MDS™ TransNEXT

MDS TransNEXT Technical Manual, Rev. C
December 2025

(covering firmware 3.1.0 and higher)

GE VERNOVA

Technical Manual

TABLE OF CONTENTS

Copyright and Trademark

RF Regulatory Information

RF Exposure Notice (English and French)

RF Exposure

Concentrated energy from a directional antenna may pose a health hazard to humans. Do not allow people to come closer to the antenna than the distances listed in the table below when the transmitter is operating. More information on RF exposure can be found online at the following website: www.fcc.gov/oet/info/documents/bulletins

l'exposition aux RF

Concentré d'énergie à partir d'une antenne directionnelle peut poser un risque pour la santé humaine. Ne pas permettre aux gens de se rapprocher de l'antenne que les distances indiquées dans le tableau ci-dessous lorsque l'émetteur est en marche. Plus d'informations sur l'exposition aux RF peut être trouvé en ligne à l'adresse suivante: www.fcc.gov/oet/info/documents/bulletins

Antennas must not be co-located. All transmission antennas must be at least 20 cm apart to comply with FCC co-location rules.

TransNEXT Minimum RF Safety Distance

TransNEXT Model	Minimum Safety Distance from Antenna operating with a 10dBd (12.15dBi) antenna and so configured for the maximum allowable EiRP of +36dBm
NET9L	34 cm
NET9B	34 cm
NET9S	34 cm

Approved Antennas

This product has been approved for use with the antennas listed in Table 1-1, below:

Manufacturer	Manufacturer's Part Number	Type	Gain (dBi)/per port	For use with (E5MDS- or 101D-)
Kathrein	OGB9-915N	Omni	11.0	NET9B/NET9L
PCTEL	Z2336	Yagi	12.2	NET9B/NET9L
Hana Wireless	HW-OD9-6D-NF	Dual-Polarized Omni	6.0	NET9S
PCTEL	BMYD890K-DP	Dual-Polarized Yagi	12.2	NET9S

Table 1-1. Approved Antennas for TransNEXT

Professional installation is required. The installation site must conform to 15.247/RSS-247 Conducted and Radiated Power limits. Proper feedline selection and/or radio power setpoints must be set accordingly for use with each antenna type as detailed in Table 1-2.

Radio Model	Antenna Model	Radio Power Setpoint (dBm)	Minimum Cable Loss required for this configuration (dB)	Conducted Power into antenna (dBm) *Note 1*	EIRP (dBm) *Note 2*
NET9B/NET9L	OGB9-915N	30	5.0	25	36
		25	0.0	25	36
NET9B/NET9L	Z2336	30	6.2	23.8	36
		24	0.2	23.8	36
NET9S	HW-OD9-6D-NF	30	3.0	30	36
		27	0.0	30	36
NET9S	BMYD890K-DP	30	8.0	25	36
		22	0.0	25	36

Note 1: Conducted Power into antenna is the sum of the power of both transmitter feedline outputs for NET9S
Note 2: EIRP is the sum of the radiated power of all polarizations for NET9S

Table 1-2. Feedline losses and radio power setpoints for ERP and Conducted Power compliance for TransNEXT installations.

FCC Part 15 Notice and Industry Canada RSS Notices

This device complies with Part 15 of the FCC rules for a Class A digital device. Operation of this device subject to the following two conditions:

(1) this device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation. Any unauthorized modification or changes to this device without the express approval of the manufacturer may void the user’s authority to operate this device. Furthermore, this device is intended to be used only when installed in accordance with the instructions outlined in this guide. Failure to comply with these instructions may void the user’s authority to operate this device.

(a) Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

(b) The radio transmitters described herein (IC ID: 101D-NET9L and 101D-NET9S) have been approved by Industry Canada to operate with the antenna types listed in Table 1-1 with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Cet appareil est conforme à la Partie 15 des règlements de la FCC et Industrie Canada exempts de licence standard RSS (s). Son utilisation est soumise à deux conditions:

(1) ce dispositif ne peut causer des interférences,
(2) cet appareil doit accepter toute interférence pouvant causer un mauvais fonctionnement du dispositif.

(a) En vertu des règlements d'Industrie Canada, cet émetteur radio ne peut fonctionner avec une antenne d'un type et un maximum (ou moins) approuvés pour gagner de l'émetteur par Industrie Canada. Pour réduire le risque d'interférence aux autres utilisateurs, le type d'antenne et son gain doivent être choisies de façon que la puissance isotrope rayonnée équivalente (PIRE) ne dépasse pas ce qui est nécessaire pour une communication réussie.
(b) Les émetteurs radio décrits ici (IC ID : 101D-NET9L et 101D-NET9S) ont été approuvés par Industrie Canada pour fonctionner avec les types d'antennes répertoriés dans le tableau (Table 1-1) avec le gain maximum autorisé et l'impédance d'antenne requise pour chaque type d'antenne indiqué. Les types d'antennes non inclus dans cette liste, ayant un gain supérieur au gain maximum indiqué pour ce type, sont strictement interdits pour une utilisation avec cet appareil.

IEEE-1613 Compliance

The TransNEXT is IEEE-1613 compliant provided that unshielded cables are <= 2 meters in length.

Operational Safety Notices

The TransNEXT may not be used in an environment where radio frequency equipment is prohibited or restricted in its use. This typically includes aircrafts, airports, hospitals, and other sensitive electronic areas.

Do not operate RF devices in an environment that may be susceptible to radio interference resulting in danger, specifically:

- **Areas where prohibited by law -** Follow any special rules and regulations and obey all signs and notices. Do not use the TransNEXT when you suspect that it may cause interference or danger.
- **Near Medical and life support equipment -** Do not use the TransNEXT in any area where medical equipment, or life support equipment may be located, or near any equipment that may be susceptible to any form of radio interference.
- **All cables and conductors making connections to the units need to be rated at 85 °C or higher.**
- **Use Copper Conductors Only**
- **Use 18 AWG wire**

NOTE The TransNEXT does not support Voice Communications.

Regulatory Limitations

Some product options including hardware and software configuration settings may be restricted based on applicable region-specific regulatory constraints.

FCC / IC IDs

As of the printing date, the following identifiers are assigned to the TransNEXT models listed below.

Model	FCC ID	IC ID
NET9B	E5MDS-NET9L	101D-NET9L
NET9L	E5MDS-NET9L	101D-NET9L
NET9S	E5MDS-NET9S	101D-NET9S

Country-Specific Installation Data

Refer to APPENDIX D – Country Specific Information at the back of this manual for important notices regarding installation in specific countries.

Servicing Precautions

No user-serviceable parts are contained inside this equipment. Opening of the unit by unauthorized personnel voids the warranty. All servicing must be performed by an authorized repair facility.

When servicing energized equipment, be sure to wear appropriate Personal Protective Equipment (PPE). During internal service, situations could arise where objects accidentally contact or short circuit components and the appropriate PPE would alleviate or decrease the severity of potential injury. When servicing equipment, all workplace regulations and other applicable standards for live electrical work should be followed to ensure personal safety.

Manual Revision and Accuracy

This manual was updated to cover a specific version of firmware code. Accordingly, some screens and features may differ from the actual unit you are working with. While every reasonable effort has been made to ensure the accuracy of this publication, product improvements may also result in minor differences between the manual and the product shipped to you. If you have additional questions or need an exact specification for a product, please contact GE Vernova using the information at the back of this guide. In addition, manual updates can be found on our website at https://www.gevernova.com/grid-solutions/automation/critical-infrastructure-communications#industrial-wireless.

Environmental Information

The manufacture of this equipment has required the extraction and use of natural resources. Improper disposal may contaminate the environment and present a health risk due to hazardous substances contained within. To avoid dissemination of these substances into our environment, and to limit the demand on natural resources, we encourage you to use the appropriate recycling systems for disposal. These systems will reuse or recycle most of the materials found in this equipment in a sound way. Please contact GE Vernova or your supplier for more information on the proper disposal of this equipment.

Cyber Security Policy

As part of GE Vernova's commitment to product safety, quality and reliability and to reduce risk exposure for GE Vernova and our customers, the "GE Vernova Product Cyber Security Standard" (the Policy) outlines the requirements that GE Vernova Business Units must meet. The Policy, requires each GE Vernova Business Unit to implement reasonable, industry-specific measures designed to protect all GE Vernova products and services, including all relevant components and services sourced from third parties, from cyber security threats throughout their supported life cycle.

Safety Regulatory Information

MET
E116185

MET Mark and Safety Notice

This product is approved for use in Class 1, Division 2, Groups A, B, C & D Hazardous Locations. Such locations are defined in Article 500 of the National Fire Protection Association (NFPA) publication NFPA 70, otherwise known as the National Electrical Code. The transceiver has been recognized for use in these hazardous locations by MET Laboratories, Inc. which issues both a US and Canadian MET mark. Certification is in accordance with UL 121201:2017 - Ninth Edition and CSA STD C22.2 No. 213-17 - Third Edition.

For Class I, Division 2, the product shall be installed in a tool secured enclosure providing a suitable degree of protection against deterioration of the equipment that would adversely affect its suitability for use in the hazardous locations area and to avoid USB-C diagnostic port /connectors from being accessible during normal operation. The antenna port shall be used with a passive antenna only. The final installation is subject to acceptance of Met Laboratories or the local inspection authority having jurisdiction.

⚠ *WARNING – EXPLOSION HAZARD. DO NOT REMOVE OR REPLACE WHILE CIRCUIT IS LIVE UNLESS THE AREA IS FREE OF IGNITIBLE CONCENTRATIONS*

⚠ *WARNING – EXPLOSION HAZARD. DO NOT CONNECT OR DISCONNECT WHEN ENERGIZED*

⚠ *AVERTISSEMENT – RISQUE D'EXPLOSION. NE PAS RETIRER OU REMPLACER LORSQUE LE CIRCUIT EST SOUS TENSION À MOINS QUE LA ZONE NE SOIT EXEMPTE DE CONCENTRATIONS INFLAMMABLES*

⚠ *AVERTISSEMENT – RISQUE D'EXPLOSION. NE PAS CONNECTER OU DÉCONNECTER LORSQU'IL EST SOUS TENSION*

1.0 Product Overview and Applications

1.1 Introduction

This manual describes the MDS TransNEXT ™. The TransNEXT is the successor to the MDS TransNET™ 900 MHz unlicensed radio. Setting the standard for reliable, long-range wireless serial data transmission utilizing proven Frequency Hopping Spread Spectrum (FHSS) technology, the next generation TransNEXT is backwards-compatible with its predecessor, TransNET. The TransNEXT' s backwards compatibility enables the continued use of legacy serial networks while also adding new capabilities to migrate networks with secure Ethernet connectivity.

In addition to TransNET backward compatibility, TransNEXT offers additional modes for Point-to-Multipoint Ethernet Bridging and Mirrored Bits™ compatible operation.[1]

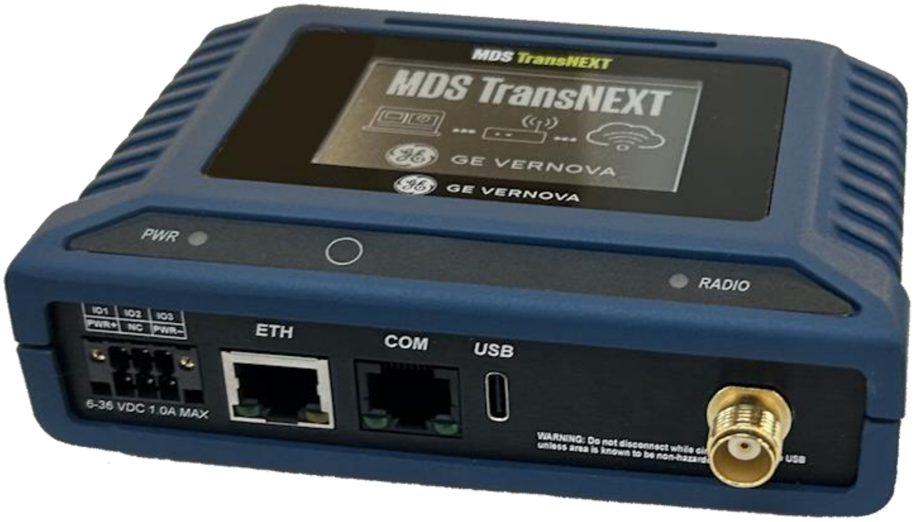


Figure 1-1. TransNEXT with Display
(model NXTNET9B)

Information on other MDS brand industrial wireless products can be found by visiting our website at https://www.gevernova.com/grid-solutions/automation/critical-infrastructure-communications#industrial-wireless.

1.2 Feature Offerings and Compatibility

The TransNEXT is offered with different factory-configured options and provides various user-level feature and mode controls. Some features are mode-dependent and will not be applicable or available in certain modes of operation.

[1] "Mirrored Bits" is a registered trademark of Schweitzer Engineering Laboratories, Inc. (SEL).

1.3 About This Manual

This manual is intended for systems engineers, network administrators and others responsible for planning, commissioning, installing, using and troubleshooting the wireless system. Electronic copies of all user documentation are available free of charge at https://www.gevernova.com/grid-solutions/resources?prod=TransNEXT&type=3&node_id=4693

Software Command Notations

The product is designed for software control via a connected PC. To show the names of software commands, keyboard entries, or other information displayed on a PC screen, a bolded font is used throughout the manual. In some cases, italics or non-bolded sections may be used to distinguish fixed syntax from portions of a command where the user must supply specific data.

For example:

```
[1234567] Login: admin
```

NOTE Software commands and responses shown in this manual are representative and are based on data from units operating in a lab environment. Information displayed may differ from field service units and may differ based on active software version.

2.0 Product Description

The TransNEXT is a rugged license-free wireless communication device well suited for a variety of SCADA and telemetry solutions using serial and IP/Ethernet.

2.1 Key Features

TransNEXT units include the following key features:

- **Backwards-Compatible –** Over-the-Air Compatible with TransNET, with similar or better RF performance in real-world field installations**.**
- **Ethernet Bridging (*select models only*)** – Layer 2 bridging of Ethernet packets over the air.
- **Mirrored Bits – Compatible (*select models only*)** – Point-to-Point connection of devices that run SEL Mirrored Bits™ protocol
- **IP Payload -** First introduced in the MDS SD™ this facility performs conversion of local ethernet to serial over-the-air, providing an efficient means to connect compatible ethernet devices to a serial network.
- **Over-the-air (OTA) Reprogramming –** This facility provides a simple means to non-intrusively broadcast a firmware upgrade to an entire field of remotes, using a copy of the firmware image currently running in the TransNEXT master radio. This feature operates slowly to avoid conflicting with payload data and to allow interoperability through an existing TransNET network.
- **Optional E-ink display (*select models only*)** – This display provides a convenient tool for installation, local diagnostics, and troubleshooting. The E-ink display maintains the last screen image following a power failure.
- **Small Form Factor**—The unit is housed in a rugged enclosure suited for operation in harsh industrial environments. It requires only protection from direct exposure to the weather and may be easily mounted inside a NEMA enclosure for outdoor applications when required.
- **User Interface**—Multiple user interfaces are provided for configuration and monitoring of the unit. These include USB, web, SSH and local serial *(using "+++" to temporarily override the payload data interface*)

NOTE The TransNEXT is designed for secure environments. As such, management of the device does not support Telnet, but instead implements the more secure SSH protocol.

NOTE For units certified and installed in hazardous locations, use only the serial or Ethernet connections on the unit's front panel. Do *not* use the USB port in hazardous locations.

- **Network Management System**— TransNEXT is supported by MDS PulseNET, a Network Management System (NMS), providing monitoring of small- and large-scale deployment of all MDS devices. (*** for interoperability, TransNEXT appears as a TransNET device)

2.2 Typical Applications

MDS TransNEXT is the successor to the MDS TransNET radio. It builds on the flexibility of the predecessor product and serves a wide variety of traditional applications.

Multiple Address Systems (MAS)

This is the most common application of the transceiver. It consists of a central control station (Master) and two or more associated Remote units. An MAS network provides communications between a central host computer and remote terminal units (RTUs) or other data collection devices. The operation of the radio system is transparent to the computer equipment. When used in this application, the transceiver provides an excellent alternative to traditional (licensed) MAS radio systems.

Point-to-Point System

A point-to-point configuration is a simple arrangement consisting of just two radios—a Master and a Remote. This provides a half-duplex communications link for the transfer of data between two locations.

Adding a Tail-End Link to an Existing Network

A tail-end link can be used to extend the range of a traditional (licensed) MAS system. This might be required if an outlying site is blocked from the MAS Master station by a natural or man-made obstruction. In this arrangement, a TransNEXT radio links the outlying Remote site into the rest of a licensed MAS system by sending data from that site to an associated TransNEXT installed at one of the licensed Remote sites.

As the data from the outlying site is received at the licensed Remote site, it is transferred to the licensed radio (via a local cable connection) and is then transmitted to the MAS Master station in the usual manner.

Extending a TransNEXT Network with a Network Repeater

Similar to a Tail-End Link, Store-and-Forward (SAF) offers a way to physically extend the network range, but in a simple and economical manner. SAF works by dividing a network into a vertical hierarchy of two or more sub-networks. Extension radios (designated in TransNEXT as radio.mode “x”) serve as single-radio repeaters that link adjacent sub-networks and move data from one sub-network to the next one.

Interworking with a TransNET network

Each of the application types above can be supported by introducing a TransNEXT radio into an existing TransNET network, replacing older radios or extending communication and new features to new sites.

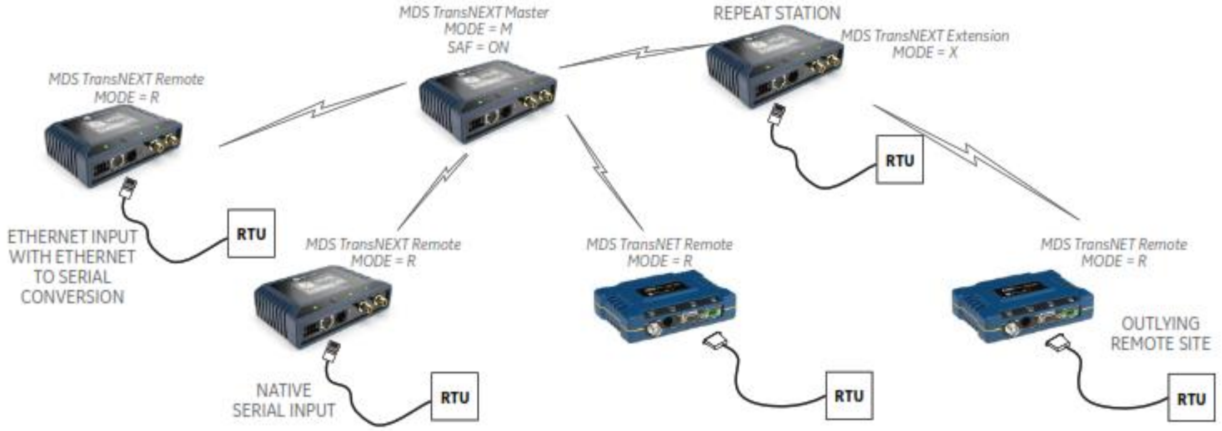


Figure 2-1. Mixed TransNEXT & TransNET Application

On-Demand and Report-by-Exception using Ethernet and Serial

In Bridge mode, the TransNEXT employs a high-performance media access control method to share the channel and support unsolicited communication. In the example below a Data Control Center communicates with a mixed field of ethernet and serial RTUs. Devices can be polled or can send data autonomously.

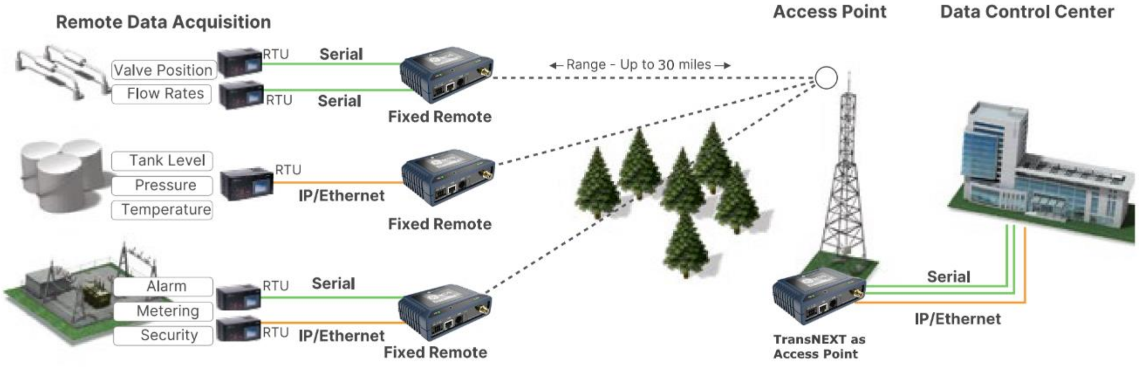


Figure 2-2. Ethernet and Serial Application

2.3 TransNEXT Connectors and Indicators

Figure 2-3 shows the unit's front panel connectors and indicators. These items are referenced in the text that follows. The unit's LED Indicator / Button Panel is described in Figure 2-6.

.

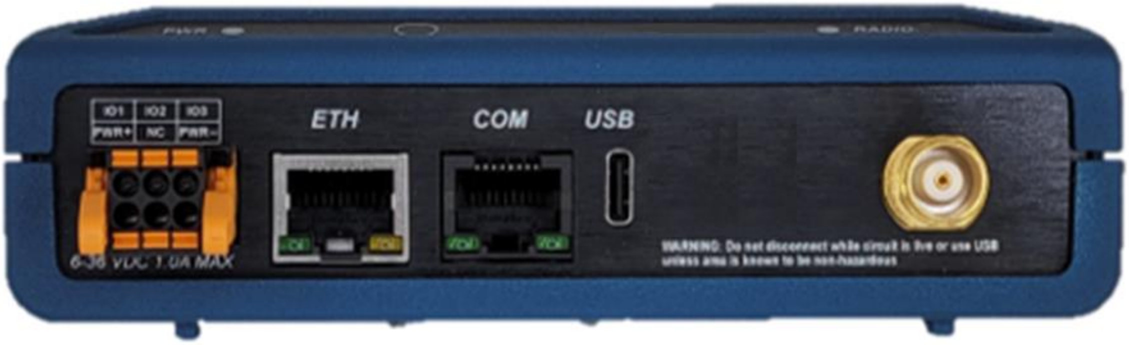

PWR
RADIO
IO1
IO2
IO3
PWR+
NC
PWR–
ETH
COM
USB
6-36 VDC 1.0A MAX
WARNING: Do not disconnect while circuit is live or use USB unless area is known to be non-hazardous

Figure 2-3. TransNEXT, Connectors and Indicators

PWR & I/O —Two-conductor DC input connection and I/O

- A latching 6-pin connector is used (Figure 2-4). It is keyed and can only be inserted one way.
- PWR+ (shown with red wire attached) is Vin.
- PWR- (shown with black wire attached) is Ground.
- IO1, IO2, and IO3 are reserved for future I/O capability.
- Use Copper Conductors Only
- Use 18 AWG wire
- Tighten wire clamps to 5 in-lb. (0.6 Nm)
- Connector is P/N 73-1194A85, Phoenix Contact MFG P/N 1711658

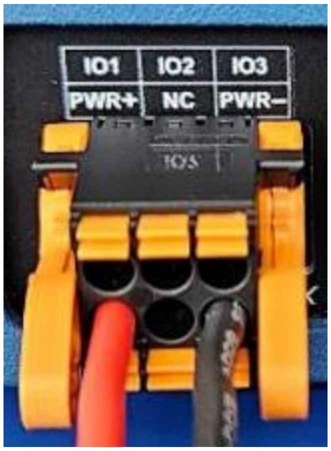


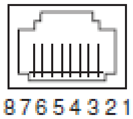
Figure 2-4. 6-pin Power & I/O Connector (P/N 73-1194A85)

NOTE The unit is designed for use in negative ground DC power systems only. Only use the power supply provided by the manufacturer for the product or a certified LPS power supply rated for nominal power 6-36 VDC, 1.6 A maximum must be used. Otherwise, safety of the product may be impaired. In case of doubt, please consult the local authorized suppliers.

Input voltage to the unit must be well filtered and within the nominal range of 6-36 VDC. The maximum rated power consumption of the device is 10 watts, but actual power is typically much less. The power supply must be capable of supplying the expected maximum power for the installation. For expected power requirements in common configurations, see "
on Page 77.

