DPS Telecom

"Your Partners In Network Alarm Monitoring"

NetGuardian 216F

USER MANUAL

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

March 19, 2019 **D-UM-NETGF**

Revision History

March 19, 2019	Minor updates
March 22, 2018	General Updates
September 28, 2017	Updated Data ports section
August 17, 2017	Added monitoring SFP Ports and Fiber Fault Deteciton
June 4, 2009	Revisions to Data Ports
June 3, 2009	Revisions for BAS Optional Accessory
December 11, 2008	NetGuardian 216F User Manual (D-OC-UM08C.11100) released.

Notice

The material in this manual is for information purposes and is subject to change without notice. DPS Telecom shall not be liable for errors contained herein or consequential damages in connection with the furnishing, performance, or use of this manual.

Contents

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

1 NetGuardian 216F Overview

The NetGuardian 216F has all the tools you need to manage your remote site

The NetGuardian 216F — The Intelligent RTU for Complete Site Management
The NetGuardian 216F is a wide temperature range, SFP Fiber Interface, and Ethernet-based, SNMP/DCPx remote telemetry unit. The NetGuardian has all the tools you need to manage your remote sites, including a 7 port 10/100/1000BaseT Ethernet switch, built-in alarm monitoring, paging, and e-mail capabilities that can eliminate the need for an alarm master.

The NetGuardian is the ideal solution for collecting equipment and environmental alarms from your outdoor enclosures and reporting these alarm conditions. The 7 port Ethernet switch can also be utilized to provide connectivity to other far-end devices from the SFP Fiber Interface.

Benefits of the NetGuardian 216F include:

- Integrated 7 port switch - Saves space, provides Ethernet connectivity for other equipment
- Web Browser support for monitoring and configuring the units–Convenient access
- Remote Firmware download ability–Easy initial deployment, and avoids costly trips to the sites for routine upgrades. Firmware upgradable via Ethernet or SFP Fiber Interface.
- Unique wire-wrap termination–Quick and easy installation and enables the unit to be removed without rewiring.
- Multiple master support–Disaster recovery scenarios.
- Alarm qualification times–Reduce nuisance alarm, avoids alarm desensitization.
- Extreme temperature rating– -22°F to 158°F (-30°C to 70°C)–A must in harsh environments.
- Multi-level password access–Control who accesses your units and to what level.
- Ping IP network devices and verify that they're online and operating.
- Optional build would include 4 additional data ports. Contact DPS Sales for more information at **(800) 622-3314**
- Expandable up to 160 discrete alarm inputs and 26 control outputs with the NetGuardian DX chassis.
-

The NetGuardian 216F is a 1 rack unit alarm remote that supports 16 discrete alarms that are "software reversible" to support both N/O and N/C alarm wiring, 8 analog inputs (4 general purpose, 1 for monitoring internal temperature, and 2 for monitoring battery feeds). The sensor probe has 10-ft long leads, so once connected to the NetGuardian 216F, it may be placed in the most appropriate location within the cabinet. The NetGuardian 216F also allows you to remotely control external devices via its 2 internal relays. These controls are a convenient and time efficient way of remotely switching equipment in the field. The Web browser interface allows you to have quick and convenient access for programming or simply to spot-check the alarm status for any given site.

The NetGuardian 216F's operational temperature range of -22°F to 158°F (-30°C to 70°C) makes it ideal for deployment in very harsh environments. It's hardened design means it will continue to deliver real time telemetry when the weather is at its worst.

The NetGuardian can be configured many different ways including TTY for the initial IP settings through the front craft port, standard Web browser software, and a Windows-based utility called Edit216F, included at no additional cost. This software will allow you to create a NetGuardian 216F configuration file without being connected to the NetGuardian 216F, then download that database remotely from the SFP Fiber Interface, Ethernet, or serial connection.

2 About This Manual

There are three separate user manuals for the NetGuardian 216F: the Hardware Manual (which you're reading now), the Edit216F User Manual, and the NetGuardian 216F Web Interface User Manual.

This Hardware Manual provides instructions for hardware installation and using the TTY interface. The Edit216F and Web Interface User Manuals, included on the NetGuardian Resource CD, provide instructions for configuring the NetGuardian using the Windows-based Edit216F utility software or the Web Interface.

3 Shipping List

Please make sure all of the following items are included with your NetGuardian 216F. If parts are missing, or if you ever need to order new parts, please refer to the part numbers listed and call DPS Telecom at **1-800-622-3314**.

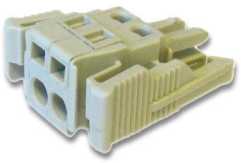
NetGaurdian 216F
D-PK-NETGF-12001

NetGuardian BSM Resource CD

NetGuardian 216F Hardware Manual
D-UM-NETGF

x1

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



x2

WAGO Connectors (Main Power)

x4

3/4-Amp GMT Fuses
2-741-00250-00

x2

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

4 Pin Analog Connector

x1

14ft. Ethernet Cable
D-PR-932-10B-14

x8

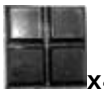
3/8" Ear Screws
2-000-60375-05

x4

Standard Rack Screws
1-000-12500-06

x4

Metric Rack Screws
2-000-80750-03



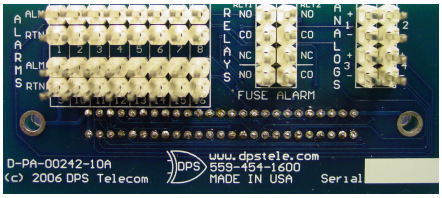
x4

Pads
2-015-00030-00

x4

Zip Ties
1-012-00106-00

3.1 Optional Shipping Items - Available by Request



Wire-Wrap Back Panel
D-PA-00242-10A
The NetGuardian 216F's Wire-Wrap back panel allows for wire-wrap connections for the discrete alarms, analog alarms, and control relays.

Temperature Sensor
D-PR-998-10A-07
The NetGuardian 216F's external temperature sensor cable for manual hook-up.
Note: The NetGuadian 216F also has an internal temperature sensor.

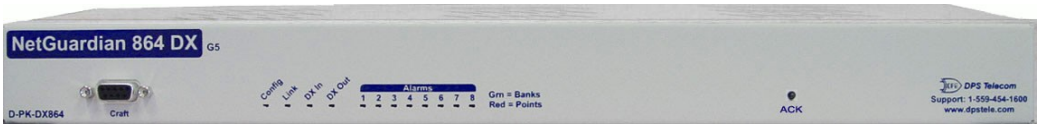
Pluggable Back Panel
D-PK-16PAN
The NetGuardian 216's pluggable back panel allows for screw-in barrier plug connections for the
NetGuardian's alarms and control relays.

23" Rack Ear
D-CS-325-10A-01
The NetGuardian may also come with 23" rack ears, available on request.

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)
D-PK-NETDX-12001
The NetGuardian Expansion provides an additional 48 discrete alarm points. Up to three NetGuardian Expansions can be daisy-chained off one NetGuardian, providing a total of 160 alarm points.



NetGuardian 864 DX Expansion
D-PK-DX864-12001
The NetGuardian 864 DX G5 is another option to achieve both discrete and analog expansion. Each chassis adds 64 alarm points, providing a total of 208 when 3 DX Expansion units are daisy-chained from the NetGuardian 216F.

Entry Control Unit G2
D-PK-ECUG2
The Building Access System (BAS) is a comprehensive building entry management system that can provide centralized door access control to your NetGuardian. The four part system consists of the NetGuardian 216F, the Entry Control Unit (ECU), and optional keypad and/or proximity card reader. With the system in place, the NetGuardian can maintain a database of all personnel access as well as the time of day and location that access was granted. It can also receive a control from the T/Mon master to remotely open a door. However, should the NetGuardian lose connection with the T/Mon, the unit is still able to make local entry decisions. Front panel LEDs indicate communication activity between the NetGuardian and the ECU.

5 Specifications

Key Specifications:

- 1 RU, 19" Mountable
- 16 Discrete alarms, 8 analog alarms (4 general purpose, 2 for temperature monitoring, 2 for battery monitoring), 2 controls
- 2 SFP Fiber Interfaces
- 7 ports of 10/100/1000BaseT Ethernet available for client use. Internally, an 8 port switch.
- Dual -48VDC power feed

- Front Craft port and LEDs
- Extended temp range, -22°F to 158°F (-30°C to 70°C)
- Firmware downloadable via LAN or SFP Fiber Interface
- Web browser with multi-level security access
- SNMP–Traps to at least 2 masters natively
- Special amphenol to Wire Wrap termination module
- Includes our new digital temperature probe on 10-ft lead, connects to rear of unit via pluggable screw lug connector.
- Windows-based configuration utility (Serial/LAN/SFP Fiber Interface)

Analog Input Range:	(–94 to 94 VDC or 4 to 20 mA)
Control Relays:	Form A or Form C
Maximum Voltage:	60 VDC/120 VAC
Maximum Current:	3/4 Amp, AC/DC
Discrete Alarms:	16
Ping Alarms:	16
Protocols:	SNMPv1, v2c and v3 DCPx, DCPf, TRIP, SMTP, TAP
Interfaces:	2 SFP Fiber Interfaces (1000Base-X) 7 RJ45 10/100/1000BaseT Ethernet ports 1 DB9 RS-232 Craft port 1 RJ45 Yost RS-232 port 4 RJ45 Yost RS-232 ports (*optional build*) 1 50-pin amphenol connectors (discretes, controls, and analogs) 1 4-pin screw connector (external temp sensor) 1 stereo input jack (for external temp sensor)
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:	+/- 24 – 48VDC (–40 to –70 VDC)
Current Draw:	375 mA max (at -48V)
Fuse:	3/4 amp GMT for power inputs
Visual Interface:	12 bicolor LEDs 11 unicolor LEDs
Operating Temperature:	-22°–158° F (-30°–70° C)
Operating Humidity:	0%–95% noncondensing

6 Hardware Installation

6.1 Tools Needed

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

PC with Edit216F software

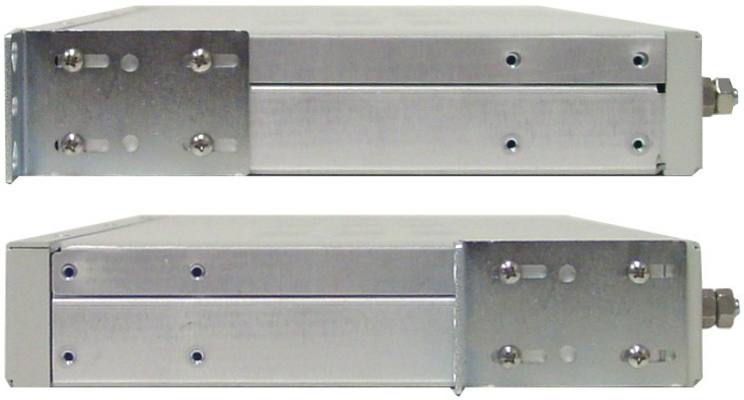
Wire Strippers/Cutter

Phillips No. 2 Screwdriver

Punch Down Tool (if 66 blocks are used)

Small Standard No. 2 Screwdriver

6.2 Mounting



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 above.

