PROFESSIONAL DIGITAL TWO-WAY RADIO SYSTEM

MOTOTRBO™ CONNECT PLUS INTERCONNECT GATEWAY

XRI INTERCONNECT GATEWAY USER GUIDE

Declaration of Conformity

This declaration is applicable to your radio only if your radio is labeled with the FCC logo shown below.

Declaration of Conformity

Responsible Party

Name: Motorola Solutions, Inc.

Address: 1303 East Algonquin Road, Schaumburg, IL 60196-1078, U.S.A.

Phone Number: 1-800-927-2744

Hereby declares that the product:

Model Name: **XRI 9100**

conforms to the following regulations:

FCC Part 15, subpart A

Class B Digital Device

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference in a residential area, the user is required to correct the interference at his own expense.

NOTICE: The user is cautioned that changes or modifications not expressly approved by Motorola could result in the equipment being noncompliant with FCC Class A requirements and void the user's authority to operate the equipment.

This page intentionally left blank.

Contents

Commercial Warranty

Limited Warranty

MOTOROLA COMMUNICATION PRODUCTS

What This Warranty Covers and For How Long

MOTOROLA SOLUTIONS INC. (“MOTOROLA”) warrants the MOTOROLA manufactured Communication Products listed below (“Product”) against defects in material and workmanship under normal use and service for a period of time from the date of purchase as scheduled below:

XRI 9100 Interconnect Gateway	Two (2) Years

Motorola, at its option, will at no charge either repair the Product (with new or reconditioned parts), replace it (with a new or reconditioned Product), or refund the purchase price of the Product during the warranty period provided it is returned in accordance with the terms of this warranty. Replaced parts or boards are warranted for the balance of the original applicable warranty period. All replaced parts of Product shall become the property of MOTOROLA.

This express limited warranty is extended by MOTOROLA to the original end user purchaser only and is not assignable or transferable to any other party. This is the complete warranty for the Product manufactured by MOTOROLA. MOTOROLA assumes no obligations or liability for additions or modifications to this warranty unless made in writing and signed by an officer of MOTOROLA. Unless made in a separate agreement between MOTOROLA and the original end user purchaser, MOTOROLA does not warrant the installation, maintenance or service of the Product.

MOTOROLA cannot be responsible in any way for any ancillary equipment not furnished by MOTOROLA which is attached to or used in connection with the Product, or for operation of the Product with any ancillary equipment, and all such equipment is expressly excluded from this warranty. Because each system which may use the Product is unique, MOTOROLA disclaims liability for range, coverage, or operation of the system as a whole under this warranty.

General Provisions

This warranty sets forth the full extent of responsibilities of Motorola regarding the Product. Repair, replacement or refund of the purchase price, at the option of Motorola, is the exclusive remedy. THIS WARRANTY IS GIVEN IN LIEU OF ALL OTHER EXPRESS WARRANTIES. IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE LIMITED TO THE DURATION OF THIS LIMITED WARRANTY. IN NO EVENT SHALL MOTOROLA BE LIABLE FOR DAMAGES IN EXCESS OF THE PURCHASE PRICE OF THE PRODUCT, FOR ANY LOSS OF USE, LOSS OF TIME, INCONVENIENCE, COMMERCIAL LOSS, LOST PROFITS OR SAVINGS OR OTHER INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE SUCH PRODUCT, TO THE FULL EXTENT SUCH MAY BE DISCLAIMED BY LAW.

State Law Rights

SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATION OR EXCLUSIONS MAY NOT APPLY.

This warranty gives specific legal rights, and there may be other rights which may vary from state to state.

How to Get Warranty Service

You must provide proof of purchase (bearing the date of purchase and Product item serial number) in order to receive warranty service and, also, deliver or send the Product item, transportation and insurance prepaid, to an authorized warranty service location. Warranty service will be provided by Motorola through one of its authorized warranty service locations. If you first contact the company which sold you the Product, it can facilitate your obtaining warranty service. You can also call Motorola at 1-888-567-7347 US/Canada.

What This Warranty Does Not Cover

1. Defects or damage resulting from use of the Product in other than its normal and customary manner.
2. Defects or damage from misuse, accident, water, or neglect.
3. Defects or damage from improper testing, operation, maintenance, installation, alteration, modification, or adjustment.
4. Breakage or damage to antennas unless caused directly by defects in material workmanship.
5. A Product subjected to unauthorized Product modifications, disassemblies or repairs (including, without limitation, the addition to the Product of non-Motorola supplied equipment) which adversely affect performance of the Product or interfere with Motorola's normal warranty inspection and testing of the Product to verify any warranty claim.
6. Product which has had the serial number removed or made illegible.
7. Rechargeable batteries if:
   - any of the seals on the battery enclosure of cells are broken or show evidence of tampering.
   - the damage or defect is caused by charging or using the battery in equipment or service other than the Product for which it is specified.
8. Freight costs to the repair depot.
9. Product, does not function in accordance with MOTOROLA’s published specifications or the FCC type acceptance labeling in effect for the Product at the time the Product was initially distributed from MOTOROLA.
10. Scratches or other cosmetic damage to Product surfaces that does not affect the operation of the Product.
11. Normal and customary wear and tear.

Patent and Software Provisions

MOTOROLA will defend, at its own expense, any suit brought against the end user purchaser to the extent that it is based on a claim that the Product or parts infringe a United States patent, and MOTOROLA will pay those costs and damages finally awarded against the end user purchaser in any such suit which are attributable to any such claim, but such defense and payments are conditioned on the following:

1. that MOTOROLA will be notified promptly in writing by such purchaser of any notice of such claim;
2. that MOTOROLA will have sole control of the defense of such suit and all negotiations for its settlement or compromise; and
3. should the Product or parts become, or in MOTOROLA's opinion be likely to become, the subject of a claim of infringement of a United States patent, that such purchaser will permit MOTOROLA, at its

option and expense, either to procure for such purchaser the right to continue using the Product or parts or to replace or modify the same so that it becomes noninfringing or to grant such purchaser a credit for the Product or parts as depreciated and accept its return. The depreciation will be an equal amount per year over the lifetime of the Product or parts as established by MOTOROLA.

MOTOROLA will have no liability with respect to any claim of patent infringement which is based upon the combination of the Product or parts furnished hereunder with software, apparatus or devices not furnished by MOTOROLA, nor will MOTOROLA have any liability for the use of ancillary equipment or software not furnished by MOTOROLA which is attached to or used in connection with the Product. The foregoing states the entire liability of MOTOROLA with respect to infringement of patents by the Product or any parts thereof.

Laws in the United States and other countries preserve for MOTOROLA certain exclusive rights for copyrighted MOTOROLA software such as the exclusive rights to reproduce in copies and distribute copies of such Motorola software. MOTOROLA software may be used in only the Product in which the software was originally embodied and such software in such Product may not be replaced, copied, distributed, modified in any way, or used to produce any derivative thereof. No other use including, without limitation, alteration, modification, reproduction, distribution, or reverse engineering of such MOTOROLA software or exercise of rights in such MOTOROLA software is permitted. No license is granted by implication, estoppel or otherwise under MOTOROLA patent rights or copyrights.

Governing Law

This Warranty is governed by the laws of the State of Illinois, USA.

This page intentionally left blank.

Computer Software Copyrights

Open Source Software Legal Notices

This Motorola Product contains Open Source Software. For information regarding licenses, acknowledgements, required copyright notices, and other usage terms, refer to the Documentation for this Motorola Product at:

https://businessonline.motorolasolutions.com/

Go to:

Motorola Online>Resource Center>Product Information>Manuals>MOTOTRBO>Connect Plus

This page intentionally left blank.

Chapter 1

Introduction

Thank you for choosing the XRI 9100 Interconnect Gateway, the centralized telephone interconnect equipment in MOTOTRBO™ Connect Plus digital trunking solutions. The XRI is a powerful multiprocessor computer designed to provide SIP-based telephone interconnection and real-time resource management. It is designed as an Ethernet Internet Protocol (IP) device that can be configured for MOTOTRBO Connect Plus single site or multisite trunking operation.

The main features supported by the MOTOTRBO Connect Plus Telephone Interconnect include:

The XRI will connect to up to four Cisco SPA8800 SIP Gateways which in turn connect to the PSTN via standard RJ-11 phone cables. Each SPA8800 can connect to four telephone lines. Alternatively, the XRI can connect to one Cisco Unified Call Manager (CUCM) when the XRI is enabled with the Connect Plus SIP Telephony feature license. When connected to the CUCM, the number of simultaneous phone calls supported by the XRI is determined by the feature license (up to a maximum of 20). The flexibility of the XRI allows it to be located anywhere in the Connect Plus IP network where it can reach both the SIP Gateway and the XRC. The SIP Gateways must be purchased separately, either through Motorola or another supplier.

- Inbound group and Inbound/Outbound private telephone calls
- Disable/enable phone feature privilege per Radio ID & Talkgroup ID
- Configurable call timers
- Manual Dial
- Over Dial, Buffer Dial, and Live Dial
- Manual or VOX keying options
- Custom Voice Announcements
- PIN access
- Event and Call logs

NOTICE: Refer to the MOTOTRBO Connect Plus System Planner for more details on system configurations and trunking features.

This page intentionally left blank.

Chapter 2

Safety Information

For your protection, this product has been tested to various national and international regulations and standards. The scope of this regulatory testing includes electrical and mechanical safety, radio frequency interference, acoustics, and known hazardous materials. Where applicable, approvals obtained from the third-party test agencies are shown on the product label.

2.1 Grounding

This is a safety class I product and has protective grounding terminals. There must be an uninterruptible safety earth ground from the main power source to the product's input wiring terminals, power cord, or supplied power cord set.

IMPORTANT: Whenever it is likely that the protection has been impaired, disconnect the power cord until the ground has been restored.

If your LAN covers an area served by more than one power distribution system, ensure that their safety grounds are securely interconnected.

CAUTION: LAN cables may occasionally be subject to hazardous transient voltages such as lightning or disturbances in the electrical utilities power grid. Handle exposed metal components of the network with caution.

2.1.1 Network Connected Equipment

The installation must provide a ground connection for the network equipment.

2.1.2 Cable Connections

All Ethernet and serial ports are designed for connecting to equipment that is located in the same building as the device. Do **not** connect these ports directly to wiring that exits the building where the device is located.

2.2 Servicing

There are no user-serviceable parts inside this product. Any servicing, adjustment, maintenance, or repair must be performed only by a service-trained personnel.

This product has a power switch that must be used to power on the unit after the power cord is plugged in.

2.2.1 Lithium Battery Warning

The Lithium Battery used in device may not be replaced by the user. The Lithium Battery must be replaced by authorized service personnel with the same or equivalent type.

This page intentionally left blank.

Chapter 3

Installation

WARNING: This equipment must be provided with a proper AC protective earth (PE) ground connection.

3.1
Unpacking and Checking Equipment

The device comes wrapped in a plastic bag and secured in Styrofoam protective packaging.

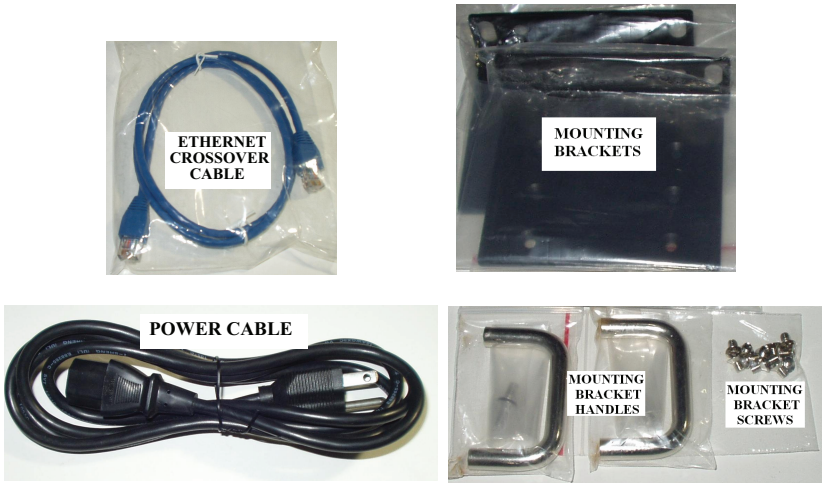
Procedure:

1. Unpack all the individual parts.

   The packaging comes with the following list of items:

   - The device.
   - Power cable terminating in 120 Volt, male, 3-prong connector, if specified in order.
   - Ethernet Crossover Cable.
   - Quick Start Guide CD.
   - Mounting kit:
     - (2) Handles with screws.
     - (2) Rack mounting brackets.
     - (1) Bag of (12) Rack mounting screws.

   Figure 1: List of Supplied Items



2. Inspect the unit for any shipping damage.

   If you discover any damages, contact Motorola Solutions immediately. Keep the original packing material in case you need to ship the equipment.

3.2 Initial Power Up

3.2.1 Power Requirements

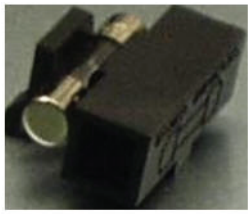
Input Voltage	100 to 240 VAC auto-ranging (47 to 63 Hz for AC power)
Power Consumption	40 Watts

3.2.2 Fuse

The fuse is located underneath the AC Power Input connector (located on the right side of the rear panel).

The fuse can be replaced by using a small flathead screwdriver to remove the fuse holder.

Figure 2: Fuse



3.2.3 Connecting the Power Cable

When and where to use:

IMPORTANT: Power should not be applied until all cables are attached and the unit is ready to operate.

Procedure:

1. Attach the cable-mounted female connector of the power cord to the panel-mounted male connector (inlet) of the device.
2. Attach the male end of the power cord to a properly grounded 100/240 VAC, 50/60 Hz outlet, UPS, power strip, or wall socket.

   Figure 3: Power Input Connector

3.2.4
On/Off Switch

The device activates once it has power applied through the power cord.

A short press of the On/Off switch powers the device up or down. Powering down by this method can take up to 30 seconds.

A long press of the On/Off switch powers down the device immediately. However, this method should be avoided, if at all possible (see the following caution).

NOTICE: If the device is powered down with the On/Off switch and then, the power is removed from the unit (unplugging the cord, power failure, etc), the device automatically powers up when power is restored to the unit.

CAUTION: Immediate shutdown (long press of the On/Off switch) can result in loss and/or corruption of data. This method should only be used if the normal power-down is unsuccessful. Any sudden loss of power (such as removing the power cord) can result in loss and/or corruption of data. This is why it is critical to utilize a UPS with the device.

3.2.5
Power Indicator

On the front panel of the unit is a green LED marked with the power symbol.

The LED illuminates when power is properly supplied to the unit and the power switch is turned to the on position.

If the LED does not illuminate, check to see if the fuse is blown.

3.3
Getting Acquainted with the 9100 Model

The sections which follow introduce the front panel and rear panel of the 9100 model device.

3.3.1
Front Panel

This section explains the indicators and ports found in the front panel of the device.

3.3.2
Front Panel Photo

The following image shows the front panel of the XRI 9100:

Figure 4: XRI 9100 Front Panel

3.3.3
Indicators

3.3.3.1
Power LED

On the front panel of the device is a green LED marked with the POWER symbol. The LED illuminates when power is properly supplied to the unit and the POWER switch it turned to the on position.

Figure 5: Power LED

3.3.3.2
Storage Activity LED

The yellow LED is located on the left side of the front panel and below the Power LED.

The yellow LED indicates the storage (Hard Drive) activity, eg., the LED lights up when the Hard Drive is being accessed.

Figure 6: Storage Activity LED

3.3.3.3
PWR1 and PWR2 LEDs

PWR1 and PWR2 are red LEDs that are not currently used.

They are located to the immediate right of the Power and Storage Activity LEDs.

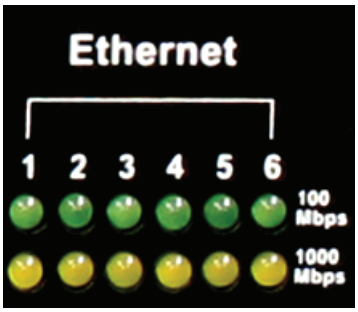
3.3.3.4
Ethernet Activity LEDs

The six pairs of Ethernet LEDs are labeled 1-6.

The number above the LED corresponds to the Ethernet port number (LAN1-LAN6) on the Rear Panel of the device. For each Ethernet port, there is a green LED and a yellow LED. The LED illuminates continuously when carrier is present but no messages are being passed. The LED blinks when messages are present.