ETH— Ethernet connection port. This port supports both device management and payload data transport. This is a standard RJ-45 jack and features MDIX auto-sensing capability, allowing straight-through or crossover cables to be used.

Connecting to the unit via SSH supports device management and provides a similar user interface available using the unit's serial COM port.



(As viewed from the outside the unit)

Table 2-1. ETH1/2 Pin Details

Pin	Function	Pin	Function
1	Transmit Data (TX) High	5	Unused
2	Transmit Data (TX) Low	6	Receive Data (RX) Low
3	Receive Data (RX) High	7	Unused
4	Unused	8	Unused

USB Port—This port provides a USB-C connection to a laptop or PC. The port provides a local console for management of the device. A standard host-to-USB-C cable may be used.

COM Port—This connector serves as the serial interface port for payload data. The COM port serves as the primary interface for connecting the unit to an external DTE serial device supporting RS-232 or RS-485. If necessary, an adapter may be used to convert the unit's RJ-45 serial jack to a DB-9F type (MDS 73-2434A25).

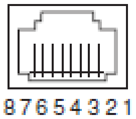
NOTE TransNEXT typically uses the unit's USB port to access the device management interface (CLI). As an alternate access method typing "+++" on the COM port (at roughly half second intervals) will cause it to drop out of payload mode and present the CLI interface. Issuing a logout command will revert the unit to payload data mode.

The COM port supports a serial data rate of 300-115200 bps (115200 default, asynchronous only). The unit is hardwired as a DCE device.

Supported data formats for the COM port are:

	com1.databits	com1.paritybits	com1.stopbits
8N1 - 8 char bits, no parity, 1 stop bit *(Default)*	8	“N”	1
8N2 - 8 char bits, no parity, 2 stop bits	8	“N”	2
8O1 - 8 char bits, odd parity, 1 stop	8	“O”	1
8O2 - 8 char bits, odd parity, 2 stop bits	8	“O”	2
8E1 - 8 char bits, even parity, 1 stop bit	8	“E”	1
8E2 - 8 char bits, even parity, 2 stop bits	8	“E”	2
7O1 - 7 char bits, odd parity, 1 stop	7	“O”	1
7E1 - 7 char bits, odd parity, 1 stop	7	“E”	1

The tables on the following page provide pin descriptions for the COM data port in RS-232 mode and RS-485 modes, respectively.



(As viewed from the outside the unit)

Table 2-2. COM Port Pin Details (RS-232)

Pin Number	Input / Output	Pin Description
1	OUT	ALARM Output
2	OUT	DCD (Data Carrier Detect)
3	IN	SLEEP Input
4	Ground	Connects to ground (negative supply potential) on chassis
5	OUT	RXD (Received Data)—Supplies received data to the connected device
6	IN	TXD (Transmitted Data)—Accepts TX data from the connected device
7	OUT	CTS (Clear to Send)
8	IN	RTS (Request to Send)

Table 2-3. COM1 Port Pin Details (RS-485)

Pin Number	Input/Output	Pin Description
1	OUT	ALARM Output
2	OUT	DCD (Data Carrier Detect)
3	Reserved	--
4	Ground	Connects to ground (negative supply potential) on chassis

Table 2-3. COM1 Port Pin Details (RS-485)

5	OUT	TXD+/TXB (Transmitted Data +)—Non-inverting driver output. Supplies received payload data to the connected device.
6	IN	RXD+/RXB (Received Data +) — Non-inverting receiver input. Accepts payload data from the connected device.
7	OUT	TXD-/TXA (Transmitted Data -)—Inverting driver output. Supplies received payload data to the connected device.
8	IN	RXD-/RXA (Received Data -) — Inverting receiver input. Accepts payload data from the connected device.

COM1 Port notes and wiring arrangements (for RS-485)

- The COM1 port supports 4-wire and 2-wire RS-485 mode as follows:
  - RXD+ / RXB and RXD– / RXA are data sent *into* the unit
  - RXD+ / RXB is positive with respect to RXD– / RXA when the line input is a “0”
  - TXD+ / TXB and TXD– / TXA are data sent *out* by the unit
  - TXD+ / TXB is positive with respect to the TXD– / TXA when the line output is a “0”
- 2-wire RS-485 mode connections:
  - Connect pins 5&6 (TXD+/RXD+) together and connect to (TXD+/RXD+) tied together on connected device
  - Connect pins 7&8 (RXD-/TXD-) together and connect to (TXD-/RXD-) tied together on connected device
- 4-wire RS-485 mode connections:
  - Connect pin 5 (TXD+) to RXD+ of connected device
  - Connect pin 6 (RXD+) to TXD+ of connected device
  - Connect pin 7 (TXD-) to RXD- of connected device
  - Connect pin 8 (RXD-) to TXD- of connected device

Figure 2-5 illustrates the 2-wire and 4-wire connections described above.

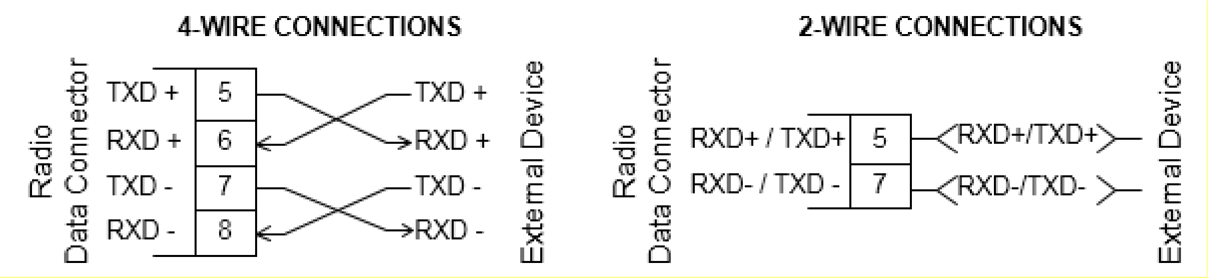
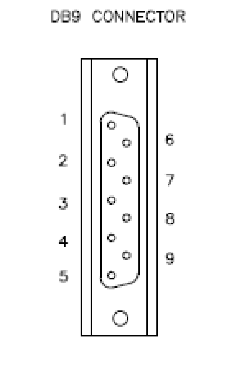


Figure 2-5. EIA-485 4-Wire/2-Wire Connections

NOTE MDS part number 73-2434A25 provides a custom RJ45 to DB9 Adapter for use with the TransNEXT and other MDS products. The chart below provides details for connections made using this adapter.

WIRING CHART

RJ-45 PIN	FUNCTION	DB9 PIN
1	DSR	6
2	DCD	1
3	DTR	4
4	GND	5
5	RXD	2
6	TXD	3
7	CTS	8
8	RTS	7



LED / Button Panel —The LEDs on the top of the unit provide visual indications of device status. The push button (appearing like a thin white circle) is used for special functions like controlling the optional E-ink display screen.

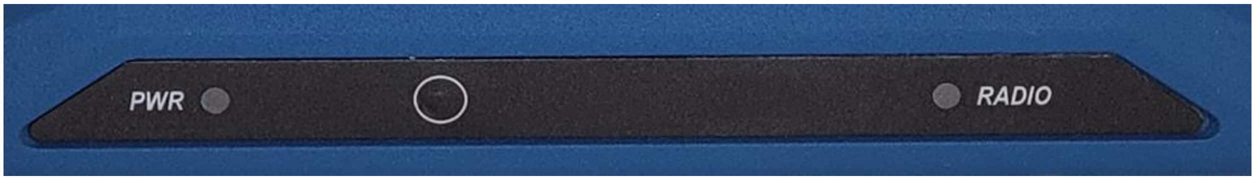


Figure 2-6. LED Indicators & Push Button

The LEDs are multi-color to convey different types of status conditions as shown in the following chart:

Table 2-4. Description of LED Status Indicators

LED Name	LED State	Description
PWR	Off	No power to unit.
(DC Power)	Solid Green	Unit is powered; no problems detected.
	Flashing Red (0.5s ON/ 0.5s OFF)	Alarm indication.
	Flashing Green (0.5s ON/ 0.5s OFF)	Unit is being programmed.
	Solid Red	Unit is booting up.
	Fast Alternating (Red/Yellow/Green)	Unit is booting up and processing a firmware update.
RADIO	Off	Interface disabled.
(master)	Solid Green + flicker	Radio will flicker on data.
(remote)	Solid Color + flicker on data	Radio is synchronized to a master.
	[*Color based on RSSI]*	LED will flicker on data.
	Green:	RSSI >= -70 dBm
	Yellow:	-70 dBm < RSSI <= -85 dBm
	Violet:	-85 dBm < RSSI <= -100 dBm
	Red:	RSSI < -100 dBm
	Flashing Red (1.0s ON/1.0s OFF)	Remote radio is not synchronized.
(all)	Multi-Color (rotating) (1.0s ON per color)	Radio is in **setup** mode.

2.4 Grounding Considerations

To minimize the chance of damage to the unit and its connected equipment, a safety ground (NEC Class 2 compliant) is recommended, which bonds the chassis, antenna system(s), power supply and connected data equipment to a *single-point* ground, keeping all ground leads as short as possible.

Normally, the unit is adequately grounded if mounted with the flat brackets to a well-grounded metal surface. If the unit is not mounted to a grounded surface, it is recommended that a safety ground wire be attached to the screw provided on the bottom corner of the enclosure, in the recessed flat area. Alternatively, a safety ground wire may be attached to one of the mounting bracket screws.

The use of a lightning protector is recommended where the antenna cable enters the building. Bond the protector to the tower ground, if possible. All grounds and cabling must comply with applicable codes and regulations. One source for lightning protection products may be found online at http://www.protectiongroup.com/PolyPhaser.

2.5 Mounting Options

The unit may be mounted with flat mounting brackets *or* an optional 35 mm DIN rail attachment.

NOTE To prevent moisture from entering the unit, do not mount the case with the cable connectors pointing up. Also, dress all cables to prevent moisture from running along the cables and into the unit.

2.5.1 Optional DIN Rail Mounting

If ordered with the DIN rail mounting option, two choices are available. For vertical mounting the unit is supplied with a DIN rail clip attached to an integrated bracket on the unit's case. For horizontal mounting a special bracket is used. In both cases the bracket allows for quick installation and removal from a DIN mounting rail. See Figure 2-7.

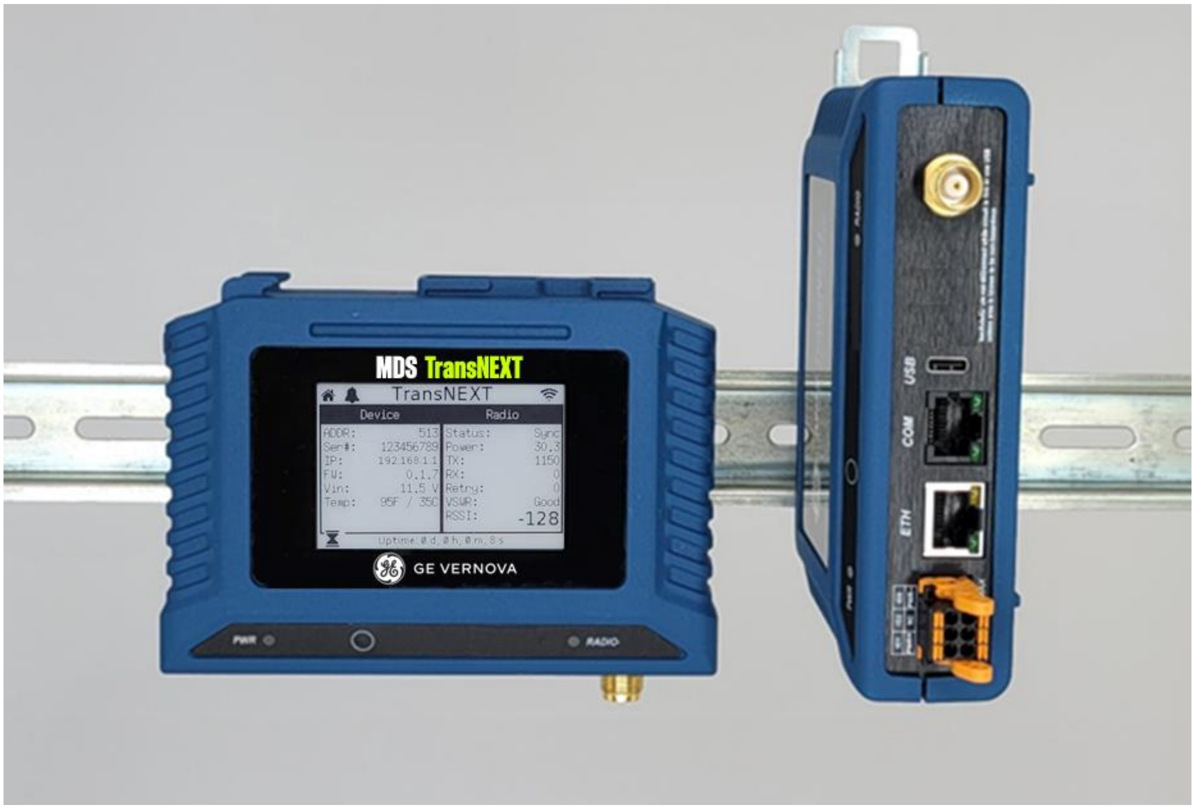


Figure 2-7. DIN Rail Attachment examples
(Pull down tab to release from rail)

2.6 Antenna Planning and Installation

Consideration must be taken to select appropriate antennas for optimal RF performance. The use of non-approved antennas may result in a violation of FCC rules and subject the user to FCC enforcement action. Note that with any installation, there needs to be a minimum 20 cm spacing between all transmit antennas to avoid co-location difficulties.

900 MHz ISM Antennas —Antenna connection is a TNC connector. Multiple antenna options are available for this unlicensed operation. Use the connector labeled *RADIO* as the primary connector. Professional installation is required.

NOTE For regions governed by FCC/IC compliance the maximum EIRP must be limited to 36 dBm. If (`(antenna gain - feed line loss) + power output setting)` >36), then the power output of the TransNEXT must be reduced.

Table 2-5. Signal Loss in Coaxial Cables (at 900 MHz)

Cable Type	10 Feet (3 Meters)	50 Feet (15 Meters)	100 Feet (30.5 Meters)	500 Feet (152 Meters)
RG-214	0.76 dB	3.80 dB	7.60 dB	Unacceptable Loss
LMR-400	0.39 dB	1.95 dB	3.90 dB	Unacceptable Loss
1/2 inch HELIAX	0.23 dB	1.15 dB	2.29 dB	11.45 dB
7/8 inch HELIAX	0.13 dB	0.64 dB	1.28 dB	6.40 dB
1-1/4 inch HELIAX	0.10 dB	0.48 dB	0.95 dB	4.75 dB
1-5/8 inch HELIAX	0.08 dB	0.40 dB	0.80 dB	4.00 dB

Accessories and Spares

The table below lists common accessories and spare items for use with the TransNEXT. GE Vernova also offers an *Accessories Selection Guide* listing an array of additional items that may be used with the product. Contact your factory representative or visit https://www.gevernova.com/grid-solutions/automation/critical-infrastructure-communications#industrial-wireless to obtain a copy of the guide.

Table 2-6. Accessories & Ancillary Items

Item	Description	Part Number
DC Power Plug, 6-pin, polarized	Mates with power connector on the unit's case. Screw terminals are provided for wires, threaded locking screws to prevent accidental disconnect.	73-1194A85
COM Port Adapter	Converts the unit's RJ-45 serial jack to a DB-9F type.	73-2434A25
Ethernet Surge Suppressor	Surge suppressor for protection of the Ethernet port against lightning.	29-4018A01
Bandpass Filter	Antenna system filter that helps eliminate interference from nearby paging transmitters.	20-2822A02

2.7 Initial Settings Overview

2.7.1 Setting Basic Parameters—First Steps

Setup will vary based on the application. But these minimal tasks should always be performed after initial startup and connection to a PC:

1. Change the login passwords.
2. Configure the radio.addr (Network Address) for your system
3. Configure the Serial COM port and ETH port as needed

When configuring a new network one radio will have to be designated as a master. On that radio

4. Configure the radio.mode ("m" = master)

Finally:

5. Make sure to save configuration

Section 3.0 Device Management that follows provides more information on how to use the CLI.

2.8 Special Product Features

2.8.1 Using the Radio's Sleep Mode (*Remote Units Only*)

In some installations, such as at solar-powered sites, it may be necessary to keep Remote transceivers' power consumption to an absolute minimum. This can be accomplished using the radio's Sleep Mode feature. Power in the Sleep Mode at 13.6 Vdc is approximately 3 mA.

Sleep Mode can be enabled under RTU control by asserting a ground (or EIA/RS-232 low) on Pin 3 of the radio's COM port. All normal functions are suspended until it is awakened. The radio stays in Sleep Mode until a built-in timer "awakens" it for resynchronization, or the low is removed from Pin 3.

When Pin 3 is opened (or an EIA/RS-232 high is asserted), the radio will be ready to receive data within 75 milliseconds or less. The radio can be awakened more often if desired, by your RTU.

NOTE radio.sleep must be set to "on"; without this, a ground on Pin 3 will be ignored.

It is important to note that power consumption will increase somewhat as communication from the Master station degrades. This is because the radio will spend a greater period of time "awake" looking for synchronization messages from the Master radio.

NOTE: If INTRUSIVE diagnostic polling is used by MDS Field Network Manager it is necessary to select SLEEP MODE INHIBIT ON from the Polling Options menu, on the Network Wide Diagnostic Polling screen.

Sleep Mode Example

The following example describes Sleep Mode implementation in a typical system. Using this information, you should be able to configure a system that meets your own particular needs.

Suppose you need communications to each Remote site only once per hour. Program the RTU to raise an EIA/RS-232 line once each hour (DTR for example) and wait for a poll and response before lowering it again. Connect this line to Pin 3 of the radio's COM connector. This will allow each RTU to be polled once per hour, with a dramatic reduction in power consumption.

2.8.2 Using Low-Power Mode (LPM) *(Master-enabled*)

Low-Power Mode (LPM) puts Remote radios into a configuration similar to Sleep, but with some important distinctions. The most important difference is the radio will automatically go to sleep in this mode, regardless of the condition of Pin 3 of the COM interface connector.

This feature trades increased latency to gain power savings. The low-power mode (LPM) automatically saves power at a Remote by instructing the Remote to shut down for long periods of time between SYNC messages. Master transmissions are automatically blocked while the Remotes are asleep. Note, both Masters and Remotes are adaptive and will suppress a normal sleep interval until after the end of a current data transmission or reception.

Setup Commands

These are the command options and their applications:

- Setting radio.lpm 1 at the Master enables low-power mode network-wide; all Remotes pick it up and start saving power by automatically sleeping.

- Setting radio.lpm 0 at the Master is used to disable low-power mode (LPM) (This is the default)

With settings radio.lpm 1 and radio.repeat 0, a Remote with no data to send will consume about 1/4 of its normal power consumption.

NOTE radio.sleep must be set to "on" on remote units for LPM to function.

Power Consumption Influence by HOPTIME and SAF Settings

The table below shows estimated current consumption and data delay values for various settings of TransNEXT radios setup for Low Power Mode. It assumes the primary power voltage is 13.8 Vdc and the polling rate is minimized to yield best-case power consumption (current) values.

The more each RTU is polled and asked to transmit, the more current will be consumed. Therefore, these values are the lowest that can be expected. Power consumption (current) is inversely related to data delay as shown in the table. When a radio is sleeping (LPM) mode, it is also waiting longer to deliver the payload data.

Table 2-7. Power Consumption versus Hoptime and SAF Settings

HOPTIME	SAF	Current Estimate (ma)	Data Delay (minimum)
7	OFF	16	350 ms
7	ON	10	780 ms
28	OFF	7	1620 ms
28	ON	4	3360 ms

2.8.3 Low-Power Mode versus Remote's Sleep Mode

The Low-Power Mode (LPM) puts Remote radios into an operational configuration similar to Sleep, but there are some important differences. Below is a comparison of the two modes.

Table 2-8. Power-Conservation Modes Comparison

	Sleep mode	Low Power mode
Features	• Manual control by connected equipment • Selective application of Sleep control • User determines length and frequency of sleep periods	• Automatic radio-controlled timing • Automatic sleep during absence of directed traffic • Network-wide implementation through Master station
Benefits	• Low latency • Low standby power, • ≤ 4 mA at 13.8 Vdc • Greatest potential for power savings	• Less complicated implementation • Simple configuration

NOTE Both Power-Conservation modes are intended for use in low power serial applications. Ethernet operation is not supported for these modes.

2.8.4 Seamless Mode Emulation

Setting a value with the com1.rxd parameter can be an efficient way to implement seamless mode. This process assumes the payload message will be ready for transmission after the delay period has expired. If there is a chance the payload data may be delayed, it is recommended to use com1.buff "on" to make sure the entire message is received before delivery is started. Using the com1.buff "on" setting provides a highly reliable seamless operating mode, but can be very slow to start, especially if it waits for the reception of long messages before passing on the message.

2.8.5 Co-Located and Close-Proximity Masters

If your requirements call for multiple TransNEXT networks at the same location, you need to ensure that interference between the systems in minimized to prevent overload that will diminish the performance of the radios. Traditionally, vertical separation of the antennas of co-located radios was required in order to reduce the interference to the point where overload of one network by the other will not occur. The radio.csaddr attribute will provide relief from this antenna separation requirement by operating the networks in a TDD mode and ensuring that all Masters transmit at the same time to avoid interference. 35 dB isolation between units may still be required.

Master Station Configuration

On all Masters for which you wish to synchronize transmissions, establish one Master as the "Clock-Sync Master by setting its radio.csaddr value to its own Network Address (radio.addr). Then, set all other dependent Masters radio.csaddr values to the Network Address (radio.addr) of the Clock-Sync Master.

Make sure that you use a different Network Address for each Master. This value will be used to identify all units associated with this Master's network.

Note that all Masters must be set to the same radio.csaddr setting, except one where the radio.csaddr matches its own radio.addr; this is the Clock-Sync Master.

radio.csaddr = radio.addr — Unit serving as a Clock-Sync Master

radio.csaddr ≠ radio.addr — Unit serves as a Dependent Master (Clock Slave)

radio.csaddr = 0 — Co-located Master feature disabled (0 = NONE, default)

NOTE Important: radio.hoptime, radio.fec, and radio.saf must be set to the same values on the Clock-Sync Master and all Dependent Masters.

NOTE If a Dependent Master station is unable to find the Clock-Sync Master station, it will not be able to operate properly, and the associated network will be out-of-service.

Antenna System for Co-Located Master Stations

Using this Clock Sync mode will ensure both masters synchronize timing for receiving and greatly reduce the antenna separation requirements to near zero. Under this arrangement, the antennas of co-located Masters may be placed a few feet (less than a meter) apart horizontally, or just above or below vertically with no ill effects.

There are two common antenna system arrangements:

Separate Antennas — Ideally, co-located Masters should use separate antennas. They can share an antenna only if isolation is sufficient. If sufficient isolation is not guaranteed, degraded performance will result.

Sharing an Antenna — It is possible to share an antenna between multiple Masters using standard power dividers, provided the extra loss associated with these devices is considered in your RF budgeting process. Masters in this configuration must be operating with radio.csaddr enabled. The power divider must be capable of handling 1 Watt and have >25 dB isolation between TX ports. In some cases, up to 35 dB of isolation is required. Isolation is improved by adding attenuators between the TransNEXT radios and the splitters.

2.8.6 IP/Payload

IP/Payload provides a way to introduce ethernet to a serial system. It is a product feature that acts like a terminal server with a *virtual* serial port, where the data from this *virtual* serial port is routed internally as over-the-air streaming traffic. We sometimes refer to this as “reverse terminal” server, because the IP-to-serial conversion happens at the closest point in the network instead of at the far end.

IP/Payload was first introduced in the MDS SD licensed radio family as an efficient way for an ethernet polling host to collect serial data from remote assets. The term IP/Payload refers to the *user data portion of IP traffic* being carried over the radio link, excluding lower-layer radio framing and overhead.

For this method to be viable a customer’s application must use a polling model where the polls contain addressing information that a remote can respond it.

IP/Payload is available both for interoperable (“TransNEXT”) mode and for “Bridge” mode.

