Date	Date the event occurred
Time	Time the event occurred
Grp	Alarm Group
State	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.

Table 13.3.4.A. *Event Log field descriptions*

13.5.5 Backing Up NetGuardian Configuration Data via FTP

1. From the Start menu on your PC, select RUN.

2. Type "ftp" followed by the IP address of the NetGuardian you are backing up (e.g. ftp 126.10.120.199).

3. After the connection is made press Enter.

4. Enter the password of the NetGuardian (default password is dpstelecom), then press Enter.

5. Type "binary" and press Enter (necessary for NetGuardian file transfer).

6. Type "lcd" and press Enter (this allows you to change the directory of your local machine).

7. Type "get" followed by the name you wish to define for the NetGuardian backup file. Add the extension ".ngd" to the file name (e.g. get ngdbkup.ngd) and press Enter.

8. After reloading, type "bye" and press Enter to exit.

Note: The backup file name can have a maximum of eight characters before the file extension.

13.5.5.1 Reloading NetGuardian Configuration Data

1. From the Start menu on your PC, select RUN.

2. Type "ftp" followed by the IP address of the NetGuardian you are backing up (e.g. ftp 126.10.120.199).

3. After the connection is made press Enter.

4. Enter the password of the NetGuardian (default password is dpstelecom), then press ENTER.

5. Type "binary" and press Enter (necessary for NetGuardian file transfer).

6. Type "lcd" and press Enter (this allows you to change the directory of your local machine).

7. Type "put" followed by the name you defined for the NetGuardian backup file and press Enter (e.g. put ngdbkup.ngd).

8. Type "literal REBT" to reboot the NetGuardian.

9. After reloading, type "bye" and press Enter to exit.

13.5.6 Debug Input and Filter Options

Debug Input Options	
ESC	Exit Debug
B	Show BAC status points
T	Show task status
U	Show DUART information
R	Show network routing table
X	Clear debug enable bitmap. Turn all debug filters OFF
?	Display Options
Debug Filter Options:	
a	(1) Alarm toggle switch. Shows posting of alarm data
A	(2) Analog toggle switch. Shows TTY interface debug
c	(3) Config toggle switch. Shows TTY interface debug
C	(4) Control relay toggle switch. Shows relay operation
d	(5) DCP responder toggle switch. Shows DCP protocol
D	(6) Device toggle switch. Shows telnet and proxy information and NGEdit4 serial communication.
e	(7) Expansion poller toggle switch. Shows NGDdx polling
E	(8) ECU Interrogator toggle switch. Shows BAC processing
f	(9) FTP Command toggle switch. Shows command string parsing
F	(10) FTP Data toggle switch. Shows FTP Read / Write
G	(11) GLD poller toggle switch. Shows GLD polling
h	(12) HTML debug switch. Shows Web Browser processing
H	(13) HWACS debug switch. Shows hardware access operation
i	(14) PING toggle switch
k	(15) Socket toggle switch. Shows current dcu resources
l	(16) LED toggle switch. Shows current LED state
L	(17) LCD display toggle switch. Shows LCD control and text
m	(18) Modem toggle switch. Shows modem vectored initialization
M	(19) Undefined
o	(20) Osstart toggle switch. Miscellaneous application debug, including NVRAM read and write operation, and event posting
O	(21) Undefined
p	(22) SPORT toggle switch. Port init debug and channeled port debug
P	(23) PPP toggle switch. Shows PPP functioning
q	(24) QAccess toggle switch. Reserved for future use
Q	(25) Undefined
r	(26) Report toggle switch. Shows reporting event activity, including SNMP, pagers, email, etc. Also shows PPP negotiation for NG client PPP mode.
s	(27) SNMP toggle switch. Reserved for future use
S	(28) STAK toggle switch. Shows network processing and IPA of arp requests. Also shows packets discarded by Filter IPA.
t	(29) TERM toggle switch. Shows UDP/TCP port handling. The camera and

	network time (NTP) jobs also use the TERM toggle switch
V	(30) Undefined
w	(31) HTTP toggle switch. Shows handling of web browser packets
W	(32) WEB toggle switch 2. Dump HTML text from web browser