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

6.3 Power Connection

Power connectors and fuses

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

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 Fuse A and Fuse B 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 properly ground the unit.

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**. The LED by the power connector will be off if the power feed is reversed.

6. Repeat Steps 2–5 for Power Connector B.

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

6.4 LAN Connection

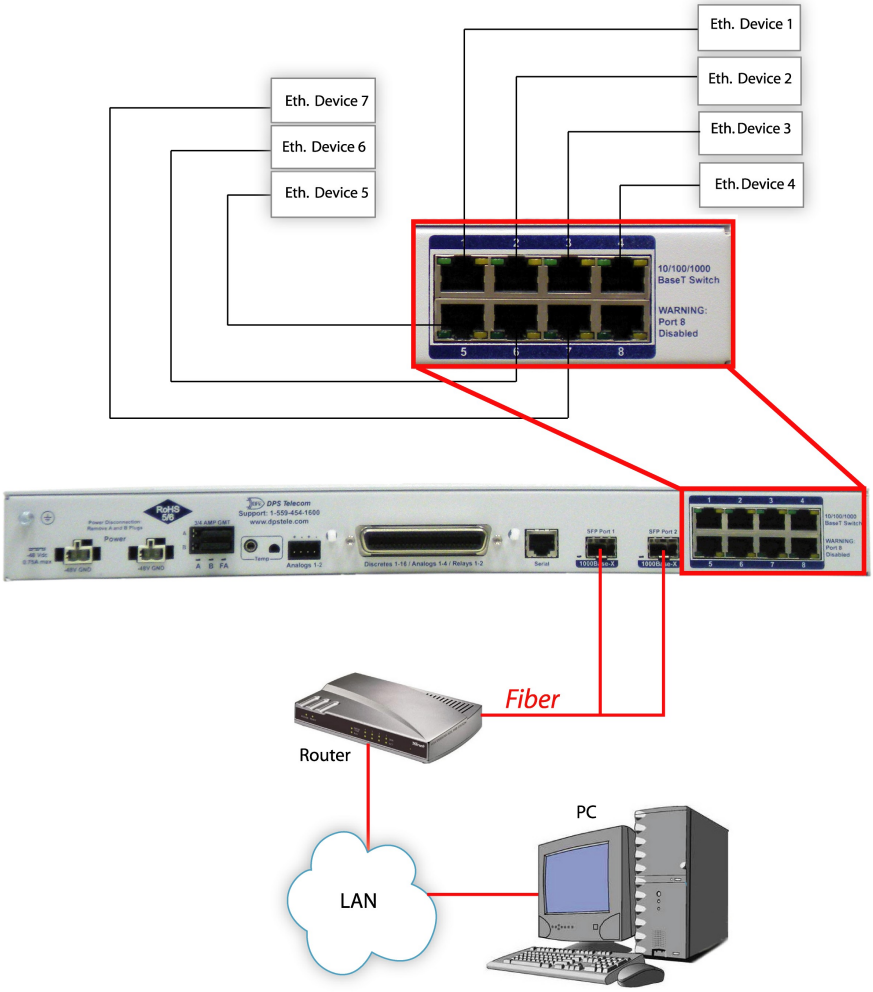
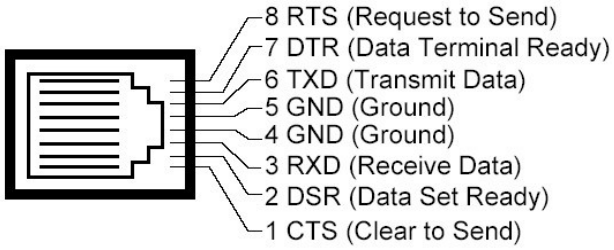


Chart of Ethernet and SFP Fiber Interface Connections

The NetGuardian 216F has a 10-BaseT Ethernet switch for connecting through LAN. To connect the NetGuardian 216F to the LAN, insert a standard RJ45 Ethernet cable into one of the Ethernet ports.

From the NetGuardian 216F, the connection can be routed via Ethernet to a local subnet of up to 7 devices.

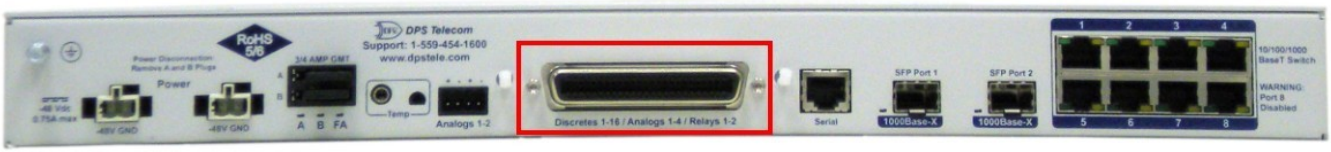
Yost RS-232 RJ45 Connector



Ethernet port pinout

The pinout diagram for the Ethernet switch port is shown above.

6.5 Alarm and Control Relay Connections



Alarm and control relay connectors

The NetGuardian's discrete alarm inputs, control relay outputs, and analog alarm inputs are connected through the 50-pin connectors labeled "Discretes 1–16, Analogs 1-4, and Relays 1-2" on the back panel.

6.5.1 Alarm and Control Relay Connector Pinout Table

Discretes 1–16					
	RTN	ALM		RTN	ALM
ALM 1	1	26	**ALM 9**	9	34
ALM 2	2	27	**ALM 10**	10	35
ALM 3	3	28	**ALM 11**	11	36
ALM 4	4	29	**ALM 12**	12	37
ALM 5	5	30	**ALM 13**	13	38
ALM 6	6	31	**ALM 14**	14	39
ALM 7	7	32	**ALM 15**	15	40
ALM 8	8	33	**ALM 16**	16	41

Alarm, amphenol connector, and control relay pinout (continued on next page)

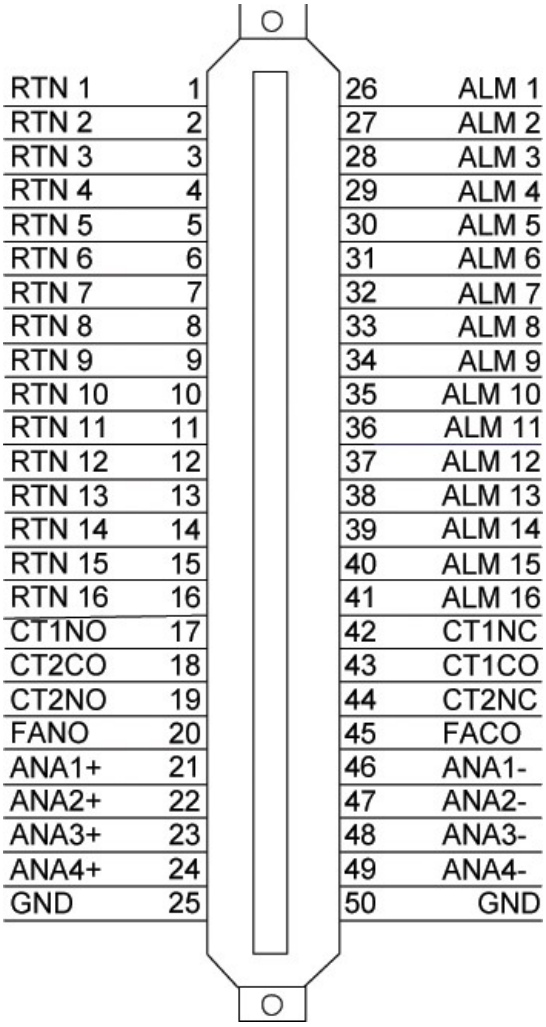
Analogs 1–4		
	+	–
ANA 1	21	46
ANA 2	22	47
ANA 3	23	48
ANA 4	24	49
GND	25	50

Control Relatys 1–2		
	NO/NC	CO
CTRL 1	17/42	43
CTRL 2	19/44	18
FUSE	20/NA	45

Alarm, amphenol connector, and control relay pinout

The table shows the pinouts for the 50-pin connectors "Discretes 1-16," and "Analogs 1-4" and "Control Relays 1-2."