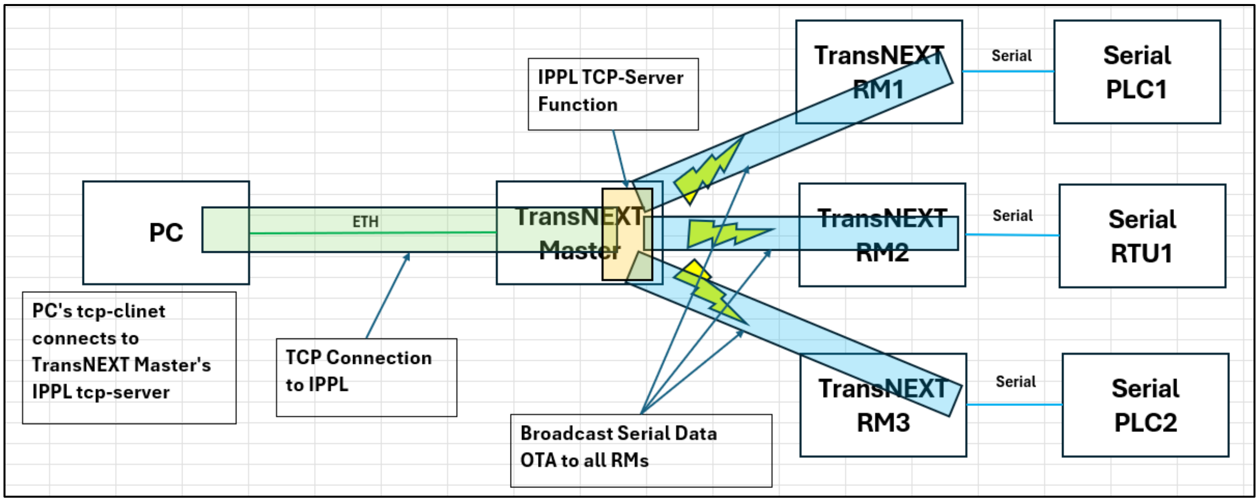


Figure 2-8. IP/Payload Example

2.8.7 Terminal Server

The Terminal Server feature provides IP network access to serial ports of remote radios. Options are available to use either UDP or TCP (selectable in either *client* or *server* mode). For TCP, a special option exists to perform local conversion of MODBUS TCP to MODBUS RTU.

Terminal Server operation relies on sending ethernet traffic over-the-air, so it is only applicable when the TransNEXT is in Bridge mode.

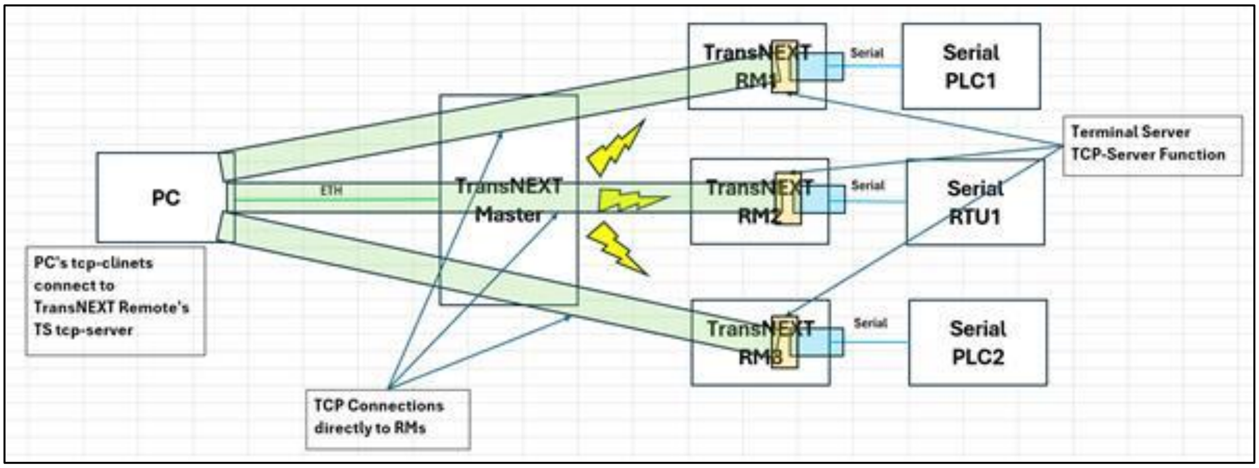

TransNEXT RM1
Serial
Serial PLC1
Terminal Server TCP-Server Function
PC
ETH
TransNEXT Master
TransNEXT RM2
Serial
Serial RTU1
PC's tcp-clinets connect to TransNEXT Remote's TS tcp-server
TransNEXT RM3
Serial
Serial PLC2
TCP Connections directly to RMs

Figure 2-9. Terminal Server Example

2.8.8 MIRRORED BITS™ Protocol Support

Select TransNEXT models are available with a compatibility mode for devices running Schweitzer Engineering Laboratories (SEL) Mirrored Bits™ MB8 Protocol.

Mirrored Bits™ communication is an established method invented by SEL that offers cost-effective, high-efficiency direct communication between relays. The transmitted messages carry data that facilitates the direct exchange of internal logic among relays. This technology is applicable in various scenarios such as line protection pilot schemes, remote control and monitoring of devices, remote tripping of relays, automated sectionalizing and load recovery, bus protection, and numerous other uses

TransNEXT can efficiently transport Mirrored Bits™ data wirelessly and securely over long distances allowing the connection of remote Mirrored Bits™ enabled assets.

Mirrored Bits™ compatibility mode is selected by setting system.mode "MBits".

NOTE When operating in “MBits” mode many standard features are not available due to conflict with the precise timing requirements of Mirrored Bits™. Notably store-and-forward, over-the-air reprogramming and PulseNET NMS monitoring are not supported.

2.8.9 Bridge Mode

TransNEXT models are now available with bridging support. Bridging is enabled by setting system.mode "Bridge".

Bridge mode changes overall system behavior to use Medium Access Control. This prevents data collisions and enables over-the-air ethernet support. Radios may communicate at any time but will only transmit after requesting and receiving access to the radio channel. This supports on-demand/push-traffic for serial as well as ethernet data.

For ethernet, TransNEXT bridging is a way to extend a LAN over a wireless link like a virtual Ethernet cable. At Layer 2 (Data Link layer), devices forward Ethernet frames based on MAC addresses, not IP addresses. The bridge learns which MAC addresses are on which ports and forwards frames to the appropriate radio accordingly.   MAC addresses are preserved end to end. Broadcasts, ARP, and other Layer 2 traffic pass transparently.

Ethernet Bridging is useful for IP based meters, RTUs, relays, PLCs, and other equipment that is distributed across disperse locations but still wants to operate on the same subnet. Common examples include Modbus and DNP3 networks.

Bridge mode also elevates the security posture of the network. All remotes authenticate prior to sending data. If bridge security is enabled (i.e., set to a value other than "none") the system performs authentication and data encryption based on a user programmed pre-shared key. This applies to serial data as well was ethernet.

NOTE NOTE: For bridging all radios in the network must be set to system.mode "Bridge". Units with conflicting system.mode settings will not synchronize or pass data.

3.0 Device Management

This section describes the steps for connecting a PC, logging in and setting unit parameters. The focus here is on the local serial console interface, but other methods of connection are available and offer similar capabilities. The key differences are with initial access and appearance of data.

TransNEXT offers several interfaces to allow device configuration and monitoring of status and performance. These include local serial console, USB, and Secure Shell (SSH) for local access via the WAN and LAN networks. The serial console, USB and SSH services offer a command line interface (CLI). There are three user accounts/roles for management access: admin, tech and oper.

NOTE The TransNEXT device is designed for high security environments. As such, management of the device does not support Telnet, but instead implements the more secure SSH protocol.

Configuring and managing the TransNEXT is done by changing configuration data via the Web User Interface (UI) or from the Command Line Interface (CLI). Either way requires two steps. The first step is to use a user interface to add, remove, or alter a piece of configuration data. The second step is to use the user interface to *save* the configuration change. Multiple changes can be made prior to committing them. This two-step process allows users to make multiple changes to the configuration and control when to apply.

3.1 Using the Web User Interface

The *Web User Interface* works with your PC's browser to provide an intuitive, web-style presentation of all unit information, settings, and diagnostics. Web management uses the unit's Ethernet RJ-45 connector.

To connect to the unit and manage it via the Web, you will need the following:

- A PC with a web browser program installed.

- An Ethernet cable connected between the PC and the TransNEXT as shown in PC Connection for Web Management.
- The unit's IP address. Check with your Network Administrator or determine the address via a command line interface connection. The default address for a factory supplied unit is 192.168.1.1.
- The user name and password for the unit. Check with your Network Administrator, or, if a username and password have not been set, login as **admin** using the default password unique to this unit. (For security, a new password should be established as soon as possible after login.)

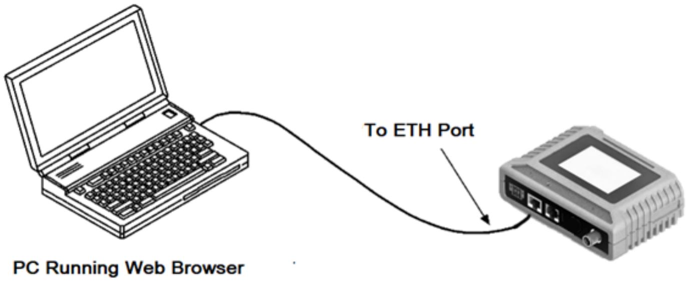
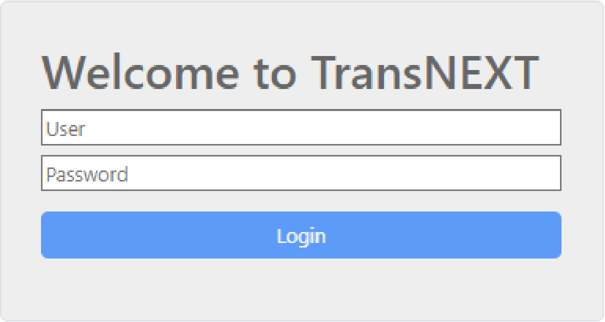


Figure 3-1. PC Connection for Web Management

Use of a current browser is highly recommended.

Logging On

1. Connect the unit to a PC via an Ethernet connection.
2. Configure your PC network settings to an IP address on the same subnet as the unit. The default subnet mask is 255.255.255.0.
3. Enter the unit's IP address in a web browser window, just as you would enter a website address. When the login screen appears (Figure 3-2. Login Screen), enter the User Name and Password for the unit. (The default entries for a new unit are "admin" for username and a unique 10-character password printed on the unit.) Click the **Login** button.



Welcome to TransNEXT

User

Password

Login

Figure 3-2. Login Screen

After successful login the initial web page is displayed. Every page includes a banner section at the top similar to what is shown in Figure 3-3 below:

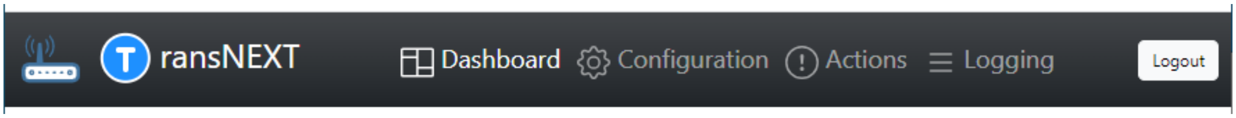


Figure 3-3. Web UI / banner

The default page after login is the “Dashboard”. Other pages are available by clicking any of the selections to the right of the TransNEXT name.

Choices are:

- Dashboard
- Configuration
- Actions
- Logging
- Network (*this section is only shown when system.mode is “Bridge”)*

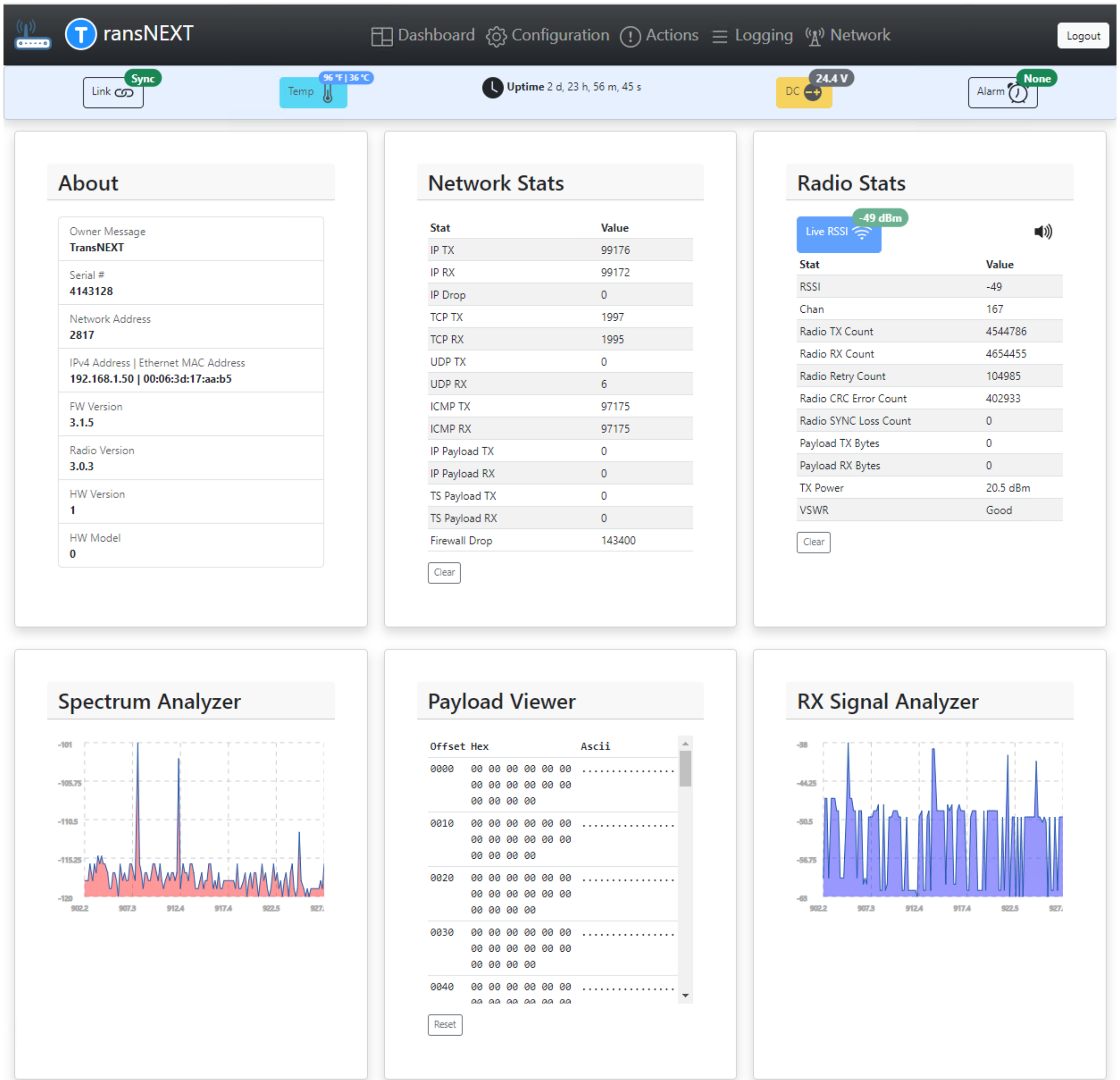
Clicking the “Logout” button on the far right terminates the current Web UI session and brings the device back to the Login Screen.

NOTE Using the browser’s screen refresh button will behave like selecting “Logout”. Please avoid use of screen refresh unless a logout is intended.

Each of the main page selections is explained below.

3.1.1 Dashboard

The “Dashboard” is the default page after login. The screen is organized into 6 sections as shown:



Uptime 2 d, 23 h, 56 m, 45 s

About

Owner Message
TransNEXT

Serial #
4143128

Network Address
2817

IPv4 Address | Ethernet MAC Address
192.168.1.50 | 00:06:3d:17:aa:b5

FW Version
3.1.5

Radio Version
3.0.3

HW Version
1

HW Model
0

Network Stats

Stat	Value
IP TX	99176
IP RX	99172
IP Drop	0
TCP TX	1997
TCP RX	1995
UDP TX	0
UDP RX	6
ICMP TX	97175
ICMP RX	97175
IP Payload TX	0
IP Payload RX	0
TS Payload TX	0
TS Payload RX	0
Firewall Drop	143400

Radio Stats

Stat	Value
RSSI	-49
Chan	167
Radio TX Count	4544786
Radio RX Count	4654455
Radio Retry Count	104985
Radio CRC Error Count	402933
Radio SYNC Loss Count	0
Payload TX Bytes	0
Payload RX Bytes	0
TX Power	20.5 dBm
VSWR	Good

Spectrum Analyzer

Payload Viewer

```
Offset Hex                  Ascii
0000   00 00 00 00 00 00    ................
       00 00 00 00 00 00
       00 00 00 00
0010   00 00 00 00 00 00    ................
       00 00 00 00 00 00
       00 00 00 00
0020   00 00 00 00 00 00    ................
       00 00 00 00 00 00
       00 00 00 00
0030   00 00 00 00 00 00    ................
       00 00 00 00 00 00
       00 00 00 00
0040   00 00 00 00 00 00    ................
       00 00 00 00 00 00
```

RX Signal Analyzer

The 3 boxes on the top row provide the most commonly accessed information.

- The About section is for common fixed radio info. It provides Owner Message, Serial#, Network Address, Firmware and Hardware versions
- Network Stats are associated with the ethernet port. They provide running counts of IP traffic, broken down by TCP, UDP, ICMP (ping), IP payload.
- Radio Stats are associated with the operation of the radio itself. This includes RSSI, Output Power, VSWR status Good/Bad, and link layer counts for Transmission and Reception

The 3 boxes on the bottom row are designed to aid in system troubleshooting:

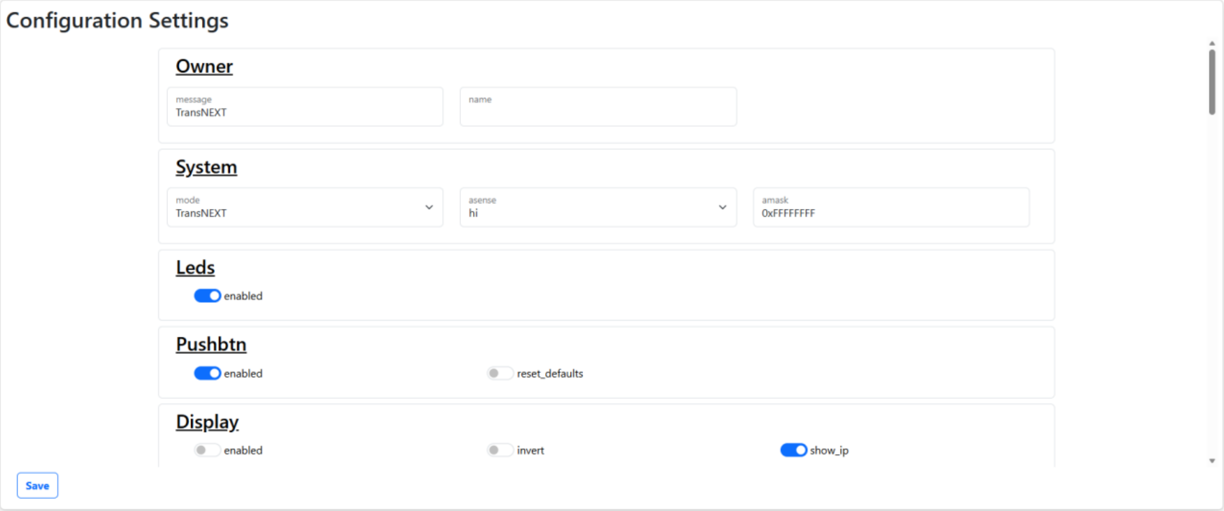
- The Spectrum Analyzer shows the noise floor across the channel. It works by passively sampling on hops when the TransNEXT is not on the air.
- The Payload Viewer provides a running window for displaying the last received OTA payload data
- The RX Signal Analyzer shows the signal strength across the channel of based on receipt of TransNEXT OTA packets. Note that a master radio will not show any activity until at least one remote is sync'd and passing data.

3.1.2 Configuration

The "Configuration" page allows a Web UI user to change device configuration using the same parameter syntax visible in the CLI.

There are two forms of Web UI on the configuration page – the first one is a graphical series of boxes and toggle switches to click to change the parameters. The second one is the original window loading the config file.

To effect a change, move the scrollbar on the right to the appropriate configuration group (com1, radio, etc.) Next, find the specific attribute in the group to modify. In the graphical Web UI, clicking the boxes or toggle switches will change the attribute options, as seen in the example below (just scroll down to see all the options):



Configuration Settings

Owner

message: TransNEXT

name:

System

mode: TransNEXT

asense: hi

amask: 0xFFFFFFFF

Leds

☑ enabled

Pushbtn

☑ enabled

☐ reset_defaults

Display

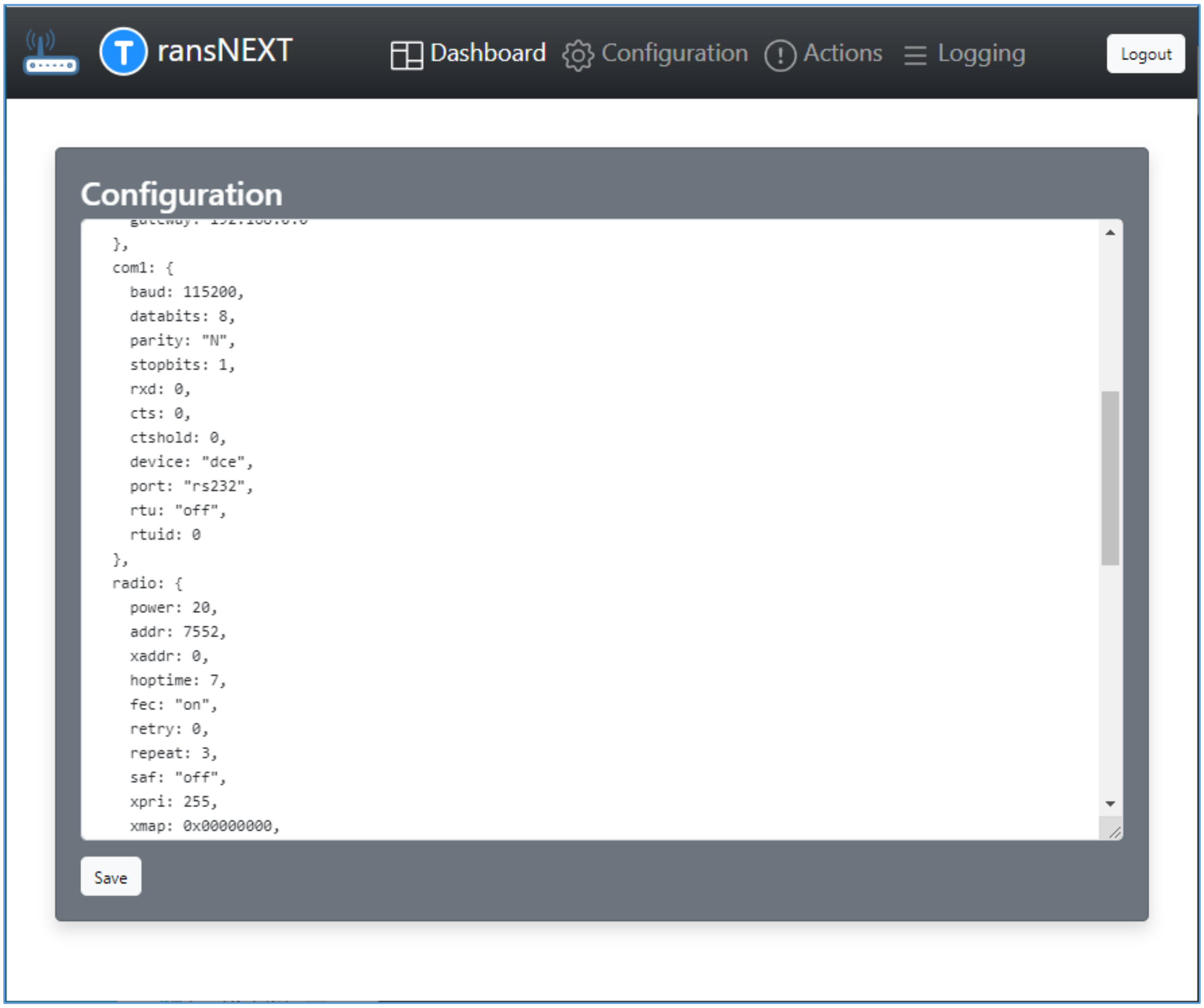
☐ enabled

☐ invert

☑ show_ip

Once you have made your changes, click the "Save" button on the bottom left.