Table. 13.3.A. Debut Input and Filter Options

14 Reference Section

14.1 Display Mapping

Port	Address	Display	Description	Set	Clear
99	1	1	Discrete Alarms 1-32	8001-8032	9001-9032
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
99	1	12	NetGuardian Expansion 1 Alarms 1-48	6001-6064	7001-7064
99	1	12	NetGuardian 480 (as DX) Alarms 1-64	6001-6064	7001-7064
99	1	13	NetGuardian Expansion 1 Relays 1-8 or NetGuardian 480 (as DX) Relays 1-4	6065-6072	7065-7072
99	1	13	NetGuardian 480 (as DX) Alarms 65-80	6081-6096	7081-7096
99	1	14	NetGuardian Expansion 2 Alarms 1-48	6129-6177	7129-7177
99	1	15	NetGuardian Expansion 2 Relays 1-8	6193-6200	7193-7200
99	1	16	NetGuardian Expansion 3 Alarms 1-48	6257-6305	7257-7305
99	1	17	NetGuardian Expansion 3 Relays 1-8	6321-6328	7321-7328
99	1	26	DSCP ALG 1/2(Propane Sensor, Battery Voltage)	6449-6452	7449-7452
99	1	27	DSCP ALG 3/4	6513-6516	7513-7516
99	1	28	DSCP ALG 5/6	6577-6580	7577-7580

Table 14.1.A. Display descriptions and SNMP Trap numbers for the NetGuardian

*   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.

		SNMP Trap #s	
Points	**Description**	**Set**	**Clear**
1	Relays	8641	9641
2	Relays	8642	9642
3	Relays	8643	9643
4	Relays	8644	9644
5	Relays	8645	9645
6	Relays	8646	9646
7	Relays	8647	9647
8	Relays	8648	9648
17	Timed Tick	8657	9657
18	Exp. Module Callout	8658	9658
19	Network Time Server	8659	9659
21	Duplicate IP Address	8661	9661
33	Power Up	8673	9673
36	Lost Provisioning	8676	9676
37	DCP Poller Inactive	8677	9677
38	LAN not active	8678	9678
41	Modem not responding	8681	9681
42	No Dial Tone	8682	9682
43	SNMP Trap not Sent	8683	9683
44	Pager Que Overflow	8684	9684
45	Notification failed	8685	9685
46	Craft RcvQ full	8686	9686
47	Modem RcvQ full	8687	9687
48	Serial 1 RcvQ full	8688	9688
49	Serial 2 RcvQ full	8689	9689
50	Serial 3 RcvQ full	8690	9690
51	Serial 4 RcvQ full	8691	9691
52	Serial 5 RcvQ full	8692	9692
53	Serial 6 RcvQ full	8693	9693
54	Serial 7 RcvQ full	8694	9694
55	Serial 8 RcvQ full	8695	9695
56	NetGuardian DX 1 fail	8696	9696
57	NetGuardian DX 2 fail	8697	9697
58	NetGuardian DX 3 fail	8698	9698
59	GLD 1 fail	8699	9699
60	GLD 2 fail	8700	9700
61	GLD 3+ fail	8701	9701
62	Chan. Port Timeout	8702	9702
63	Craft Timeout	8703	9703
64	Event Que Full	8704	9704

Table 14.1.B *Display 11 System Alarms point descriptions*

Note: See Section 14.1.1, "System Alarms Display Map," for detailed descriptions of the NetGuardian's system alarms.

14.1.1 System Alarms Display Map

Display	Points	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.
	22	DSCP Poller Inactive	The unit has not received a signal from the DSCP Poller after a certain period of time.	Check configuration of DSCP Poller. Check battery power. Make sure signal is not physically obstructed.
	23	Sensor Power Fault	Power to DSCP unit is shorting or cannot provide enough current causing a fault with the sensor power.	Check sensor wiring for any faulty connections or shortened cables.
	24			

		Sensor Power Low	DSCP unit is not providing enough power to the sensors.	Check sensor wiring for any faulty connections or shortened cables.
	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.

Table 14.1.1.A. System Alarms Descriptions

Note: Table 14.1.1.A. continues on following pages.