- The green LED lights up if the corresponding Ethernet port has activity at a 100 Mbps communications rate.
- The yellow LED lights up if the corresponding Ethernet port has activity at a 1000 Mbps communications rate.

Figure 7: Ethernet Activity LEDs



3.3.3.5

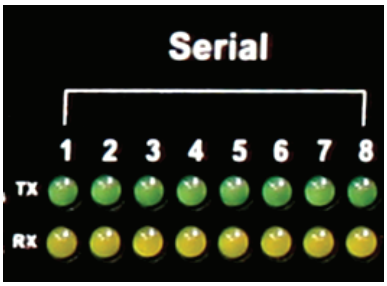
Serial Activity LEDs

The eight pairs of Serial LEDs are labeled 1-8.

The number above the LED corresponds to the Serial port number (P1-P8) on the Rear Panel of the device. For each Serial port, there is a green LED and a yellow LED.

- The green LED lights up for transmit (TX) activity on the corresponding Serial port.
- The yellow LED lights up for receive (RX) activity on the corresponding Serial port

Figure 8: Serial Activity LEDs



3.3.3.6

Programmable LEDs

The eight LEDs located in the area labeled “Programmable LED” are not currently used.

3.3.4

Rear Panel

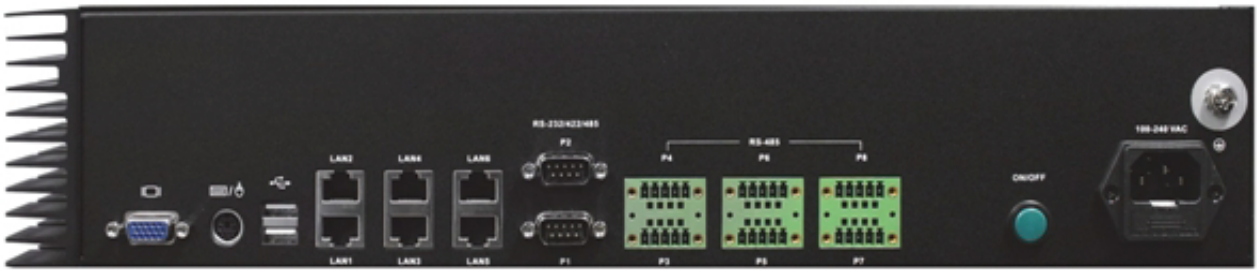
This section explains the ports found in the rear panel of the device.

3.3.4.1

Rear Panel Photo

The following image shows the rear panel of the device.

Figure 9: XRI Rear Panel



3.3.4.2
Ports

3.3.4.2.1
Video (VGA) Port

The VGA port is located on the left side of the rear panel. It can be used to attach a display monitor to the unit.

Figure 10: Video (VGA) Port

3.3.4.2.2
PS/2 Port

The PS/2 port is located on the left side of the rear panel and to the right of the VGA port. It is used for connecting a keyboard or a mouse.

Figure 11: PS/2 Port

3.3.4.2.3
Universal Serial Bus (USB)

There are two USB ports located on the right side of the front panel. The USB port is used for memory expansion, where applicable.

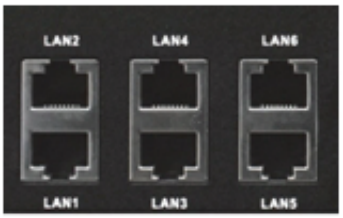
Figure 12: Universal Serial Bus (USB)

3.3.4.2.4

Ethernet Ports (6)

There are six Gigabit Ethernet LAN ports (labeled LAN1 to LAN6) are located on the rear panel and to the right of the USB ports.

Figure 13: Ethernet Ports



3.3.4.2.5

RS-232/422/485 Serial Ports (P1-P2)

There are two RS-232/422/485 Serial (COM) Ports labeled P1 and P2. They are located on the rear panel and to the right of the Ethernet LAN ports.

NOTICE: Only P1 (COM1) port is currently supported by Connect Plus for external serial communications.

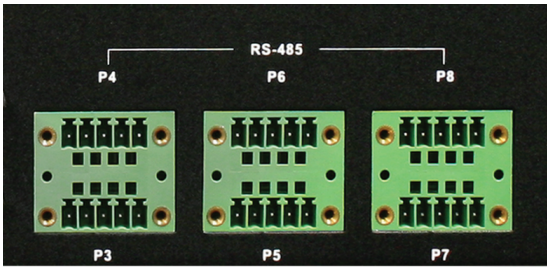
Figure 14: RS-232/422/485 Serial Ports (P1-P2)

3.3.4.2.6

RS-485 Serial Ports (P3-P8)

There are six RS-485 Serial (COM) Ports labeled P3 through P8. These ports are located on the rear panel and to the right of the P1 and P2 Serial Ports. They are not currently used.

Figure 15: RS-485 Serial Ports (P3-P8)



3.3.4.2.7

Grounding Connection

The device panel provides a screw as a grounding point. The screw is identified with the symbol for Earth Ground and is located above and to the right of the Power Input.

Figure 16: Grounding Connection

3.3.5

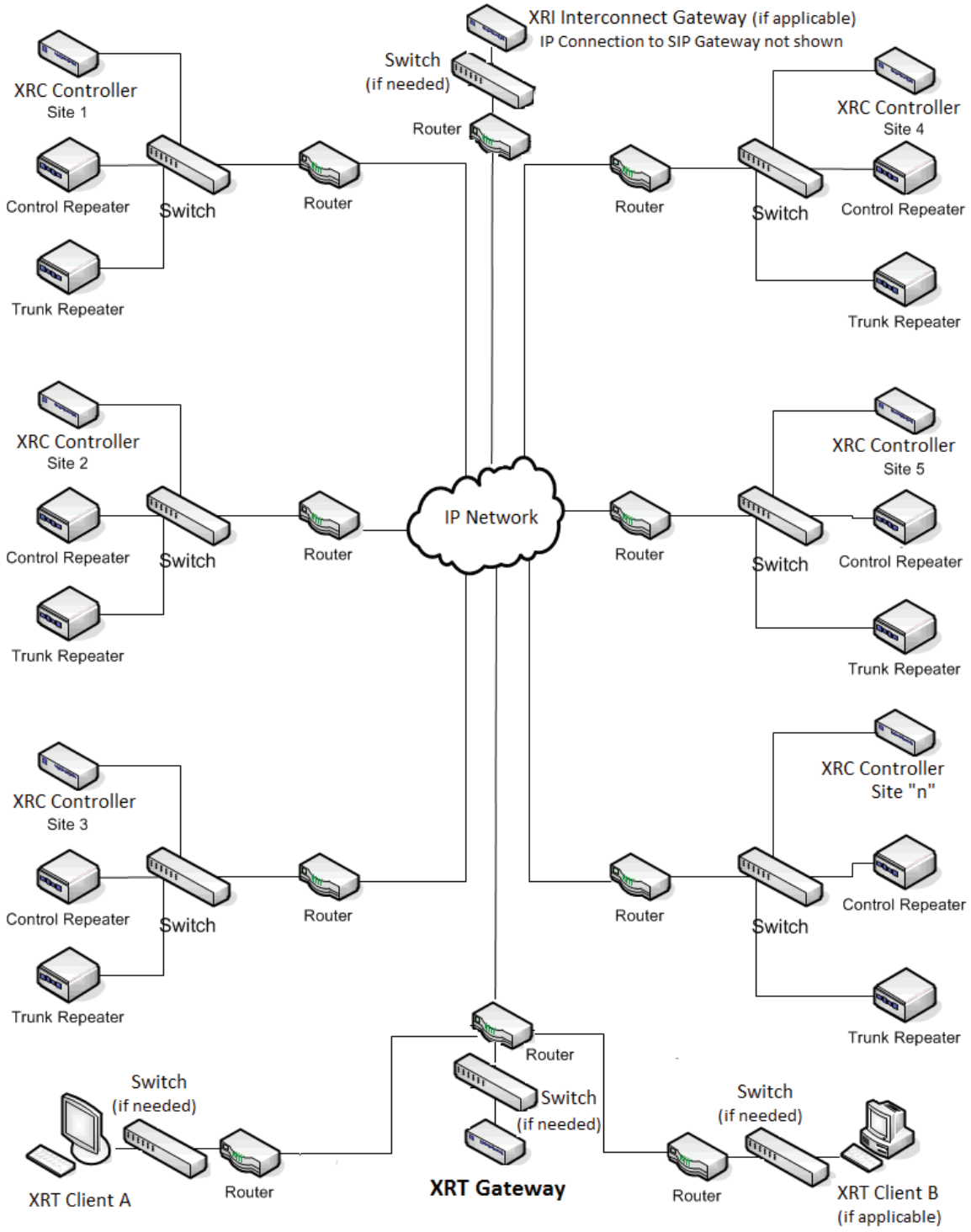
System Connections

This section describes how to connect the device into a Connect Plus system.

3.3.5.1

Block Diagram

The following figure provides a general overview of Connect Plus network hardware. The figure is provided as example, and is not representative of every network or topology. Please note that the XRC, XRT, and XRI do not currently support multicast IP traffic. The System Administrator must design or configure the IP network such a way that no Multicast messages are sent to the XRC, XRT or XRI. The XRT and XRT Client can be co-located, if desired, as long as this important guideline is followed.



NOTICE: See the MOTOTRBO Connect Plus System Planner for more information on network topologies and IP considerations.

3.3.5.2

PC Connection for Initial Configuration

There are multiple methods to connect to the device. The two most common methods are described in the following sections.

3.3.5.2.1

Ethernet Port Connection of the Device

The Network Parameters of the PC will have to be temporarily changed to match the default Network Parameters of the device. Once the Network Parameters of the device are set for your network, then the Network Parameters of the PC can be returned to their original settings. See PC Connection for Initial Configuration on page 28

3.3.5.2.2

Direct Connection: PC to Device

Plug one end of a Category 5 Ethernet crossover cable into the LAN1 port, located on the left side of the rear panel of the device. Plug the other end of the cable into any available Ethernet port on the PC.

Figure 17: Connect the PC to the device using a LAN cable

3.3.5.2.2.1

Connecting to the Device Through An Ethernet Switch

Prerequisites: Minimum switch requirements:

- 100 Mbps ports
- Managed (recommended but not required)

Procedure:

1. Plug one end of a straight-through Category 5 Ethernet cable into the LAN1 port located on the left side of the rear panel of the device.
2. Plug the other end of the cable into any available port on the Ethernet Switch.
3. Plug the other end into the site Ethernet switch.

3.3.5.2.3

Connecting Through the Serial Port of the Device

Procedure:

1. Plug one end of a null modem cable into P1 serial port (COM1 port) located in the middle of the rear panel of the device.
2. Plug the other end of the cable into any available serial port on a Personal Computer.

Figure 18: Null Modem Cable

3.3.5.3

Site Installation

Because the device connects via IP to the SIP Gateway(s) and to the Controller sites of the device, this provides flexibility as to where the device is physically installed. For information on installing the device in a rack, see Mounting the Device In A Rack on page 30

3.3.5.3.1

Power Recommendations

3.3.5.3.1.1

Primary Power Source

The primary power source can be supplied through the following:

- AC power receptacles (wall sockets)
- Rack mount power distribution unit
- Rack mount power strip
- Vertical power strips

Figure 19: Primary Power Source

3.3.5.3.1.2

Backup Power Source

Emergency backup power systems usually consist of two components: a UPS and a generator. This section only describes the UPS; the selection of the generator is beyond the scope of this document.

A UPS can serve a number of purposes such as filtering out power events, conditioning and providing power if primary power source fails. On the average, the time a UPS is expected to do this, is under five minutes which gives enough time to shut down equipment and for the backup power generator to take over the load.

Depending on your configuration and needs, the following areas require different emphasis:

- Surge Suppression
- Power Conditioning

- Battery Backup

It is strongly recommended that the XRI and its supporting network equipment (router and switches) are backed up by UPS. The XRI is a 40 W unit. Check the power requirements of other devices (such as network equipment) when calculating the required capacity of a UPS system.

See Appendix A Determining the UPS Capacity on page 95.

3.3.5.3.1.2.1
Importance of Providing Back-Up Power

This device is a power-computing device, and like other computers, a power-loss causes the device to lose information not saved to the hard drive or non-volatile memory.

3.3.5.3.2
Mounting the Device In A Rack

The device can be mounted in a system rack.

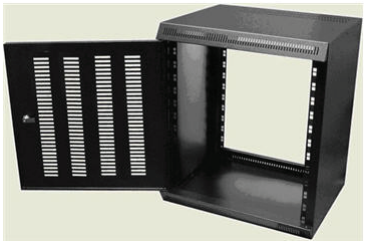
Prerequisites: There are different types of racks, as follows:

- Rails and base only

- Enclosure without a door

- Enclosure without a door on wheels

- Enclosure with a door

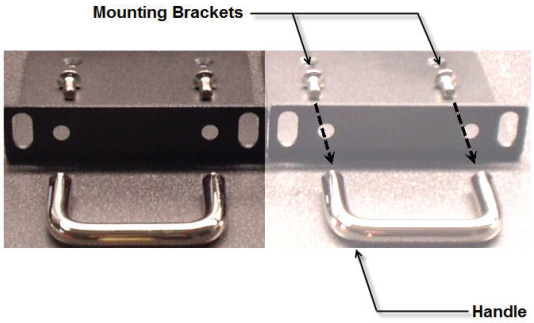


- Enclosure with a glass door

Select the mounting type that is suitable for your environment.

Procedure:

1. Using four screws, attach the handles to the mounting brackets by fastening them via the through holes.



2. Line up the six screw holes in the mounting brackets with the six screw receptacles in each side panel of the device. Use the mounting bracket screws to attach the brackets to the device.
3. Install the device in the rack.
4. Adjust the mounting bracket to fit.

   Adjustment should not be required for standard EIA racks.
5. Using four rack screws, secure the unit to the mounting rails.

3.3.5.3.3
Connection of the Device to the SIP Gateway

The device is not directly connected to the SIP Gateway.

The two devices communicate via IP networking via the LAN or WAN. There are configuration parameters in both devices that allow them to communicate via the network. The LAN1 port of the device is the primary LAN port that is used for all network communications.

This page intentionally left blank.

Chapter 4

Communicating with the Device

This chapter describes the communication with the device after physical installation and after electrical connections are in place.

Before proceeding, ensure that all the connections are still in place and secure.

4.1 Configuring the PC Network for Initial Configuration

Prerequisites: The following procedure is for Microsoft® Windows Vista™ Operating System. For other operating systems, consult your IT department.

Procedure:

1. From the **Start** menu select the **Control Panel**.
2. Select **Network and Internet.**
3. Select **Network and Sharing Center**.
4. Click **Manage network connections**.
5. Select **Local Area Connection** from the list.
6. From the sub-menu, select **Change settings of this connection**.

   The Local Area Connection Properties window appears.
7. Select **Internet Protocol Version 4 (TCP/IPv4)** connection and click the **Properties** button.

   The Internet Protocol (TCP/IP) Properties window appears.
8. Select the **Use the following IP address** radio button and enter the following information:

   IP address: 192.168.1.21 (192.168.1.15 through 192.168.1.20 are the default IP addresses for LAN1 – LAN6 of the device respectively)

   Subnet mask: 255.255.255.0

   Default gateway: 192.168.1.1
9. Click the **OK** button to return to the Local Area Connection Properties window.
10. Click the **OK** button in the Local Area Connection Properties window to complete the PC Network Communications setup.

4.2 Connect Plus Network Manager Connection Tool Software

Microsoft .NET Framework Requirement: A PC can (and frequently does) have multiple versions of Microsoft .NET Framework. To utilize Network Manager versions prior to Connect Plus System Release 1.3, the PC must have at least one of the following .NET Framework versions: 2.0, 3.0 or 3.5.

To utilize a Network Manager version for Connect Plus System Release 1.3 (or later), the PC must have .NET Framework version: 4.0. To see what versions are on your PC, check Control Panel>Add or Remove Programs.

4.2.1
Installing MOTOTRBO Connect Plus Network Manager Connection Tool on the PC

Prerequisites: Download the Installation folder from Motorola Online (MOL). The folder includes two (2) files:

Setup.exe
This is the application that is used to install the MOTOTRBO Connect Plus Network Manager Connection Tool software on your PC.

MOTOTRBO Connect Plus Network Manager Connection Tool Setup.msi
Microsoft Windows Installation file.