6.5.2 Discretes 1–16 Connector Pinout Diagram

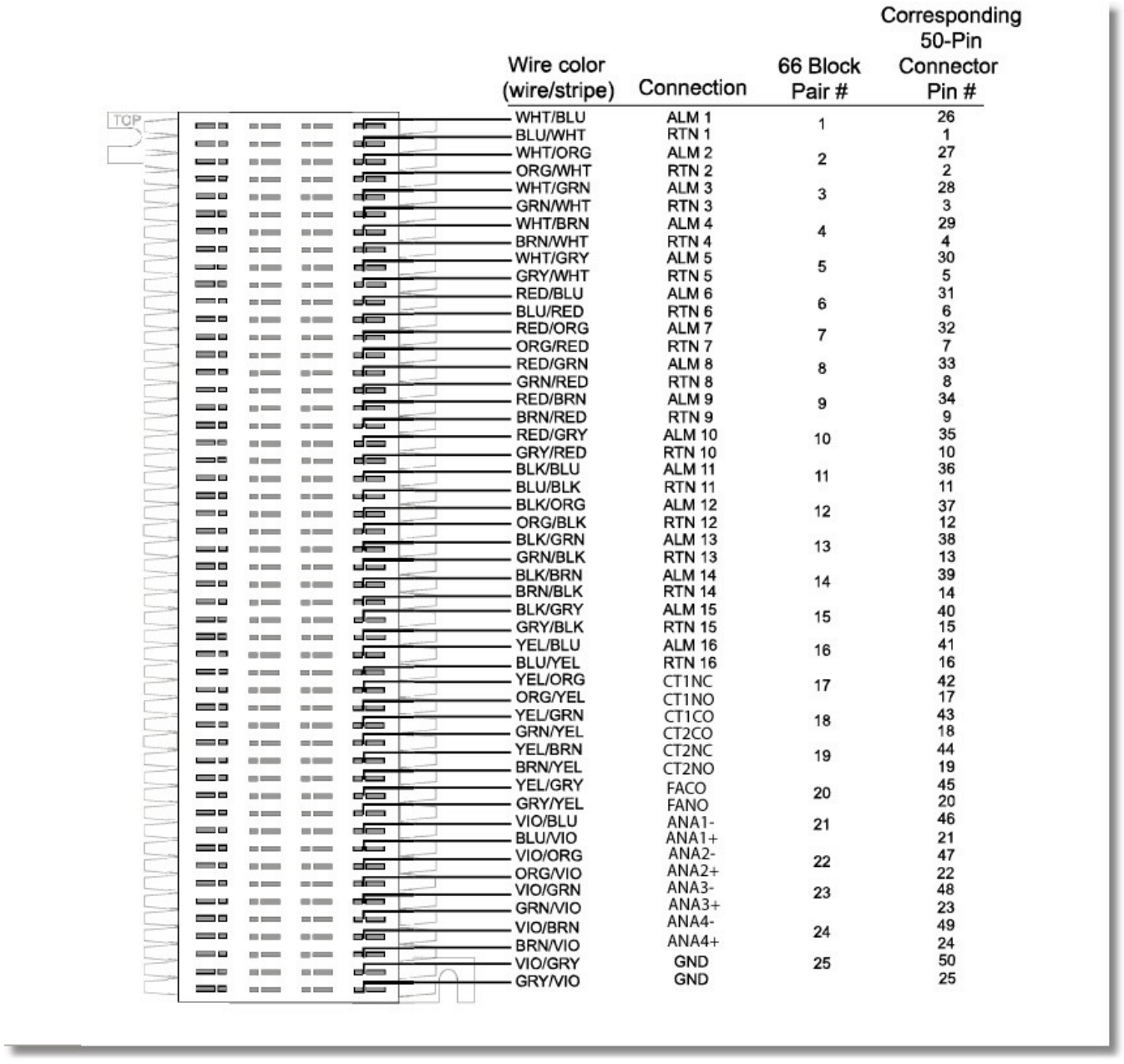


Pinout Diagram for Discretes 1-16 connector

6.5.3 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 diagram below for Discretes 1–16.

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	CT1NC	17	42
ORG/YEL	CT1NO		17
YEL/GRN	CT1CO	18	43
GRN/YEL	CT2CO		18
YEL/BRN	CT2NC	19	44
BRN/YEL	CT2NO		19
YEL/GRY	FACO	20	45
GRY/YEL	FANO		20
VIO/BLU	ANA1-	21	46
BLU/VIO	ANA1+		21
VIO/ORG	ANA2-	22	47
ORG/VIO	ANA2+		22
VIO/GRN	ANA3-	23	48
GRN/VIO	ANA3+		23
VIO/BRN	ANA4-	24	49
BRN/VIO	ANA4+		24
VIO/GRY	GND	25	50
GRY/VIO	GND		25

Optional 66 block pinout for Discretes 1–16

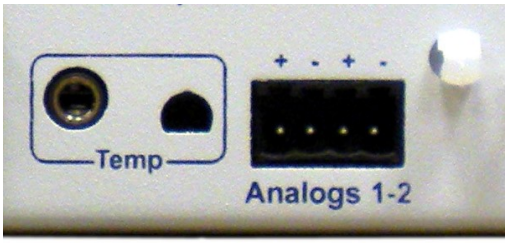
6.5.4 Integrated Temperature and Battery Sensor

The integrated temperature and battery sensor monitors the ambient temperature and the NetGuardian's power feeds. This option is available only if it was ordered with your NetGuardian. The integrated temperature sensor measures a range of -22° F to 158° F (-30° C to 70° C) within an accuracy of ± 1°.

Analog Function	Location	Channel Mapping
User Channel 1	Amphenol or 4-pin connector	Reported as analog channel 1
User Channel 2	Amphenol or 4-pin connector	Reported as analog channel 2
User Channel 3	Amphenol only	Reported as analog channel 3
User Channel 4	Amphenol only	Reported as analog channel 4
Monitor Power Feed A	Internal	Reported as analog channel 5
Monitor Power Feed B	Internal	Reported as analog channel 6
Monitor Internal Temperature	Internal	Reported as analog channel 7
Monitor External Temperature	1/4 inch stereo jack	Reported as analog channel 8

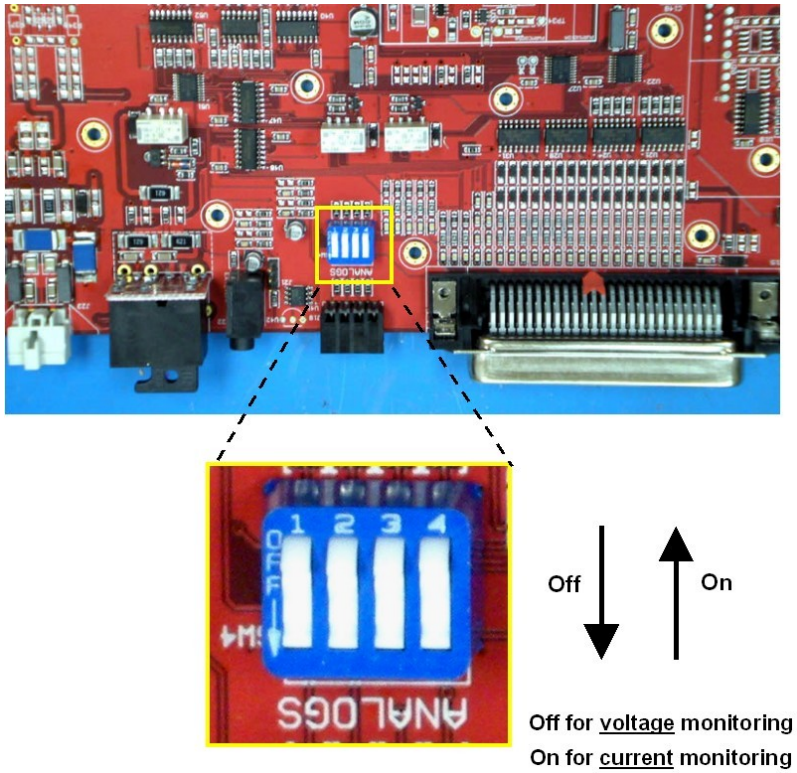
Integrated sensor connection options

Between the Amphenol connector and Fuse B resides the 1/4 inch stereo jack for the external temperature sensor, as well as the 4-pin connection for Analogs 1-2, as shown below.



Temperature Sensor and Analog Connectors

6.5.5 Analog Dipswitches



Dipswitch and layout

The analogs are controlled by the dipswitches to the left of the Amphenol connector (located at the back of the unit). For milliamp sensor operation, turn the dipswitch on by placing it in the on position. For normal operation, place the dipswitch in the off position. Note that the dipswitch is internal, and requires the case to be opened in order to change the setting.

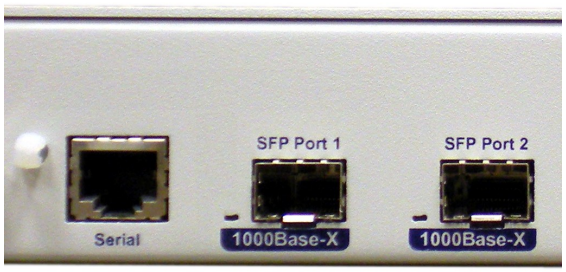
Hot Tip!

WARNING

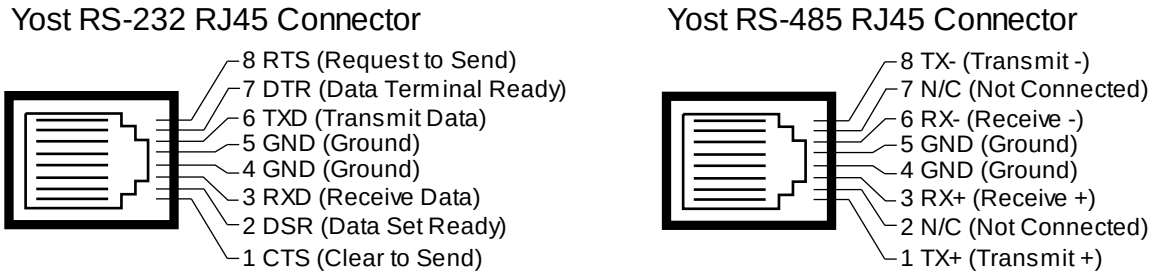
WARNING: Do not put the dipswitches in the on position unless you are sure of the analog setting. Having the dipswitches on will put a 250 ohm resistor across the input lines. Any voltage beyond 5V or 20 mA will damage components.

6.5.6 Data Port

The port can function as a DPC or ECU port.



Data ports on the NetGuardian 216F

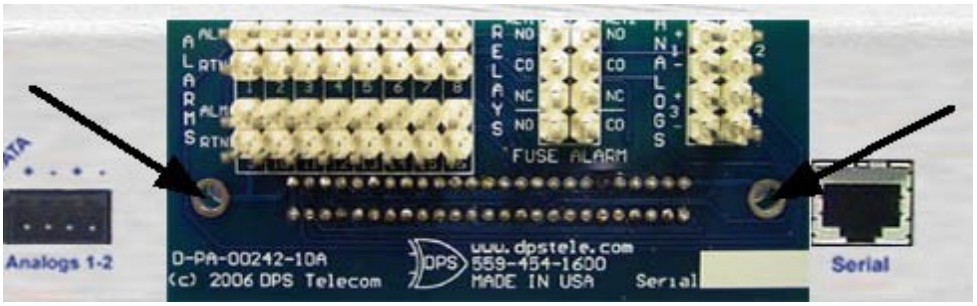


Data Port Pinout

6.5.6.1 Connecting NetGuardian Accessories

If you are using a NetGuardian Expansion, connect it to the Serial port. Additional configuration requires using Edit216F for Windows configuration software.