Down below the web UI banner is the configuration file in a browser window, as shown below:



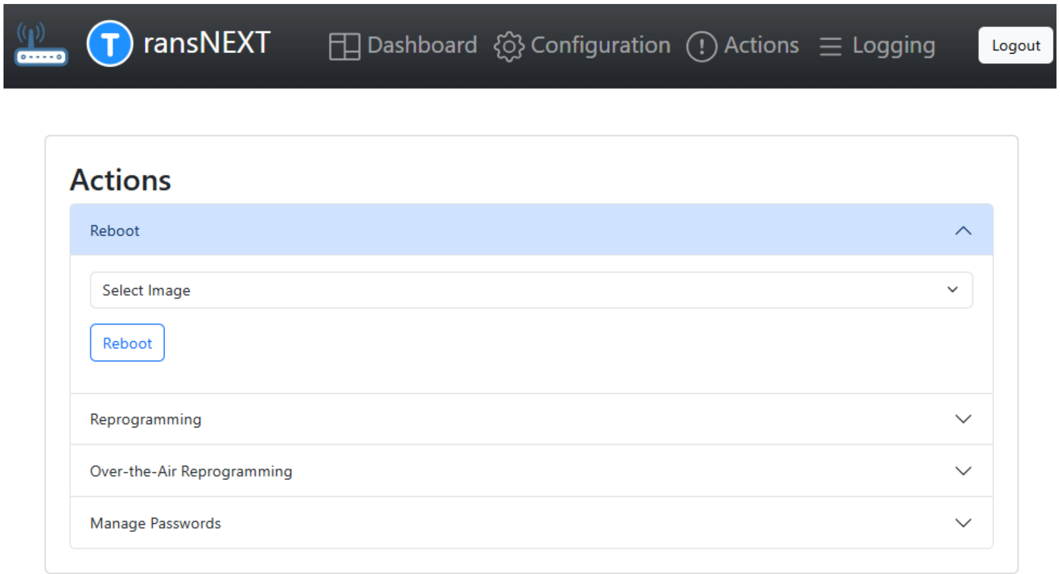
```
    gateway: 192.168.0.0
  },
  com1: {
    baud: 115200,
    databits: 8,
    parity: "N",
    stopbits: 1,
    rxd: 0,
    cts: 0,
    ctshold: 0,
    device: "dce",
    port: "rs232",
    rtu: "off",
    rtuid: 0
  },
  radio: {
    power: 20,
    addr: 7552,
    xaddr: 0,
    hoptime: 7,
    fec: "on",
    retry: 0,
    repeat: 3,
    saf: "off",
    xpri: 255,
    xmap: 0x00000000,
```

The attribute’s current value is shown immediately to the right of the colon. To effect a change, move the scrollbar to the appropriate configuration, then make the needed changes, and “save”.

The attribute’s current value is shown immediately to the right of the colon. If multiple changes are desired, repeat the process above. To save the configuration and cause the new settings to go into effect, click the “Save” button on the bottom left.

3.1.3 Actions

The “Actions” page is used to control device reboot and reprogramming. Click the caret symbol on the right to expand or collapse a section.



Reboot
Allows reboot into either the current image or the inactive image.

Reprogramming
Allows specification of an application .MPK file. Selecting “upload” automatically loads the firmware to the current inactive image. This process protects against accidental corruption of the current image. After reprogramming is complete, returning to the reboot section allows a reboot to the newly loaded image.

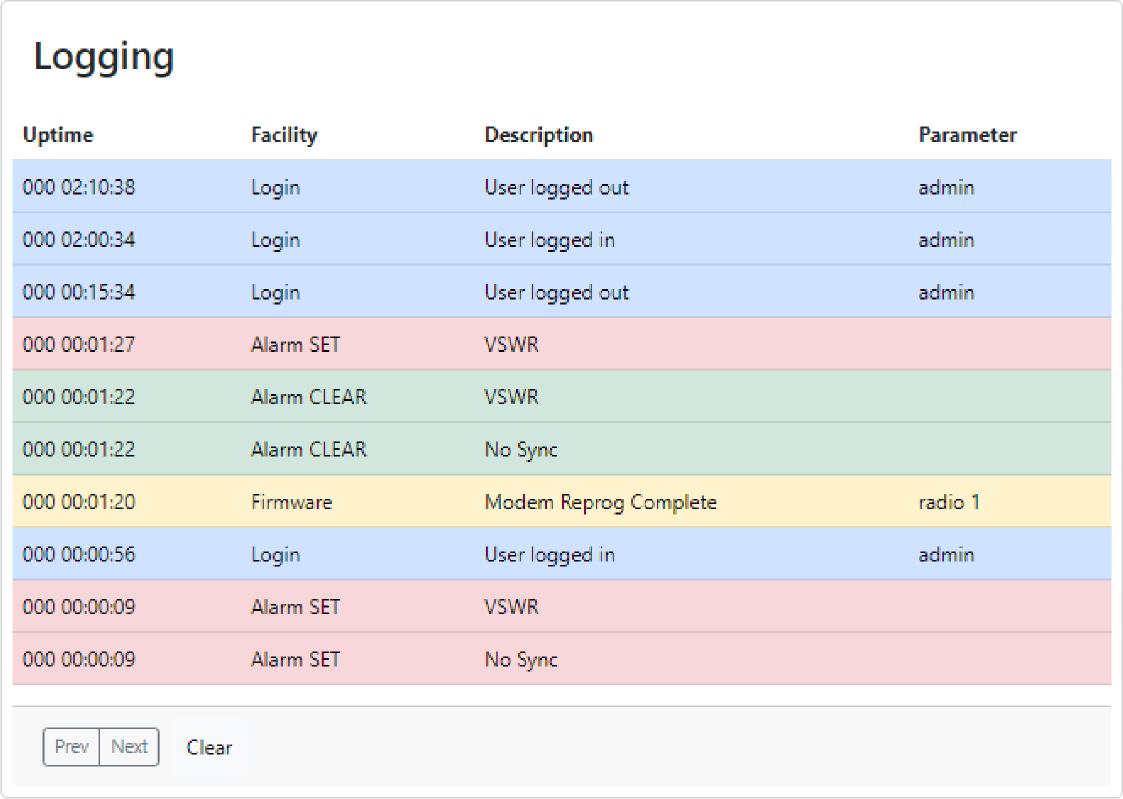
Over-the-Air reprogramming
Allows the current firmware image running on a master radio to be broadcast over the air to the entire network of TransNEXT remotes. The operation relies on unacknowledged broadcast transmission with variable repeats. Choose the transmission mode setting based on the characteristics of the connected network. **Robust** mode may take several days to operate but it is the most reliable. Other choices include **Slow**, **Medium**, or **Fast**. Additional controls include Passive or Active transmission, to limit the effect on the polling operation. The Reboot control specifies whether remotes should automatically reboot to the new image once the reprogramming operation is complete.

Manage Passwords
Allows management of passwords for each of the user roles: Admin, Tech, and Oper. Current password rules will be displayed when expanded; choose a user role to work with and set the new password.

NOTE Varying RF environmental conditions may prevent Over-the-Air Reprogramming from successfully updating all devices. The operation may be repeated as needed to attempt to pick up units missed during a prior session. If a remote unit has a particularly poor signal OTA reprogramming may be impractical and it may be necessary to reprogram the device locally.

3.1.4 Logging

The “Logging” page is used to display the non-volatile history of logged system events. Each log entry is timestamped relative to uptime. The timestamp format is ddd HH:MM:SS. (ddd represents uptime in days, HH = hours, MM=minutes, SS=seconds) The logs are displayed in reverse chronological order. The most recent items will always be displayed first.



Logging

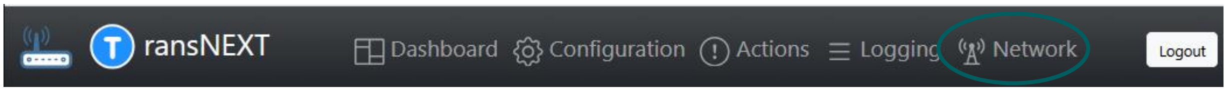
Uptime	Facility	Description	Parameter
000 02:10:38	Login	User logged out	admin
000 02:00:34	Login	User logged in	admin
000 00:15:34	Login	User logged out	admin
000 00:01:27	Alarm SET	VSWR	
000 00:01:22	Alarm CLEAR	VSWR	
000 00:01:22	Alarm CLEAR	No Sync	
000 00:01:20	Firmware	Modem Reprog Complete	radio 1
000 00:00:56	Login	User logged in	admin
000 00:00:09	Alarm SET	VSWR	
000 00:00:09	Alarm SET	No Sync	

The “Prev” and “Next” buttons at the bottom of the page provide the ability to traverse the history of logged events. The “Clear” button clears the entire log history.

NOTE If the log contains a set of events spanning *multiple* reboots, the timestamps will not always be monotonic. If the timestamp of a pair of sequential logs jumps from a lower number to a higher number, that means that the events occurred during a different boot instance. Each group of events will be timestamped relative to its specific reboot instance.

3.1.5 Network

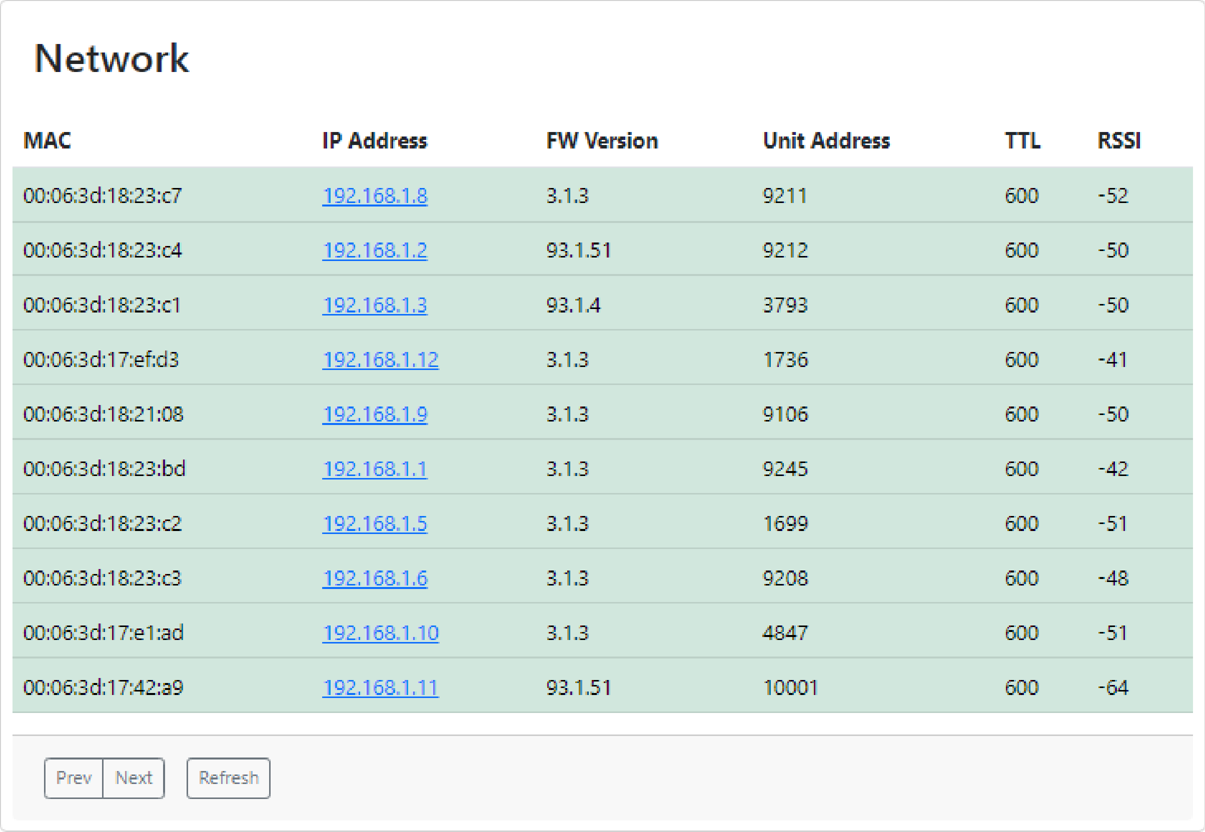
When system.mode is set to “Bridge” the “Network” page becomes selectable on the far right of the Web UI banner.



Network entries are shown as a table of all connected (authenticated) remotes in the system. Each table element includes remote MAC address, IP address, Firmware Version, Unit Address, TTL setting, and signal strength for last received packet (in dBm).

Entries are color coded based on signal strength for easy signal recognition:

- -128 = black
- < - 90 = red
- < - 80 = yellow
- > -80 = green (*as shown below*)



Network

MAC	IP Address	FW Version	Unit Address	TTL	RSSI
00:06:3d:18:23:c7	192.168.1.8	3.1.3	9211	600	-52
00:06:3d:18:23:c4	192.168.1.2	93.1.51	9212	600	-50
00:06:3d:18:23:c1	192.168.1.3	93.1.4	3793	600	-50
00:06:3d:17:ef:d3	192.168.1.12	3.1.3	1736	600	-41
00:06:3d:18:21:08	192.168.1.9	3.1.3	9106	600	-50
00:06:3d:18:23:bd	192.168.1.1	3.1.3	9245	600	-42
00:06:3d:18:23:c2	192.168.1.5	3.1.3	1699	600	-51
00:06:3d:18:23:c3	192.168.1.6	3.1.3	9208	600	-48
00:06:3d:17:e1:ad	192.168.1.10	3.1.3	4847	600	-51
00:06:3d:17:42:a9	192.168.1.11	93.1.51	10001	600	-64

The “Prev” and “Next” buttons at the bottom of the page provide the ability to traverse the table. The table automatically refreshes every few seconds and may also be manually refreshed using the “Refresh” button.

3.2 Using the Command Line Interface (CLI)

3.2.1 Differences between USB, Serial and SSH

USB, Serial and SSH each use different methods of access, but all require a login and will present an equivalent Command Line Interface after login is complete.

NOTE The login prompt will appear as "**[0000000] Login**:" where 0000000 is the device serial number.

Any terminal emulator can be used, but Tera Term from the Open Source Development Network is recommended.

USB access requires connecting the USB port on a laptop or PC to the USB-C port on the radio. Recommended cable length is 2 meters or less. This is typically the simplest way to connect to the unit and is the recommended method for CLI operation.

Serial access uses an RS-232 serial connection from a PC to the unit's COM port. Maximum cable length for an IEEE-1613 compliant serial connection is 2 meters. The serial port defaults to operation as a payload data port, using a pre-configured baud rate (default is 115.2kbps). To temporarily enter into command line mode on the payload port it is necessary to type the escape sequence "+++".

SSH access uses an Ethernet PC connection to the unit's ETH port. SSH can be connected to the unit from any network point that has connectivity with the PC, including remotely over the Internet, or using other networks.

3.2.2 Establishing Communication— SSH

Follow these steps to configure the unit for SSH:

1. Connect to the unit with a PC that is in the same IP network as the TransNEXT. Launch an SSH client program (like PuTTY) and connect to the unit using its programmed IP address.

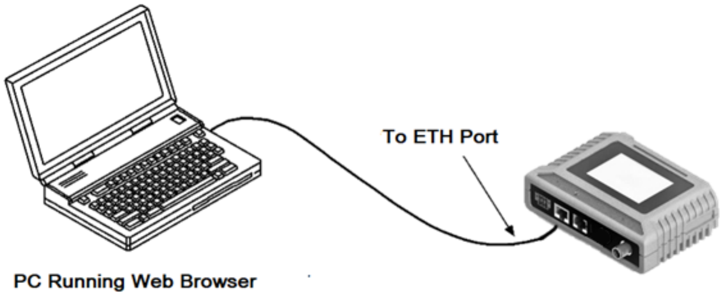


Figure 3-4. PC Connection for Programming/Management

2. The default IP address for the unit is 192.168.1.1. If you do not know the current IP address of the unit, follow the serial configuration instructions below, where you can determine the address and continue configuration, or check with your network administrator.
3. Login with the user name "**admin**" and default admin password for this unit.
4. The SSH connection will confirm with the message:

```
> You are connected to the TransNEXT SSH Server
>
```

3.2.3 Establishing Communication— USB

Follow these steps to configure the unit for USB:

1. Connect a PC to the unit’s USB port as shown in Figure 3-6. Maximum recommended cable length is 6 ft/2 m.

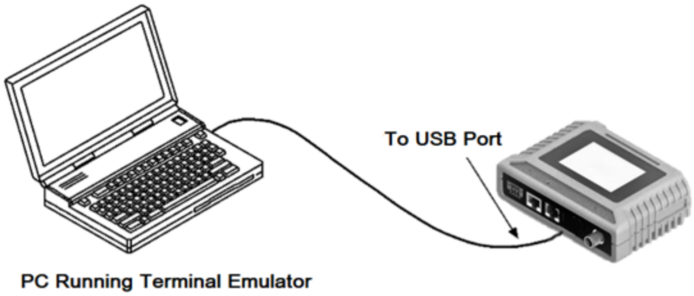


Figure 3-5. PC Connection for Programming/Management

2. The USB will instantiate a COM port to the PC
3. Launch a terminal communications program, such as Tera Term or PuTTY, with the COM port matching the USB port instantiated by the TransNEXT device.

NOTE If a message like the one below is displayed, that means that an SSH CLI session is already active. Pressing “D” will force the SSH connection to drop, freeing the USB port to continue with login.

```
Remote SSH console session in progress.
Please press D to disconnect remote console user.
```

4. Login with the user name “admin” and default admin password for this unit.

3.2.4 Establishing Communication—Serial Interface

Follow these steps to configure the unit for its first use with serial console interface:

1. Connect a PC to the unit’s COM port as shown in Figure 3-6. Maximum recommended cable length is 6 ft/2 m.
2. Launch a terminal communications program, such as Tera Term or PuTTY, with the following communication parameters: 115200 bps (default speed), 8 bits, no parity, one stop bit (8N1) and flow control disabled. Incorrect parameter settings are a frequent cause of connection difficulties. Double check to be sure they are correct.

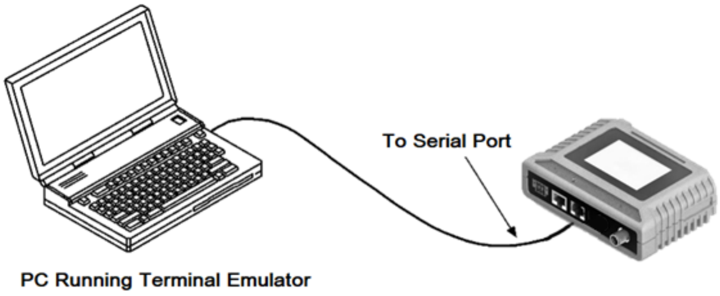
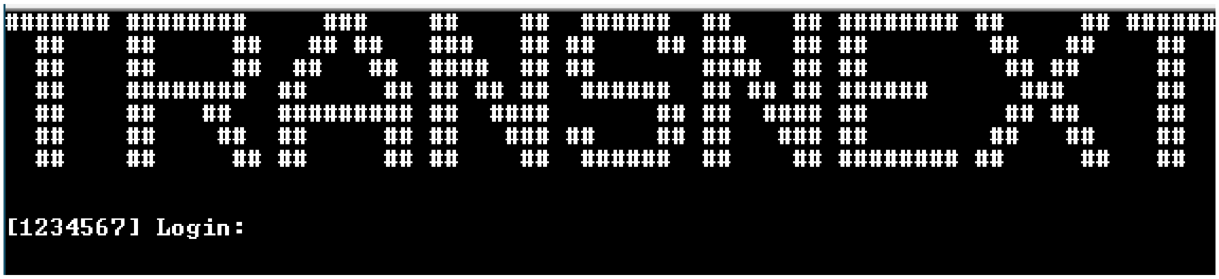


Figure 3-6. PC Connection for Programming/Management

4. Enter “+++” to cause the serial payload port to temporarily enter into command line mode.
5. At the Login: prompt, login with the user name “admin” and default admin password for this unit.

3.2.5 CLI Overview

NOTE For serial and USB operation, on timeout or logout, the TransNEXT will display an ASCII banner page followed by a new prompt for “Login:”



```
[1234567] Login:
```

After successful login, the “>” command prompt appears where you may configure and manage unit settings. Help can be requested as follows:

```
>help
help <name> for help with a specific command

Available commands:

about                    System information about this device
app                      Show application image versions
app_ota                  OTA App reprogramming
authcode                 Enter device authorization code
bootloader               Show bootloader image versions
cfg                      Configuration database
clear                    Clear system logs or stats
clos                     Enter DLINK mode
help                     Help command
logout                   Logout of active session
netdump                  Display Ethernet and IP packets
password                 Change user password
ping                     Ping a host
reboot                   Reboot radio
serdump                  Display serial payload history
setup                    Disable hopping and enter radio setup mode
show                     Show various system attributes
uptime                   Radio uptime
```

Individual commands have their own help. Enter the command name followed by help as shown in the examples below:

```
>show help
show device              Show device information
show log <debug>         Show event log, with optional debug points
show alarms              Show current system alarms
show status              Show radio status
show stats               Show radio and network statistics
show sync                Show radio synchronization status
show temp                Show system temperature
show vin                 Show radio input voltage
show uptime              Show system uptime
show rssi                Show continuous radio RSSI
show rssi!               Show radio RSSI
show eth                  Show Ethernet status
show ip                   Show current IP configuration
show nwk<!>               Show connected radios and Ethernet devices
show options              Show available feature options

>help clear
clear log                 Clear event log
clear stat <name|all>     Clear a specific stat or all stats >help nvstat

>cfg help
cfg snapshot              Save a snapshot of the database
cfg restore               Restores saved database snapshot
cfg show                  Show entire database
cfg load                  Load database from flash
cfg save                  Save database to flash
cfg get <key>             Get value assigned to key
cfg set <key>.<value>     Assign value to a key
cfg import                <Paste> in a configuration

>setup help
chan                      Get/Set setup channel [0-127] f_MHz=902.2+(.2*chan)
key                       Continuous TX key
burst                     Burst TX key
dkey                      Key down
rssi                      Sample continuous RSSI
rssi!                     Get last RSSI sample
quit                      Exit radio setup mode

>app help
app <1|2>                 Set active image
app update                Update app inactive image over Ymodem
app copy                  Copy the active image to the inactive
>
```

When working with the CLI the up and down arrows can be used to navigate previously entered commands. For example, when testing for synchronization if the "show sync" command is issued, the command can be repeated by selecting up-arrow followed by carriage return.

3.3 Device Configuration

3.3.1 Overview

Non-volatile, user-configurable parameters are controlled with the “cfg” command.

```
>
>cfg help
cfg snapshot              Save a snapshot of the database
cfg restore               Restores saved database snapshot
cfg show                  Show entire database
cfg load                  Load database from flash
cfg save                  Save database to flash
cfg get <key>             Get value assigned to key
cfg set <key>.<value>     Assign value to a key
cfg import                <Paste> in a configuration
```

Configuration items are organized into attribute groups, identified by a <key> as shown in the table below.

Table 3-1. Configuration Items (cfg)

Attribute Group <Key>	Items controlled
owner	Owner name and message.
system	System operating characteristics.
leds	Settings associated with LED control for low power.
pushbtn	Settings associated with LED panel push button behavior.
display	Settings associated with E-ink display behavior. *(only applicable for units equipped with an E-ink display.)*
password	Settings associated with password complexity control.
com1	Settings associated with serial payload interface, including baud rate, RTS/CTS handshaking, and embedded RTU simulator controls.
dlink	Diagnostic Link controls (for use by an external NMS or configuration tool.)
eth	IP address, netmask, and default gateway.
nwk	Settings associated with network access control.
bridge	Settings associated with bridge configuration.
ippl	IP/Payload controls.
ts	Terminal Server controls.
modem	Settings associated with modem operation. These attributes control how the Trans NEXT devices talk with other units over-the-air.
radio	Settings associated with TransNEXT radio behavior.