Display	Points	Alarm Point	Description	Solution
11	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 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.
	47	Modem RcvQ full	The modem port received more data than it was able to process.	Check what is connecting to the NetGuardian. 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		
	53	Serial 6 RcvQ full		
	54	Serial 7 RcvQ full		
	55	Serial 8 RcvQ full		

Table 14.1.1.A *System Alarms Descriptions (continued)*

Note: Table 14.1.1.A continues on following page.

| Display	Points	Alarm Point	Description	Solution
11	56	NetGuardian DX 1 fail	NGDdx 1 Fail (Expansion shelf 1 communication link failure)	Under Ports > Options, verify the number of configured NGDdx units. Use EXP filter debug and port LEDs to help diagnose the problem. Use DB9M to DB9M with null crossover for cabling. Verify the DIP addressing on the back of the NGDdx unit.
	57	NetGuardian DX 2 fail	NGDdx 2 Fail (Expansion shelf 2 communication link failure)	
	58	NetGuardian 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.
	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 14.1.1.A *System Alarms Descriptions (continued)*

14.2 SNMP Manager Functions

The SNMP Manager allows the user to view alarm status, set date/time, issue controls, and perform a resync. The display and tables below outline the MIB object identifiers. Table B.1 begins with dpsRTU; however, the MIB object identifier tree has several levels above it. The full English name is as follows: 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)
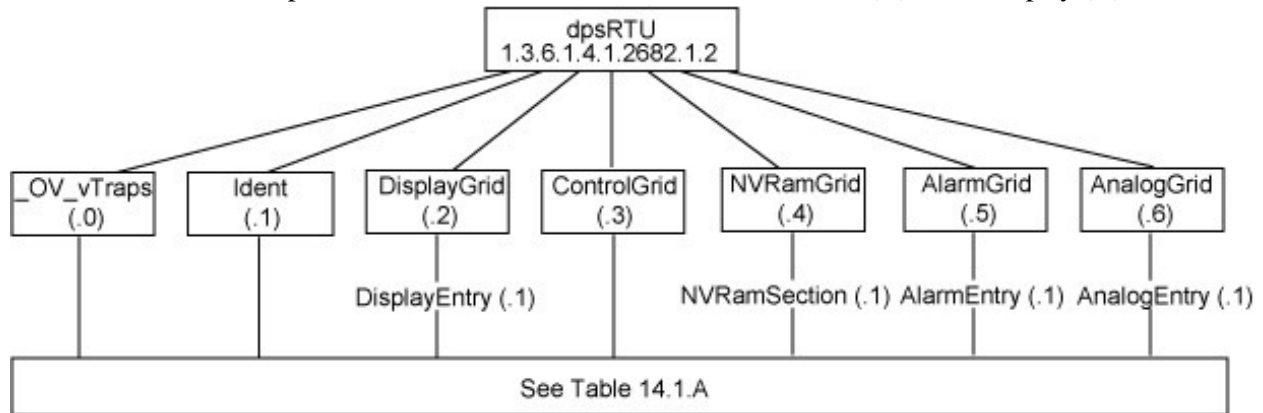
Tbl. B1 (O.)_OV_Traps points
_OV_vTraps **(1.3.6.1.4.1.2682.1.4.0)**
PointSet (.20)
PointClr (.21)
SumPSet (.101)
SumPClr (.102)
ComFailed (.103)
ComRestored (.014)
P0001Set (.10001) through P0064Set (.10064)
P0001Clr (.20001) through P0064Clr (.20064)

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 (1.3.6.1.4.1.2682.1.4.5.1)
Aport (.1)
AAddress (.2)
ADisplay (.3)
APoint (.4)
APntDesc (.5)*
AState (.6)

Tbl. B6 (.6) Analog Channels
Channel Entry **(1.3.6.1.4.1.2682.1.4.6.1)**
Channel Number (.1)
Enabled (.2)
Description (.3)
Value (.4)
Thresholds (.5)*
*If Mj, Mn is assumed

⚠ *Hot Tip!* The NetGuardian 832A OID has changed from 1.3.6.1.4.1.2682.1.2 to 1.3.6.1.4.1.2682.1.4 Updated MIB files are available on the Resource CD or upon request.