6.6 Optional Wire-Wrap Back Panel



The wire-wrap back panel (arrows indicate screw locations for mounting)

The optional wire-wrap back panel provides wire-wrap connections for the NetGuardian's alarms (discrete and analog) and control relays. Screw the board into the holes on either side of the "Discretes 1-16/Analogs 1-4/Relays 1-2 connector" (as shown in Figure 6.7.1). To connect discrete alarms, analog alarms, and control relays to the wire-wrap panel, connect them to the pin block on the front of the panel.

6.7 Integrated 10/100/1000BaseT Ethernet Switch

NetGuardian integrated Ethernet switch

The NetGuardian 216F comes equipped with an integrated 10/100/1000BaseT Ethernet switch, which provides seven regular Ethernet ports as shown above. The integrated Ethernet switch is powered by the same –48 VDC power as the NetGuardian, which provides more secure, more robust operation than switches that run off commercial power. The integrated switch also frees valuable rack space by eliminated an unnecessary extra unit.

7 Front Panel LEDs

Front panel LEDs

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

LED	Status	Description
Link	Solid Green	Ethernet link detected
Activity	Blink Green	Activity detected on Ethernet link
SFP	Off	No link detected
	Solid Green	Link detected
LAN	Blink Red	Receive traffic on LAN interface
	Blink Green	Transmit traffic on LAN interface
Serial	Blink Red	Receive traffic on Serial interface
	Blink Green	Transmit traffic on Serial interface
Loop	Solid Red	Loopback detected on SFP interface
Alarm *	Blink Red	Unacknowledged COS alarm exists
	Solid Red	Acknowledged alarm exists
Config	Blink Red	Configuration is invalid
	Blink Green	Configuration is valid
Craft	Blink Red	Receive traffic on craft interface
	Blink Green	Transmit traffic on craft interface

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

Front panel LED Status message descriptions

8 Back Panel LEDs

Back panel LEDs for Power and Ethernet connections

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

	LED	Status	Description
Power	Pwr A	Off	Power not applied or polarity incorrect
		Green	Power applied
	Pwr B	Off	Power not applied or polarity incorrent
		Green	Power applied
Fuse Alarm	---	Red	Fuse A or B is blown
10/100/1000 BaseT Switch	Green	Flashing	Activity on port detected
	Orange	Solid	Link detected
SFP Fiber Interface	Port 1	Red	SFP detected, no link
		Green	SFP detected, link is up
	Port 2	Red	SFP detected, no link
		Green	SFP detected, link is up

Back panel LED Status message descriptions

9 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 Edit216F 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 10, "Connecting to the NetGuardian."

10 Connecting to the NetGuardian

10.1 ... via Craft Port

NetGuardian Craft Port

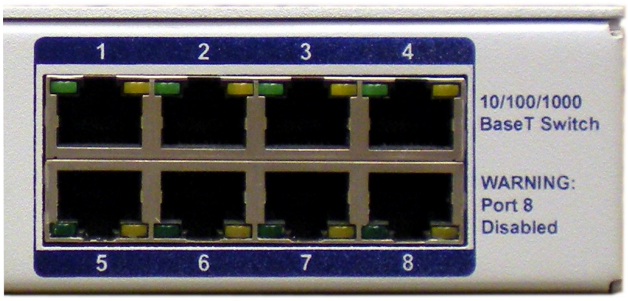
The simplest way to connect to the NetGuardian is over a physical cable connection between your PC's COM port and the NetGuardian's craft port.

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 Edit216F. You only need a connection to the unit to read or write configuration files to its NVRAM. You can use Edit216F 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.

You can perform all configuration tasks via the craft port with Edit216F — 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.

10.2 ... via LAN



NetGuardian LAN Link

Once LAN settings are provisioned, you can connect to the NetGuardian over a LAN connection by connecting to one of the seven 10/100/1000BaseT Ethernet switch ports. 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 Edit216F. You only need a connection to the unit to read or write configuration files to its NVRAM. You can use Edit216F 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: "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**.

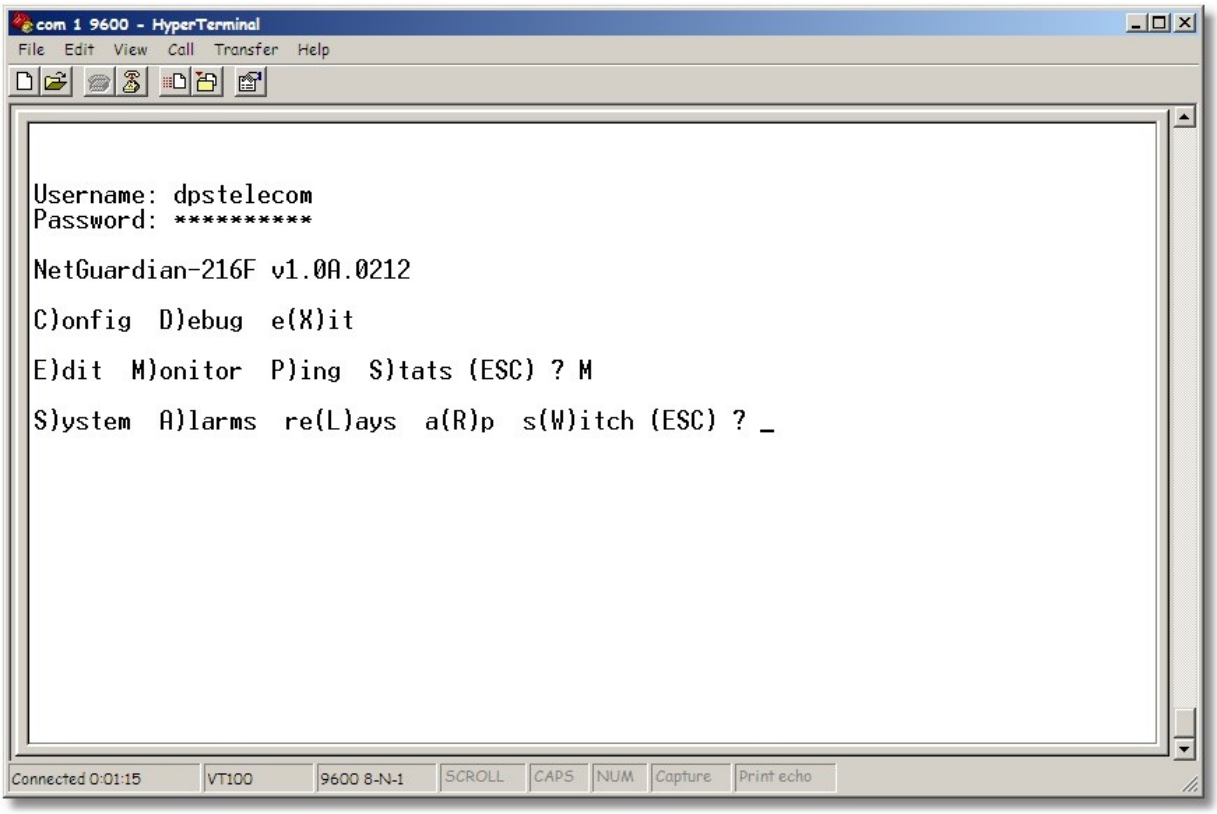
3. Reset your PC's subnet mask to **255.255.0.0**. You may have to reboot your PC to apply your changes.

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.

Note: You can ping the NetGuardian to confirm connectivity through the Ethernet switch ports.

11 TTY Interface



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 Edit216F utility.

To use the TTY interface with the NetGuardian, all you need is any PC with terminal emulation software 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. Some initial software configuration must be performed before you can use a remote connection to the NetGuardian.

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 username and password is "**dpstelecom**".

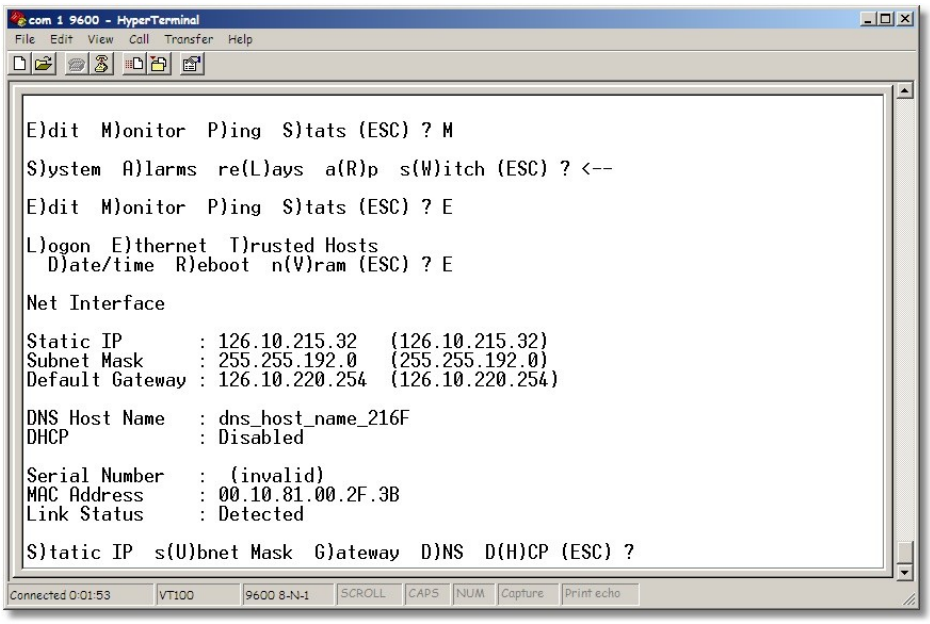
11.1 Menu Shortcut Keys

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.

11.2 Unit Configuration

11.2.1 Ethernet Port Setup

The NetGuardian must be assigned an IP address before you will be able to connect via LAN using a Telnet client or a Web browser. To connect via LAN, the minimum configuration requires setup of the IP address and subnet mask. Follow the instructions below to configure the NetGuardian's IP address, subnet mask, and default gateway for Ethernet connectivity.