Procedure:

1. From the Installation folder, double-click the setup.exe file.
2. Answer the questions and follow the prompts provided by the Installation Wizard.
3. The Installation Wizard provides a message when installation is complete. Follow the prompt to close the message and to exit the Installation Wizard.

4.2.2
Launching the MOTOTRBO Connect Plus Network Manager Connection Tool Software

When and where to use:

IMPORTANT: Do not open more than one instance of the MOTOTRBO Connect Plus Network Manager Connection Tool on the same computer, as this can result in unexpected and undesirable operation.

Procedure:

Launch the MOTOTRBO Connect Plus Network Manager Connection Tool Software through one of the following applications:

- **Desktop Icon**

Double-click on the icon shown as follows. The Setup Wizard creates an icon on the Desktop that is a shortcut to the MOTOTRBO Connect Plus Network Manager Connection Tool Application during installation.

- **Start Menu**

To run the MOTOTRBO Connect Plus Network Manager Connection Tool application through the Start menu, select **Start**, choose **All Programs**, then **Motorola Solutions**, and then select **MOTOTRBO Connect Plus Network Manager Connection Tool**.

- **Program Files Folder**

To run the MOTOTRBO Connect Plus Network Manager Connection Tool Application through the **Program Files** folder, navigate to the Program Files folder, open **Motorola Solutions** folder, locate and open the MOTOTRBO Connect Plus Network Manager Connection Tool folder, and then double-click on the **MOTOTRBO Connect Plus Network Manager Connection Tool.exe**.

4.2.3 Establishing Connection with the Device

4.2.3.1 Device Power Up and Power Down

The device activates once it has power applied through the power cord. When there is no loss of power, normal power-up accomplished with a momentary press of the On/Off switch.

The device can be powered down with a short press of the On/Off switch. This can take up to 30 seconds. This is the recommended method for powering down. If the device is powered down with the On/Off switch, and then the power is removed from the unit (unplugging the cord, power failure, etc.), the device automatically powers up when power is restored to the unit.

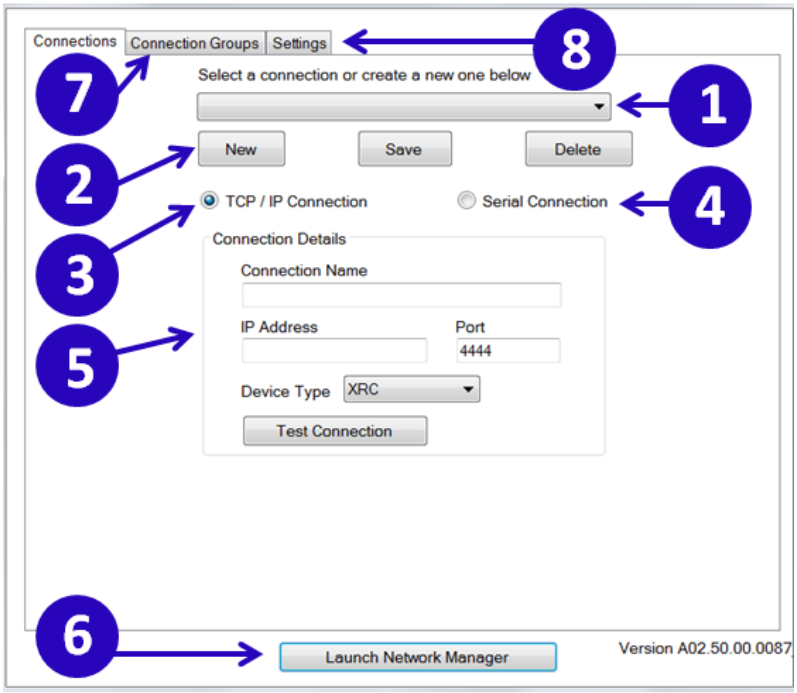
If the On/Off switch is pressed with a long press (about 10 seconds) then the unit immediately shuts down. This power-down method should be avoided, if at all possible.

CAUTION: Immediate shutdown (long press of the On/Off switch) can result in loss and/or corruption of data. It should only be used if the normal power-down is unsuccessful. Any sudden loss of power (such as removing the power cord) can result in loss and/or corruption of data. This is why it is critical to utilize a UPS with the device.

4.2.3.2 MOTOTRBO Connect Plus Network Manager Connection Tool

The MOTOTRBO Connect Plus Network Manager Connection Tool program is used to connect your PC to the XRI Interconnect Gateway and/or the XRC controller. Upon connecting to the XRI or XRC, the Network Manager Connection Tool starts the MOTOTRBO Connect Plus Network Manager, the software program that is used to monitor and configure the XRC controller and the XRI.

Figure 20: MOTOTRBO Connect Plus Network Manager Connection Tool Software



1 Saved Connection Drop-down Box

2 Connection List Controls

3 Selects TCP / IP Connection

4 Selects Serial Connection

5 Connection Detail Panel

6 Make Connection with the device

7 Connection Groups Tab

8 Settings Tab

4.2.3.3
Connection Setup

Before a connection can be made to an XRI Interconnect Gateway or an XRC Controller, a connection must be created to define the connection type (TCP/IP or serial), and to enter the Connection Details.

Once a Connection has been created, the Connection Tool is ready to attempt a connection to the desired device. When multiple connections have been defined, the Connection Tool can be used to create Connection Groups, which provide the ability to simultaneously connect to multiple Connect Plus sites.

The following sections describe the procedure for creating individual connections, and then describe how multiple individual connections can be placed into a Connection Group

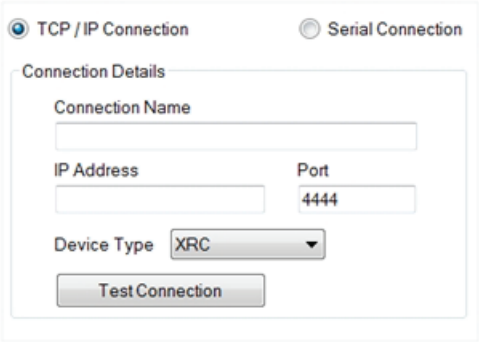
4.2.3.3.1
Connection Detail Panel

The following sections describe each field found in the Mototrbo Connect Plus Network Manager Connection Tool Software window in detail.

4.2.3.3.1.1
TCP / IP Connection

When the TCP / IP Connection radio button is selected, the Connection Details screen displays the following fields.

Figure 21: TCP / IP Connection Settings Screen



4.2.3.3.1.1.1
Connection Name

This field is used to name the connection.

There is a 255 maximum byte limit for this field. Typically, there will be at least one saved connection per device. In some cases, there may be more than one saved connection per device. For example, there might be separate connections for “Site 1 IP Connection” and “Site 1 Modem Connection”.

NOTICE: If not saving the connection settings, then this field is not required.

4.2.3.3.1.1.2
IP Address

This field is used for the IP address of the device for this connection.

Enter the IP address of the device from the perspective of this PC. The format and range for the address are (000-255).(000-255).(000-255).(000-255).

4.2.3.3.1.1.3
Port

This field is used for the MOTOTRBO Connect Plus Network Manager port of the device for this connection.

This setting is normally left at the default port value of 4444. The only exception is when this connection is going through a router utilizing port forwarding, and the router is configured to accept a different port number, and then to convert it to port 4444.

Minimum	1
Maximum	65535
Increment	1
Default	4444

4.2.3.3.1.1.4
Selecting a Device Type

Procedure:

If this connection is for an XRC Controller, select “XRC” as the Device Type. If this connection is for an XRI Interconnect Gateway, select “XRI” as the Device Type.

4.2.3.3.1.1.5
Testing Connection

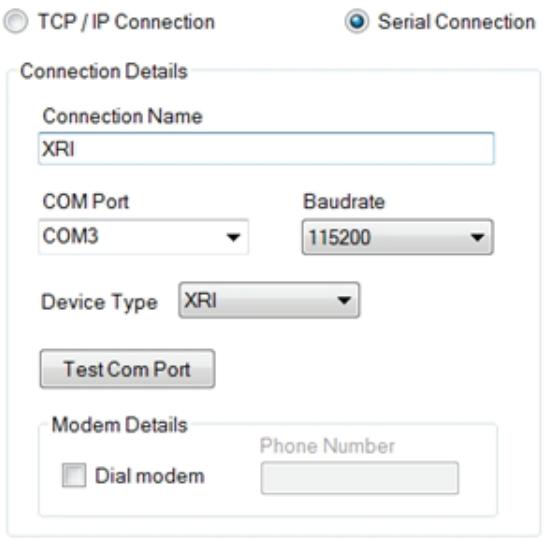
Procedure:

Use this button to test the TCP / IP settings.

If settings connect to a XRC Controller or XRI Interconnect Gateway, then “Success!” will be displayed. If the settings do not connect to a XRC Controller or XRI Interconnect Gateway, then “Failed!” will be displayed.

4.2.3.3.2
Serial Connection

When the Serial Connection radio button is selected, the Connection Details screen displays the following fields:



- Connection Name
- Com Port
- Baudrate
- Phone Number (when Dial modem is enabled)

4.2.3.3.2.1
Connection Name

This field is used to name the connection.

There is a 255 maximum byte limit for this field. Typically, there will be at least one saved connection per device. In some cases, there may be more than one saved connection per device. For example, there might be separate connections for “Site 1 IP Connection” and “Site 1 Modem Connection”.

NOTICE: If not saving the connection settings, then this field is not required.

4.2.3.3.2.2
Selecting a Com Port

This field is used to select communication port of the computer (Com Port).

Procedure:

Click the down arrow and select the appropriate Com Port. If utilizing a modem rather than a direct serial connection to the XRC or XRI, this is the Com Port that has been assigned to the modem.

4.2.3.3.2.3
Baudrate - Direct Connection

When used with a direct serial connection this field defines the Com Port baud rate. The MOTOTRBO Connect Plus Network Manager Connection Tool / MOTOTRBO Connect Plus Network Manager is optimized for the default setting of 57600 for the XRC Controller serial connection and 115200 for the XRI Interconnect Gateway serial connection.

NOTICE: For direct serial connection utilizing a null modem cable, it is advised not to change this setting from its default value.

4.2.3.3.2.4
Baudrate - Modem Connection

When used with a serial modem this field is used to select the Com Port baud rate to communicate with a modem. The baud rate utilized depends on the following:

- The capabilities and configuration of the two modems involved in the connection.
- The quality of the phone line to the site.

Any speed between 1200 to 57600 is supported for connecting to an XRC Controller but the lower the speed the slower the communication between the computer and the controller. Lower speeds will cause delays in updating the screens and information may be missed on the Real Time Display. For serial connection to an XRI Interconnect Gateway, the baudrate must be set to 115200.

4.2.3.3.2.5
Modem Details

If a serial modem is being used then check the Dial Modem checkbox and enter the telephone number of the site's modem. This box will support AT modem commands to allow custom commands required by the modem to be sent.

For example, if the user telephone system required the number 9 and a pause before the telephone number then type: 9,(xxx)yyy-zzzz , where 9 access an outside line, where "," causes a pause, where xxx is the area code and yyy-zzzz is the telephone number. Please check your modem's documentation for further information.

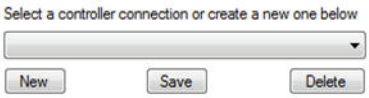
4.2.3.3.2.6
Test Com Port

This button is used to test the serial settings.

If settings connect to a XRC Controller or XRI Interconnect Gateway, then "Success!" will be displayed. If the settings do not connect to a XRC Controller or XRI Interconnect Gateway, then "Failed!" will be displayed.

4.2.3.3.3
Connection Settings Creation, Save and Delete

Figure 22: Connection Settings Window



Connection settings to an individual device can be saved in order to speed up connection time in the future (by not having to repeat the initial set-up). In some cases, the technician may want to create and save more than one connection for the same device. This is helpful, for example, when the technician wants to change between a TCP/IP and a serial connection.

For TCP/IP connections, it is possible that the technician may use different IP addresses to connect to the same device, depending on where the technician and the laptop are located. This is another case where the technician may want to create and save multiple connections for the same device.

4.2.3.3.3.1
Creating and Saving a New Connection

Procedure:

1. Click on the **New** button in Connection List Controls.

   Connection Details is cleared and TCP / IP will be selected as default.
2. Click on either TCP / IP or Serial radio button to select the connection type.
3. Enter Connection Name and fill-in the remaining fields for that connection.
4. Once all settings are entered, press the **Test Connection** button to verify connection is valid.
5. Click the **Save** button in Connection List Controls.

4.2.3.3.3.2
Editing an Existing Connection

Procedure:

1. Select desired connection from the drop down box at the top of the Connections tab. In Connection Details the information for TCP / IP will be displayed as default.
2. Click **Serial** radio button if those settings are to be changed, if not go to the next step.
3. Change the Connection Name or other setting that needs to be changed.
4. Press the **Test Connection** button to verify that connection is valid.
5. Click on **Save** in the Connection List Controls.

4.2.3.3.3.3
Deleting a Connection

Procedure:

1. Click on the **Select a connection** or create a new one below drop down box.
2. Select desired connection.
3. Click the **Delete** button in Connection List Controls.

4.2.3.3.4
Launching MOTOTRBO Connect Plus Network Manager Program

When and where to use:

IMPORTANT: Do not open more than one instance of the MOTOTRBO Connect Plus Network Manager on the same computer, as this can result in unexpected and undesirable operation.

Procedure:

1. Perform one of the following:
   - From the drop-down list, select the desired connection and proceed to Step 4.
   - Click the **New** button in Connection List Controls.
2. Select the connection type.
3. Enter connection name and fill in the remaining fields for that connection.
4. Click the **Launch Network Manager** button.
5. Enter the username and password for the site then, click the **Login** button.

The initial username is "admin" and initial password is "admin".

A Connection Status window briefly appears, showing the status of the connection. If the wrong User Name or password was entered then an error message appears. If the password authentication is successful, the Network Manager Connection Tool starts the MOTOTRBO Connect Plus Network Manager, the software program that is used to monitor and configure the XRC controller. If this is a first connection (or if the PC has an outdated copy of the Network Manager), the Network Manager Connection Tool will first have to download the latest copy of the MOTOTRBO Connect Plus Network Manager software from the controller. This is an automatic process, and the only indication to the user is the brief appearance of a download bar.

Once the MOTOTRBO Connect Plus Network Manager has been successfully launched, the Site Dashboard displays.

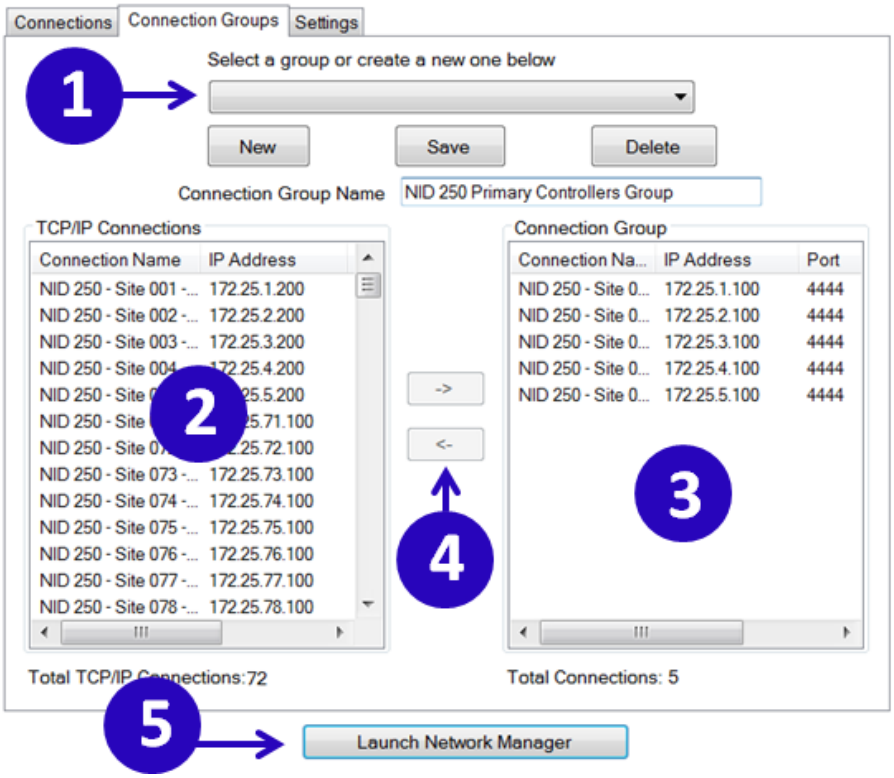
NOTICE: If multiple user connections are required, refer to User Roles in Administrator for information on limiting access to features in the Network Manager.