To display all saved user configuration settings, enter **`cfg show`** as follows:

```
>cfg show
{
  owner: {
    message: "TransNEXT",
    name: ""
  },
  system: {
    mode: "TransNEXT",
    asense: "hi",
    amask: 0xFFFFFFFF
  },
  leds: {
    enabled: "on"
  },
  pushbtn: {
    enabled: "on",
    reset_defaults: "off"
  },
  display: {
    enabled: "off",
    invert: "off",
    show_ip: "on"
  },
  password: {
    min_chars: 1,
    max_chars: 255,
    min_lower_case: 0,
    min_capital_letters: 0,
    min_numbers: 0,
    min_non_alpha_numeric: 0,
    permit_username: "on"
  },
  com1: {
    baud: 115200,
    databits: 8,
    parity: "N",
    stopbits: 1,
    buff: "off",
    rxd: 0,
    cts: 0,
    ctshold: 0,
    device: "dce",
    port: "rs232",
    rtu: "off",
    rtuid: 0
  },
  dlink: {
    enabled: "off",
    type: "node",
    tcp_access: "off",
    connection_timeout: 0,
    tcp_port: 30020,
    trend_resp_win: 0
  },
  eth: {
    enabled: "on",
    ipaddr: 192.168.1.1,
    netmask: 255.255.255.0,
    gateway: 192.168.0.0
  },
  nwk: {
    bridging: "on",
    http: "on",
    https: "on",
    ssh: "on",
    net_guard: "on",
    firewall: {
      filter: "allow-all",
      src1: [0x00:0x00:0x00:0x00:0x00:0x00],
      src2: [0x00:0x00:0x00:0x00:0x00:0x00],
      src3: [0x00:0x00:0x00:0x00:0x00:0x00],
      src4: [0x00:0x00:0x00:0x00:0x00:0x00]
    }
  },
  bridge: {
    security: "aes256-ctr",
    psk: "!$0!f@,ol<k=5C623AIkBCfTjjjAxUey1QxxsU7nnyqxrFpuJcxjhscNDJg=",
    compress: "lz",
    p2p: "off",
    ageout: 10,
    ttl: 6000
  },
  ippl: {
    enabled: "off",
    mode: "udp",
    talk_on_vrc: 1,
    listen_to_vrc: 1,
    local_ip_port: 30011,
    ip_peer_addr: 192.168.1.1,
    ip_peer_port: 30999,
    connection_timeout: 0,
    keep_alive: "off",
    modbus_tcp_rtu: "off"
  },
  ts: {
    enabled: "off",
    mode: "udp",
    talk_on_vrc: 1,
    listen_to_vrc: 1,
    local_ip_port: 30011,
    ip_peer_addr: 192.168.1.1,
    ip_peer_port: 30011,
    connection_timeout: 0,
    keep_alive: "off",
    modbus_tcp_rtu: "off"
  },
  modem: {
    speed: "106k",
    system_id: 0
  },
  radio: {
    power: 29,
    addr: 10,
    xaddr: 0,
    hoptime: 7,
    fec: "on",
    retry: 10,
    repeat: 3,
    saf: "off",
    xpri: 0,
    xmap: 0x00000000,
    skip: [0,0,0,0,0,0,0,0],
    csaddr: 0,
    rxtot: 0,
    unit_addr: 2551,
    lpm: 0,
    lpmhold: 20,
    sleep: "off",
    mode: "R",
    code: 0
  }
}
```

To display configuration settings for a single Attribute Group, enter a command like the following:

```
>cfg get owner
{
  message: "TransNEXT",
  name: ""
}
```

To display a single attribute from a group, use dot notation as follows:

```
>cfg get owner.message
"TransNEXT"
```

NOTE The **cfg show** command displays only the last saved configuration. The **cfg get** command shows the scratchpad version of attributes that include changes that are not yet saved.

To change a parameter, use the **cfg set** command. An example is shown here:

```
>cfg set radio.addr 1234
Setting radio.addr to 1234
```

When using **cfg set** commands you are only creating a planned change. The change will be saved and activate only after **cfg save** is issued.

```
>cfg save
OK
```

NOTE Failure to issue a "**cfg save**" will cause prior unsaved "**cfg set**" values to be lost or ignored.

When using **cfg set** it is important to use the same parameter syntax shown by **cfg get** and **cfg show**. For example, in the case above, radio.addr is specified as a decimal number. Other radio attribute group settings behave differently. For example, radio.mode is set by entering a quoted "m", "x", or "r" (for master, extension, or remote, respectively). Failure to enter the quotes will cause the command to fail with a syntax error.

```
>cfg set radio.mode m
Syntax error

>cfg set radio.mode "m"
Setting radio.mode to "m"
```

Settings are explained in greater detail in the sections that follow.

3.3.2 Owner settings

The Owner attribute group contains system identification info.

```
>cfg get owner
{
  message: "TransNEXT",
  name: ""
}
```

3.3.2.1 owner.message[<63 character string>]

Owner message is a 63-character string. For units equipped with a display this will appear as the text on status screen. Strings of 20 characters or less display best. Default is blank.

3.3.2.2 owner.name [<63 character string>]

Owner name is a 63-character string. Default is blank.

3.3.3 System settings

The System attribute group contains miscellaneous settings. system.mode controls the operating mode of the TransNEXT device. system.asense and system.amask control alarm output functionality.

```
>cfg get system
{
  mode: "TransNEXT",
  asense: "hi",
  amask: 0x00000000
}
```

3.3.3.1 system.mode [“TransNEXT” or “MBits” or “Bridge”]

This attribute is used to set the operating mode of the TransNEXT radio. Available options may be limited based on the type of model purchased. Factory shipping default mode is based on the model ordered.

“TransNEXT” selects the transparent serial operating mode that is interoperable with legacy TransNET serial devices. This mode is available on all devices and set by default on devices ordered with Authorized Feature set “LT”

“MBits” enables a specialized point-to-point mode compatible with devices running SEL Mirrored Bits™. This mode is available and set by default on devices ordered with Authorized Feature set “BR” (Bridge Mode Ready)

“Bridge” enables media access control and Layer 2 bridging of Ethernet data. This is the preferred mode for an all TransNEXT network operating with Ethernet devices. This mode is available and set by default on devices ordered with Authorized Feature set “MB” (Mirrored Bits)

3.3.3.2 system.asense [“hi” or “low”]

This attribute is used to set the sense of the alarm output at Pin 1 of the RJ-45 COM1 connector. The default is active “hi” which means an unmasked alarm is present when the signal on pin 1 is asserted.

3.3.3.3 system.amask [0x00000000-0xFFFFFFFF]

This attribute controls the alarm mask associated with alarm output on Pin 1 of the RJ-45 COM1 connector. The value sets the alarm bits that cause the alarm output signal to be triggered. The PWR LED will still flash, and events will be logged for all alarms, but the alarm output signal will only be activated for those alarms that have the corresponding mask bit set. The hex value for the mask aligns with numbered value displayed by the "show alarms" command. The default is 0xFFFFFFFF. Adjusting system.amask allows the user to tailor the alarm response of the device.

3.3.1 LED settings

The LED attribute group controls LED behavior.

```
leds: {
    enabled: "on"
},
```

3.3.1.1 leds.enabled ["on" or "off"]

When this item is "off" the PWR and Radio LEDs are forced to be off. This setting may be used for lower power operation. Default is "on".

3.3.2 Pushbtn settings

The Pushbtn attribute group controls LED panel push button behavior.

```
>cfg get pushbtn
{
  enabled: "on",
  reset_defaults: "off"
}
```

3.3.2.1 pushbtn.enabled ["on" or "off"]

This attribute is used to suppress push button behavior. Default is "on".

NOTE When pushbtn.enabled is "off" there is no way to wake a sleeping device other than to reboot it.

3.3.2.1 pushbtn.reset_defaults ["on" or "off"]

This attribute is used to enable the ability for the button to reset the radio to last saved configuration snapshot. When pushbtn.reset_defaults is set to "on" a press of greater than 15 seconds followed by a release will perform the equivalent of a **cfg restore** operation. Default is "on".

3.3.3 Display settings

The Display attribute group contains settings associated with the optional E-ink display. Changing these items has no effect on a unit that is not equipped with a display.

```
>cfg get display
{
  enabled: "on",
  invert: "off",
  show_ip: "on"
}
```

3.3.3.1 display.enabled [“on” or “off”]

This attribute controls whether or not the display is on. Default is “on”.

3.3.3.2 display.invert [“on” or “off”]

This attribute controls the background/foreground emphasis. When this is set to “off” the display will have a mostly a white background. Default is “off”.

3.3.3.3 display.show_ip [“on” or “off”]

This attribute allows suppression of the device IP address on the display. The facility is included to help facilitate any physical device security concerns associated with displaying the IP address. Default is “on”. When set to “off” the display will show literal xx.xx.xx.xx instead of the programmed IP.

3.3.4 Password settings

The Password attribute group contains settings associated with password management. By default, TransNEXT units ship with a unique 10-character password per device. The password policy allows customer control of what password choices are acceptable.

```
>cfg get password
{
  min_chars: 1,
  max_chars: 64,
  min_lower_case: 1,
  min_capital_letters: 0,
  min_numbers: 0,
  min_non_alpha_numeric: 0,
  permit_username: "on"
}
```

NOTE For best security practice GE Vernova recommends changing the password prior to deployment.

Passwords are changed with the **password** command.

```
>password help
password <user>          Change password for specified user
    <user> [admin, tech, oper]
```

3.3.4.1 password.min_chars [0-255]

This item specifies the minimum number of characters for a new password. Default is 10.

3.3.4.2 password.max_chars [0-255]

This item specifies the maximum number of characters for a new password. Default is 64.

3.3.4.3 password.min_lower_case [0-255]

This item specifies the minimum number of lower-case characters for a new password. Default is 1.

3.3.4.4 password.min_capital_letters [0-255]

This item specifies the minimum number of capital letters for a new password. Default is 1.

3.3.4.5 password.min_numbers [0-255]

This item specifies the minimum number of numbers (0-9) for a new password. Default is 1.

3.3.4.6 password.min_non_alpha_numeric [0-255]

This item specifies the minimum number of special characters for a new password. Default is 0.

3.3.4.7 password.permit_username [“on” or “off”]

This attribute specifies whether any of the reserved user roll names can be used as the password. Default is “off”.

3.3.5 COM1 settings

The COM1 attribute group contains settings associated with serial payload data including settings for baud, handshaking, RS232/RS485 mode, and embedded RTU simulator control.

```
>cfg get com1
{
  baud: 115200,
  databits: 8,
  parity: "N",
  stopbits: 1,
  rxd: 0,
  cts: 0,
  ctshold: 0,
  device: "dce",
  port: "rs232",
  rtu: "off",
  rtuid: 0
}
```

3.3.5.1 com1.baud [<baud list choice>]

This is the serial port baud rate in bits per second. Valid baud settings are 300, 600, 1200, 1800, 2400, 3200, 4800, 9600, 19200, 38400, 57600, and 115200. Default is 115200bps.

3.3.5.2 com1.databits [8]

This is the number of databits. Currently 8 is the only valid choice.

3.3.5.3 com1.parity ["N","O", or "E"]

This is the parity setting. N = None; O = Odd; E = Even.   Default is “N” – none.

3.3.5.4 com1.stopbits [1 or 2]

This is the number of stopbits. Default is 1 stop bit.

3.3.5.5 com1.rxd [0-255]

This is the receive data delay in milliseconds. Default is 0.

This attribute sets a delay, in milliseconds to pause after data would normally be delivered to the port. The typical intent is to remove character gaps in data delivery. When set to a value sufficient to cover radio.hoptime and retransmissions this will emulate a seamless data delivery mode. This is useful for protocols such as Modbus. Use a delay of twice the value of the radio.hoptime period; if retries are used multiply that value by the typical retry count; if radio.saf is "on", multiply by 2 again.

3.3.5.6 com1.cts [0-255]

This attribute sets a delay associated with CTS (clear-to-send) line response. Valid values are 0 to 255 milliseconds. Default is 0.

For DCE operation, the attribute specifies how long to wait after the RTS line goes high before asserting the CTS line. A timer value of zero means that the CTS line will be asserted immediately following the assertion of RTS.

For CTS Key operation (see the com1.device setting), the timer specifies how long to wait after asserting the CTS line before sending data out the COM port. A timer value of zero means that data will be sent out the com port without imposing a key-up delay. (Other delays may be in effect from other radio operating parameters.)

3.3.5.7 com1.ctshold [0-65535]

This attribute sets a delay associated with CTS (clear-to-send) hold time. Valid values are 0 to 65535 milliseconds. Default is 0.

Used when com1.device is "cts key", this command sets the amount of time in milliseconds that CTS remains present following transmission of the last character out the RXD pin of the com port. This "hold time" can be used to prevent squelch tail data corruption when communicating with other radios.

The CTSHOLD setting can range from 0 to 65535 (i.e., over 65 seconds). The default value is 0, which means that CTS will drop immediately after the last character is transmitted.

3.3.5.8 com1.device ["dce" or "cts key"]

This attribute sets the device behavior of the com port. The default is "dce".

In DCE mode, CTS will go high following RTS, subject to the com1.cts delay value. Keying is stimulated by the input of characters at the data port. Hardware flow control is implemented by dropping the CTS line if data arrives faster than it can be transmitted.

In CTS KEY mode, the radio is assumed to be controlling another radio, such as in a repeater or tail-end link system. The RTS line is ignored, and the CTS line is used as a keyline control for the other radio. CTS is asserted immediately after the receipt of RF data, but data will not be sent out the DATA port until after the com1.cts delay time has expired. (This gives the other radio time to key.) Following transmission of the last byte of data, CTS will remain asserted for the duration specified by com1.ctshold. The com1.ctshold value should be set sufficiently high.

3.3.5.9 com1.port ["rs232" or "rs485"]

This attribute sets the electrical signaling behavior of the serial port. Default is "rs232".

Pin descriptions for RS-232 are given in Table 2-2. COM Port Pin Details (RS-232).

Pin descriptions for RS-485 are given in Table 2-3. COM1 Port Pin Details (RS-485).

3.3.5.10 com1.rtu ["on" or "off"]

This attribute enables the embedded RTU simulator poll detection and response. Default is “off”.

When set to “on” this enables devices in a network to be polled using standard MDS polling utilities.

3.3.5.11 com1.rtuid [0-80]

This attribute assigns an address/ID to the local radios embedded RTU simulator. Default is “0”.

3.3.6 Dlink settings

The Dlink attribute group contains settings associated with DLINK diagnostic. DLINK is used for Network Management (PulseNET, Field Network Manager, and similar tools). In TransNEXT DLINK operation is expected to occur via TCP on the Ethernet port.

```
>cfg get dlink
{
  enabled: "on",
  type: "node",
  tcp_access: "off",
  connection_timeout: 0,
  tcp_port: 30020,
  trend_resp_win: 120
}
```

NOTE Dlink.trend_resp_win is reserved for future use.

3.3.6.1 dlink.enabled [“on” or “off”]

This attribute enables dlink network-wide diagnostics transactions. Default is “off”.

NOTE To address security concerns, TransNEXT normally ships with DLINK disabled. It is important to set dlink.enabled to “on” for each unit, prior to deployment if this operation is desired.

3.3.6.2 dlink.type [<dlink type choice>]

This attribute specifies the radio’s operational characteristics for network-wide diagnostics. Valid dlink type choices include "node", "root", "repeater", "peer", and "gate". Default is “node”

NOTE Selections "repeater", "peer", and "gate" are reserved for special use.

NODE is the most common setting, and the default. This is the basic system radio device-type. Typically, the radio network is comprised of nodes and one root. Non-intrusive diagnostics can only be conducted from the root node.

ROOT is limited to one, and only one, per network (including units associated through Extension units.) The root is the focal point of network-wide diagnostics information. The root is the only radio through which non-intrusive diagnostics can be conducted. This value should be set on Master (radio.mode “m”).

3.3.6.3 dlink.tcp_access [“on” or “off”]

This attribute enables dlink network-wide diagnostics transactions. Default is “off”.

3.3.6.4 dlink.connection_timeout [0-65535]

This attribute specifies the connection timeout in seconds for TCP dlink operation. The timeout is the maximum time the connection can remain idle before dropping the connection. 0 is reserved as a special value to mean do not apply a connection timeout. Default is 0.

3.3.6.5 dlink.tcp_port [0-65000]

This attribute specifies the TCP port for the Dlink TCP server to use. It is not used when dlink.tcp_access is “off”. The default is 30020.

3.3.7 Eth settings

The Eth attribute group contains settings associated with Ethernet. All items in this group use IPv4 dot-decimal format such as xxx.xxx.xxx.xxx.

```
>cfg get eth
{
  enabled: “on”
  ipaddr: 192.168.1.1
  netmask: 255.255.255.0
  gateway: 192.168.1.254
}
```

3.3.7.1 eth.enabled [“on” or “off”]

When this item is “off” the ethernet interface is disabled. Default is “on”.

3.3.7.2 eth.ipaddr [xxx.xxx.xxx.xxx]

This is the IP address for the radio. The radio requires a local IP address to support ssh and IP/Payload (terminal server) services. Default is “192.168.1.1”.

3.3.7.3 eth.netmask [xxx.xxx.xxx.xxx]

This attribute refers to the radio’s IPv4 local subnet mask. Default is “255.255.255.0”. This parameter is used when the radio attempts to send a locally initiated message.

3.3.7.4 eth.gateway [xxx.xxx.xxx.xxx]

This is the IPv4 address of the default gateway device, typically a router connected to the radio. Default is “192.168.1.254”.

3.3.8 Network control settings

The nwk attribute group contains settings associated with network access control.

```
>cfg get nwk
{
  bridging: "off",
  http: "on",
  https: "on",
  ssh: "on",
  firewall: {
    filter: "allow-all",
    src1: [0x00:0x00:0x00:0x00:0x00:0x00],
    src2: [0x00:0x00:0x00:0x00:0x00:0x00],
    src3: [0x00:0x00:0x00:0x00:0x00:0x00],
    src4: [0x00:0x00:0x00:0x00:0x00:0x00]
  }
}
```

3.3.8.1 nwk.bridging [“off”, “on”]

This attribute controls whether bridging over ethernet is enabled. When “on” all ethernet data that is not directed to local device will be sent over the air, subject to other firewall settings. Default is “on”.

3.3.8.2 nwk.http: [“on”, “off”]

This attribute controls whether the local device can accept HTTP connections. Default is “on”.

3.3.8.3 nwk.https [“on”, “off”]

This attribute controls whether the local device can accept HTTPS connections. Default is “on”.

3.3.8.4 nwk.ssh [“on”, “off”]

This attribute controls whether connections the local device can accept SSH connections. Default is “on”.

3.3.8.5 nwk.firewall.filter [“allow-all”, “unicast”, “unicast-arp”, “unicast-arp-dhcp”]

The filter control provides a simple way to limit the amount of ethernet traffic sent over the air, based on message type.

“allow-all” is the least restrictive. All payload ethernet data is sent over the bridge.

"unicast" restricts over the air data to only messages that sent directly to a specific IP address. Broadcast and Multicast data is discarded.

"unicast-arp" is like the "unicast" selection but also permits broadcast ARP messages to be sent over-the-air. This setting is useful for letting the system learn what devices are connected while still limiting general broadcast data.

"unicast-arp-dhcp" is like unicast but also permits broadcast ARP and DHCP messages to be sent.

3.3.8.6 nwk.firewall.src1

These 4 source list attributes (...src1 / ...src2 / ...src3 / ...src4) are used to set MAC address “allow list” entries.

The value is entered as a 6-element, colon-separated array of hexadecimal values, delimited by square braces. Each array element matches the corresponding octet of a typical 6 octet, 48-bit MAC address.

Together these 4 attributes provide a set of up to 4 MAC addresses from which the system will accept data to be sent over-the-air. Data from disallowed MAC addresses will be disregarded.

Default is [0x00:0x00:0x00:0x00:0x00:0x00] and is reserved to mean a blank entry.

If all four source list entries are blank, this means that data from ALL MAC addresses will be accepted.

3.3.9 Bridge settings

The Bridge attribute group contains settings associated with bridge mode. These options apply to both ethernet data (if bridging is on) and serial.

```
>cfg get bridge
{
  security: "none",
  psk: "",
  compress: "lz",
  p2p: "off",
  ageout: 10,
  ttl: 5000
}
```

3.3.9.1 bridge.security [“none”, “aes256-ctr”, “aes256-ccm”]

This attribute defines the authentication process for bridge mode and the subsequent encryption method for data that follows. Default is “none”.

When bridge.security is set to “none” the system performs a simple 2-way handshake authentication. Data is not encrypted. This method simply confirms to the master that the remote is a valid TransNEXT.

When bridge.security is set to “aes256-ctr” or “aes256-ccm” the system performs a 4-way handshake to authenticate using the bridge.psk value (pre-shared key). All data including ethernet and serial is encrypted. aes256-ccm is the stronger encryption mode but may introduce slight additional latency.

NOTE Bridge security should normally be the same on all units in the network. A key exception occurs when bridge.security is set to “none” on the master. Setting the master’s bridge.security to “none” will automatically disable security for the remotes. The remotes will perform simple 2-way handshake authentication and pass *unencrypted* data. This provision can be used as a facility to quickly commission and debug a system prior to enabling full security.

3.3.9.2 bridge.psk

This attribute sets the password (pre-shared key) used for device authentication and encryption. Standard user input is a clear text string of length 8-63.

Default is “” (blank), meaning no explicit key has been programmed.

NOTE Subsequent query of this field will not show the clear text entry. Instead, the output is displayed as a tagged, encrypted, base64 encoded value.

3.3.9.3 bridge.compress [“none”, “lz”]

This attribute selects whether data compression is used for transmission of bridged data. When compression is enabled the TransNEXT radio will make more efficient use of the available bandwidth at the expense of slight additional latency.

Current available options are “none” or “lz”. Default is “none” meaning compression is disabled

3.3.9.4 bridge.p2p [“off”, “on”]

NOTE Bridge.p2p is reserved for future application and is not currently used.

3.3.9.5 bridge.ageout [2-255]

This attribute controls the bridge entry age-out time, in minutes. Default is 10.

3.3.9.6 bridge.ttl [500-30000]

This attribute controls the packet time-to-live, in seconds. Default is 5000.

3.3.10 IP/Payload settings

The Ippl attribute group contains settings associated with IP/Payload. IP/Payload was originally introduced in the MDS SD licensed radio series. IP/Payload acts like a terminal server with the serial port side routed as over-the-air streaming traffic.

NOTE VRC fields for this attribute group are reserved for future application and not currently used.

```
>cfg get ippl
{
  enabled: "off",
  mode: "udp",
  talk_on_vrc: 1,
  listen_to_vrc: 1,
  local_ip_port: 30011,
  ip_peer_addr: 192.168.1.1,
  ip_peer_port: 30999,
  connection_timeout: 0,
  keep_alive: "off",
  modbus_tcp_rtu: "off"
}
```

3.3.10.1 ippl.enabled [“on” or “off”]

This attribute enables IP/Payload. Default is “off”.

3.3.10.2 ippl.mode ["udp", "tcp-client", or "tcp-server"]

This attribute enables the operational mode “udp” or “tcp” and for tcp indicates if the radio should act as a server or client.

3.3.10.3 ippl.local_ip_port [0-65000]

This attribute specifies the local_ip_port for TCP server use it. This value is only applicable when ippl.mode is equal to “tcp-server”. The corresponding IP address is the value from eth.ipaddr. The default port is 30011.

3.3.10.4 ippl.ip_peer_addr [xxx.xxx.xxx.xxx]

This attribute specifies the IP peer address for UDP and TCP client use. It is not applicable for TCP server. The value is specified in IPv4 dot decimal format. The default is 192.168.1.1.

3.3.10.5 ippl.ip_peer_port [0-65000]

This attribute specifies the IP peer port for UDP and TCP client use. It is not applicable for TCP server. The default port is 30011.

3.3.10.6 Ippl.connection_timeout [0-65535]

This attribute specifies the connection timeout in seconds for all modes. The timeout is the maximum time the connection can remain idle before dropping the connection. 0 is reserved as a special value to mean do not apply a connection timeout. Default is 0.