Configure the Ethernet port parameters

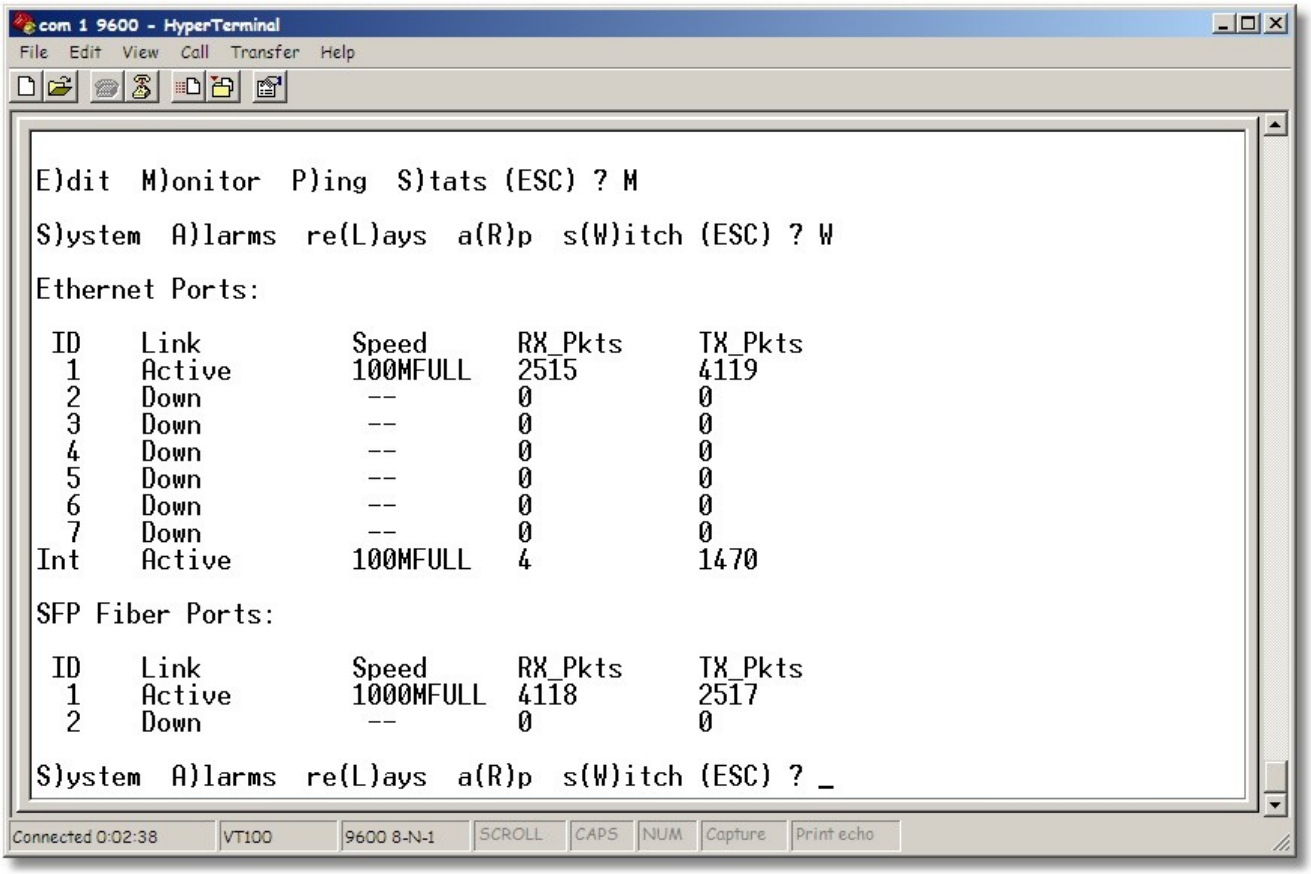
1. Once a connection is established, the NetGuardian will respond with "Password."
2. Type the default password, "dpstelecom," then press Enter.

   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.
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.

11.3 Monitoring

11.3.1 Monitoring the NetGuardian

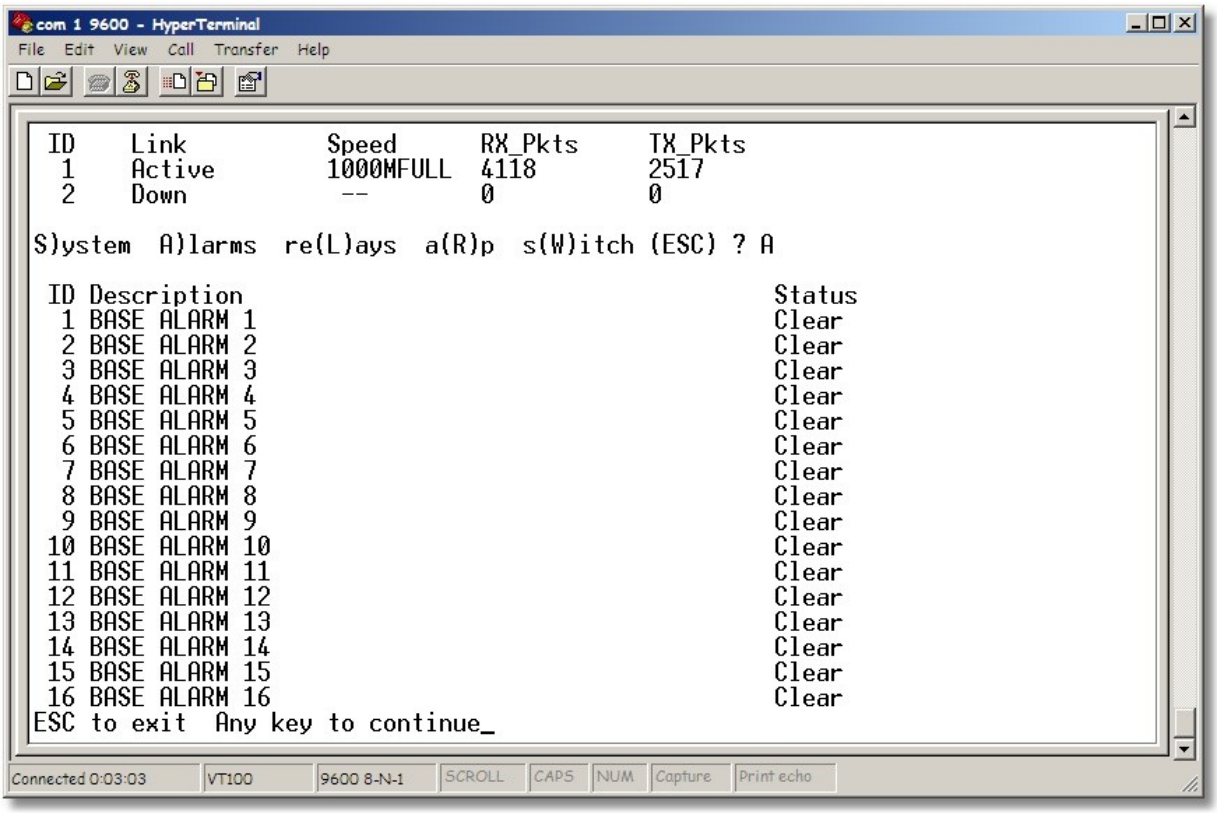
Connect a PC running terminal emulation software to the craft port or connect via LAN using a Telnet client with emulation to port 2002 to reach the monitor menu selection. This section allows you to do full system monitoring of the NetGuardian including: all alarms, ping information, relays, analogs,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



The monitor menu allows status checking on all elements

11.3.1.1 Monitoring Base Alarms

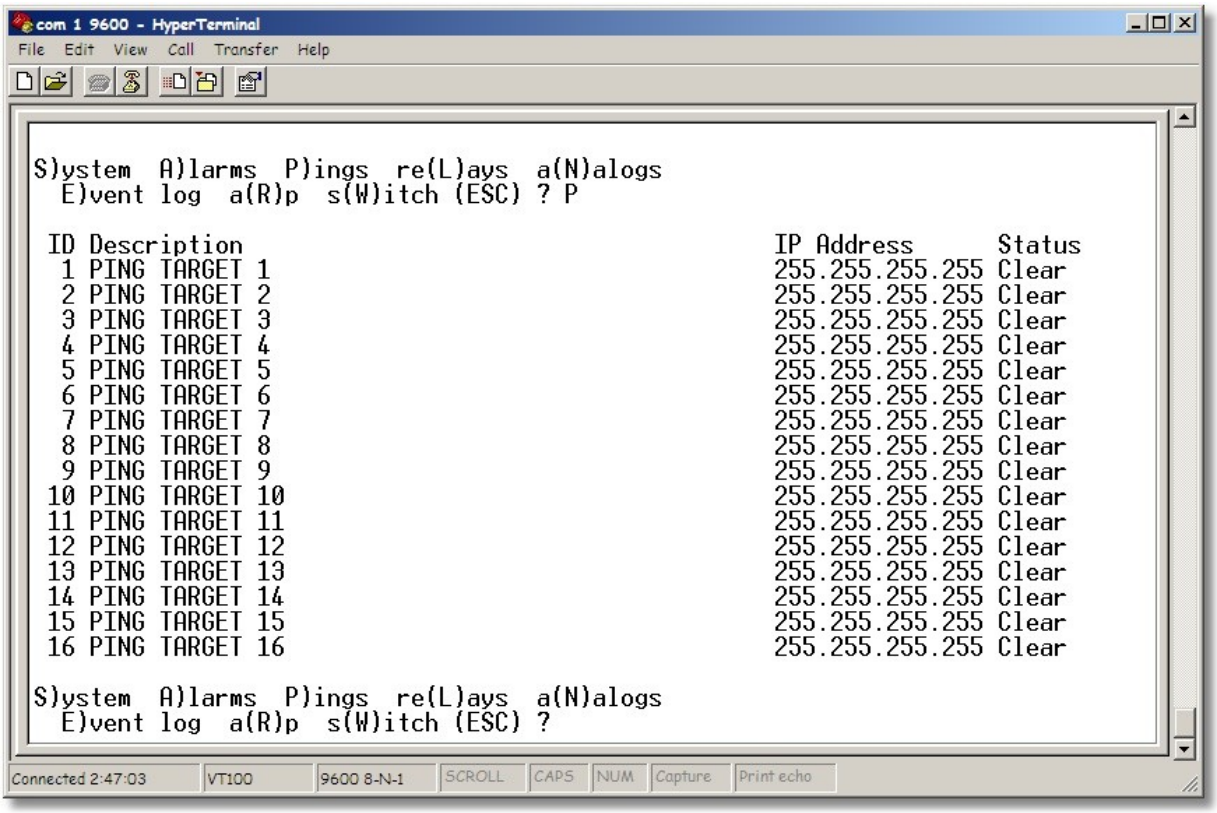
View the status of the device connected to the discrete alarms from the M)onitor menu > A)larms option. Under Status, the word Alarm will appear if an alarm has been activated and Clear will appear if an alarm condition is not present. If groups are used the user defined status will be displayed.