4.2.3.4
Connection Groups Configuration

Connection Groups allow you to connect to multiple devices simultaneously. After connecting to multiple devices in a group, it is necessary to select which specific device (XRC or XRI) you wish to monitor or configure. When you want to monitor or configure a different device, you will need to select the new device. This will automatically de-select the previous site. The process of switching between selected devices can be done quickly when they are part of the same Connection Group because the connections have already been established.

The Connection Groups tab is used to create Connection Groups. Only TCP/IP connections are eligible to be placed into a Connection Group. The Connection Groups Tab is also used to name the Group, save the Group, edit or delete Connection Groups, and to launch a connection to the desired group.

Figure 23: Connection Groups Settings Screen



1 Connection Groups Dropdown. Click here to view/select from existing connection groups.

2 Available Site Connections. (these are added/configured using the Connections tab)

3 Sites added to the Connection Group.

4 Add/Remove arrows. Click the right-facing arrow to add a selected connection to the group. Click the left-facing arrow to remove a selected connection from the group.

5 Launch Network Manager. Make Connection with Controllers in Connection Group.

4.2.3.4.1
Creating and Saving a Connection

Prerequisites:

- Devices in a connection group must all be part of the same Network (must share the same Network ID). The Connection Tool does not enforce this rule when creating the Connection Group, but it does enforce the rule when establishing connections with Connect Plus sites.
- This recommendation pertains to creating a Connection Group that contains all network sites: If a site has both Primary and Secondary controllers, do not place connections for both the Primary and Secondary in the Connection Group. Use only the connection with the Primary Controller IP address. There is no need to add a secondary controller to the connection group. The tool automatically connects to whichever controller is controlling the site at the time. Including both connections in the same group can create confusion (and possibly result in configuring the wrong XRC). If you need to connect with the inactive controller (i.e. the one not currently controlling the site), you should launch an individual connection to the Secondary Controller IP address from the “Connections” tab.
- You may create a connection group containing just one connection, but there is no advantage to doing so.

Procedure:

1. Select one or more connections from the list of available connections on the left and click the right facing arrow button to add the connection(s) to the Connection Group in the right-hand column.
2. Enter a name for the connection group.
3. Click the **Save** button.

4.2.3.4.2
Editing an Existing Connection Group

Prerequisites: To edit an existing connection group, select it from the dropdown list on the Connection Groups tab and make the desired changes.

Procedure:

1. Select the Connection Group from the drop down box at the top of the Connection Groups tab.
2. Make the desired changes.
3. Click the **Save** button.

4.2.3.4.3
Deleting a Connection Group

Procedure:

1. Select the group to delete from the drop down box at the top of the Connection Groups tab.
2. Click the **Delete** button.
3. Group is deleted.

   The connections that make up the group are not deleted

4.2.3.4.4
Connecting to Multiple Sites Using a Connection Group

Prerequisites: : If an XRI Interconnect Gateway is included in the Connection Group, it is recommended to individually connect with the XRI prior to attempting the Group connection. Verify that the XRI has an account with the same Username and Password as the XRC Controllers in the Group. If not, then create one.

Procedure:

1. Start the Network Manager Connection Tool.
2. Click on the Connection Groups tab.
3. Select the group you want to connect to from drop down box at the top of the Connection Groups tab (or create a new group).
4. Click the **Launch Network Manager** button.

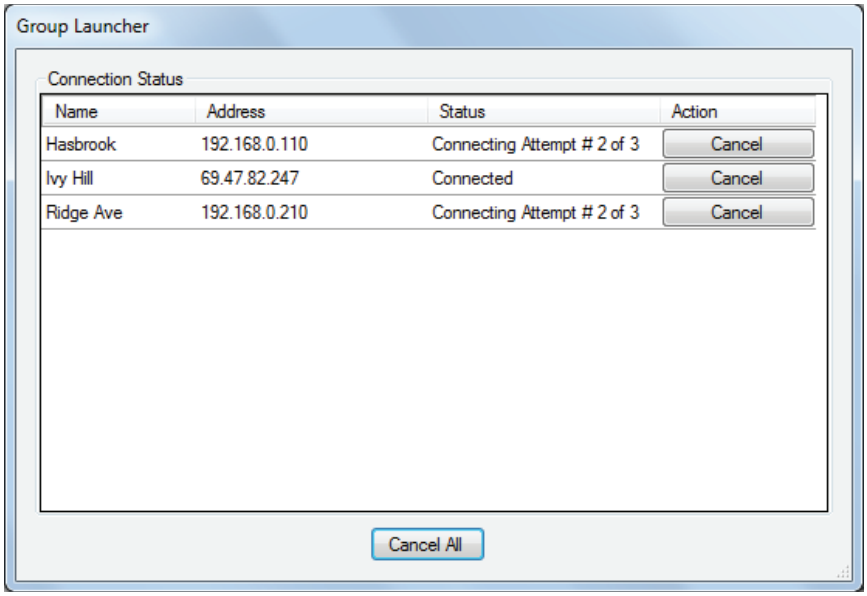
   The Login screen appears.

5. Enter the Username and Password, and then click **Login**.

   Each device in the Connection Group must have an account with the entered Username and Password. See “User Roles” in section for information on how to set up Login accounts.

NOTICE: If an XRI Interconnect Gateway is included in the Connection Group, it is recommended to individually connect with the XRI prior to attempting the Group connection. Verify that the XRI has an account with the same Username and Password as the XRC Controllers in the Group. If not, then create one.

A Connection Status window appears.



6 During the establishment of connections to the group, the Group Launcher window displays the Connection Status.

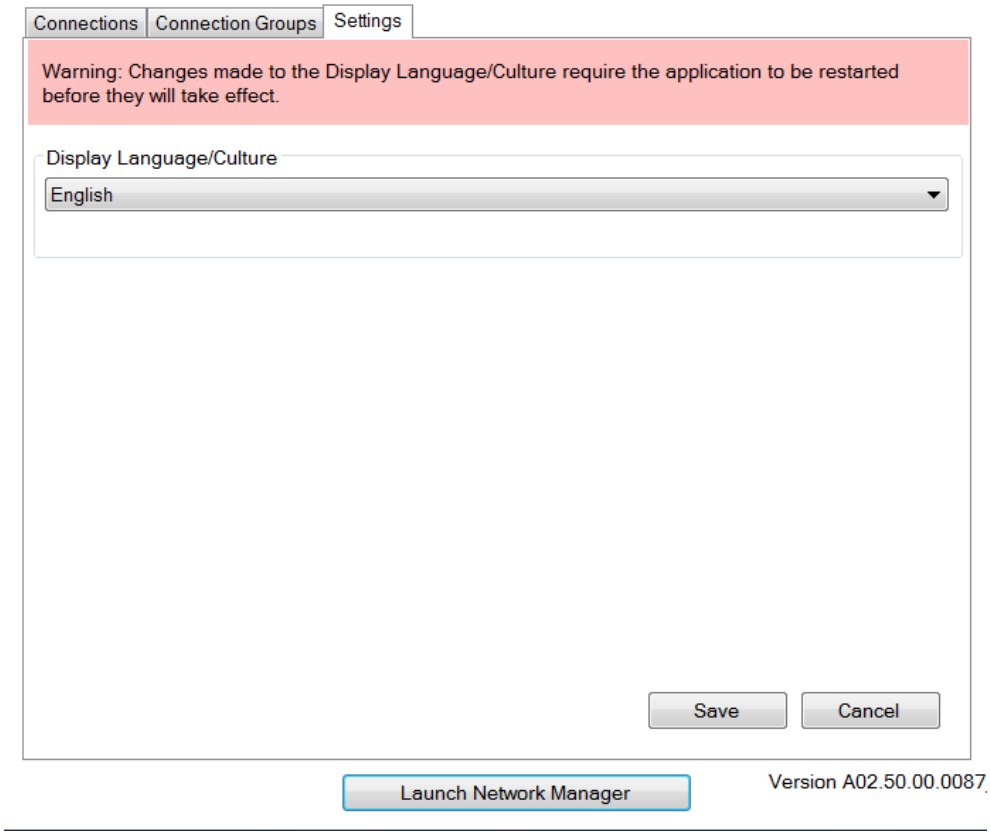
- To cancel a specific connection, press the **Cancel** button to the right of the Status column.
- To cancel all connections to this group, press **Cancel All**.

A maximum of 3 attempts per controller are made. Once the connections and attempts are complete, the window disappears and the Network Manager opens with the Site Dashboard displayed. Any connection that could not be established in 3 attempts will display with gray box in the Site Dashboard.

4.2.3.4.5
Settings Configuration

This Settings tab allows you to configure display language/culture.

Figure 24: Network Connection Tools Settings Tab



4.2.3.4.5.1
Selecting the Network Manager Connection Tool Language

The application can be configured to display in English, or in the same language as the Operating System of the computer (if other than English and supported by the application).

Procedure:

1. Click the **Settings** Tab.
2. Click the arrow under **Display Language/Culture**.

   The application displays a list of one or two languages.
3. Select the desired Language/Culture from the list and press **Save**.
4. Manually close, then re-start the application to enforce the language change immediately.

   NOTICE: The language change is automatically communicated to the Network Manager application the next time it is launched by the Network Manager Connection Tool.

Postrequisites: Changes to the Display Language/Culture require the application to be manually re-started before the changes take effect.

4.2.4
Site Dashboard

When the Connection Tool has established connections to all available sites, and has downloaded the most recent available copy of the Network Manager (if the PC does not already have the same copy – or a more recent copy), the Network Manager program launches and displays the Site Dashboard in the Details View.

The Site Dashboard supports two views: The Details View and the Icon View. The Details View is the default view when the Network Manager launches. There are two ways to switch between the Details View and the Icon View. See Switching Between Details and Icon View on page 47 for more info.

The Site Dashboard has three major functions:

1. It shows which device connections were and were not successful. If the Connection Tool was not able to establish a successful connection after three attempts, the box representing the site displays with gray highlighting in the Site Dashboard.
2. For successfully connected controllers, the Site Dashboard shows whether or not there are any active Controller Alerts or Repeater Alarms.
3. The Site Dashboard makes it possible to select a specific device for the purposes of configuring the controller or obtaining more information about the device.

The Site Dashboard allows you to quickly choose a controller to view/configure. Colors are used to quickly identify site status:

Blue highlighted text
Currently Selected Device.

Red box
Site with an active Controller Alert or Repeater Alarm, but not the Selected site.

White box
Connected to an XRC, but not the Selected device.

Light Blue box
Connected to an XRI Interconnect Gateway, but not the Selected device.

Gray box
“Not Connected” Device.

There are various reasons why a device might show as “not connected”. These include the following scenarios:

1. Failure to connect in three attempts.
2. Not able to authenticate with the device using the entered Username/ Password combination
3. The Network ID of the device was different than the Network ID of the first successfully connected device.

It is also possible for a device to initially show as connected, and then later show as disconnected. This will occur if the TCP/IP connection was initially good, but was later lost. This can occur due to a network connectivity issue, or because the device rebooted.

For each successful XRC connection, the controller’s configured role (Stand-alone, Primary, Secondary) is displayed in the column called Role/State in the Details View. The device state shows “Active” if that controller is currently in control of the site (e.g. Primary / Active). The device state shows “Inactive” if the controller is not currently in control of the site.

IMPORTANT: As a general rule, do not make configuration changes to an XRC if the word “Inactive” appears on the row at the bottom of the box representing the connection. This indicates that you have connected to the inactive controller in a redundant pair. Changes to this XRC would likely be overwritten or lost. For more information, see the Redundant Controller section of the MOTOTRBO Connect Plus System Planner.

To select a device to view/edit, click on the row corresponding to the device (Details View) or the box corresponding to the device (Icon View). The currently selected row or box is highlighted in Blue, and (for a XRC site) you can see the IP address, port number, Site Number and Network ID for the currently connected device at the bottom of the Network Manager window. The Network Manager does not allow you to switch the selected device while there are windows open for the currently selected site. If you attempt to select a different device prior to closing any open windows for your current site, you will receive a prompt, reminding you that there are open windows. If you click “Yes”, the Network Manager will close the open windows and switch to the new device. If you click “No” or “Cancel”, the Network Manager will leave the windows open (and you will remain connected to the current device).

4.2.4.1
Switching Between Details and Icon View

Procedure:

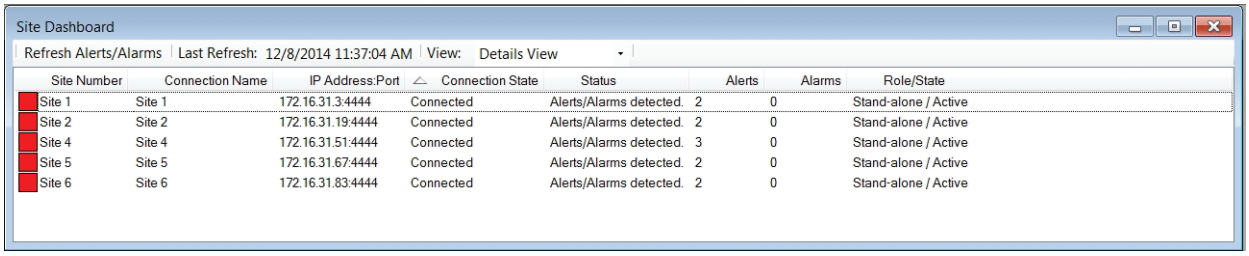
Do one of the following:

- Click on the box labeled “View:” at the top of the **Site Dashboard** window, and then select the desired view from the drop-down list.
- Right click within the **Site Dashboard** Window, and select View>Details View (or Icon View) from the pop-up menu options.

4.2.4.2
Site Dashboard in Details View

The Details View displays as a grid with rows and columns. Each row represents a device connection.

Figure 25: Site Dashboard in Details View



Column Name	Details
Site Number	Box icon to represent the connection. The color of the box conveys information about the connection. After the icon, the Network Manager displays the Site Number (for connected XRC devices), “XRC” for Disconnected XRC Controllers, or “XRI” for a Connected or Disconnected XRI Interconnect Gateway.
Connection Name	The Connection Name as configured in the Network Manager Connection Tool.
IP Address and Port	The IP Address and Port that the Network Manager uses to communicate with the device.
Connection State	**Connected** The Network Manager is connected to the device. **Connecting** The Network Manager is attempting to connect to the device.

Column Name	Details
	Disconnected The Network Manager is not connected to the device. **Rebooting** The Network Manager cannot connect because device reboot is imminent.
Status	**Alerts/Alarms detected** The connected device has reported one or more Alerts or Alarms. **Blank** The Network Manager is attempting to connect to the device. **Connected** The Network Manager is connected to the device, and no Alerts or Alarms have been reported. **Disconnected** The Network Manager is not connected to the device. **Site Alerts/Alarms failed to download** There was problem downloading Alerts/Alarms from the device.
Alerts	Shows the number of Controller Alerts reported by the device. N/A is displayed for XRI Gateways and Disconnected XRC Controllers.
Alarms	Shows the number of Repeater Alarms reported by the device. N/A is displayed for XRI Gateways and Disconnected XRC Controllers.
Role/State	The word to the left of the slash indicates the device's role. The word to the right of the slash indicates the device's current state. For Disconnected Devices, this column is blank. For Connected Devices: **Roles** Stand-alone, Primary, or Secondary, depending on the "Controller Role" as configured with the Network Manager. A connected XRI Gateway displays as "Stand-alone". **States** Active or Inactive. For XRC Controllers, "Active" indicates the device is in control of the site. "Inactive" indicates the device is not in control of the site. A connected XRI Gateway displays as "Active".

4.2.4.3
Using the Details View

When and where to use: The following adjustments can be done to in the Details View.