3.3.10.7 ippl.keep_alive [“on” or “off”]

This attribute enables connection keep alive. Default is “off”.

3.3.10.8 ippl.modbus_tcp_rtu: "off"

This attribute turns on local conversion of Modbus TCP into Modbus RTU. Default is "off".

3.3.11 Terminal Server settings

The ts attribute group contains settings associated with Terminal Server operation. Terminal Server operation allows an over-the-air ethernet connection to be converted to the serial port on the remote device.

NOTE Terminal Server operation is only valid when system.mode is set to “Bridge”.

```
>cfg get ts
{
  enabled: "off",
  mode: "udp",
  talk_on_vrc: 1,
  listen_to_vrc: 1,
  local_ip_port: 30011,
  ip_peer_addr: 192.168.1.1,
  ip_peer_port: 30011,
  connection_timeout: 0,
  keep_alive: "off",
  modbus_tcp_rtu: "off"
}
```

3.3.11.1 ts.enabled [“on” or “off”]

This attribute enables terminal server on the device. When terminal server is enabled, all serial port data on com1 is routed via the terminal server connection. Default is “off”.

3.3.11.2 ts.mode ["udp", "tcp-client", or "tcp-server"]

This attribute enables the operational mode “udp” or “tcp”, and for tcp indicates if the radio should act as a server or client.

3.3.11.3 ts.local_ip_port [0-65000]

This attribute specifies the local_ip_port for TCP server use it. This value is only applicable when ts.mode is equal to “tcp-server”. The corresponding IP address is the value from eth.ipaddr. The default port is 30011.

3.3.11.4 ts.ip_peer_addr [xxx.xxx.xxx.xxx]

This attribute specifies the IP peer address for UDP and TCP client use. It is not applicable for TCP server. The value is specified in IPv4 dot decimal format. The default is 192.168.1.1.

3.3.11.5 ts.ip_peer_port [0-65000]

This attribute specifies the IP peer port for UDP and TCP client use. It is not applicable for TCP server. The default port is 30011.

3.3.11.6 ts.connection_timeout [0-65535]

This attribute specifies the connection timeout in seconds for all modes. The timeout is the maximum time the connection can remain idle before dropping the connection. 0 is reserved as a special value to mean do not apply a connection timeout. Default is 0.

3.3.11.7 ts.keep_alive [“on” or “off”]

This attribute enables connection keep alive. Default is “off”.

3.3.11.8 ts.modbus_tcp_rtu: "off"

This attribute turns on local conversion of Modbus TCP into Modbus RTU. Default is "off".

3.3.12 Modem settings

The Modem attribute group contains settings associated with how the TransNEXT device physically communicates with other units over-the-air.

```
>cfg get modem
{
  speed: "106k",
  system_id: 0
}
```

3.3.12.1 modem.speed [“106k”]

This attribute controls the over-the-air data transfer rate. Default is “106k”.

This item cannot currently be modified. It is reserved for future use.

3.3.12.2 modem.system_id [0-7]

This attribute sets a modem level system ID allowing communication to only a matching network. Master and Remote radios in the same network must use the same value. Eight unique choices are available.

System ID differs from radio.addr in that it operates at the modem layer to improve co-channel isolation. This setting is not typically required but can be employed as a tuning control for improved performance in areas with overlapping TransNEXT or TransNET networks. Default value is “0”.

NOTE For systems operating in “TransNEXT” serial backward compatibility mode, setting the modem.system_id to “0” permits operation with legacy TransNET devices and earlier TransNEXT systems.

3.3.13 Radio settings

The Radio attribute group contains settings that control TransNEXT radio operation. Items under the radio group typically use names like the commands found in the MDS TransNET radio.

```
>cfg get radio
{
  power: 20,
  addr: 7552,
  xaddr: 0,
  hoptime: 7,
  fec: "on",
  retry: 0,
  repeat: 3,
  saf: "off",
  xpri: 255,
  xmap: 0x00000000,
  skip: [8,1,0,0,0,0,0,0],
  csaddr: 0,
  rxtot: 0,
  unit_addr: 4567,
  lpm: 0,
  lpmhold: 20,
  sleep: "off",
  mode: "M",
  code: 0
}
```

3.3.13.1 radio.power [10-30]

Power can range from 10 to 30 dBm. Default is 30dbm which is equal to 1 watt. In the USA total Effective Isotropic Radiated Power must be <= 36dbm. This means that power must be turned down for systems with antenna gain greater than 6db.

NOTE Some countries may impose lower EIRP limits. Check the regulatory rules and turn down power as needed to ensure compliance.

3.3.13.2 radio.addr [1-65000]

This is the radio's Network Address. Valid network addresses range from 1 to 65000.

A Network Address must be programmed at the time of installation and must be common across each radio in a given network. Radios are typically shipped with network address set to 0. This is a special reserved value indicating address is not set. If the address is not set the system will be in an invalid state, preventing operation and generating an alarm.

NOTE We recommend that the last four digits of the Master radio's serial number be used for the network address. This helps avoid conflicts with other users.

3.3.13.3 radio.xaddr [0-31]

This is the radio's Extended Address. The item is only applicable for a Master or Extension radio. Valid extended addresses range from 0 to 31. Default is 0.

Extended Address serves as a common address for the sub-network synchronized to this Master or Extension. This value can be listed in the radio.xpri parameter of associated Extension or Remote radios to allow them to synchronize to this radio. Setting the Master to zero (0) is recommended. It is easy to remember and works well with other radio default settings.

3.3.13.4 radio.hoptime [7 or 28]

This controls radio hop timing. The item is a value corresponding to the hop-time setting in milliseconds. 7 and 28 are the only choices. Default radio.hoptime is 7. A setting of 28 must be used when throughput exceeds 57,600 bps and is recommended when data transmission sizes exceed 256 bytes.

Changes to the radio.hoptime may only be made at the Master radio. (This is because the Master radio establishes the hop-time setting for the entire network.) At Remote radios, the hop-time setting may be read when the radio is in synchronization with the Master, but it cannot be changed.

3.3.13.5 radio.fec ["on" or "off"]

This item controls Forward Error Correction. The default setting is "on". (It needs to be turned off when throughput exceeds 57,600 bps.). The radio.fec value is set at the Master and is automatically passed on to all Remotes in a network.

3.3.13.6 *radio.retry [0-10]*

This item affects upstream data. The value represents the maximum number of times (0 to 10) that a Remote radio will re-transmit data. The default setting is 10.

This item is associated with ARQ (Automatic Repeat Request) operation of the radio and is intended for use in areas with heavy radio interference. A value of 0 represents no retries, while values of 1 or greater successively improve the chance of data delivery in spectrally harsh environments (at the expense of possibly increased latency). The radio.retry value is only settable at the Master. It is readable by a synchronized Remote.

3.3.13.7 *radio.repeat [0-10]*

This item affects downstream data. The setting causes a Master or Extension to unconditionally repeat transmissions for the specified number of times. Unlike the radio.retry behavior, there is no acknowledgment that a message has been received.

The value represents the maximum number of times (0 to 10) that a Master or Extension radio will re-transmit data. The default setting is 3.

3.3.13.8 *radio.saf ["on" or "off"]*

This item controls the operational state of Store-and-Forward (SAF) mode. The default setting is "off".

Store-and-Forward (SAF) offers a way to physically extend network range. Extension radios (designated as radio.mode "x") serve as single-radio repeaters that link adjacent sub-networks and move data from one sub-network to the next one.

The radio.saf setting affects all radios in the associated network. When SAF is on, overall system throughput is halved but does not reduce further regardless of store-and-forward depth.

When SAF is off, units programmed as radio.mode "x" behave as standard remotes.

The radio.saf value is set at the Master and is automatically passed on to all Remotes in a network.

3.3.13.9 *radio.xpri [0-31 or 255]*

The radio.xpri value is only meaningful for a Remote or Extension radio.

This item establishes a Primary Extended Address, specifying the primary radio with which this radio will attempt to synchronize and communicate. Whenever the current radio attempts to establish sync, it will limit its choice to the radio.xpri value for the first 30 seconds before allowing synchronization to other units in the radio.xmap list.

NOTE After the first 30 seconds the radio.xpri value is still always an implicitly allowed synchronization source even if it is not called out in the radio.xmap list.

The default value for radio.xpri is 0 (matching the default xaddr). A setting of 255 represents "none" and allows the unit to synchronize with any Master or Extension in the radio.xmap list.

3.3.13.10 radio.xmap [0x00000000-0xFFFFFFFF]

The radio.xmap value is only meaningful for a Remote or Extension radio.

radio.xmap is a 32-bit hexadecimal entry where the least significant bit represents xaddr 0 and the most significant bit represents xaddr 31. The full 32-bit hex value represents the set of all 32 possible extension addresses with which the radio could be allowed to communicate. A set bit means that synchronization to that xaddr is allowed; a clear bit means not allowed.

This value defaults to 0x00000000 which means that the only allowed synchronization source is the one specified by radio.xpri.

3.3.13.11 radio.skip [<8-element-array>]

This attribute indicates which combination of 8 possible frequencies zones should be removed from the radio's hop sequence. Default is [0,0,0,0,0,0,0,0] meaning no zones are skipped.

Skipping zones is one way of dealing with constant interference on one or more frequencies in the radio's operating band. See A Word About Radio Interference on Page 73 for more information on dealing with interference. Consult "APPENDIX B – Operating Frequencies" to see the frequency range covered by each zone.

The radio.skip value is entered as an 8-element, comma-separated array, delimited by square braces. Each array element may specify a zone (1 through 8) to skip. Unused array elements should be filled with "0" such that there are always 8 items. Items in the list may be specified in any order.

The radio.skip value is set at the Master and is automatically passed on to all Remotes in a network.

3.3.13.12 radio.csaddr [0 or 1-65000]

This attribute is used to specify the network address of a "Clock-Sync" Master station. The format matches the value of a corresponding radio's radio.addr setting. A value of 0 (default) is reserved to mean "none". See 2.8.5 Co-Located and Close-Proximity Masters for more detail.

3.3.13.13 radio.rxtot: [0 or 1-1440]

This attribute is the receiver time-out alarm. Default is "0". Set to a non-zero value to both enable the alarm and set the max time in minutes. Alarm is asserted if there is no data received for a time greater than this value. The alarm is cleared when data is detected.

3.3.13.14 radio.unit_addr [1-65000]

Unit address is used for network-wide diagnostics (used by PulseNET and Field Network Manager). Valid network addresses range from 1 to 65000. Default value is the last four digits of the radio's serial number. Values < 10000 must match the 4-digit default. Values >= 10000 can be arbitrary.

NOTE Keeping unit address set to the last 4 digits of serial number is recommended and should only be changed if a conflict is detected. This method helps minimize conflicts between radios.

3.3.13.15 radio.lpm [0 or 1]

This attribute controls Low-Power Mode. See 2.8.2 Using Low-Power Mode (LPM) *(Master-enabled*). Default is 0.

This feature trades increased latency to gain power savings. Low-power mode (LPM) automatically saves power at a Remote by instructing the Remote to shut down for large periods of time in between SYNC messages. Master transmissions are automatically blocked while the Remotes are asleep. Note, both Masters and Remotes are adaptive and will suppress a normal sleep interval if data transmission or reception is in progress.

- Setting radio.lpm 1 at the Master enables low-power mode network-wide; all Remotes pick it up and start saving power by automatically sleeping.

- Setting radio.lpm 0 at the Master is used to disable low-power mode (LPM) (This is the default)

NOTE radio.sleep must be set to "on" on remote units for LPM to function.

3.3.13.16 radio.lpmhold

This attribute is used in conjunction with Low Power Mode (see section 2.8.2). The value specifies how long to suppress auto-sleep following reception of the last character sent out of the RXD serial data port. The intent is for the value to be long enough to allow a polled RTU to respond before the connected radio goes back to sleep. Value can range from 0 – 1000ms. Default is 20ms.

3.3.13.17 radio.sleep ["on" or "off"]

This item controls radio low power sleep behavior. The default setting is "off". (It needs to be turned on to use either the radio.lpm or sleep input feature). The radio.sleep value must be set individually at all applicable remotes. The value is not meaningful for a master or store-and-forward unit and is ignored.

3.3.13.18 radio.mode ["m" or "r" or "x"]

The radio.mode attribute sets the operating mode of the radio. A Master radio is set with radio.mode = "m"; a Remote set by radio.mode = "r" and an Extension is set by radio.mode = "x".

All units default to Remotes; other modes must be specifically programmed with **cfg set radio.mode**.

If mode "x" is used, the mode "x" radio should be programmed with an Extended Address (XADDR). Units that need to hear this mode "x" radio must be programmed with an appropriate radio.xpri and/or radio.xmap value.

NOTE A mode "x" radio will behave like a mode "r" radio unless radio.saf is set to "on."

3.3.13.19 radio.code [0 or 1-255]

The radio.code attribute controls a primitive security attribute for compatibility with legacy TransNET systems.

The default is 0, meaning "none". Setting radio.code to a value other than 0 activates the feature. The disadvantage is increased complexity in managing the network.

When a radio.code is non-zero, all radios in the system must use the same code value. If the code value is not properly programmed, a Remote radio will not synchronize with the Master.

NOTE The "code" radio attribute is intended only provided for compatibility with legacy TransNET radio deployments. This setting is not cryptographically secure and is strongly discouraged for new installations.

3.4 System Health and Status

3.4.1 Firmware version

The CLI `about` command and the about section on the top right of Web UI Dashboard page both provide information on the current device firmware and hardware model.

For a network operating in bridge mode, the `show nwk` command and the Web UI Network each provide a table of connected remotes including the FW version running on each remote.

3.4.2 Show command

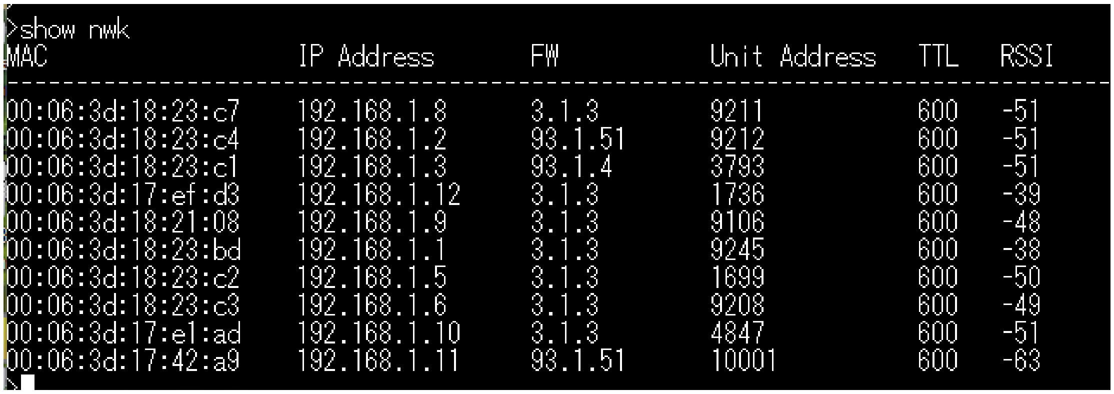
The CLI show commands provides a quick means to obtain various types of device status. Options include the following:

```
show device               Show device information
show log                  Show event log
show alarms               Show current system alarms
show status               Show radio status
show stats                Show radio and network statistics
show sync                 Show radio synchronization status
show temp                 Show system temperature
show vin                  Show radio input voltage
show uptime               Show system uptime
show rssi                 Show continuous radio RSSI
show rssi!                Show radio RSSI
show eth                  Show ethernet status
show ip                   Show current IP configuration
show nwk<!>               Show connected radios and Ethernet devices
show options              Show available feature options
```

3.4.3 Connected Remotes Table

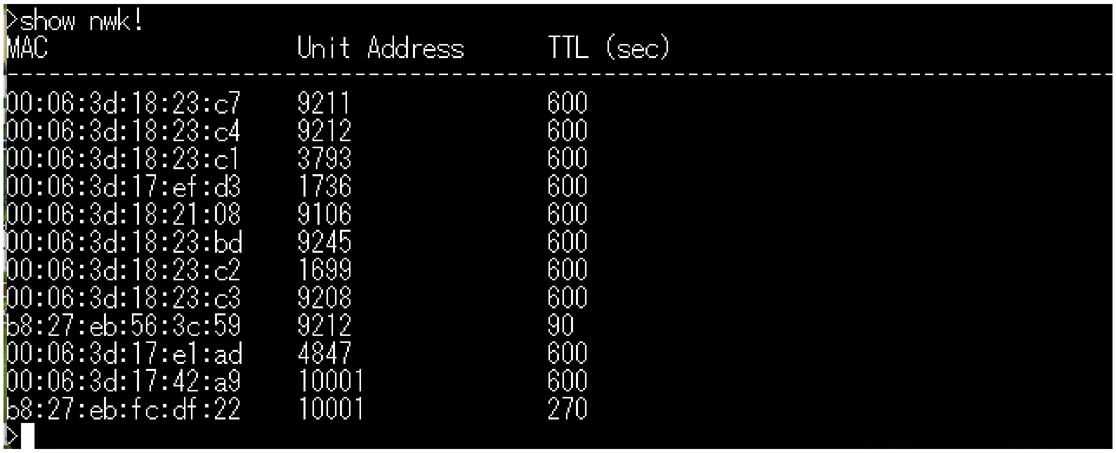
For systems operating in Bridge mode, the **`show nwk`** command provides a simple way to view the entire network.

Network entries are shown as a list of all connected (authenticated) remotes in the system. Each list element includes remote MAC address, IP address, Firmware Version, Unit Address, TTL setting, and signal strength for last received packet (in dBm).



```
>show nwk
MAC                  IP Address       FW           Unit Address   TTL   RSSI
---------------------------------------------------------------------------------
00:06:3d:18:23:c7    192.168.1.8      3.1.3        9211           600   -51
00:06:3d:18:23:c4    192.168.1.2      93.1.51      9212           600   -51
00:06:3d:18:23:c1    192.168.1.3      93.1.4       3793           600   -51
00:06:3d:17:ef:d3    192.168.1.12     3.1.3        1736           600   -39
00:06:3d:18:21:08    192.168.1.9      3.1.3        9106           600   -48
00:06:3d:18:23:bd    192.168.1.1      3.1.3        9245           600   -38
00:06:3d:18:23:c2    192.168.1.5      3.1.3        1699           600   -50
00:06:3d:18:23:c3    192.168.1.6      3.1.3        9208           600   -49
00:06:3d:17:e1:ad    192.168.1.10     3.1.3        4847           600   -51
00:06:3d:17:42:a9    192.168.1.11     93.1.51      10001          600   -63
>
```

To view all connected endpoints, use **show nwk!**. This display includes the UNIT address of the TransNEXT radio through which the endpoint is connected.



```
>show nwk!
MAC                  Unit Address      TTL (sec)
---------------------------------------------------------------------------------
00:06:3d:18:23:c7    9211              600
00:06:3d:18:23:c4    9212              600
00:06:3d:18:23:c1    3793              600
00:06:3d:17:ef:d3    1736              600
00:06:3d:18:21:08    9106              600
00:06:3d:18:23:bd    9245              600
00:06:3d:18:23:c2    1699              600
00:06:3d:18:23:c3    9208              600
b8:27:eb:56:3c:59    9212              90
00:06:3d:17:e1:ad    4847              600
00:06:3d:17:42:a9    10001             600
b8:27:eb:fc:df:22    10001             270
>
```

3.4.4 Event Logging

Key system status change conditions are stored as logged events in non-volatile memory. Examples of logged events include alarm changes, configuration changes, software updates, reboots, logins, etc.

To display logs issue the show logs command as follows:

```
>show log

Event Log:

Uptime          Facility       Description                     Parameter
```

```
-------------------------------------------------------------------------------
002 02:48:18     Login          User logged in                  admin
002 02:32:47     Login          User logged out                 admin
002 02:22:43     Login          User logged in                  admin
002 00:11:27     Login          User logged out                 admin
002 00:01:26     Login          User logged in                  admin
001 06:57:46     Login          User logged out                 admin
001 06:47:42     Login          User logged in                  admin
000 03:05:11     Login          User logged out                 admin
000 02:55:08     Login          User logged in                  admin
000 02:10:38     Login          User logged out                 admin
-- Press a key to continue (Q to quit) --
000 02:00:34     Login          User logged in                  admin
000 00:15:34     Login          User logged out                 admin
000 00:01:27     Alarm SET      VSWR
000 00:01:22     Alarm CLR      VSWR
000 00:01:22     Alarm CLR      No Sync
000 00:01:20     Firmware       Modem Reprog Complete           radio 1
000 00:00:56     Login          User logged in                  admin
000 00:00:09     Alarm SET      VSWR
000 00:00:09     Alarm SET      No Sync
000 00:00:03     Firmware       Modem Reprog Started            radio 1
000 00:00:03     Reset Source   SFT Reset
000 00:00:03     Firmware       System Boot                     radio 1
```

Each log entry is timestamped relative to uptime. The timestamp format is ddd HH:MM:SS. (ddd represents uptime in days, HH = hours, MM=minutes, SS=seconds) The logs are displayed in reverse chronological order. The most recent items will always be displayed first.

NOTE If the log contains a set of events spanning *multiple* reboots, the timestamps will not always be monotonic. If the timestamp of a pair of sequential logs jumps from a lower number to a higher number, that means that the events occurred during a different boot instance. Each group of events will be timestamped relative to its specific reboot instance.

The command will show 20 logged items and then pause asking for a key to continue or "Q" to quit.

To clear the log history, issue the "clear logs" command as shown below. Answer "y" to the "clear entire log" prompt:

```
>clear log
Clear entire log? (y/n)

Clearing log...Done.
```

3.4.5 Snapshots and System Recovery

TransNEXT provides a means to take a "snapshot" copy of the current configuration database image (see `cfg show`) for later restoration. This can be handy to roll back the unit's settings to a previous known good configuration. Note that restoring the unit to the snapshot will overwrite the current configuration, and that it cannot be undone.

TransNEXT ships with the default factory settings saved in the "snapshot".

To save a new snapshot enter:

```
>cfg snapshot
OK
```

To restore a previous snapshot as the current configuration:

```
>cfg restore
OK
```

NOTE To force a “cfg restore” without using the CLI, press and hold the button on the LED/button membrane for greater than 15 seconds, then release. This will restore settings to the last **cfg snapshot** and reset the device admin password to its original value.

3.5 Firmware Reprogramming

NOTE Information on reprogramming in this section is limited to reprogramming of device/radio *application* firmware. Bootloader firmware updates are not considered.

TransNEXT provides for two saved firmware images. The purpose is to ensure that there is always one good image to run. One image is reserved as the active image, and the other is the inactive image. Firmware reprogramming always applies to the *inactive* image. With this method if there is a problem, the active image is preserved.

GE Vernova provides signed TransNEXT firmware as proprietary .MPK files posted on our website. The CLI and Web Interface both offer facilities for local reprogramming of the saved firmware images. MPK files can be loaded directly by the Web UI. For Web reprogramming see page 43. The sections below focus on reprogramming using the CLI.

NOTE To prevent operational conflicts the TransNEXT device will automatically block downgrading of firmware to an incompatible version. In many cases this will block the user from reverting back to the previous version, following an update.

3.5.1 Local Device Reprogramming

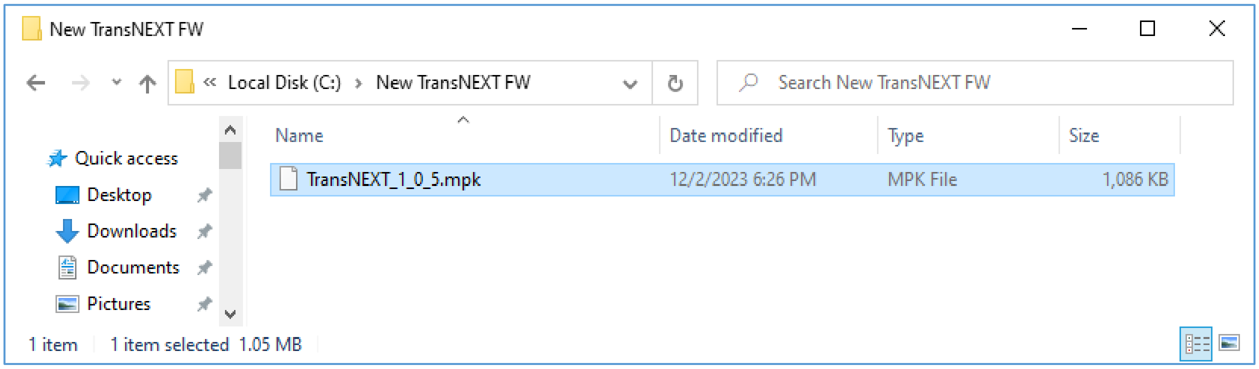
For the CLI a terminal emulator supporting YMODEM is required. Tera Term is as simple free terminal emulator that supports YMODEM. Tera Term is convenient because it will reestablish a USB/Serial connection following TransNEXT device reboot. Other terminal emulators may be used, but examples in the section are based on Tera Term.