This example shows page two of the discrete alarms

11.3.1.2 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.

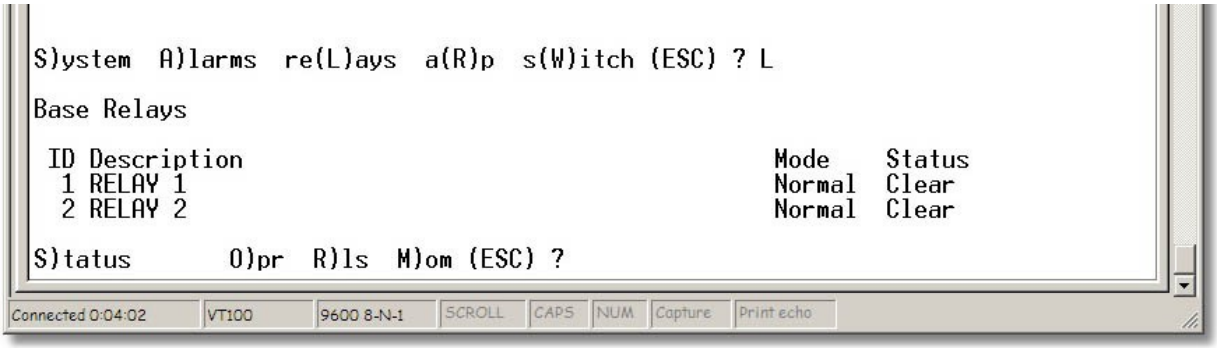


The Ping info submenu allows you to change ping targets

11.3.1.3 Monitoring and Operating Relays (Controls)

The NetGuardian comes equipped with 2 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.



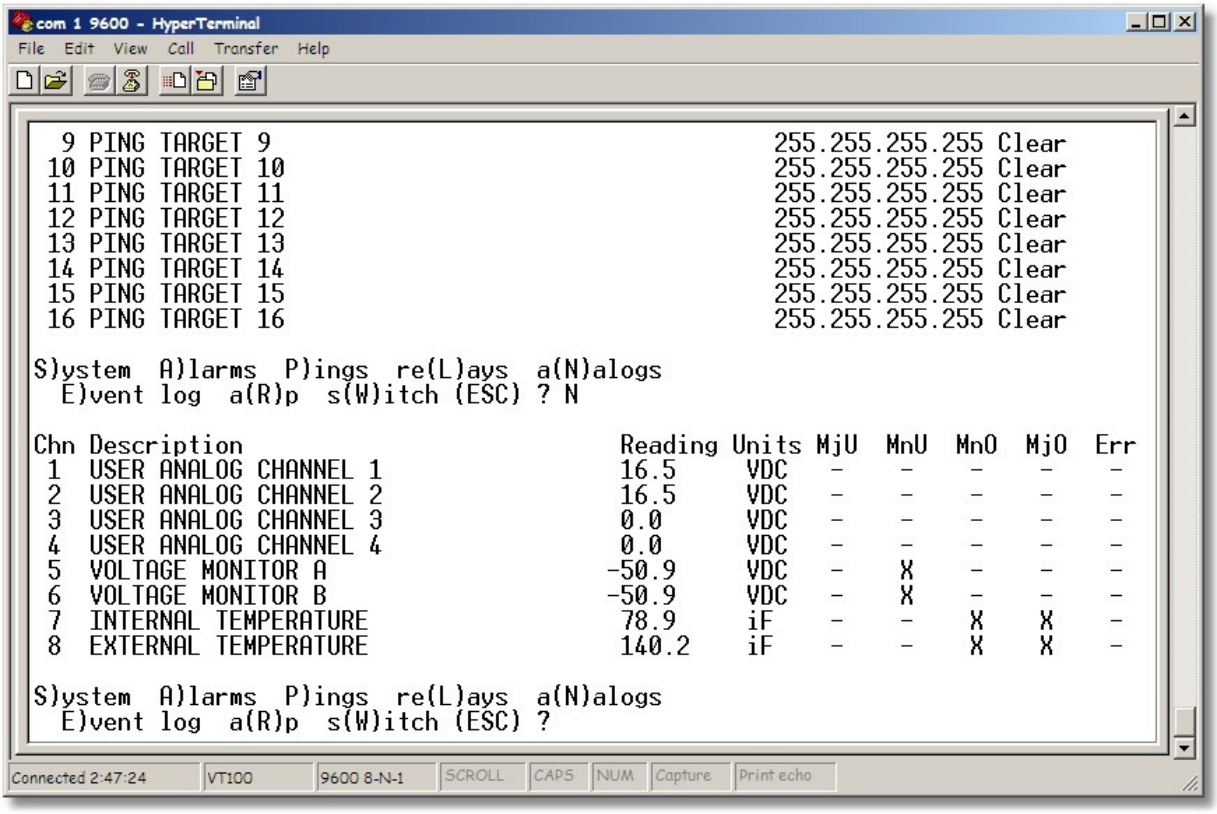
The relays can be operated from this screen

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

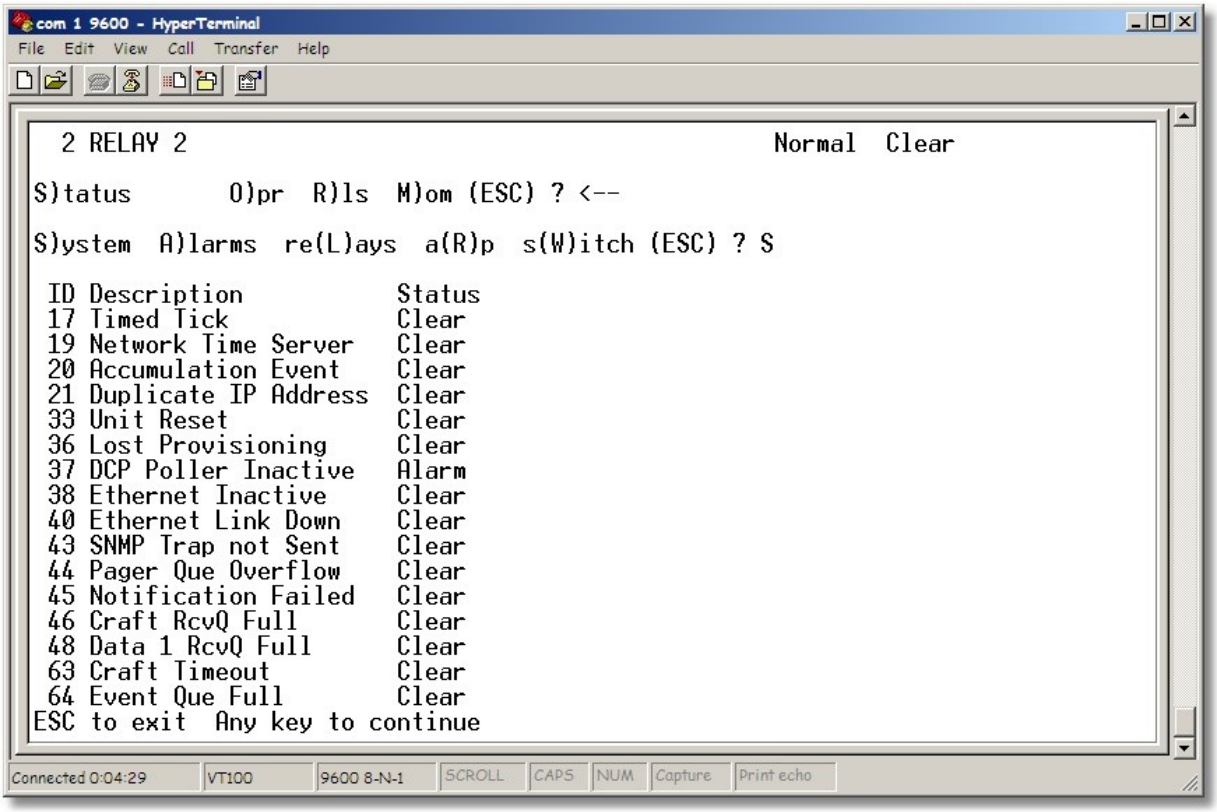
Note that channels 5 and 6 are reserved for Power Feed A and Power Feed B, respectively; and that channel 7 is reserved for internal temperature monitoring ("iF"=internal Fahrenheit) while channel 8 is for external temperature monitoring ("eF"=external Fahrenheit).



This display allows you to monitor your eight analog inputs

11.3.1.5 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 section: "System Alarms Display Map," for more information. If groups are used, the user defined status will be displayed.

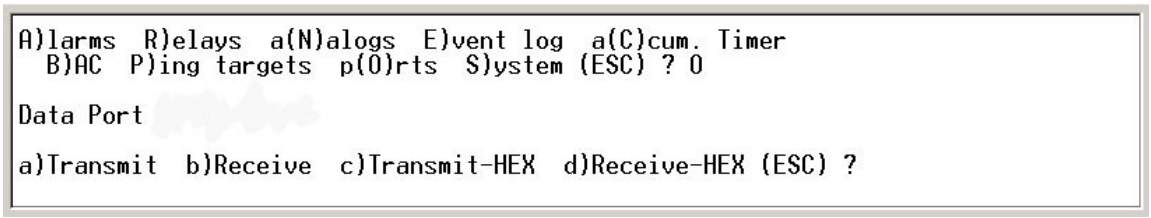


System Alarms can be viewed from the M)onitor menu > S)ystem option

11.3.1.6 Monitoring Data Port Activity

View the status of the NetGuardian's data port from the M)onitor menu > p(O)rts option.

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 Section 12.4, "ASCII Conversion," for specific ASCII symbol conversion.