Procedure:

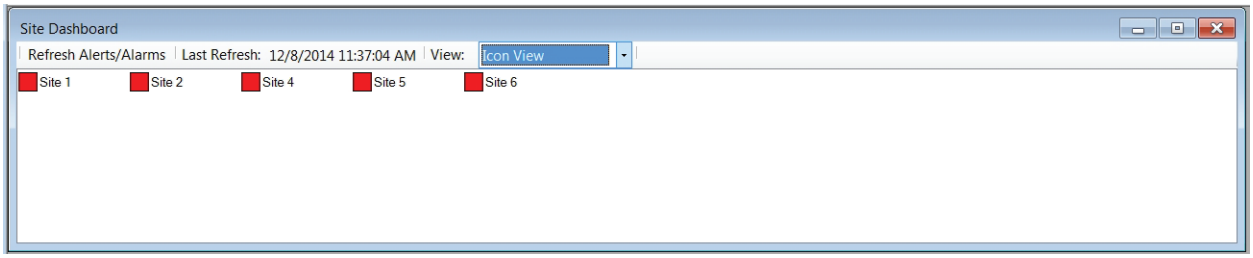
- Adjust the width of the columns in the Details View by dragging the lines that separate the column headings to the left or right.
- Sort the information in Details View by clicking on the column heading which will be used as search criteria to perform an alphanumeric sort (or a reverse alphanumeric sort, depending on how the information is displayed to begin with).

  Following the sort, the Up or Down arrow shows how the information is sorted. The Up arrow indicates the information is sorted 0-9, A-Z. The Down arrow indicates the information is sorted 9-0, Z-A.

4.2.4.4
Site Dashboard in Icon View

The Icon View contains an icon (a square box) for each attempted connection and some brief text to describe the connection or device. The Icon View contains no other information, but is useful for representing a large number of device connections within the Site Dashboard window.

Figure 26: Site Dashboard in Icon View



4.2.4.5
Disconnection and Connection via the Right-Click Menu

This feature allows the user to disconnect from a specific device (without closing the Network Manager), or to connect/re-connect to a specific device, via a right-click option from the Site Dashboard.

This feature is supported with the following constraints:

- The feature is available for TCP/IP Connections only. It is not available for modem connections.
- It is not possible to change user roles for a subsequent connection via this method. To change user roles, it will be necessary to first close down the Network Manager (by selecting “Disconnect” from the Menu bar), and then to re-launch the Network Manager Connection Tool.
- Reconnection via the right-click menu is not allowed following a site firmware upgrade. To re-connect following a site firmware upgrade, it will be necessary to first close down the Network Manager (by selecting “Disconnect” from the Menu bar), and then to re-launch the Network Manager Connection Tool.

4.2.4.5.1
Disconnecting via the Right-Click Menu

Procedure:

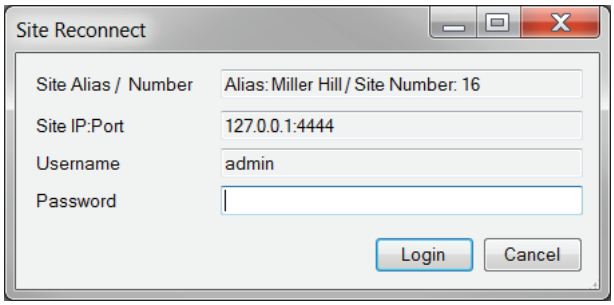
To disconnect from a specific device (without disconnecting from all sites or closing the Network Manager), position the pointer over the row or icon that corresponds to the desired device, right-click, and select “Disconnect” from the popup menu.

4.2.4.5.2
Connecting (or Re-connecting) via the Right-Click Menu

Procedure:

1. If a device did not connect on the initial attempt, or the device disconnected following the initial connection, attempt to reconnect as follows, position the pointer over the row or icon that corresponds to the desired device, right-click, and select “Connect” from the pop-up menu.

   The Site Reconnect Window appears.



2 On the Site Reconnect window, review the connection details (Site Alias, Site Number, Site IP address: Network Manager TCP Port, and Username), enter the Password, and press “Login” (or Cancel). The Network Manager will then attempt to connect to the site. The icon or row that represents the site on the Site Dashboard will show whether the connection attempt is successful.

NOTICE: Depending on the reason that the device failed to connect (or the reason that the device disconnected), the “Connect” option may not be available via the right-click menu. In this event, it will be necessary to first close down the Network Manager (by selecting “Disconnect” from the Menu bar), and then to re-launch the Network Manager Connection Tool.

4.2.4.5.3
XRI and Other Devices Configuration

The remainder of this User Guide provides guidance for configuring the XRI Interconnect Gateway.

There are several configurable settings in the XRC Controller that directly impact Telephone Interconnect operation. These settings include (1) XRI TCP Listen Port (2) Private Phone Response TOT, (3) Allow Phone Access checkbox on the Group records in the subscriber database and (4) the Private Phone Call Init and Private Phone Call RX checkboxes on the unit records in the subscriber database. For guidance on configuring the XRC Trunking Controller, please refer to the MOTOTRBO Connect Plus XRC Controller User Guide.

There are at least two configurable settings in the XRT Gateway that directly impact Telephone Interconnect operation for XRT Clients. These settings include (1) XRI TCP Listen Port and (2) the Allow Phone Access checkbox on the Group records in the subscriber database. For guidance on configuring the XRT Gateway, please refer to the MOTOTRBO Connect Plus XRT Gateway User Guide.

For a general discussion of SIP Gateway configuration, please see the MOTOTRBO Connect Plus System Planner. For specific configuration guidelines for your SIP Gateway device, please refer to the manufacturer’s official product documentation.

For instructions on how to configure the Connect Plus subscriber radios, please refer to the MOTOTRBO Connect Plus CPS Help file. For instructions on how to initiate and receive a phone call with the subscriber radio, please refer to the MOTOTRBO Connect Plus User Guide for your specific radio model(s).

Chapter 5

Device and Network Configuration

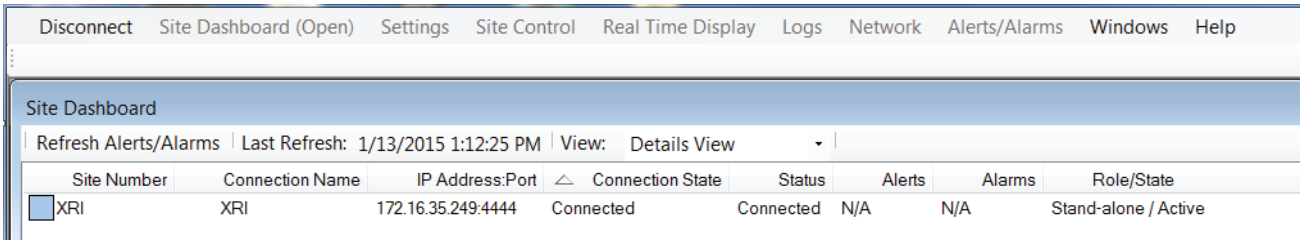
5.1 Configuring the XRI

5.1.1 Launching the Main Menu

Procedure:

To select the XRI for configuration, click on the box representing the XRI connection in the Network Manager Site Dashboard.

This activates the Main Menu bar as shown in the following image.



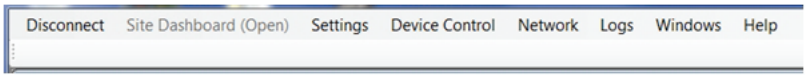
5.1.2 Status Bar

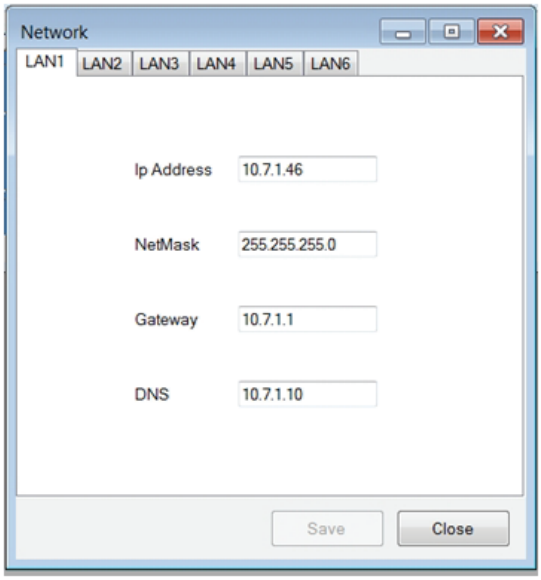
The Status Bar is located at the bottom of the Network Manager screen.

After the XRI is selected for configuration, the Status Bar shows the IP Address and Port to which the Network Manager is connected. The Status Bar also shows the XRI firmware version.

5.1.3 Network Configuration

To open the Network Screen, click on Network in the Menu bar.





The Network Screen supports IP address configuration for each of the XRI's six LAN ports. The default IP Addresses are as follow:

- LAN1: 192.168.1.15
- LAN2: 192.168.1.16
- LAN3: 192.168.1.17
- LAN4: 192.168.1.18
- LAN5: 192.168.1.19
- LAN6: 192.168.1.20

For most customer installations, the XRI uses LAN1 to communicate with the SIP Gateway(s) and with the XRC and XRT site(s). For any LAN port that will be utilized, replace the default IP address with the IP address assigned by the IT manager or other responsible party.

For each LAN port, the XRI supports the settings mentioned in the following sections.

5.1.3.1
Entering the IP Address

Procedure:

1. Enter the IP address that the IT Manager has assigned for this XRI on its Local Area Network.

   The format and range for the address are (000-255).(000-255).(000-255).(000-255).

   NOTICE: The XRI must be assigned a static IP address.

5.1.3.2
Entering the Netmask

Procedure:

Enter the subnet mask (IP Mask or Netmask) assigned by the IT manager.

The format and range for the address are (000-255).(000-255).(000-255).(000-255).

5.1.3.3
Entering the Gateway

Procedure:

Enter the IP Address of the network node responsible for routing messages to/from this Local Area Network as assigned by the IT Manager.

The format and range for the address are (000-255).(000- 255).(000-255).(000-255).

5.1.3.4
Entering the Domain Name Server(s)

Procedure:

Enter the IP Address of the preferred Domain Name Server (DNS) as assigned by the IT Manager.

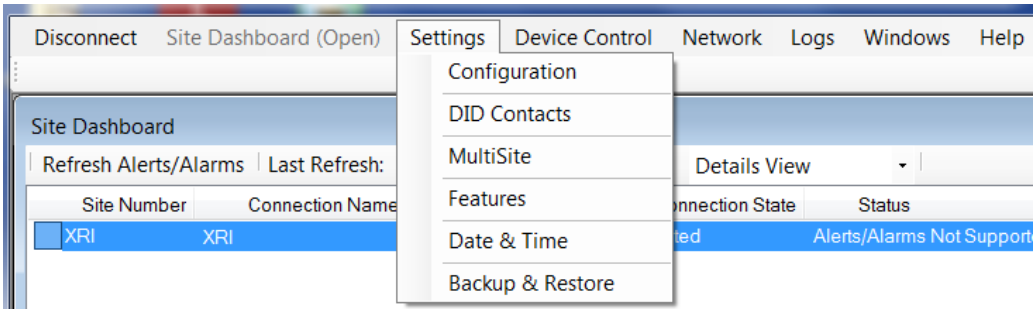
The format and range for the address are (000-255).(000-255).(000-255).(000-255). Use of this parameter is optional.

5.1.4
Using the XRI Configuration Tabs

This information provided in this section applies to all four tabs of the XRI Configuration screen. Subsequent sections discuss the configurable settings for each tab.

Procedure:

1 Click on Settings in the Menu Bar.



2 Select Configuration from the Settings menu.

The XRI Configuration screen displays. The XRI Configuration screen has four tabs; **Configuration**, **Multisites**, **SIP Gateway Config**, and **PIN Access Config.**

5.1.4.1
XRI Configuration Screen Buttons

The section discusses the **Save** and **Close** buttons, which apply to all four tabs.

The Network Manager user can enter or edit information on multiple tabs, and then save the information to the XRI at one time by clicking the Save Configuration button. If the Network Manager user has not edited any Critical Setting, this saves the information to the XRI, and the Network Manager displays a confirmation message.

By clicking **OK** the confirmation message closes and returns to the XRI Configuration screen.

If the Network Manager user has edited any Critical Setting, then the Network Manager displays a message to warn the user that the device must reboot to save the information. The message asks, “Are you sure you want to continue”, and provides three buttons; **Yes**, **No** and **Cancel**.

- By clicking **Yes**, changes are saved and the device reboots. This results in the Network Manager disconnecting from the XRI and re-connection is necessary (if desired) after the reboot is complete.
- Clicking **No** or **Cancel** closes the message and returns to the XRI Configuration Screen.

5.1.4.2

List Items on the XRI Configuration Screen

This section discusses how to enter, edit and delete list items.

Each of the four tabs on the XRI Configuration has one or more lists. The lists are presented in table format (rows and columns). The left-most column is the “Row Header” column, which utilizes the following icons:

▶	**Right Facing Arrow Icon** Indicates that the row, or a cell within the row, has been selected for editing.
	**Pencil Icon** Indicates that a cell within the row is being edited.
✳	**Asterisk Icon** Indicates a new row in the list. (See information below on “Creating a new row in the list.”).

Creating a new row in the list

The Network Manager automatically adds a new row to the end of the list when the Network Manager user enters data into the previous row. If the Network Manager cannot create a new row (because the list has the maximum number of entries), the asterisk icon disappears when the user enters data in the last row of the list.

Entering information in cell

To enter or edit information in a cell, navigate to the desired cell, and then edit as desired.

Delete a row from the list

To delete a row from the list, highlight the entire row by clicking on the left-most column in the row, and then press the “Delete” key on the computer keyboard.

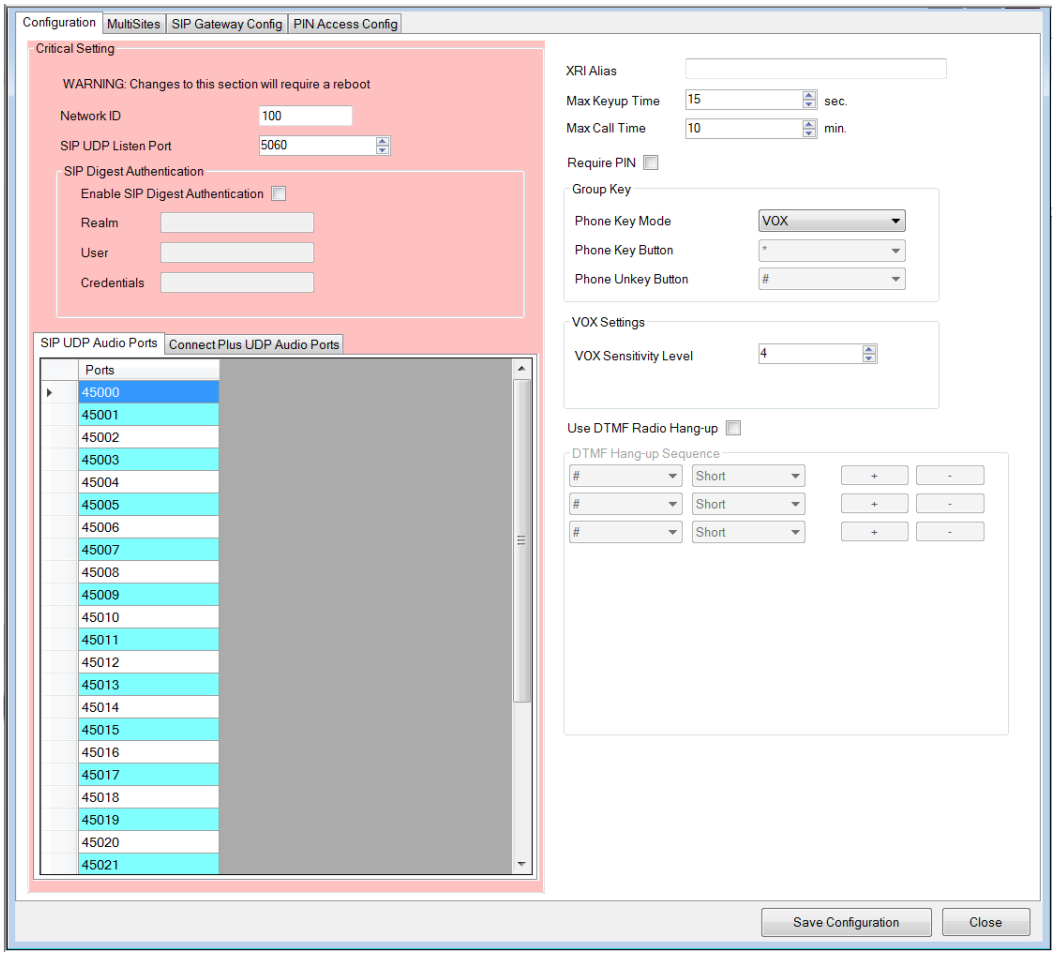
5.1.4.3

Launching the Configuration Tab

Procedure:

1. Click on **Settings** in the Menu Bar.
2. Select **Configuration** from the Settings menu.

3 The XRI Configuration screen displays.



4 If Configuration Tab is not selected, click on the **Configuration** Tab.

WARNING: Settings in the red-shaded area are Critical Settings. Changes to Critical Settings will require a reboot.