	Description	Port	Address	Display	Points
Disp 1	No data*	99	1	1	1-32
	Undefined**	99	1	1	33-64
Disp 2	No data*	99	1	2	1-32
	Undefined**	99	1	2	33-64
Disp 3	Analog 1	99	1	3	1-4
	Undefined**	99	1	3	5-64
Disp 4	Analog 2	99	1	4	1-4
	Undefined**	99	1	4	5-64
Disp 5	Analog 3	99	1	5	1-4
	Undefined**	99	1	5	5-64
Disp 6	Analog 4	99	1	6	1-4
	Undefined**	99	1	6	5-64
Disp 7	Analog 5	99	1	7	1-4
	Undefined**	99	1	7	5-64
Disp 8	Analog 6	99	1	8	1-4
	Undefined**	99	1	8	5-64
Disp 9	Analog 7	99	1	9	1-4
	Undefined**	99	1	9	5-64
Disp 10	Analog 8	99	1	10	1-4
	Undefined**	99	1	10	5-64
Disp 11	No Data*	99	1	11	1-8
	Undefined**	99	1	11	9-16
	Timed Tick	99	1	11	17
	Exp. Module Callout	99	1	11	18
	Network Time Server	99	1	11	19
	Undefined**	99	1	11	20
	Duplicate IP Address	99	1	11	21
	Undefined**	99	1	11	22-32
	Power up	99	1	11	33
	Undefined**	99	1	11	34-35
	Lost	99	1	11	36
	DCP poll inactive	99	1	11	37
	LAN not active	99	1	11	38
	Undefined**	99	1	11	39-40
	Modem not	99	1	11	41
	No dial-tone	99	1	11	42
	SNMP trap not	99	1	11	43
	Pager Que	99	1	11	44
	Notification	99	1	11	45
	Craft RCVQ full	99	1	11	46
	Modem RCVQ	99	1	11	47
	Data 1-8 RCVQ	99	1	11	48-55
	NGDdx 1-3 fail	99	1	11	56-58
	GLD 1-3 fail	99	1	11	59-61

| | CHAN timeout | 99 | 1 | 11 | 62 |
| | CRFT timeout | 99 | 1 | 11 | 63 |

Table 14.2.A. *Alarm Point Descriptions*

* "No data" indicates that the alarm point is defined but there is no description entered.
** "Undefined" indicates that the alarm point is not used.

14.3 SNMP Granular Trap Packets

Tables 14.3.A and 14.3.B provide a list of the information contained in the SNMP Trap packets sent by the NetGuardian.

SNMP Trap managers can use one of two methods to get alarm information:
1. Granular traps (not necessary to define point descriptions for the NetGuardian)

or

2. The SNMP manager reads the description from the Trap.

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

Table 14.3.A *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
NetGuardian 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

Table 14.3.B. SNMP Headers and descriptions

14.4 Trap SNMP Logic

NET1	NET2	Trap Dest.		Result
Subnet 1 & Gateway	Not Defined	Subnet 3		Trap goes out NET1's Gateway
Subnet 1 & Gateway	Subnet 2, No Gateway	Subnet 3		Trap goes out NET1's Gateway
Subnet 1 & Gateway	Subnet 2 & Gateway	Subnet 3		Trap goes out NET2's Gateway
Subnet 1 & Gateway	Subnet 2 & Gateway	Subnet 2		Trap goes out NET2
Subnet 1 & Gateway	Subnet 2 & Gateway	Subnet 1		Trap goes out NET1
Subnet 1, No Gateway	Subnet 2 & Gateway	Subnet 1		Trap goes out NET1
Subnet 1, No Gateway	Subnet 2 & Gateway	Subnet 2		Trap goes out NET2
Subnet 1, No Gateway	Subnet 2 & Gateway	Subnet 3		Trap goes out NET2

Table 14.3.C. Trap SNMP Logic

14.5 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

Table 14.4.A. ASCII symbols

15 Frequently Asked Questions

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

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

15.1 General FAQs

Q. How do I telnet to the NetGuardian?
A. You must use **Port 2002** to connect to the NetGuardian. Configure your Telnet client to connect using TCP/IP (**not** "Telnet," or any other port options). For connection information, enter the IP address of the NetGuardian and Port 2002. For example, to connect to the NetGuardian using the standard Windows Telnet client, click Start, click Run, and type "telnet <NetGuardian IP address> 2002."

Q. How do I connect my NetGuardian to the LAN?
A. To connect your NetGuardian to your LAN, you need to configure the unit IP address, the subnet mask and the default gateway. A sample configuration could look like this:
Unit Address: 192.168.1.100
subnet mask: 255.255.255.0
Default Gateway: 192.168.1.1
Save your changes by writing to NVRAM and reboot. Any change to the NetGuardian's IP configuration requires a reboot.