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

11.3.1.7 Monitoring SFP Ports and Fiber Fault Detection

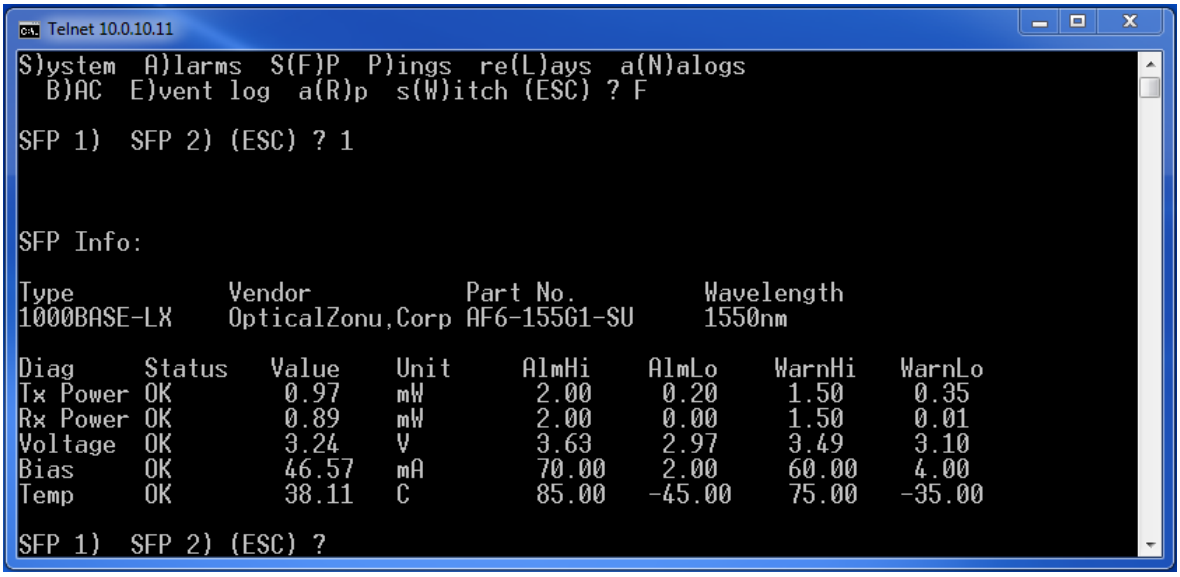
The NG216F can support 2 SPF connections.

When using a compatible OpticalZonu SFP transceiver, the contents of their registers can be read and the fiber connection status and parameters are displayed in the TTY interface.

The TTY interface displays information about the transceiver such as its Type, Vendor, Part No., and Wavelength, as well as diagnostic information on the connection status such as TX Power, RX Power, Voltage, Bias, and Temperature.

You can monitor SFP port 1 and port 2 individually by entering in the following commands, depending on which port you wish to monitor:

Port 1:
C)onfig → M)onitor → S(F)P → SFP 1) to view SFP port 1
Port 2:
C)onfig → M)onitor → S(F)P → SFP 2) to view SFP port 2



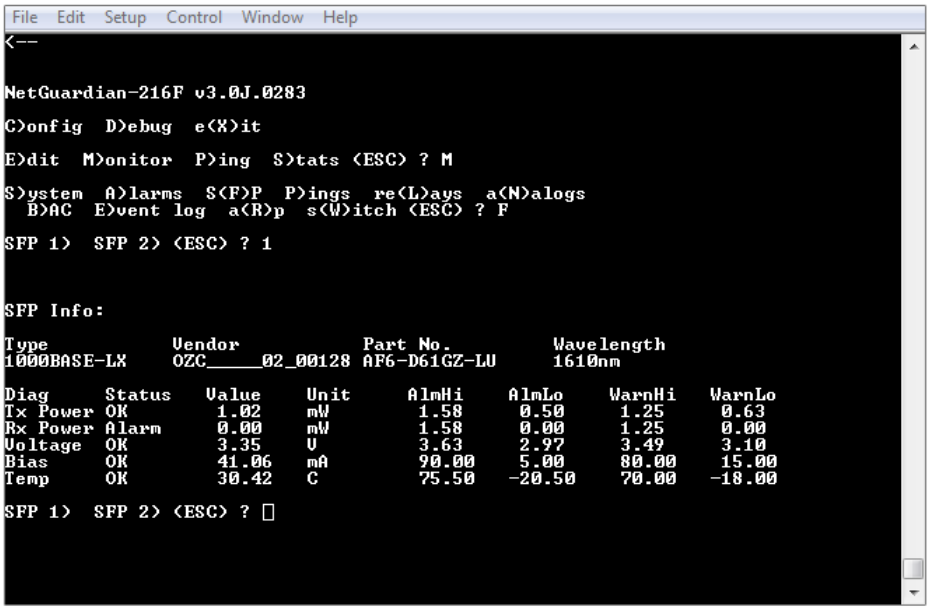
Fiber Fault Detection and Micro OTDR

If the SFP transceivers are Micro OTDR capable, the distance to the fiber fault will be displayed in this TTY interface when a fault is detected.

It will take 15 - 30 seconds after power up for the micro OTDR to run.

Once micro OTDR runs, the vendor name field will change from OpticalZonu,Corp to OZC followed by OTDR data:

1. The first number after OZC indicates the number of reflections (02 in the example below).
2. The second number x2 indicates distance to the farthest fault (00128 in the example below means fault is 256m away [128 x 2]).



11.3.2 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.