5.1.4.3.1
Entering the Network ID

Procedure:

Enter the Network ID of the XRC Controllers on this radio network.

Range	
Minimum	1
Maximum	4095
Increment	1

5.1.4.3.2
Entering the SIP UDP Listen Port

Procedure:

Enter the UDP port number where the XRI shall listen for the SIP Gateway device(s) request a connection.

Minimum	100
Maximum	65535
Increment	1
Default	5060

5.1.4.3.3
Creating SIP UDP Audio Ports

Procedure:

Create a list of up to 32 UDP port numbers the XRI will listen to for incoming digital voice from the SIP Gateway(s).

This number must be at least equal to the number of simultaneous calls supported by the XRI, but it can be greater.

Range	
Minimum	4000
Maximum	65535
Increment	1

5.1.4.3.4
Creating Connect Plus UDP Audio Ports

Procedure:

Create a list of up to 32 UDP port numbers the XRI will listen to for incoming voice packets from XRC and XRT sites.

This number must be at least equal to the number of simultaneous calls supported by this XRI, but it can be greater.

Range	
Minimum	4000
Maximum	65535
Increment	1

5.1.4.3.5
Enabling SIP Digest Authentication

SIP Digest Authentication is supported for connection to a SIP Digital Telephony Gateway only. When connected to a SIP to PSTN Gateway, the feature is not currently supported and should **not** be enabled.

When and where to use: When SIP Digest Authentication is enabled, the XRI Interconnect Gateway and the connected SIP Digital Telephony Gateway check whether they have been configured with matching SIP Digest settings. Telephone calls are not allowed unless the devices confirm a match.

Procedure:

1. To enable the feature in the XRI, check the **Enable SIP Digest Authentication** checkbox.
2. In the **Realm** field, enter the characters that match the equivalent setting in the SIP Digital Telephony Gateway device. Maximum of 255 characters.
3. In the **User** field, enter the characters that match the equivalent setting in the SIP Digital Telephony Gateway device. Maximum of 255 characters.
4. In the **Credentials** field, enter the characters that match the equivalent setting in the SIP Digital Telephony Gateway device. Maximum of 255 characters.

Postrequisites: If SIP Digest Authentication is enabled in the XRI, then it must also be enabled in the SIP Digital Telephony Gateway (and vice versa), and both devices must be configured with the same SIP Digest character strings. The setting names may be somewhat different in the in the XRI and in the SIP Gateway, and the SIP Digest settings may have to be configured into more than one location in the SIP Gateway device configuration software.

5.1.4.3.6
Entering the XRI Alias

Procedure:

Enter an Alias for this XRI.

The field supports up to 255 bytes of data.

5.1.4.3.7
Entering the Max Keyup Time

Procedure:

Enter the maximum length of a single key-up from the phone line to the radio network in a Group Call.

Range	
Minimum	15 seconds
Maximum	495 seconds
Increment	1 second

5.1.4.3.8
Entering the Max Call Time

Procedure:

Enter the maximum total length of a Private Phone Call.

Range	
Minimum	1 minute
Maximum	255 minutes
Increment	1 minute

5.1.4.3.9
Checking the Require PIN Box

Procedure:

Check the box if the phone user should be prompted to enter a valid PIN prior to placing a call to the radio network. If the box is not checked, the PIN requirement is by-passed. Require PIN is supported when the XRI is connected to a SIP to PSTN Gateway. The feature is not currently supported, and should **not** be enabled, when connected to a SIP Digital Telephony Gateway.

5.1.4.3.10
Group Key Settings

These settings control how the XRI will key-up and de-key a phone user that is participating in a Group Call.

5.1.4.3.10.1
Setting the Phone Key Mode

Procedure:

Set to Manual if the Phone user must press a key (or keys) to key-up and de-key during a Group Phone Call. Set to VOX if voice detection should be used as the Key Mode during a Group Call. In VOX mode, the XRI automatically keys and de-keys the phone user, based on the presence or absence of audio from the phone line. Regardless of which Key Mode is configured, during a Group Call the XRI and the radio network do not accept phone user key-ups when there is incoming audio from a radio user.

5.1.4.3.10.2
Defining the Phone Key Button

Procedure:

When the Group Key Mode is set to Manual, enter the phone keypad key press (DTMF tone) that shall be used to initiate phone user Key-up.

Supported characters: 0-9, #, *

5.1.4.3.10.3
Defining the Phone Unkey Button

Procedure:

When the Group Key Mode is set to Manual, enter the phone keypad key press (DTMF tone) that shall be used to de-key the phone user.

Supported characters: 0-9, #, *

5.1.4.3.10.4
VOX Settings

When VOX is selected as the Group Call Key Mode of the phone user, the VOX Settings help determine when the XRI keys and de-keys the call based on audio detection (or lack thereof) from the phone line. There is currently one configurable VOX Setting.

5.1.4.3.10.4.1
VOX Sensitivity Level

This feature adjusts the VOX sensitivity level. Of the seven available levels, Level 1 is the most sensitive level, while Level 7 is the least sensitive level. VOX sensitivity should be configured properly to avoid situations where VOX is frequently triggered unintentionally or where it is difficult to trigger VOX.

Range	
Minimum	1
Maximum	7
Increment	1

5.1.4.3.10.4.2
Using the DTMF Radio Hang-up

Procedure:

1. Check this box if the XRI should support subscriber radio termination for a private phone call via a DTMF Radio Hang Up Sequence.

   NOTICE: Even if DTMF Radio Hang-up is not enabled on the XRI, the radio user can still request the XRI to terminate the private phone call by pressing the Back button on a display-equipped, full keypad radio, or pressing the Phone Exit configurable button on a non-display or limited display radio.

5.1.4.3.10.4.3
Entering the DTMF Hang-up Sequence

Procedure:

When DTMF Radio Hang Up Sequence is enabled, enter the specific DTMF sequence that the radio user sends to terminate the call.

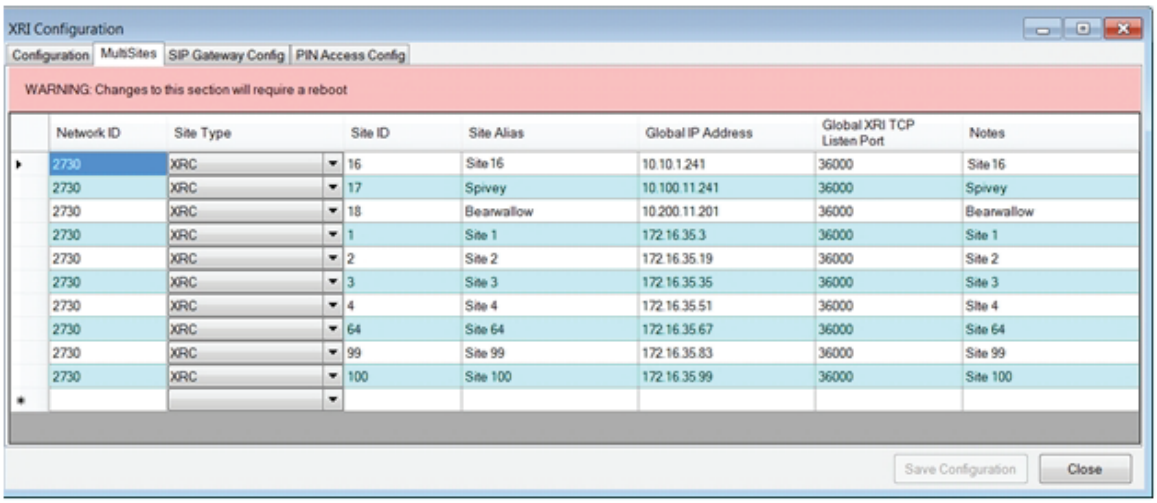
The sequence can contain between one to five DTMF digits (0-9) and/or symbols (*, #). For each DTMF tone in the sequence, the XRI can be configured to expect a long or short tone. Use the “+” button to add a character to the sequence. Use the “-” button to remove a character from the sequence.

5.1.5
Launching the Multisites Configuration Tab

Procedure:

1. Click on **Settings** in the Menu Bar.
2. Select one of the following options:
   - Multisites
   - Configuration

   The Configuration screen displays.



Network ID	Site Type	Site ID	Site Alias	Global IP Address	Global XRI TCP Listen Port	Notes
2730	XRC	16	Site 16	10.10.1.241	36000	Site 16
2730	XRC	17	Spivey	10.100.11.241	36000	Spivey
2730	XRC	18	Bearwallow	10.200.11.201	36000	Bearwallow
2730	XRC	1	Site 1	172.16.35.3	36000	Site 1
2730	XRC	2	Site 2	172.16.35.19	36000	Site 2
2730	XRC	3	Site 3	172.16.35.35	36000	Site 3
2730	XRC	4	Site 4	172.16.35.51	36000	Site 4
2730	XRC	64	Site 64	172.16.35.67	36000	Site 64
2730	XRC	99	Site 99	172.16.35.83	36000	Site 99
2730	XRC	100	Site 100	172.16.35.99	36000	Site 100

3. Click on the Multisites Tab.

   The Network Manager automatically enters the Network ID information from the Configuration Tab.

Postrequisites: Changes to Multisite settings will require a reboot. Enter the information in the following sections for each site entry.

5.1.5.1
Network ID

The Network Manager automatically enters the Network ID information from the Configuration Tab.

5.1.5.2
Site Type

The site type (XRC or XRT) can be selected from the pull-down list.

5.1.5.3
Site ID

This parameter defines the site number of the device referenced by this entry.

NOTICE:

Minimum	1 for an RF site. 251 for an XRT Gateway.
Maximum	250 for an RF site. 255 for an XRT Gateway.

Increment	1
Default	Blank

5.1.5.4
Site Alias

This field is to be entered with the alias of the XRC Controller or XRT Gateway referenced by this entry. The field supports up to 255 bytes of data.

5.1.5.5
Global IP Address

The IP Address entered into this field is used for UDP/IP communications with the site represented by the entry.

The Global IP address could be either a private or public IP address, depending on whether the device configured site is located in the same LAN as the site referenced by this entry. The format and range for the address are (000-255).(000-255).(000-255).(000-255).

5.1.5.6
Global XRI TCP Listen Port

This field is for the Port number used to reach the XRI TCP Listen Port of the XRC Controller or XRT Gateway referenced by this entry.

Minimum	1
Maximum	65535
Increment	1
Default	Blank

5.1.5.7
Notes

This field allows the user to create a note (alphanumeric string) about the network site corresponding to this entry. The maximum number of characters is 255.

NOTICE: This field is optional.

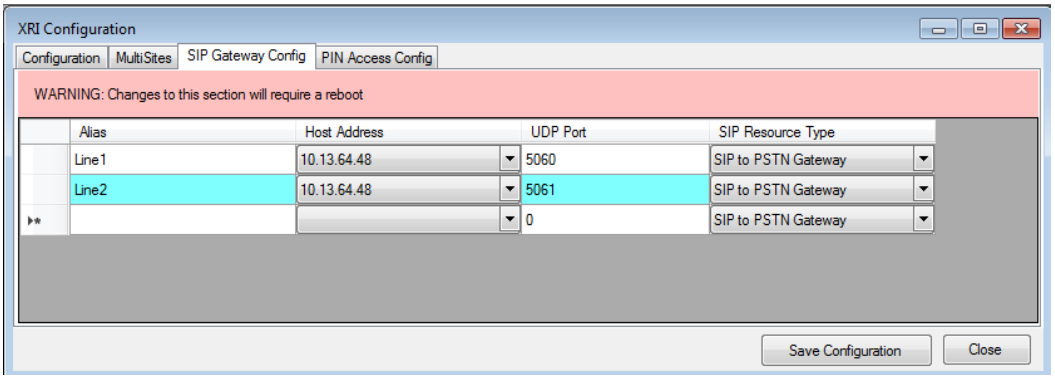
5.1.6
Launching the SIP Gateway Configuration Tab

Procedure:

1. Click on Settings in the Menu Bar.
2. Select Configuration from the Settings menu.

   The Configuration screen displays.

The following image shows an example of the SIP Gateway Config tab when the Key Manager File authorizes connection to a SIP to PSTN Gateway.



3 Click on the SIP Gateway Config Tab.

SIP Gateway Config tab supports IP configuration for up to sixteen SIP Resources.

Postrequisites: Changes to SIP Gateway settings requires a reboot. Enter the information found in the following sections.

5.1.6.1
Alias

This field is to be entered with an alias for the SIP Resource. The field supports up to 255 bytes of data. If the resource is a phone line, the alias can be the phone line's telephone number, if desired.

5.1.6.2
Host Address

Prior to configuring the Host Address field, the Network Manager user must upload a Key Manager File that contains one or more authorized IP Addresses. After uploading the file to the XRI, the application user is asked to confirm the SIP Gateway type and the IP Address (or IP Addresses) specified in the file. For more information, see Obtaining and Using a Key Manager File on page 77. To select which authorized SIP Gateway IP address should be used for this entry, click on the arrow in the **Host Address** field. The application displays a pull-down list of one or more authorized addresses. Select the SIP Gateway IP address desired for this entry.

5.1.6.3
UDP Port

This parameter is to be entered with the Destination UDP Port of the SIP Gateway hosting this resource.

Minimum	4000
Maximum	65535
Increment	1

5.1.6.4
SIP Resource Type

When the Key Manager File indicates that the SIP Gateway Type is SIP Digital Telephony, the application displays one option for SIP Resource Type; SIP Digital Telephony Gateway. When the Key

Manager File indicates that the SIP Gateway Type is SIP to PSTN, the application displays two options for SIP Resource Type; SIP to PSTN Gateway and DID (Direct Inward Dial).

There SIP Resource Types are as follow:

SIP Digital Telephony Gateway

Indicates that multiple calls can be routed based on the Host IP address and UDP Port information configured in this entry. When a phone user makes a call to a radio, the phone user is not prompted by the XRI to enter the Call Type and Destination ID. Instead, the phone user typically enters a numerical string from the keypad as part of phone call set-up. The string includes the Call Type (1 for Group and 2 for Private) and the Destination ID. The string is sometimes preceded by other digits that are required by the SIP Gateway but not conveyed to the XRI.

SIP to PSTN Gateway

When SIP to PSTN Gateway is selected, and when a phone user makes a call to a radio, the phone user is prompted by the XRI to enter the Call Type (Group or Private) and the Destination ID. This option was called “Gateway” prior to MOTOTRBO Release 2.6.

DID (Direct Inward Dial)

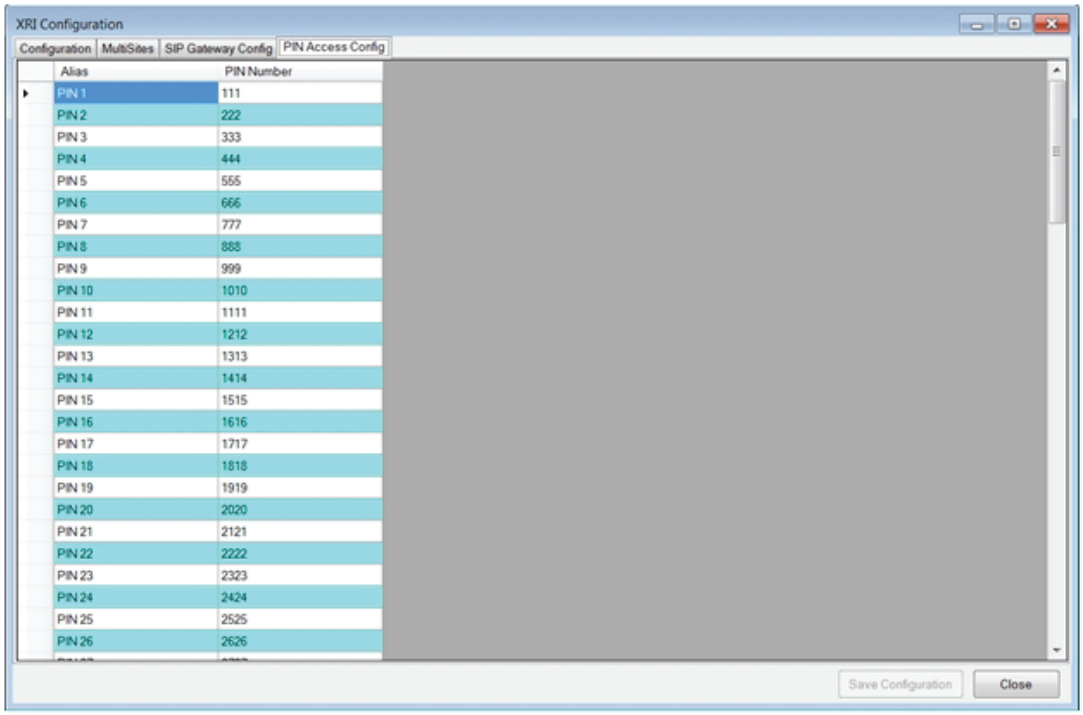
When DID (Direct Inward Dial) is selected, and when a phone user makes a call to a radio, the phone user is not prompted to enter the Call Type and Destination ID. Instead, the XRI initiates a call to a specific Group ID or Private ID, depending on the alphanumeric string (alias) sent by the SIP Gateway and the configuration of the DID Contacts screen of the XRI. This feature requires support and special configuration in the SIP Gateway device.