Prior to upgrading firmware, it is good practice to confirm what firmware is currently loaded and active.

To check the current firmware, issue the **app** command as shown.

```
>app
Image 1 Version:   1.0.5 (active)
Image 2 Version:   1.0.5
```

In this example we see that both the active and inactive image are 1.0.5. Next identify and locate which firmware you want to load.



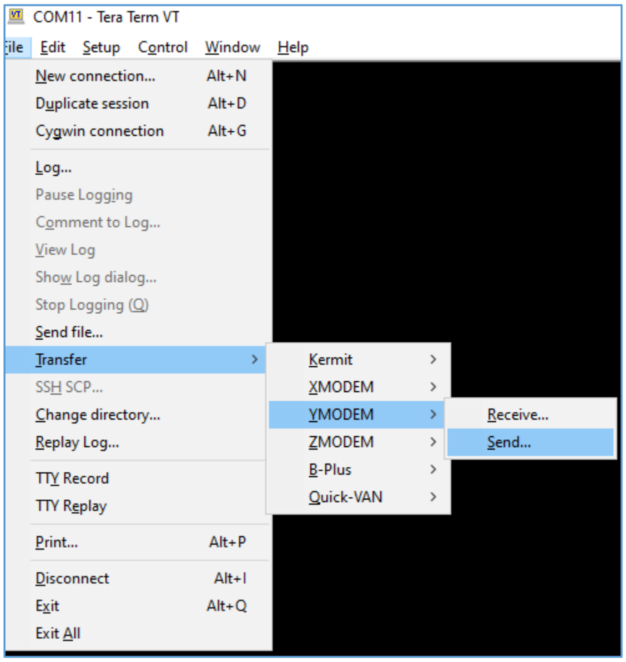
Name	Date modified	Type	Size
TransNEXT_1_0_5.mpk	12/2/2023 6:26 PM	MPK File	1,086 KB

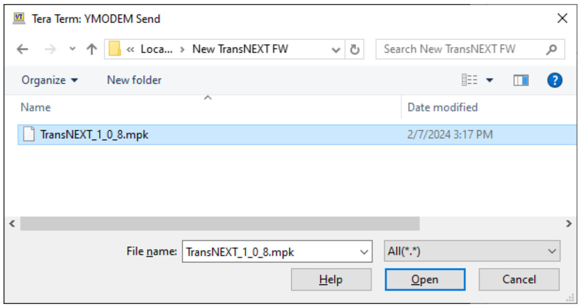
1 item 1 item selected 1.05 MB

To update to FW 1.0.8 issue the **app update** command. The TransNEXT will prompt you to initiate a YMODEM transfer:

```
>app update
Start YMODEM transfer, send file now...
Hit Ctrl-X twice to cancel
C
```

Select the YMODEM transfer like the example here:



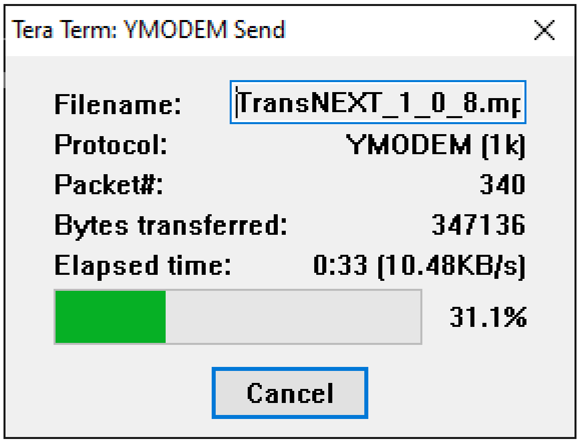


TransNEXT_1_0_8.mpk 2/7/2024 3:17 PM

File name: TransNEXT_1_0_8.mpk

All(*.*)

Progress is shown as follows:



Filename: TransNEXT_1_0_8.mp

Protocol: YMODEM (1k)

Packet#: 340

Bytes transferred: 347136

Elapsed time: 0:33 (10.48KB/s)

31.1%

At completion the display will show:

```
Transfer complete: 1115020 bytes
Validating MPK.....
Updating image...
  /
OK
>
```

Now use the **app** command to verify that the new 1.0.8 firmware is now loaded as the inactive image.

```
>app
Image 1 Version:   1.0.5 (active)
Image 2 Version:   1.0.8
```

Finally use the **app** command to make image 2 the new active image.

```
>app 2
Confirm switch to Image 2? (y/n)
  -
Reboot to APP image: 2  ......
```

NOTE The process of the **app 2** command above will take a few minutes to complete.

At the completion of this stage the TransNEXT will automatically switch to the new image and reboot. After reboot the UI connection will need to be reestablished. If using Tera Term, the TransNEXT device will have a small delay and finally return to the banner and login prompt.

Upon logging in the device may still be finishing programming on an internal radio processor. During this time the app command will show “unavailable”.

```
>app
Access Denied:
 Modem FW Update in Progress
Command failed!
>
```

After a few minutes the internal operation is complete, and the **app** command will show the new active version.

```
>app
Image 1 Version:   1.0.5
Image 2 Version:   1.0.8 (active)
```

3.5.2 Over-the-Air Reprogramming

Over-the-Air Reprogramming section allows the current firmware image running on a master radio to be broadcast over the air to the entire network of TransNEXT remotes. The operation relies on unacknowledged broadcast transmission with variable repeats.

NOTE Varying RF environmental conditions may prevent Over-the-Air Reprogramming from successfully updating all devices. The operation may be repeated as needed to attempt to pick up units missed during a prior session. If a remote unit has a particularly poor signal OTA reprogramming may be impractical and it may be necessary to reprogram the device locally.

From the CLI the command is app_ota. Help is as follows:

```
>help app_ota
method <active|passive>   OTA App transfer mode
reboot <true|false>       OTA App reboot after update
start <speed>             Start OTA App reprogramming
    <speed> [robust, slow, medium, fast, turbo]
stop                      Stop OTA reprogramming
```

The command can be used at the master or remote to query current status of over-the-air transfer.

```
>app_ota
Status: Inactive
```

The command can be used query default settings as follows:

```
>app_ota method
Passive

>app_ota reboot
True
```

Setting the method and reboot parameters are done as separate lines prior to kicking off a transfer.

Method indicates if the TransNEXT will send intrusively or non-intrusively. The **method** argument is “active” or “passive”. **Passive** is non-intrusive while **Active** may cause some interference with payload data polling.

```
>app_ota method passive
>OK
```

Reboot indicates if the remote TransNEXT units will automatically reboot at the end of a transmission sequence when the new firmware image has been properly received. The **reboot** argument is “**true**” or “**false**”.

```
>app_ota reboot true
>OK
```

Prior to initiating the Broadcast OTA session, determine the transmission mode setting based on the characteristics of the connected network.

For weak signal networks “robust” is recommended and provides the best chance of hitting all units, but it may take a week or more for the system to update. For smaller networks with excellent signal strength other options may work well and complete much faster.

NOTE Operational behavior of the speed controls varies based on the system.mode selection. Bridge mode uses longer packets with longer inter-message delay. For given speed setting, overall time in Bridge is generally faster than the corresponding TransNEXT mode.

Table 3-2. OTA broadcast speed controls for TransNEXT mode

Speed setting	Transmission Sequence Repeat Count	Inter-Message Delay
robust	20	5 ms
slow	10	50 ms
medium	5	100 ms
fast	2	150 ms

Table 3-3. OTA broadcast speed controls for Bridge mode

Speed setting	Transmission Sequence Repeat Count	Inter-Message Delay
robust	15	2000 ms
slow	7	1000 ms
medium	5	500 ms
fast	4	100 ms

The line below initiates the broadcast FW OTA operation from the master at the desired speed using previously set values for “method” and “reboot”. The parameter following start is the speed argument shown in the table below:

```
>app_ota start robust
OK
```

Querying status at the Master will then show:

```
>app_ota
Status: Active: 0%
```

To terminate a session at the Master, use the “**stop**” argument on the command line:

```
>app_ota stop
OK
```

Checking status will show the following:

```
>app_ota
Status: Canceled
```

NOTE Avoid frequent queries on the UI during reprogramming – especially when using the faster transmission selections. It may interfere with successful transfer.

From the remote’s perspective, cancellation of an OTA session at the master is not immediately recognized. Once an **app_ota** operation is started by the Master and a remote joins the process, that remote will remain in that state even across reboots. The remote will continue report x.x.x (OTA Update in Progress) in the inactive image until one of the following occurs:

- A local firmware update is started, or
- The Remote completes the OTA reprogramming process (presumes master is still transmitting it)

4.0 TECHNICAL REFERENCE

4.1 A Word About Radio Interference

All units must meet the basic requirements listed below for proper operation. Check these items first when troubleshooting a system problem:

The TransNEXT shares the frequency spectrum with other services and unlicensed devices. As such, near 100% error free communications may not be achieved in a given location, and some level of interference should be expected. However, the radio's flexible design and hopping techniques should allow adequate performance if care is taken in choosing station location, configuration of radio parameters and software/protocol techniques.

In general, keep the following points in mind when setting up your communications network:

1. Systems installed in rural areas are least likely to encounter interference; those in suburban and urban environments are more likely to be affected by other devices operating in the license-free frequency band and by adjacent licensed services.

2. If possible, use a directional antenna at Remote sites. Although these antennas may be more costly than omnidirectional types, they confine the transmission and reception pattern to a comparatively narrow lobe, which minimizes interference to (and from) stations located outside the pattern.

3. If interference is suspected from a nearby licensed system (such as a paging transmitter), it may be helpful to use horizontal polarization of all antennas in the network. Because most other services use vertical polarization in these bands, an additional 20 dB of attenuation to interference can be achieved by using horizontal polarization.

4. Multiple transceiver systems can co-exist in proximity to each other with only very minor interference if they are each assigned a unique network address. Each network address has a different hop pattern.

   Additional RF isolation can be achieved by using separate directional antennas with as much vertical or horizontal separation as is practical. Vertical separation of antennas is more effective per foot/meter than horizontal.

5. If constant interference is present in a particular frequency zone, it may be necessary to "lock out" that zone from the radio's hopping pattern. The radio includes built-in tools to help users remove blocked frequency zones. Refer to the discussion of the radio.skip attribute for more information. In the USA, a maximum of four zones may be skipped, per FCC rules. Check the regulatory requirements for your region.

6. Interference can also come from out-of-band RF sources such as paging systems. Installation of a bandpass filter in the antenna system may bring relief. Contact the GE Vernova CIC (Critical Infrastructure Communications) Customer Service Department for recommendations and sources of suitable filters.

7. Proper use of the radio.retry and radio.repeat may be helpful in areas with heavy interference.

The radio.retry sets the maximum number of times (0 to 10) that a radio will re-transmit upstream data over the air. Values greater than 0 successively improve the chances of a message getting through when interference is a problem.

The radio.repeat sets a fixed number of unconditional retransmissions for downstream data.

8. The RF power output of all radios in a system should be set for the lowest level necessary for reliable communications. This lessens the chance of causing unnecessary interference to nearby systems.

4.2 Troubleshooting

All units must meet the basic requirements listed below for proper operation. Check these items first when troubleshooting a system problem:

- Adequate and stable primary power
- Secure cable connections (RF, data, and power)
- A clear transmission path between Master and each Remote
- An efficient and properly aligned antenna system providing adequate received signal strength.
- Proper programming of the transceiver’s parameters
- The correct interface between the transceiver and the connected data equipment (correct cable wiring, proper data format, timing, etc.)

4.2.1 LED Status Indicators

The PWR LED typically provides the quickest field indication of a system problem. If the PWR LED is flashing Red, then an alarm condition is present. (Additional details on LED status are available in Section 2.3 TransNEXT Connectors and Indicators on page 20).

The “show alarms” command will indicate current active alarm conditions. An example is show below:

```
>show alarms
Current Alarms:
0.) No ADDR programmed
13.) No Sync
```

Alternatively, via the web UI click on the alarm icon on the far right of the status banner. A pop-up window will indicate current alarms.

4.2.2 Event Log

Event logs provide a history of alarm status and can help indicate if a recent change caused a problem. See section 3.4.4 Event Logging for more information.

4.2.3 Setup Mode

Setup mode can be useful for troubleshooting radio issues in bench top settings. Entering the command "**setup**" temporarily takes the TransNEXT out of normal hopping mode and allows for direct test of transmit and receive functions. Setup mode is confirmed when the command prompt changes from ">" to "**SETUP>**".

In Setup mode, the transmit and receive frequencies are set by the "**chan**" (channel) command. Channel 0 corresponds to 902.2MHz and channel 128 corresponds to 927.6MHz. To key on channel type "key" for a continuous signal or "burst" for a burst operation. Use "dkey" to key down. To check RSSI use the "**rssi**" command for continuous sampling (until <CR> is entered); alternatively use "rssi!" for a 1-shot sample that returns to the "SETUP>" prompt.

Note that the transmission functions of setup mode are not intended for field use. Setup mode can be terminated at any time by typing "**quit**" at the "**SETUP>"** prompt. Duration of Setup mode is timed and will expire after 10 minutes as a protection to keep a unit from accidentally being left in this state.

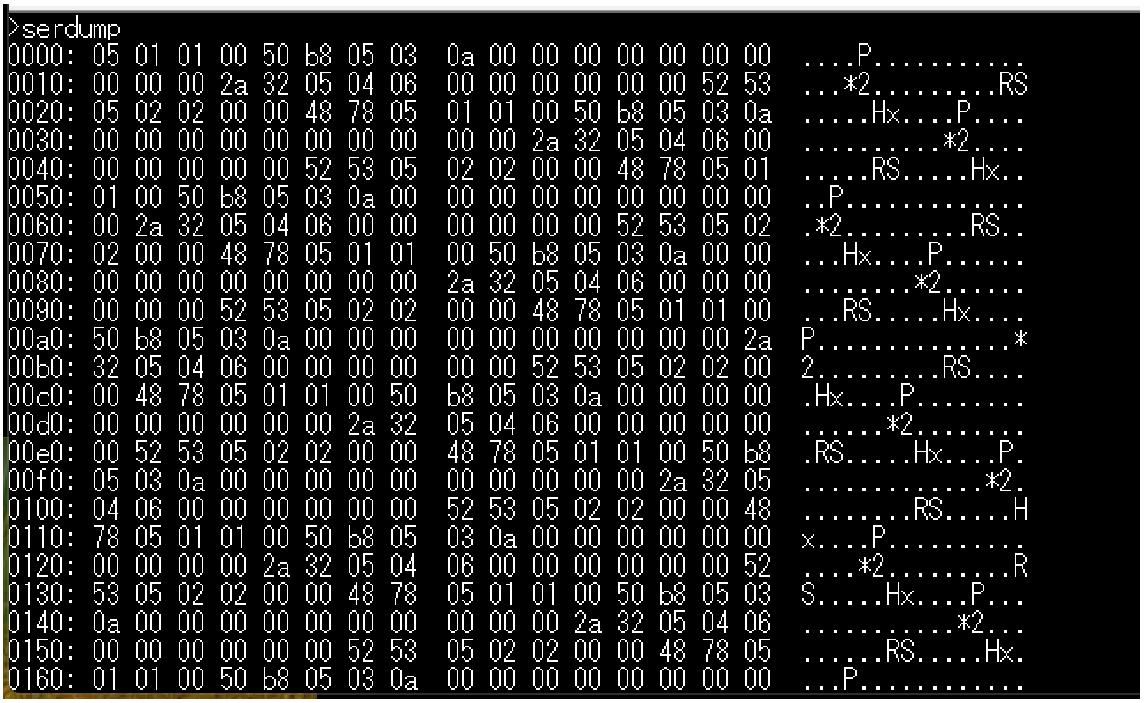
4.2.4 Serial and Ethernet Traffic Sniffers

TransNEXT has built-in traffic monitoring tools that are useful for analyzing serial and ethernet traffic. These tools function as primitive protocol analyzers to view data coming into and out of the radio, facilitating the diagnosis of network issues.

`serdump` is for serial traffic analysis; **`netdump`** is for ethernet.

4.2.4.1 serdump

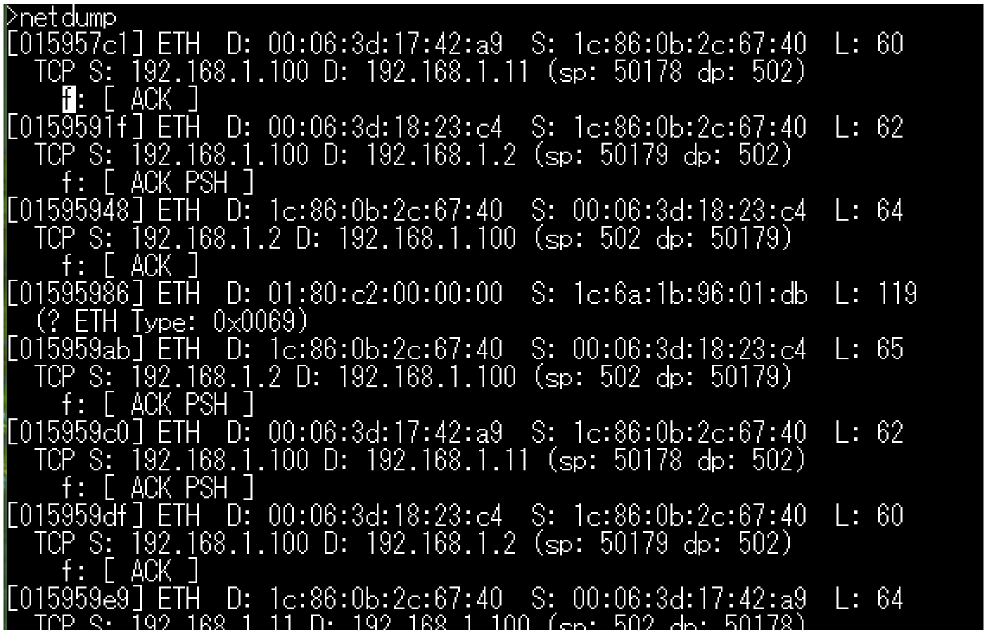
The **`serdump`** command shows both incoming data to be transmitted over-the-air (TXD) and received over-the-air data that has been delivered (RXD). The data is also available on the Payload Viewer of the dashboard page The example below shows an extract of a Modbus polling session.



```
>serdump
0000: 05 01 01 00 50 b8 05 03  0a 00 00 00 00 00 00 00  ....P...........
0010: 00 00 00 2a 32 05 04 06  00 00 00 00 00 00 52 53  ...*2.........RS
0020: 05 02 02 00 00 48 78 05  01 01 00 50 b8 05 03 0a  .....Hx....P....
0030: 00 00 00 00 00 00 00 00  00 00 2a 32 05 04 06 00  ..........*2....
0040: 00 00 00 00 00 52 53 05  02 02 00 00 48 78 05 01  .....RS.....Hx..
0050: 01 00 50 b8 05 03 0a 00  00 00 00 00 00 00 00 00  ..P.............
0060: 00 2a 32 05 04 06 00 00  00 00 00 00 52 53 05 02  .*2.........RS..
0070: 02 00 00 48 78 05 01 01  00 50 b8 05 03 0a 00 00  ...Hx....P......
0080: 00 00 00 00 00 00 00 00  2a 32 05 04 06 00 00 00  ........*2......
0090: 00 00 00 52 53 05 02 02  00 00 48 78 05 01 01 00  ...RS.....Hx....
00a0: 50 b8 05 03 0a 00 00 00  00 00 00 00 00 00 00 2a  P..............*
00b0: 32 05 04 06 00 00 00 00  00 00 52 53 05 02 02 00  2.........RS....
00c0: 00 48 78 05 01 01 00 50  b8 05 03 0a 00 00 00 00  .Hx....P........
00d0: 00 00 00 00 00 00 2a 32  05 04 06 00 00 00 00 00  ......*2........
00e0: 00 52 53 05 02 02 00 00  48 78 05 01 01 00 50 b8  .RS.....Hx....P.
00f0: 05 03 0a 00 00 00 00 00  00 00 00 00 00 2a 32 05  .............*2.
0100: 04 06 00 00 00 00 00 00  52 53 05 02 02 00 00 48  ........RS.....H
0110: 78 05 01 01 00 50 b8 05  03 0a 00 00 00 00 00 00  x....P..........
0120: 00 00 00 00 2a 32 05 04  06 00 00 00 00 00 00 52  ....*2.........R
0130: 53 05 02 02 00 00 48 78  05 01 01 00 50 b8 05 03  S.....Hx....P...
0140: 0a 00 00 00 00 00 00 00  00 00 00 2a 32 05 04 06  ...........*2...
0150: 00 00 00 00 00 00 52 53  05 02 02 00 00 48 78 05  ......RS.....Hx.
0160: 01 01 00 50 b8 05 03 0a  00 00 00 00 00 00 00 00  ...P............
```

4.2.4.2 *netdump*

The **netdump** command displays ethernet traffic. Specifying **netdump bridge** shows only the traffic that is sent or received over the air.



```
>netdump
[015957c1] ETH  D: 00:06:3d:17:42:a9  S: 1c:86:0b:2c:67:40  L: 60
  TCP S: 192.168.1.100 D: 192.168.1.11 (sp: 50178 dp: 502)
    f: [ ACK ]
[0159591f] ETH  D: 00:06:3d:18:23:c4  S: 1c:86:0b:2c:67:40  L: 62
  TCP S: 192.168.1.100 D: 192.168.1.2 (sp: 50179 dp: 502)
    f: [ ACK PSH ]
[01595948] ETH  D: 1c:86:0b:2c:67:40  S: 00:06:3d:18:23:c4  L: 64
  TCP S: 192.168.1.2 D: 192.168.1.100 (sp: 502 dp: 50179)
    f: [ ACK ]
[01595986] ETH  D: 01:80:c2:00:00:00  S: 1c:6a:1b:96:01:db  L: 119
  (? ETH Type: 0x0069)
[015959ab] ETH  D: 1c:86:0b:2c:67:40  S: 00:06:3d:18:23:c4  L: 65
  TCP S: 192.168.1.2 D: 192.168.1.100 (sp: 502 dp: 50179)
    f: [ ACK PSH ]
[015959c0] ETH  D: 00:06:3d:17:42:a9  S: 1c:86:0b:2c:67:40  L: 62
  TCP S: 192.168.1.100 D: 192.168.1.11 (sp: 50178 dp: 502)
    f: [ ACK PSH ]
[015959df] ETH  D: 00:06:3d:18:23:c4  S: 1c:86:0b:2c:67:40  L: 60
  TCP S: 192.168.1.100 D: 192.168.1.2 (sp: 50179 dp: 502)
    f: [ ACK ]
[015959e9] ETH  D: 1c:86:0b:2c:67:40  S: 00:06:3d:17:42:a9  L: 64
  TCP S: 192.168.1.11 D: 192.168.1.100 (sp: 502 dp: 50178)
```

4.3 Technical Specifications

GENERAL

Input Power

6 to 36 VDC, 1.0 Amp max. 6.0 Watts maximum (NET9L / NET9B)
6 to 36 VDC, 1.6 Amp max. 9.6 Watts maximum (NET9S)

Below are power consumption estimates:

Table 4-1. TransNEXT Power Consumption:

Mode	**NET9L** **NET9B**	**NET9S**
Transmit	6.0 W	9.6 W
Receive	760 mw	970 mw
Sleep *(@13.8v)*	40 mw	40 mw

Ethernet Port

RJ-45 10/100 Mbps Auto-MDIX

Serial Port

RJ-45, supporting RS-232/RS-485

LAN Protocols

802.3 (Ethernet), TCP/IP, ICMP, ssh, http/https

Networking

N/A

Configuration

Serial console, SSH, HTTP/HTTPS

Security

Secure Boot, Signed Firmware, Roll-based Access Control

Physical

Size

5.3” long (13.46 cm), 3.8" wide (9.65 cm), 1.6" high (4.06 cm)

Housing

Die-cast Aluminum

Weight

1.20 lbs. (0.54kg). without mounting hardware (NET9L)
1.25 lbs. (0.57kg). without mounting hardware (NET9B, with display)

Environmental

Operating Temperature Range

-40°C to +70°C

NOTE Operating temperature range may be reduced based on model configuration. See product label for detail.