Q. When I connect to the NetGuardian through the craft port on the front panel it either doesn't work right or it doesn't work at all. What's going on?
A. Make sure your using the right COM port settings. Your COM port settings should read:
Bits per second: 9600 (9600 baud)
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None
Important! Flow control **must** be set to **none**. Flow control normally defaults to hardware in most terminal programs, and this will not work correctly with the NetGuardian.

Q. I can't change the craft port baud rate.
A. If you select a higher baud rate, you must set your terminal emulator program to the new baud rate and then type DPSCFG and press Enter. If your terminal emulator is set to a slower baud rate than the craft port, normal keys can appear as a break key — and the craft port interprets a break key as an override that resets the baud rate to the standard 9600 baud.

Q. How do I use the NetGuardian to access TTY interfaces on remote site equipment?
A. If your remote site device supports RS-232, you can connect it to one of the eight data ports located on the NetGuardian back panel. To make the data port accessible via LAN, configure the port for TCP/IP operation. You now have a LAN-based proxy port connection that lets you access your device's TTY interface through a Telnet session.

Q. How do I telnet to the NetGuardian?
A. Configure your Telnet client with these options:
- Connect using TCP/IP (**not** "Telnet," or any other port options)

- Enter the IP address of the NetGuardian
- Enter **Port 2002**

Example:

To connect using the Windows Telnet client, click Start, click Run, and type telnet 126.12.220.8 2002.

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, the NetGuardian must be rebooted. Whenever you make changes, remember to write them to the NetGuardian's NVRAM so they will be saved when the unit is rebooted.

Q. The LAN link LED is green on my NetGuardian, but I can't poll it from my T/Mon.

A. Some routers will not forward packets to an IP address until the MAC address of the destination device has been registered on the router's Address Resolution Protocol (ARP) table. Enter the IP address of your gateway and your T/Mon system to the ARP table.

Q. What do the terms "port," "address," "display" and "alarm point" mean?

A. These terms refer to numbers that designate the location of a network alarm, from the most general (a port to which several devices are connected) to the most specific (an individual alarm sensor).

Port: A number designating a serial port through which a monitoring device collects data.

Address: A number designating a device connected to a port.

Display: A number designating a logical group of 64 alarm points.

Alarm Point: A number designating a 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 an open/close sensor in a door. These terms originally referred only to physical things: actual ports, devices, and contact closures. For the sake of consistency, port-address-display-alarm point terminology has been extended to include purely logical elements: for example, the NetGuardian reports internal alarms on Port 99, Address 1.

Q. What characteristics of an alarm point can be configured through software? For instance, can point 4 be used to sense an active-low signal, or point 5 to sense a level or a edge?

A. The NetGuardian's standard configuration is for all alarm points to be level-sensed. You **cannot** use configuration software to convert alarm points to TTL (edge-sensed) operation. TTL alarm points are a hardware option that must be specified when you order your NetGuardian. Ordering TTL points for your NetGuardian does not add to the cost of the unit What you can do with the configuration software is change any alarm point from "Normal" to "Reversed" operation. Switching to Reversed operation has different effects, depending on the kind of input connected to the alarm point:

- **If the alarm input generates an active-high signal,** switching to Reversed operation means the NetGuardian will declare an alarm in the absence of the active-high signal, creating the practical equivalent of an active-low alarm.
- **If the alarm input generates an active-low signal,** switching to Reversed operation means the NetGuardian will declare an alarm in the absence of the active-low signal, creating the practical equivalent of an active-high alarm.
- **If the alarm input is normally open,** switching to Reversed operation converts it to a normally closed alarm point.
- **If the alarm input is normally closed,** switching to Reversed operation converts it to a normally open alarm point.

Q. Every time my NetGuardian starts up, I have to reenter the date and time. How can I get the NetGuardian to automatically maintain the date and time setting?

A. You have three options for keeping the correct time on your NetGuardian:

Real Time Clock Option: You can order your NetGuardian with the Real Time Clock hardware option. Once it's set, the Real Time Clock will keep the correct date and time, regardless of reboots.

Network Time Protocol Synchronization: If your NetGuardian has Firmware Version 2.9F or later, you can configure the unit to automatically synchronize to a Network Time Protocol (NTP) server.