5.1.7
Launching the PIN Access Configuration Tab

Procedure:

1. Click on **Settings** in the Menu Bar.
2. Select **Configuration** from the Settings menu.

   The **Configuration** screen displays.



Alias	PIN Number
PIN 1	111
PIN 2	222
PIN 3	333
PIN 4	444
PIN 5	555
PIN 6	666
PIN 7	777
PIN 8	888
PIN 9	999
PIN 10	1010
PIN 11	1111
PIN 12	1212
PIN 13	1313
PIN 14	1414
PIN 15	1515
PIN 16	1616
PIN 17	1717
PIN 18	1818
PIN 19	1919
PIN 20	2020
PIN 21	2121
PIN 22	2222
PIN 23	2323
PIN 24	2424
PIN 25	2525
PIN 26	2626

3 Click on the **PIN Access Config** Tab.

If “Require PIN” is enabled in the XRI, the phone user must enter a PIN number that has been configured on this screen. Up to 100 entries are supported. Require PIN is supported when the XRI is connected to a SIP to PSTN Gateway. The feature is not currently supported when connected to a SIP Digital Telephony Gateway.

Postrequisites: For each entry, enter the information found in the following sections.

5.1.7.1
Alias

This parameter defines the alphanumeric alias of the MOTOTRBO Subscriber Unit, Group or Multigroup. The maximum number of characters is 255.

5.1.7.2
PIN Number

This parameter is for a four-digit PIN number.

Range	
Minimum	0000
Maximum	9999
Increment	1

5.1.8
Launching the DID Contacts Configuration Screen

DID is a telephone industry acronym for “Direct Inward Dial”. The DID Contacts screen supports inbound call initiation to a specific Connect Plus Group or Private ID based on an alphanumeric Alias provided to the XRI in a special message sent by the SIP Gateway. DID Contacts screen supports up to 10000 entries. The DID Contacts feature is supported when the XRI is connected to a SIP to PSTN Gateway. The feature is not currently supported when connected to a SIP Digital Telephony Gateway.

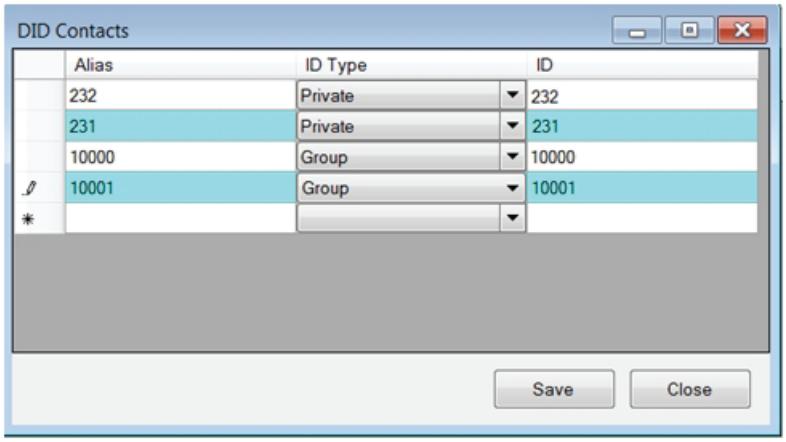
Prerequisites: This feature requires the SIP Resource type to be configured as DID. This feature also requires support and special configuration in the SIP Gateway device.

Procedure:

1 Click on **Settings** in the Menu Bar.

2 Select **DID Contacts** from the Settings menu.

The **DID Contacts** screen displays.



Postrequisites: Changes to DID Contacts will require a reboot. For each entry, enter the information found in the following sections.

5.1.8.1
Alias

The field supports up to 255 bytes of data. The Alias that is entered in this parameter will be sent in the special message by the SIP Gateway device.

5.1.8.2
ID Type

There are two ID types in the pull-down list: Group or Private. This determines whether the XRI should initiate a Group Call or Private Phone Call when it receives a special SIP message containing this Alias.

5.1.8.3
ID

This parameter should be entered with the target ID that the XRI should contact when it receives a special SIP message containing this Alias. If the ID Type is Group, this will be a Talk Group ID. If the ID Type is Private, this will be a Private Radio ID.

Range	
Minimum	1
Maximum	16776351
Increment	1

This page intentionally left blank.

Chapter 6

Device Management

6.1
XRI Backup/Restore Utility

This screen is used to create a backup file containing the XRI configurable settings.

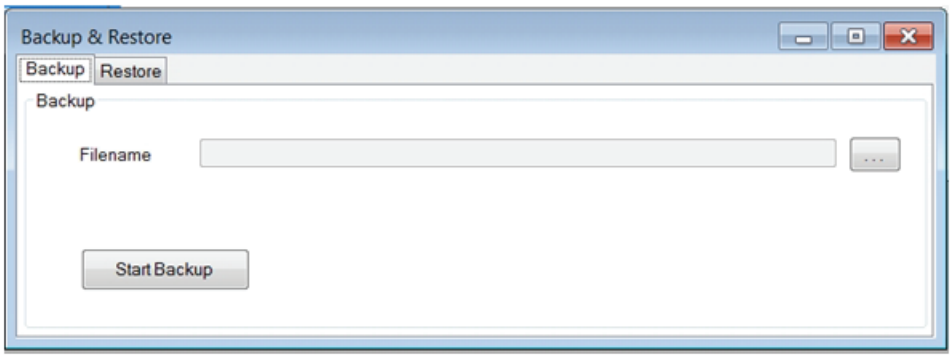
6.1.1
Saving the XRI Configuration To A File

Procedure:

1 Click on **Settings** in the Menu Bar.

2 Select **Backup & Restore Utility** from the Settings menu.

The Backup & Restore Utility screen displays.



3 If the Backup Tab has not been selected, click on the **Backup** Tab.

4 Click on the Browse icon select where it will be saved and click **Save**.

5 Click on **Start Backup** button.

“Backup completed successfully!” displays next to the Start Backup button.

6.1.2
Restoring the XRI Configuration From A File

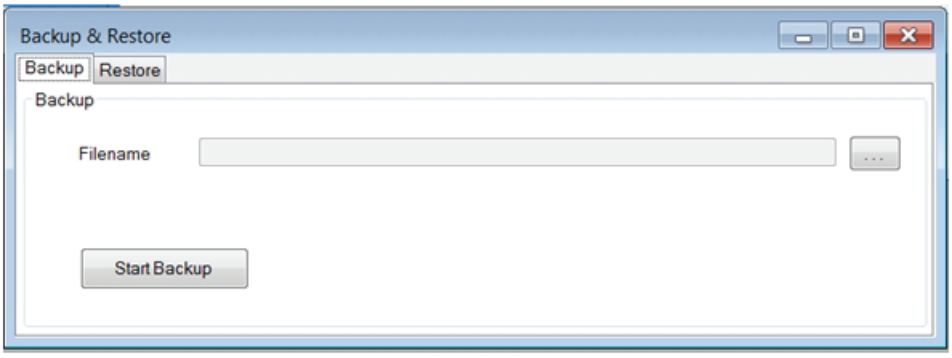
Procedure:

1 Click on **Settings** in the Menu Bar.

2 Select Backup & Restore Utility from the Settings menu.

The Backup & Restore Utility screen displays.

3 Click on the **Restore** Tab.



4 Click on the Browse icon select where it will be saved and click **Save**.

5 Click on **the Start Restore** button.

A dialog box displays to confirm restoration & reboot.

6 Select one of the following answers:

- Answer **Yes** to restore.
- Answer **No** or Cancel to stop the restore.

"File restore completed successfully! Rebooting…" displays under to the Start Restore button along with a progress bar.

6.2 XRI Device Control

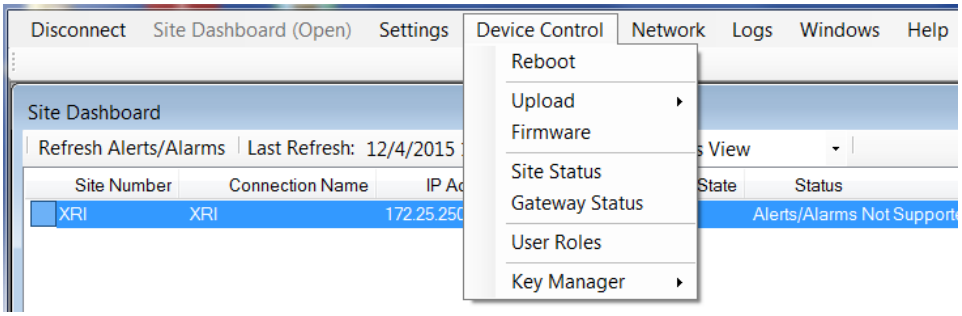
6.2.1 Rebooting the XRI

When and where to use:

WARNING: Rebooting an operational XRI has a significant impact on Connect Plus Telephone Interconnect operation. If a Reboot must occur, it should be done at a time that will have the least possible impact on XRI operation (if possible).

Procedure:

1 Click **Device Control** in the **Menu** Bar.



2 Select Reboot from the Device Control menu.

A warning screen displays.

3 Select one of the following options:

- Select **Yes** to reboot.

- Select **No** or **Cancel** to stop the reboot.

When the XRI reboots:

- All Network Manager sessions are disconnected from the device.
- Any call sessions in progress at time of reboot are terminated.
- Any information that has not been saved to permanent memory is lost.
- The XRI temporarily loses its connection to all XRC and/or XRT sites, and to any SIP Gateways.

The XRI will have to re-establish connections to XRC and/or XRT sites after the Reboot. The SIP Gateway(s) will have to re-establish their connections to the XRI following Reboot.

6.2.2
Voice Prompt Manager

The Voice Prompt Manager screen is used to upload custom voice prompts to replace the system default voice prompts (if desired). The factory default prompts are in US English.

The screen shows a list of generic Voice Prompt names used by the XRI. The Voice Prompt Manager screen can be used to replace the default Voice Prompt with the contents of a custom voice prompt file uploaded by the Network Manager user. If a custom voice prompt is uploaded, the file contents must meet certain requirements in order for the prompt to play as expected. The Network Manager and the XRI do not check the file to verify these requirements are met, so it is the responsibility of the Network Manager user to assure that the custom file meets the following requirements:

- The file must contain 16 bit, uncompressed, PCM digital audio
- The file must **not** contain any file header
- The sample rate must be 8kHz
- The byte order must be little endian

In the list of generic Voice Prompt names, the Voice Prompt Manager screen uses colors to show whether the XRI is using the default prompt, or whether the prompt has been replaced with a customized prompt. For a default prompt, the name displays in black text. If the default prompt has been replaced, the name displays in blue text.

The Voice Prompt Manager screen provides four buttons, which are described as follows:

Use Default
If the currently selected prompted has been replaced with a customized prompt, this button will return the currently selected prompt to its default prompt (U.S. English).

Use Default All
Returns all prompts to their default prompts (U.S. English).

Replace
The Replace button is used to overwrite the currently selected prompt with the contents of a file on the PC of the user. The prompt name as displayed on the Prompt Manager Screen does not change. The source file name and directory from the PC will not be retained by the Network Manager or the XRI. It is suggested that the Network Manager user make a note of the source file name and directory from his/her PC for future reference.

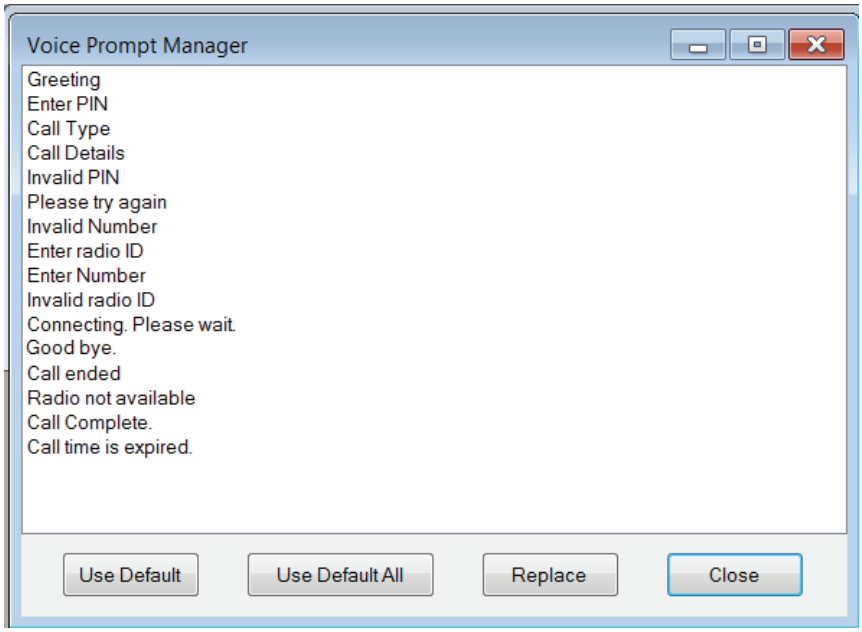
Close
This button closes the Voice Prompts Manager Window.

6.2.2.1
Launching the Voice Prompt Manager

Procedure:

1. Click on **Device Control** in the Menu Bar.
2. Select **Upload** from the Device Control menu.
3. Select **Voice Prompt Manager** from the sub-menu.

   The Voice Prompt Manager screen displays.



6.2.3
Uploading and Upgrading the XRI Firmware

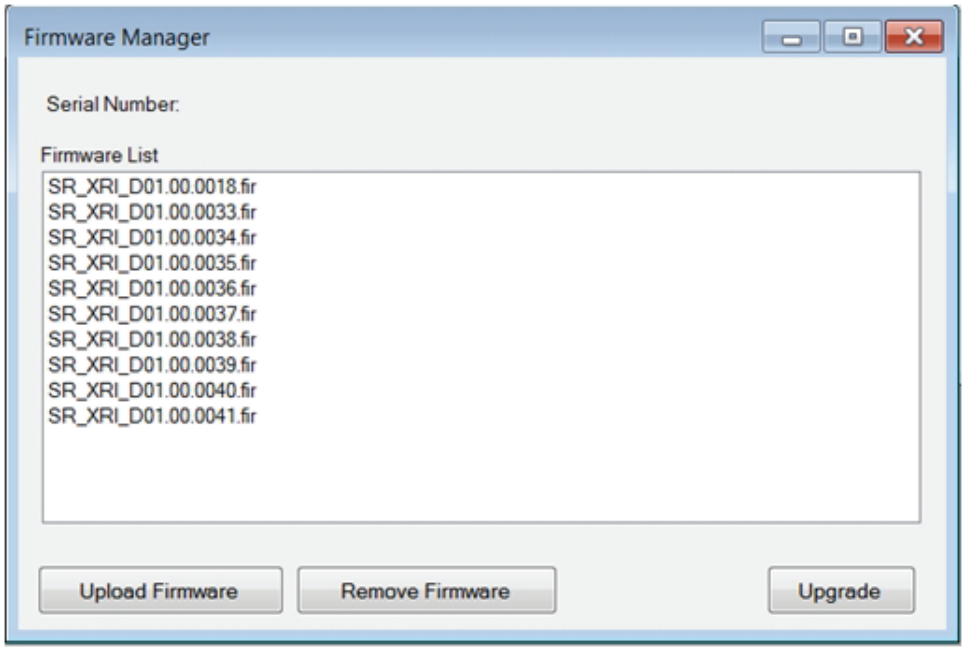
This section (and its subsections) describes the procedure for Uploading, Removing, and/or Upgrading the XRI firmware file (file extension *.fir).