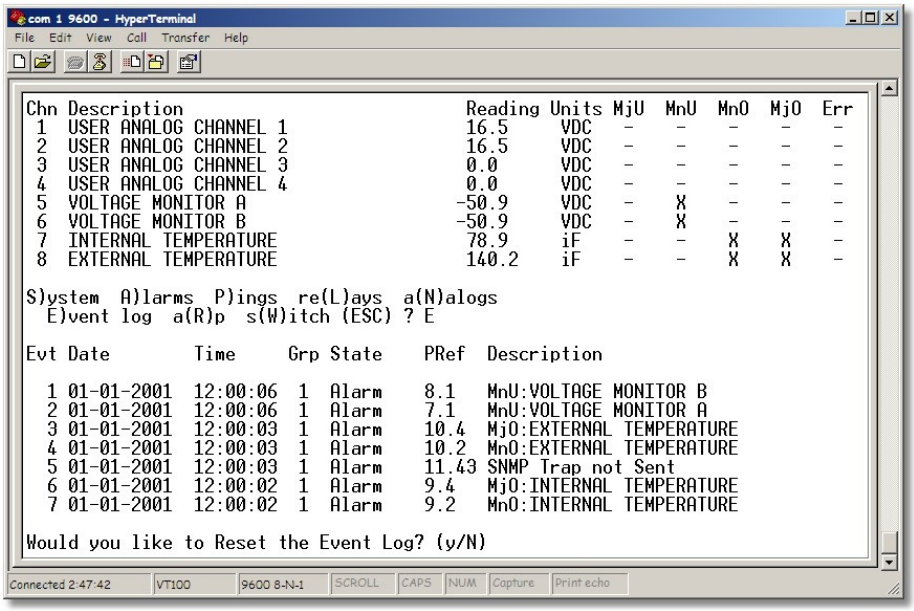
```
E)dit  M)onitor  P)ing  S)tats  R)eset Port (ESC) ? P

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

Continuously ping an IP address that has been defined in the NetGuardian's ping table

11.3.3 Event Logging

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

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



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.

Event Log field descriptions

11.3.4 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 (example: 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 (example: 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.

11.3.4.1 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 (example: 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 (example: put ngdbkup.ngd).
8. Type "literal REBT" to reboot the NetGuardian.
9. After reloading, type "bye" and press Enter to exit.

11.3.5 Debug Input and Filter Options

Debug Input Options	
ESC	Exit Debug
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	Alarm toggle switch. Shows posting of alarm data
A	Analog toggle switch. Shows TTY interface debug
c	Config toggle switch. Shows TTY interface debug
C	Control relay toggle switch. Shows relay operation
d	DCP responder toggle switch. Shows DCP protocol
D	Device toggle switch. Shows telnet and proxy information and NGEdit4 serial communication.
e	Expansion poller toggle switch. Shows NGDdx polling
f	FTP Command toggle switch. Shows command string parsing
F	FTP Data toggle switch. Shows FTP Read / Write
G	GLD poller toggle switch. Shows GLD polling
h	HTML debug switch. Shows Web Browser processing
H	HDLC debug switch. Shows SFP Fiber Interface channel protocol activity
i	PING toggle switch
k	Socket toggle switch. Shows current dcu resources
o	Osstart toggle switch. Miscellaneous application debug, including NVRAM read and write operation, and event posting
b	IP broadcasting block. Shows IPA
p	SPORT toggle switch. Port init debug and channeled port debug
q	QAccess toggle switch. Reserved for future use
r	Report toggle switch. Shows reporting event activity, including SNMP, pagers, email, etc. Also shows PPP negotiation for NG client PPP mode.
s	(SNMP toggle switch. Reserved for future use
S	STAK toggle switch. Shows network processing and IPA of arp requests. Also shows packets discarded by Filter IPA.
t	TERM toggle switch. Shows UDP/TCP port handling. The camera and network time (NTP) jobs also use the TERM toggle switch
w	HTTP toggle switch. Shows handling of web browser packets
W	WEB toggle switch 2. Dump HTML text from web browser

Debug Input and Filter Options (previous page)

12 Reference Section

12.1 Display Mapping

Port	Address	Display	Description	Set	Clear
99	1	1	Discrete Alarms 1-16	8001-8016	9001-9016
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–Power Feed A**	8385-8388	9385-9388
99	1	8	Analog Channel 6–Power Feed B**	8449-8452	9449-9452
99	1	9	Analog Channel 7–Internal Temp Sensor**	8513-8516	9513-9516
99	1	10	Analog Channel 8–External Temp Sensor**	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	13	NetGuardian Expansion 1 Relays 1-8	6065-6072	7065-7072
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

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
9	Undefined**	8649	9649
10	Undefined**	8650	9650
11	Undefined**	8651	9651
12	Undefined**	8652	9652

Display 11 System Alarms point descriptions (continues on next page)

		SNMP Trap #s	
Points	**Description**	**Set**	**Clear**
13	Undefined**	8653	9653
14	Undefined**	8654	9654
15	Undefined**	8655	9655
16	Undefined**	8656	9656
17	Timed Tick	8657	9657
18	Exp. Module Callout	8658	9658
19	Netw ork Time Server	8659	9659
20	Accumulation Event	8660	9660
21	Duplicate IP Address	8661	9661
22	Undefined**	8662	9662
23	Undefined**	8663	9663
24	Undefined**	8664	9664
25	Undefined**	8665	9665
26	Undefined**	8666	9666
27	Undefined**	8667	9667
28	Undefined**	8668	9668
29	Undefined**	8669	9669
30	Undefined**	8670	9670
31	Undefined**	8671	9671
32	Undefined**	8672	9672
33	Unit Reset	8673	9673
34	Undefined**	8674	9674
35	Undefined**	8675	9675
36	Lost Provisioning	8676	9676
37	DCP Poller Inactive	8677	9677
38	NET1 not active	8678	9678
40	NET Link Dow n	8680	9680
41	Modem not	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	Data 1 RcvQ full	8688	9688
49	Data 2 RcvQ full	8689	9689
50	Data 3 RcvQ full	8690	9690
51	Data 4 RcvQ full	8691	9691
52	Data 5 RcvQ full	8692	9692
53	Data 6 RcvQ full	8693	9693
54	Data 7 RcvQ full	9694	9694

Display 11 System Alarms point descriptions (continues on next page)

		SNMP Trap #s	
Points	**Description**	**Set**	**Clear**
55	Data 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/BSU 1 Fail	8699	9699
60	GLD/BSU 2 Fail	8700	9700
61	GLD/BSU 3 Fail	8701	9701
62	CHAN timeout	8702	9702
63	Craft Timeout	8703	9703
64	Event Que Full	8704	9704

Display 11 System Alarms point descriptions (continued)

***** Data Ports 2-5 are included on optional expansion card.

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

12.1.1 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.
	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.
	21	Duplicate IP Address	The unit has detected another node with the same IP Address.	Unplug the LAN cable and contact your network administrator. Your network and the unit will most likely behave incorrectly. After assigning a correct IP Address, reboot the unit to clear the System alarm.
	33	Power Up	The unit has just come-online. The set alarm condition is followed immediately by a clear alarm condition.	Seeing this alarm is normal if the unit is powering up.
	36	Lost Provisioning	The internal NVRAM may be damaged. The unit is using default configuration settings.	Use Web or latest version of NGEditG5 to configure unit. Power cycle to see if alarm goes away. May require RMA.
	37	DCP Poller Inactive	The unit has not seen a poll from the Master for the time specified by the DCP Timer setting.	If DCP responder is not being used, then set the DCP Unit ID to 0. Otherwise, try increasing the DCP timer setting under timers, or check how long it takes to cycle through the current polling chain on the Master system.
	38	Ethernet not active	The Net1 LAN port is down.	Check LAN cable. Ping to and from the unit. (If not using Net1 or Net2, set IP, Subnet and Gateway to 255's)
	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.
	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.

System Alarms Descriptions (continues on next page)

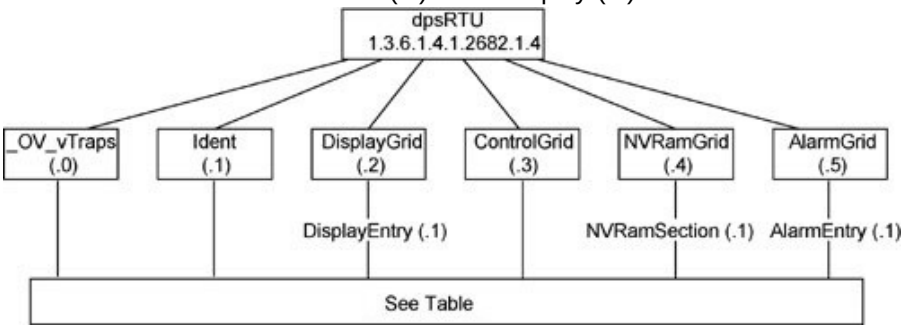
Display	Points	Alarm Point	Description	Solution
11	48	Serial 1 RcvQ full	Serial port 1 (or appropriate serial port number) receiver filled with 8 K of data (4 K if BAC active).	Check proxy connection. The serial port data may not be getting collected as expected.
	49	Serial 2 RcvQ full		
	50	Serial 3 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		

System Alarms Descriptions (continued)

*Data Ports 2-5 are included on optional expansion card.

12.2 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 1.3.6.1.4.1.2682.1.2. Each level beyond dpsRTU adds another object identifying number. For example, the object identifier of the Display portion of the Control Grid is 1.3.6.1.4.1.2682.1.2.3.3 because the object identifier of dpsRTU is 1.3.6.1.4.1.2682.1.2 + the Control Grid (.3) + the Display (.3).



Tbl. B1 (O.)_OV_Traps points
_OV_vTraps (1.3.6.1.4.1.2682.1.2.0)
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 (1.3.6.1.4.1.2682.1.2.1)
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 (1.3.6.1.4.1.2682.1.2.2.1)
Port (.1)
Address (.2)
Display (.3)
DispDesc (.4)*
PntMap (.5)*

Tbl. B3 (.3) ControlGrid points
ControlGrid (1.3.6.1.4.1.2682.1.2.3)
Port (.1)
Address (.2)
Display (.3)
Point (.4)
Action (.5)

Tbl. B5 (.5) AlarmEntry points
AlarmEntry (1.3.6.4.1.2682.1.2.5.1)
Aport (.1)
AAddress (.2)
ADisplay (.3)
APoint (.4)
APntDesc (.5)*
AState (.6)
* For specific alarm points, see Table B6

Hot Tip! The NetGuardian 216F OID has changed from 1.3.6.1.4.1.2682.1.4 to 1.3.6.1.4.1.2682.1.2 Updated MIB files are available on the Resource CD or upon request.

	Description	Port	Address	Display	Points
Disp 1	Discrete Alarms	99	1	1	1-32
	Undefined**	99	1	1	33-64
Disp 2	Ping Targets	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	Relays 1-8	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
	Accumulation Event	99	1	11	20
	Duplicate IP Address	99	1	11	21
	Undefined**	99	1	11	22-32
	Unit Reset	99	1	11	33
	Undefined**	99	1	11	34-35
	Lost Provisioning	99	1	11	36
	DCP poll inactive	99	1	11	37
	NET 1 not active	99	1	11	38
	NET 2 not active	99	1	11	39
	NET link down	99	1	11	40
	Modem not responding	99	1	11	41
	No dial-tone	99	1	11	42
	SNMP trap not sent	99	1	11	43
	Pager Queue Overflow	99	1	11	44
	Notification failed	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

Alarm point descriptions (continues on next page)

	Description	Port	Address	Display	Points
	NGDdx 1-3 fail	99	1	11	56-58
	GLD/BSU 1-3 fail	99	1	11	59-61
	CHAN timeout	99	1	11	62
	CRFT timeout	99	1	11	63
	Event Que Full	99	1	11	64

Alarm point descriptions (continued)

* "No data" indicates that the alarm point is defined but there is no description entered.
** "Undefined" indicates that the alarm point is not used.
^ Data Ports 2-5 are included on optional expansion card.

12.3 SNMP Granular Trap Packets

Tables 12.3.A and 12.3.B provide a list of the information contained in the SNMP Trap packets sent by the NetGuardian.

SNMP Trap managers can access alarm information via either:

- Granular traps (not necessary to define point descriptions for the NetGuardian)

Or

- The SNMP manager reads the description from the Trap.

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

UDP Headers and descriptions

SNMP Header	Description
0	Version
Public	Request
Trap	Request
1.3.6.1.4.1.2682.1.2	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 216F v1.0B	Value
1.3.6.1.2.1.1.6.0	Object
1-800-622-3314	Value
1.3.6.1.4.1.2682.1.2.4.1.0	Object
01-02-1995 05:08:27.760	Value
1.3.6.1.4.1.2682.1.2.5.1.1.99.1.1.1	Object
99	Value
1.3.6.1.4.1.2682.1.2.5.1.4.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.2.5.1.3.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.2.5.1.2.99.1.1.1	Object
1	Value
1.3.6.1.4.1.2682.1.2.5.1.5.99.1.1.1	Object
Rectifier Failure	Value
1.3.6.1.4.1.2682.1.2.5.1.6.99.1.1.1	Object
Alarm	Value

SNMP Headers and descriptions

12.4 ASCII Conversion

The information contained in Table 12.4.A 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 port. 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. [lF]).
- A received BREAK will appear as <BRK>.

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

ASCII symbols

13 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.dpstele.com .**

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

13.1 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 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.

Telnet is connected through the 10BaseT switch. Make sure you're connected to one of the switch's 7 connectors.

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 Edit216F 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 Edit216F

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 Edit216F 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.

13.2 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 two 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 Edit216F 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.

14 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 voicemail message(the only time DPS allows voicemail!!). You will be asked to enter your phone number. An on-call technical support representative will return your call as soon as possible. If the on-call staff is unable to resolve the problem, they will be able to escalate the call to the appropriate DPS personnel.*

Technical support features have been built into many of our products. In many cases, our technicians, in conjunction with customer permission, can dial directly into our units to correct problems first-hand.

15 RMA Policy

DPS Telecom guarantees all products for two years. We will repair any deficiency in workmanship during this warranty period free of charge. DPS Telecom products not under warranty can still be repaired with a service charge.

In the event that a DPS Telecom product needs repaired, contact Technical Support and a technician can help solidify the field diagnosis, and issue and RMA number if needed. An RMA will be issued if the product has a failed feature or component, if the technicians are unable to resolve the issue remotely, or if the wrong product is ordered or shipped.

DPA Telecom, on average, returns RMA units within 4 weeks and will email the RMA submitter on the return shipment with a tracking number.

Under urgent circumstances, DPS Telecom will issue an advanced replacement. DPS Telecom will send a replacement unit in advance if the problem affects service or if technicians can better troubleshoot an issue. In both cases the advance replacement depends on DPS Telecom stock on hand.

16 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.

Index

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

DPS Telecom

"Your Partners in Network Alarm Management"

www.dpstelecom.com

4955 E Yale • Fresno, CA 93727

559-454-1600 • 800-622-3314 • 559-454-1688 fax