Caution: This device may exceed safe handling temperatures when operated in an ambient temperature above 55°.

Agency/Regulatory Approvals

FCC	NET9B – E5MDS-NET9L NET9L – E5MDS-NET9L NET9S – E5MDS-NET9S
IC - Industry	NET9B – 101D-NET9L NET9L – 101D-NET9L NET9S – 101D-NET9S

900 MHz ISM - Unlicensed

Frequency Range	902 to 928 MHz
Power Output	10 dBm to 30 dBm in 1.0 dBm steps (DEFAULT = 30 dBm)
Output Impedance	50 Ohms
Permissible Antennas	Various options depending on local regulatory, including: MDS 93-/97-3194A14, 10dBd (12.15dBi) YAGI Antenna MDS 93-/97-3194A23, 7dBd (9.15dBi) 5/8 wavelength OMNI MDS 93-/97-1864A27, OMNI, 890-960 MHz, 9 dBd Gain, N female connector. Includes integral dual purpose pipe mount.
Antenna Connector	TNC female
Number of Frequency Channels	Selectable 64 to 128
Channel Separation	200.0 kHz minimum
Modulation Type	2-Level FSK
Data Rates	106kbps (uncompressed OTA)
20db Bandwidth per 15.247	128kHz
Dwell Time	7 or 28 ms (default = 7)

NOTE All specifications are subject to change without notice or obligation.

5.0 Glossary of Terms and Abbreviations

If you are new to wireless communications systems, some of the terms used in this guide may be unfamiliar. The following glossary explains many of these terms and will prove helpful in understanding the operation of the unit. While some of these terms may not appear in the text, they are included here to promote a more complete understanding of wireless technology.

Access Point (AP): An access point is a device that bridges data from remotes in the wireless network to a wired backhaul. In TransNEXT a “Master” radio acts as the access point.

Ageout: Time before de-authentication (aging out) when there is no traffic between endpoints.

Authentication: Refers to the process where devices verify each other’s identity prior to passing data. It prevents unauthorized parties from snooping or impersonating an authorized device.

Antenna System Gain: A figure, normally expressed in dB, representing the power increase resulting from the use of a gain-type antenna. System losses (from the feedline and coaxial connectors, for example) are subtracted from this figure to calculate the total antenna system gain.

Bit: The smallest unit of digital data, often represented by a one or a zero. Eight bits (plus start, stop, and parity bits) usually comprise a byte.

Bits-per-second: See *BPS*.

BPS (Bits-per-second): A measure of the information transfer rate of digital data across a communication channel.

Bridging: (see Ethernet Bridging)

Byte: A string of digital data usually made up of eight data bits and start, stop and parity bits.

CLI: Command Line Interface. A method of user control where commands are entered as character strings to set configuration and operating parameters.

Compression: Refers to payload data compression**.** LZ and other formats compress data so that it can be transferred in a shorter timeframe.

CTS: Clear to Send

Decibel (dB): A measure computed from the ratio between two signal levels. Frequently used to express the gain (or loss) of a system.

Data Circuit-terminating Equipment: See *DCE*.

Data Communications Equipment: See *DCE*.

Data Terminal Equipment: See *DTE*.

dBi: Decibels referenced to an “ideal” isotropic radiator in free space, frequently used to express antenna gain.

dBd: Decibels referenced to a dipole antenna, used to express antenna gain.

dBm: Decibels referenced to one milliwatt. An absolute unit used to measure signal power, as in transmitter power output, or received signal strength.

DCE (Data Circuit-terminating Equipment) (or Data Communications Equipment): In data communications terminology, this is the “modem” side of a computer-to-modem connection. The unit described in this manual is hardwired as a DCE device.

DLINK: MDS Proprietary diagnostic link protocol

DTE (Data Terminal Equipment): A device that provides data in the form of digital signals at its output. DTE connects to the DCE device.

ETH: Ethernet

Ethernet Bridging: Layer 2 bridging creates transparent data transmission between multiple network segments, making them appear as a single network for seamless communication.

Fade Margin: The greatest tolerable reduction in average received signal strength that will be anticipated under most conditions. It provides an allowance for reduced signal strength due to multipath, slight antenna movement or changing atmospheric losses. A fade margin of 10 dB is usually sufficient in most ISM systems.

FHSS: Frequency Hopping Spread Spectrum radio.

Hardware Flow Control: A feature used to prevent data buffer overruns when the unit is handling high-speed data from an RTU or PLC. When the buffer approaches overflow, the unit drops the clear-to-send (CTS) line, which instructs the RTU or PLC to delay further transmission until CTS again returns to the high state.

Host Computer: The computer installed at the master unit, which controls the collection of data from one or more remote sites.

HTTP: Abbreviation for Hypertext Transfer Protocol.

HTTPS: Abbreviation for Hypertext Transfer Protocol Secure

IP: Internet Protocol

IP/Payload: An MDS product feature that acts like a terminal server with a *virtual* serial port, where the serial data is routed internally as over-the-air streaming traffic.

ISM: Abbreviation for “Industrial, Scientific, Medical” band. The 900MHz ISM band is where TransNEXT operates.

LAN: Local Area Network

LED: Light Emitting Diode

LPM: Low Power Mode. An available feature of the unit whereby data is buffered at the master and sent to remotes only at designated “wake-up” times.

mA: Milliamperes

MAC (Media Access Control) Address: A unique identifier assigned to a NIC for use in network communications.

Master Radio: A TransNEXT radio configured as a master. A master radio (sometimes referred to as an AP or Access point) provides the synchronization signal for remotes to connect and establish a network.

NIC: Abbreviation for Network Interface Controller

P2P: Peer to peer – When remote devices are allowed to address each other as well as the master unit.

Poll: A request for data issued from the host computer (or master PLC) to a Remote unit.

PLC (Programmable Logic Controller): A dedicated microprocessor configured for a specific application with discrete inputs and outputs. It can serve as a host or as an RTU.

PPM: Parts per Million

PSK: Abbreviation for Pre-Shared Key.

Programmable Logic Controller: See *PLC.*

Remote Radio: A TransNEXT radio configured as a remote. Remotes typically monitor field assets and must synchronize to a master radio in order to be able to communicate.

Remote Terminal Unit: See *RTU.*

RTS: Request-to-send

RTU: Remote Terminal Unit. A data collection device installed at a Remote unit site.

RX: Abbreviation for “Receive.”

SAF (Store and Forward): An available feature of the unit whereby data is stored by a designated Remote and then retransmitted to a station beyond the communication range of the Master.

SCADA (Supervisory Control And Data Acquisition): An overall term for the functions commonly provided through a multiple address radio system.

Signal-to-Noise Ratio: *See SNR.*

Sleep: A term for lower power consumption. TransNEXT supports sleep via Low Power Mode (LPM) and via a Sleep Line input control.

SNR (Signal-to-Noise ratio): A measure of how well the signal is being received at a radio relative to noise on the channel.

SSH: Secure Shell protocol for a network that allows users to open a window on a local PC and connect to a remote PC as if they were present at the remote.

Supervisory Control And Data Acquisition: See *SCADA.*

Terminal Server: A facility that provides IP network access to serial ports.

TTL (Time to Live): This is the amount of time data is considered valid before it is discarded.

TX: Abbreviation for “Transmit.”

Unlicensed: Typically referring to unlicensed operation, whereby end users do not need to apply for license prior to installing or using certain classes of radios. TransNEXT is a FHSS radio designed for use in the unlicensed 900MHz ISM band.

YMODEM: This is a simple file transfer protocol originally introduced in 1985. TransNEXT uses YMODEM to support uploads of MPK firmware.

6.0 APPENDIX A –Electronic Ink Display

6.1 Introduction

Select TransNEXT models are equipped with an Electronic Ink display.

Electronic Ink is lower power technology ideally suited for low power applications. It uses reflected light from the environment and provides a persistent display of the last image written even after power is removed.

NOTE Even though the display will hold a persistent image indefinitely, the TransNEXT software will periodically update the data. When an update cycle occurs, the display will flash momentarily as the screen is fully erased and a new set of data is written. This is normal operation.

The TransNEXT display provides three key functions organized into three screens: a status page, a spectrum analyzer, and an antenna alignment tool. Based on which screen is active the TransNEXT will use a different data update cycle. After a time-out period the screen will return to the home screen.

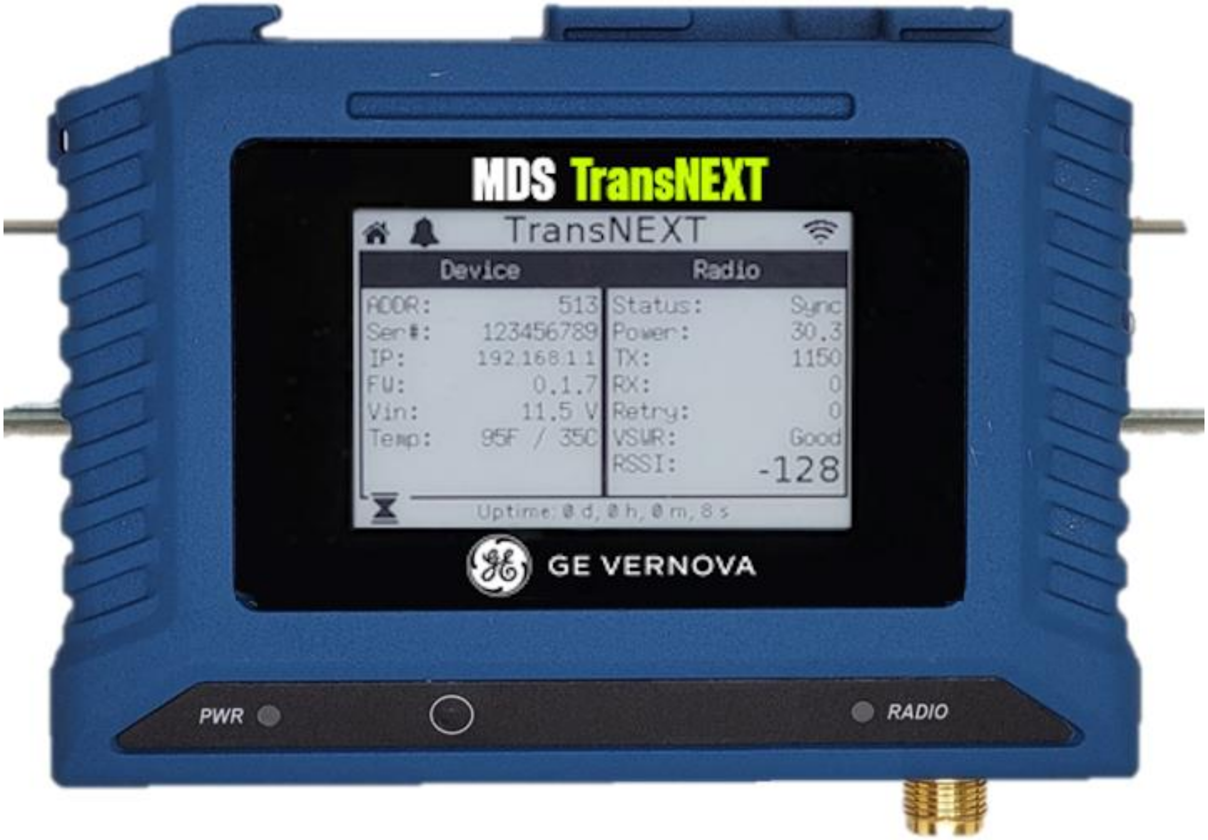
Pressing the white circular button on the LED panel allows the user to control behavior.

- Pressing the button once forces a screen update.
- Pressing twice causes an advance to the next screen.
- Pressing three times sets the current page as the new default.

NOTE Pressing and holding the button for greater than 15 seconds, followed but a release, will force a **cfg restore** operation. This will restore settings to the last **cfg snapshot** *and* reset the device admin password to its original value.

6.2 Status Page

The status page is the default home screen. It includes the owner message, uptime, device data, and radio data. The data refresh rate defaults to 2 minutes. An example is shown below:



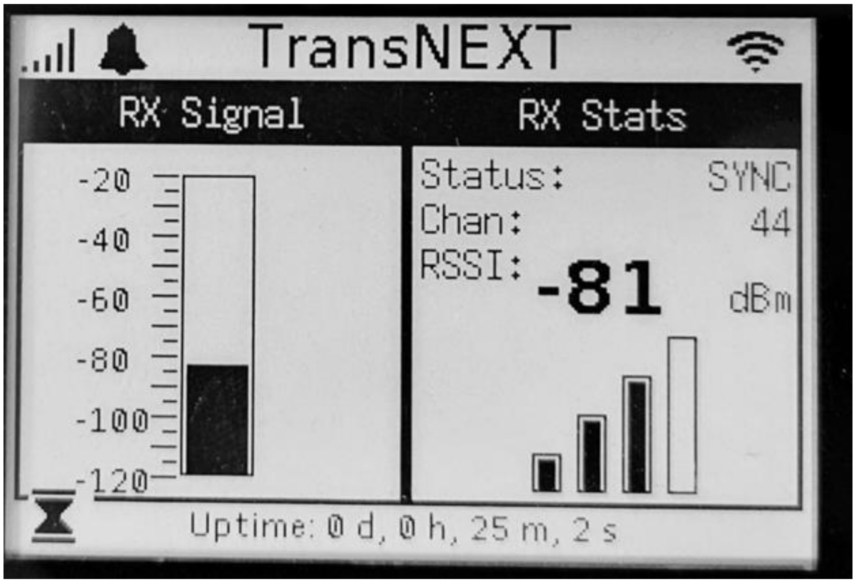
TransNEXT

Device		Radio	
ADDR:	513	Status:	Sync
Ser#:	123456789	Power:	30.3
IP:	192.168.1.1	TX:	1150
FW:	0.1.7	RX:	0
Vin:	11.5 V	Retry:	0
Temp:	95F / 35C	VSWR:	Good
		RSSI:	-128

Uptime: 0 d, 0 h, 0 m, 8 s

6.3 Antenna Alignment Page

The antenna alignment page uses a 10-sec refresh to see the effects of different antenna positions. This is intended as a simple tool to assist in initial installation.



TransNEXT

RX Signal

RX Stats

Status: SYNC

Chan: 44

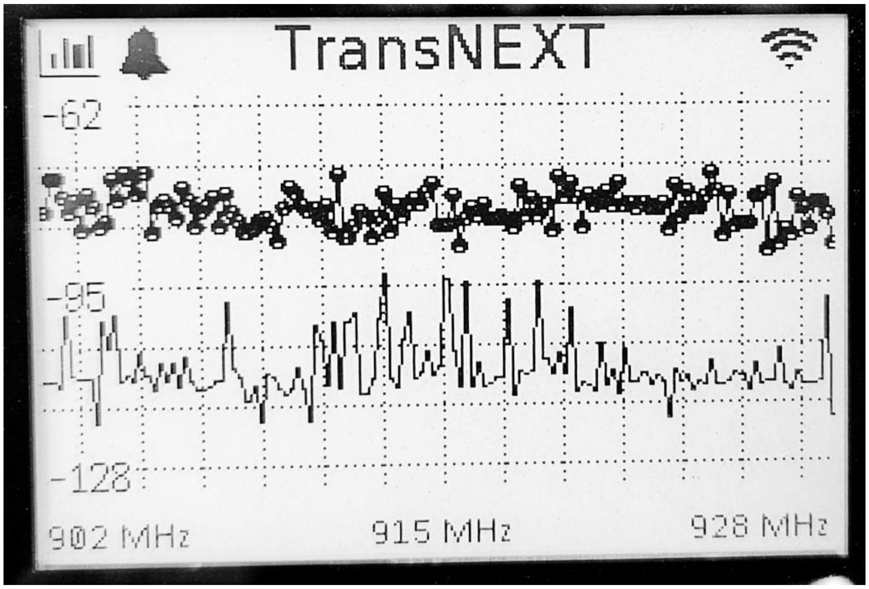
RSSI: -81 dBm

Uptime: 0 d, 0 h, 25 m, 2 s

6.4 Spectrum Analyzer Page

The page is intended to assist in initial installation and in field maintenance. The analyzer will plot data over the operating range (902-928MHz) providing a simple overview of the spectral environment in which the device is operating.

The upper line provides a sample of the system based on received TransNEXT and TransNET messages. The lower line provides a sample of the system based on times when the channel is not in use. The lower line represents the noise floor of the environment in which the TransNEXT is operating.



NOTE The Spectrum Analyzer Page is intended as a simple tool to detect easily identified blockers in the FHSS band. It is based on a simple collection of signal strength and only operates over the bands in which the radio operates. For advanced troubleshooting use of RF test equipment is still recommended.

MDS TransNEXT

7.0 APPENDIX B – Operating Frequencies

The TransNEXT is a Frequency-Hopping Spread Spectrum (FHSS) radio that can be configured to operate in a subset of all available frequencies in the 902-928MHz range.

TransNEXT divides the available frequencies into a set of 8 configurable zones with 16 discrete, 200KHz bandwidth channels per zone. The table below illustrates the 900MHz frequency ranges that apply to each zone. The “skip” parameter under radio settings defined which zones to skip. By default, no zones are skipped which provides a total of 128 different channels in the hop pattern.

NOTE The module may be configured by the factory to limit the number of skipped zones or disallow operation in specific frequency ranges (zones) in order to meet country specific regulatory requirements. These settings can NOT be changed or modified by the user.

ZONE 1	ZONE 2	ZONE 3	ZONE 4	ZONE 5	ZONE 6	ZONE 7	ZONE 8
902.2	905.4	908.6	911.8	915.0	918.2	921.4	924.6
to	to	to	to	to	to	to	to
905.2	908.4	911.6	914.8	918.0	921.2	924.4	927.6

8.0 APPENDIX C– Licenses

8.1 Open Source License Declaration

The MDS TransNEXT product includes Open Source Software. Usage is governed by the corresponding licenses which are listed on the GE Vernova website, as "TransNEXT License Declaration". The current file can be found under the “Resources” page for "TransNEXT - Software" as listed here:

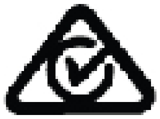
https://www.gevernova.com/grid-solutions/resources?prod=TransNEXT&type=7&node_id=4693

Upon request, in accordance with certain software license terms, GE Vernova MDS LLC will make available a copy of Open Source code contained in this product. This code is provided to you on an “as is” basis, and GE Vernova makes no representations or warranties for the use of this code by you independent of any GE Vernova provided software or services. For more information, contact Grid Automation Technical Support for your region (Page 1).

9.0 APPENDIX D – Country Specific Information

The table below identifies any country-specific installation requirements or warning required by the country for the TransNEXT. Operation of the unit must be in full compliance with all country and regional requirements.

Table 9-1. Country-Specific Installation Data

Country	Applicable Symbol(s)	Installation/Operating Requirements
Australia		For professional use only, not for sale to the general public. Hot surface—this product is only suitable for installation restricted access locations.
Brazil	ANATEL Agência Nacional de Telecomunicações	Certificate No: 01464-16-00450
Mexico		Certificate No.: NYC-2302CT1755

10.0 APPENDIX E – Alarm Codes

The TransNEXT has a facility to report alarm conditions and assert an external alarm signal based on configuration settings.

Alarm Codes include the following:

Table 18. Alarm Codes

Alarm Code	Alarm Type	Description
00	Major	The network address is not programmed. radio.addr = 0
01	Major	Improper firmware detected for this radio model.
08	Major	The system is reporting that it has not been calibrated. Factory calibration is required for proper radio operation.
11	Major	Not Authenticated. Radio failed to authenticate (applicable only in Bridge mode)
12	Major	Receiver time-out alarm
13	Major	Not Synchronized
14	Major	Bad VSWR detected (>=5.0)
15	Major	Input Voltage out-of-range (6-36v)
16	Minor	The unit address is not programmed.
29	*Minor*	*RF output power fault detected. (Power differs by more than 2 dB from set level.) Often caused by high antenna system SWR. Check antenna, feedline, and connectors. (future)*
30	*Minor*	*The system is reporting an RSSI reading below –105 dBm. (future)*
31	Minor	The transceiver's internal temperature is approaching an out-of-tolerance condition. If the temperature drifts outside of the recommended operating range the transceiver may fail.

11.0 APPENDIX F – Feature Interoperability Matrix

Availability of TransNEXT features varies based on mode selection. See the table below for a summary of applicable features in different modes. Note that table contains the most common items but may not be exhaustive for all features.

Table 11-1. Feature Interoperability

	system.mode = "TransNEXT"	system.mode = "Bridge"	system.mode = "MBits"
Web UI and CLI management with secure login	✓	✓	✓
TransNET interoperability	✓	xxx	xxx
Store and Forward	✓	xxx	xxx
Sleep and LPM mode	✓	xxx	xxx
Collocated Master support	✓	xxx	xxx
Serial Polling	✓	✓	xxx
Mirrored Bits™ compatible	xxx	xxx	✓
Ethernet Over-the-Air	xxx	✓	xxx
Authentication and Encryption	xxx	✓	xxx
Ethernet Payload Compression	xxx	✓	xxx
Serial report by exception	xxx	✓	xxx
IP/Payload	✓	✓	✓ (not recommended)
Terminal Server	xxx	✓	xxx
RS-232 / RS-485	✓	✓	✓
RTS/CTS controls	✓	✓	✓
RX timeout monitor	✓	✓	✓
Over-the-air reprogramming	✓	✓	xxx
System ID	✓	✓	✓
DLINK management	✓	✓	xxx
Seamless mode radio.buff	✓	✓ (automatic)	xxx
Selectable radio attribute control for retry / repeat / fec	✓	✓	xxx

NOTES

IN CASE OF DIFFICULTY...

Our products are designed for long life and trouble-free operation. However, this equipment, as with all electronic equipment, may have an occasional component failure. The following information will assist you in the event that servicing becomes necessary.

TECHNICAL ASSISTANCE

Technical assistance for MDS products is available from the GE Vernova Grid Automation Support team. Please provide the complete model number of the product, along with a description of the trouble/symptom(s) that you are experiencing. In many cases, problems can be resolved without the need for returning the unit to the factory.

For product support, please contact the GE Vernova support team as follows:

Region	E-mail	Telephone
Global Contact Centre	GA.support@GE.com	+44 1785 250070
Central, East Asia, Pacific	GA.supportCEAP@GE.com	+65 6749 0777
India	GA.supportIND@GE.com	+91 44 2264 8000
Middle East, North Africa, Turkey	GA.supportMENAT@GE.com	+971 429 9666
Europe, Russia, CIS, Sub-Saharan Africa	GA.supportERCIS@GE.com	+34 94 485 8854
North America	GA.supportNAM@GE.com	+1 877 605 6777
Latin America	GA.supportLAM@GE.com	+55 48 2108 0300

REPAIR SERVICE

Component level repair of this equipment is not recommended in the field. Many components are installed using surface mount technology, which requires specialized training and equipment for proper servicing. For this reason, the equipment should be returned to the factory for any PC board repairs. The factory is best equipped to diagnose, repair and align your unit to its proper operating specifications.

If return of the equipment is necessary, you must obtain a return authorization number before shipment. This number helps expedite the repair so that the equipment can be returned to you as quickly as possible. Please be sure to include the number on the outside of the shipping box, and on any correspondence relating to the repair. No equipment will be accepted for repair without an authorization number.

Contact Technical Support in your region to obtain an authorization number:

The radio must be properly packed for return to the factory. The original shipping container and packaging materials should be used whenever possible. All factory returns should be addressed to:

GE Vernova MDS LLC
Product Services Department
(Auth. No. XXXX)
175 Science Parkway
Rochester, NY 14620 USA

When repairs have been completed, the equipment will be returned to you by the same shipping method used to send it to the factory. Please specify if you wish to make different shipping arrangements.

REPLACEMENT PARTS

Many spare and replacement items are available for purchase by contacting your factory sales representative, or by visiting our online store at https://store.gegridsolutions.com .

GE VERNOVA