- To get the latest NetGuardian firmware, sign in to MyDPS at www.dpstelecom.com/mydps.
- For instructions on configuring your NetGuardian to use NTP synchronization, see your NGEdit4 or NetGuardian Web Browser Interface user manual.

T/Mon RTU Time Sync Signal: You can configure your T/Mon NOC to send an RTU Time Sync signal at a regular interval, which you can set to any time period between 10 and 10,080 minutes. The Time Sync will automatically synchronize the NetGuardian's clock to the T/Mon's clock. And if you set your T/Mon to NTP synchronization, you'll make sure you have consistent, accurate time stamps throughout your monitoring network.

Q. How do I back up my NetGuardian configuration?

A. There are two ways to back up NetGuardian configuration files:

Use NGEdit4

NGEdit4 can read the configuration of a NetGuardian unit connected to your PC via LAN, modem or COM port. You can then use NGEdit4 to save a NetGuardian configuration file on your PC's hard disk or on a floppy disk. With NGEdit4 you can also make changes to the configuration file and write the changed configuration to the NetGuardian's NVRAM.

Use FTP

You can use File Transfer Protocol (FTP) to read and write configuration files to the NetGuardian's NVRAM, but you can't use FTP to edit configuration files.

15.2 SNMP FAQs

Q. Which version of SNMP is supported by the SNMP agent on the NetGuardian?

A. SNMP v1 and v2.0c.

Q. How do I configure the NetGuardian to send traps to an SNMP manager? Is there a separate MIB for the NetGuardian? 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 NetGuardian begins sending traps as soon as the SNMP managers are defined. The NetGuardian MIB is included on the NetGuardian Resource CD. The MIB should be compiled on your SNMP manager. (**Note:** MIB versions may change in the future.) The unit supports a main SNMP manager, which is configured by entering its IP address in the Trap Address field of Ethernet Port Setup. You can also configure up to eight secondary SNMP managers, which is configured by selecting the secondary SNMP managers as pager recipients. Community strings are configured globally for all SNMP managers. To configure the community strings, choose System from the Edit menu, and enter appropriate values in the Get, Set, and Trap fields.

Q. Does the NetGuardian support MIB-2 and/or any other standard MIBs?

A. The NetGuardian supports the bulk of MIB-2.

Q. Does the NetGuardian SNMP agent support both NetGuardian and T/MonXM variables?

A. The NetGuardian SNMP agent manages an embedded MIB that supports only the NetGuardian's RTU variables. The T/MonXM 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 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. The NetGuardian manual talks about eight control relay outputs. How do I control these from my SNMP manager?

A. The control relays are operated by issuing the appropriate set commands, which are contained in the DPS Telecom MIB. For more information about the set commands, see Appendix, "Display Mapping," in any of the NetGuardian software configuration guides.

Q. How can I associate descriptive information with a point for the RTU granular traps?

A. The NetGuardian alarm point descriptions are individually defined using the Web Browser, TTY, or NGEdit4 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 NetGuardian and the SNMP manager are both on the network. Use the NetGuardian's ping command to ping the SNMP manager.

15.3 Pager FAQs

Q. Why won't my alpha pager work?

A. To configure the NetGuardian 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 service's 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 NetGuardian'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 NetGuardian dials your pager number and the time the NetGuardian 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. What do I need to do to set up e-mail notifications?

A. You need to assign the NetGuardian an e-mail address and list the addresses of e-mail recipients. Let's explain some terminology. An e-mail address consists of two parts, the user name (everything before the "@" sign) and the domain (everything after the "@" sign). To assign the NetGuardian an e-mail address, choose System from the Edit menu. Enter the NetGuardian'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: netguardian
Location: proactive.com

Then e-mail notifications from the NetGuardian will be sent from the address "netguardian@proactive.com." The next step is to list the e-mail recipients. Choose Pagers from the Edit menu. For each e-mail recipient, enter his or her e-mail domain in the Phone/Domain field and his or her user name in the PIN/Rcpt/Port field. You must also enter the IP address of an SNMP server in the IPA field.

16 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.*

17 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.

*"**D**ependable, **P**owerful **S**olutions*
that allow users to monitor larger,
more complicated networks with a
smaller, less trained staff"