6.2.3.1
Opening the Firmware Manager Screen

Procedure:

1. Click on **Device Control** in the Menu Bar.
2. Select **Firmware** from the Device Control menu.

   The **Firmware Manager** displays.



6.2.3.2

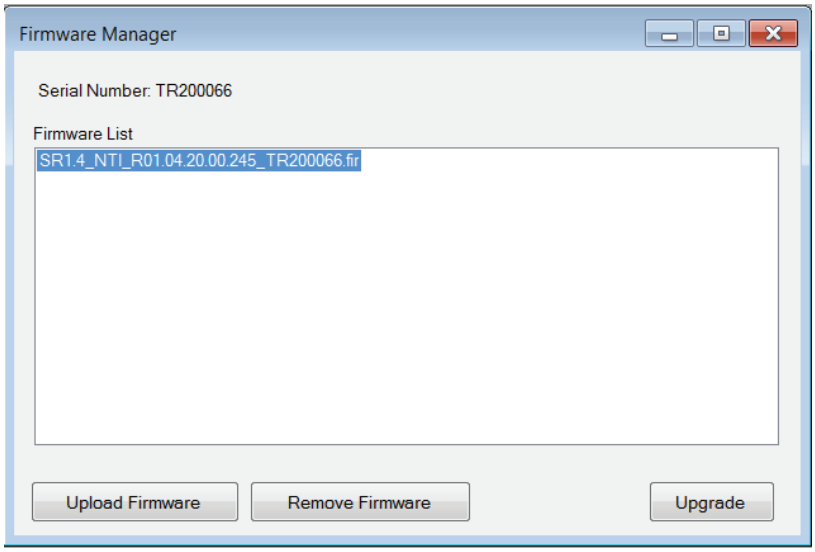
Uploading the Firmware File

Prerequisites: Obtain the new firmware file and place it in a known file directory.

Procedure:

1 From the **Site Control** menu, choose the **Firmware** option.

The Firmware Manager window appears.



2 Click the **Upload Firmware** button.

Firmware files extension is .fir. Operating System upgrade file extension (9100 model only) is .osu

The “Open File” dialogue screen displays.

3 Browse to the directory containing the firmware file.

4 Select the file and click **Open**.

A progress bar appears at the bottom of the screen showing the status of the upload, including an estimation of time remaining.

6.2.3.3
Removing Firmware File

Procedure:

1 Click on **Device Control** in the Menu Bar.

2 Select **Firmware** from the Device Control menu.

The **Firmware Manager** displays.

3 Select the firmware file to be removed.

4 Click the **Remove Firmware** button.

5 Click **Yes** to confirm removal.

6.2.3.4
Upgrading the Firmware

Procedure:

1 From the **Site Control** menu, choose the **Firmware** option.

The Firmware Manager window appears.

2 Select the firmware file to be sent to the device and click the **Upgrade** button.

A dialog box appears, asking to confirm the upgrade.

3 Click **Yes** to upgrade or **No** or **Cancel** to stop the upgrade.

6.2.4
Site Status Screen

The Site Status screen indicates whether or not the XRI has an active connection to each XRC and XRT site configured on the Multisites Tab.

The **Refresh** button is used to refresh the information on the screen.

The **Close** button is used to close the screen.

For each site entry on the Multisites Tab, the XRI displays the following information on the Site Status Screen:

Site Number
This column displays the Site Number of the XRC or XRT site.

Alias
This column displays the Alias of the site. The field supports up to 255 bytes of data.

Host
This column displays the IP Address that the XRI uses to communicate with the site.

Connected
This column shows whether the XRI currently has an TCP/IP connection to the site.
True: The XRI is currently connected to the site.

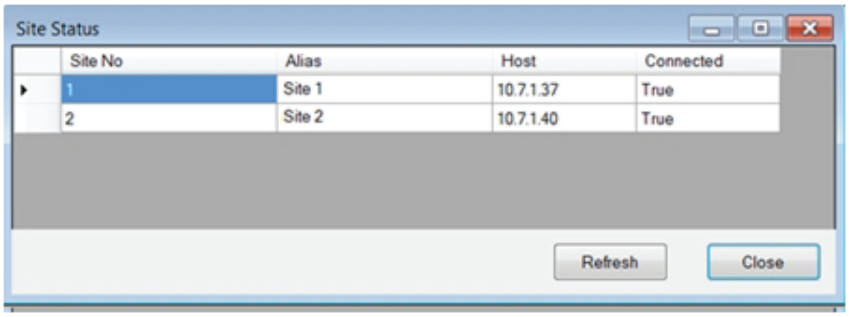
False: The XRI is NOT currently connected to the site.

6.2.4.1
Launching the Site Status Screen

Procedure:

1. Click on **Device Control** in the Menu Bar.
2. Select **Site Status** from the Device Control menu.

   The **Site Status** screen displays.



6.2.5
Gateway Status Screen

The Gateway Status screen indicates whether or not the XRI has an active connection to each SIP Gateway Resource configured on the SIP Gateway Config Tab.

The **Refresh** button is used to refresh the information on the screen.

The **Close** button is used to close the screen.

For each entry on the SIP Gateway Config Tab, the XRI displays the following information on the Gateway Status Screen:

Alias
This column displays the Alias of the SIP Gateway Resource. The field supports up to 255 bytes of data.

IP Address
This column displays the IP Address that the XRI uses to communicate with the SIP Gateway resource.

Port
This column displays the Port that the XRI uses to communicate with the SIP Gateway resource.

Connected
This column shows whether the XRI currently has an IP connection to the SIP Gateway resource.
True: The XRI is currently connected to the SIP Gateway resource.

False: The XRI is NOT currently connected to the SIP Gateway resource.

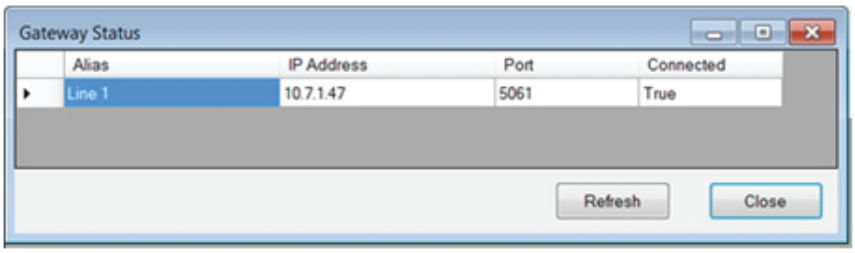
6.2.5.1
Launching the Gateway Status Screen

Procedure:

1. Click on Device Control in the Menu Bar.

2 Select Gateway Status from the Device Control menu.

The Gateway Status screen displays.



6.2.6 User Roles

6.2.6.1 User Roles Access

The following sub-sections describe the privileges for the User Roles (Admin, Manager, Monitor, Accountant) when connected to a XRI Gateway.

6.2.6.1.1 Admin

Admins have access to all features. Features which are exclusive to Admins are:

- Firmware Files
  - Uploading firmware files
  - Removing existing firmware files
  - Upgrading the XRI with a firmware file
- Voice Prompt Uploads
  - Viewing the Voice Prompts Manager
  - Uploading voice prompts with the Voice Prompts Manager
- User Roles
  - Adding new users
  - Removing existing users
  - Changing passwords

6.2.6.1.2 Manager

The following are features available to Managers. Managers also have access to features available to Monitors (see Monitor for those features).

- Site Configuration
  - Saving configuration
- Multisite Configuration
  - Saving new/existing sites
  - Removing sites
- SIP Gateway Configuration

  - Saving new/existing SIP Gateway entries
  - Removing SIP Gateway entries
- PIN Access Configuration
  - Saving new/existing PIN Access entries
  - Removing PIN Access entries
- DID Contacts Configuration
  - Saving new/existing DID Contact entries
  - Removing DID Contact entries
- Network Settings
  - Viewing network settings
  - Saving network settings
- Rebooting the device
- Date / Time configuration
  - View date & time
  - Set date & time
- Event Log Viewer
  - Clear event log
- Backup & Restore Utility
  - Save configuration to a file
  - Restore configuration from a saved file

6.2.6.1.3
Monitor

Monitors only have access to view most features. They are not allowed to make any modifications.

- Site Configuration
  - View configuration
- Multisite Configuration
  - View existing sites
- SIP Gateway Configuration
  - View existing SIP Gateway entries
- PIN Access Configuration
  - View existing PIN Access entries
- DID Contacts Configuration
  - View existing DID Contact entries
- Site Status
  - View site status
- SIP Gateway Status
  - View SIP Gateway
- Event Log Viewer
  - View event log

6.2.6.1.4
Accountant

Accountants only have access to download and/or clear Call Logs.

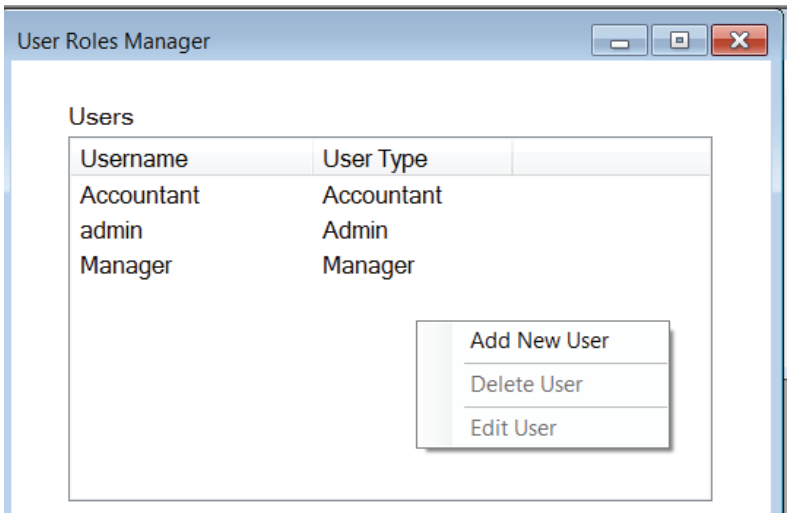
6.2.7
Users Setup

6.2.7.1
Adding New User

Procedure:

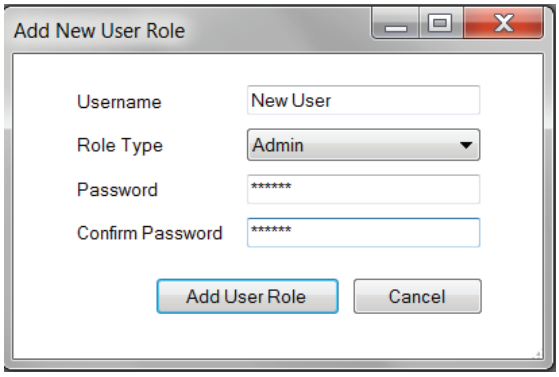
1 Click on **Device Control** in the Menu Bar and select **User Roles**.

The User Roles Manager window appears.



2 Right-click anywhere within the window and select the **Add New User** option from the submenu.

The **Add New User Role** window appears.



3 Perform the following actions in the **Add New User Role** screen:

a Enter User Name.

b Select Role Type from the drop down box.

c Enter password.

d Confirm password.

4 Click the **Add User Role** button.

6.2.7.2
Deleting User

Procedure:

1 Click on **Device Control** in the Menu Bar.

2 Select **User Roles**.

The User Roles Manager screen displays.

3 Right-Click the **User Name** to be deleted.

4 Select **Delete User** from the sub-menu.

A dialog box asking to confirm the deletion appears.

5 Click Yes to delete a user.

6.2.7.3
Changing Password

Procedure:

1 Click on **Device Control** in the Menu Bar.

2 Select **User Roles** from the Device Control menu.

The User Roles Manager screen displays.

3 Right-click the **User Name** to be changed.

a Choose **Edit User**.

b If the Old Password field displays, then enter the Old Password.

4 Enter the New Password and confirm.

5 Click the **Save Changes** button.

6.3
Obtaining and Using a Key Manager File

Beginning with MOTOTRBO Release 2.6, the SIP Gateway IP Addresses that are used by this XRI must be encoded in a special Key Manager File and uploaded to the XRI. The following process is used when configuring SIP Gateway IP addresses for the first time, and must also be followed when changing (editing) the configured SIP Gateway IP addresses for the XRI.

Prerequisites: Obtain the Device Public Key for this XRI Device. The process is described in a subsequent sub-section.

Procedure:

1 Send the XRI Public Key to Motorola Solutions Customer Service along with the IP Address (or addresses) of the SIP Gateway Device(s) that is used with the XRI.

The number of IP addresses needed varies from 1 to 4, depending on the type of SIP Gateway device that is used. Include the SIP Gateway device manufacturer and model name in the communication with customer service. Send the IP Address (or addresses) exactly as they should appear in the Host Address field(s) of the SIP Gateway Config tab. See Host Address on page 62 for more information. Motorola Customer Service provides a Key Manager file containing the encoded IP address (or addresses) and the SIP Gateway device type.

2. The Key Manager file must be uploaded to the XRI device as described in a subsequent sub-section.

   After uploading the file, you are asked to confirm the SIP Gateway device type and the IP Addresses.

3. Configure the IP Addresses (or addresses) into the Host IP Address field (or fields) on the SIP Gateway Config Tab by selecting from the IP address (or addresses) encoded in the uploaded Key Manager File.

6.3.1
Copying the XRI Public Key

Follow the procedure to copy the XRI Public Key so that it can be pasted into the e-mail or other communication that is sent to Motorola Customer Service when obtaining a Key Manager File for this XRI. Due to the length and complexity of the XRI Public Key, the copy and paste method is recommended. For more information on obtaining a Key Manager File, see Obtaining and Using a Key Manager File on page 77.

Procedure:

1. Click **Device Control** in the **Menu** Bar.
2. Click **Key Manager** in the **Settings** menu.
3. Click **Device Public Key** in the **Key Manager** sub-menu.

   The application displays an informational window containing the Public Key for the connected XRI Interconnect Gateway device. The Public Key consists of several groups of alphanumeric characters separated by dashes.

4. Carefully move the cursor over the XRI Public Key to highlight all characters in the string, right-click on the highlighted string, and select **Copy** from the right-click menu.

   The highlighted characters are placed on the Windows clipboard.

5. To close the message containing the XRI Public Key, click **OK**.
6. Paste the XRI Public Key character string from the Windows clipboard into the desired e-mail or other document.

6.3.2
Uploading the Key Manager File

Follow the procedure to upload the Key Manager file.

Prerequisites: Obtain the Key Manager file for this XRI Interconnect Gateway device and place it in a known location on the PC or network. For more information, see Obtaining and Using a Key Manager File on page 77.

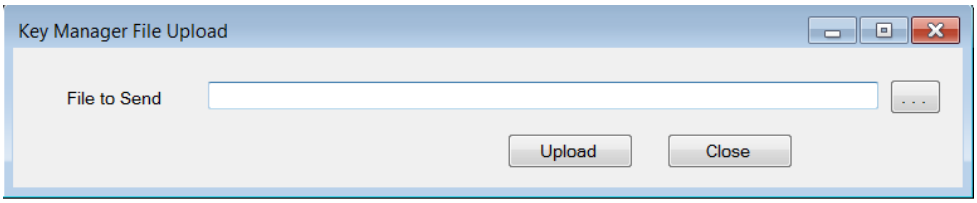
When and where to use:

Procedure:

1. Click **Device Control** in the **Menu** Bar.
2. Click **Key Manager** in the **Settings** menu.
3. Click **Key Manager File Upload** in the **Key Manager** sub-menu.

   The **Key Manager File Upload** window displays.

Figure 27: Key Manager File Upload window



4 Click the browse ... icon and navigate to the directory containing the file.

5 Select the file to be uploaded and click **Open**.

NOTICE: Key Manager files have a file extension of `.xkm`.

When the upload completes, the application displays a confirmation message containing the SIP Gateway type and the IP Address (or IP Addresses) contained in the Key Manager File.

6 Do one of the following:

- To confirm that the displayed information is correct for your SIP Gateway device, and to reboot the XRI Interconnect Gateway, click **Yes**.
- If the information is incorrect or to cancel, click **No**.

7 Optional: If the application displays an error message after uploading the Key Manager file, or if the information displayed in the confirmation message is not correct, perform the following checks prior to contacting Motorola Solutions customer support.

a If connecting to a SIP Digital Telephony Gateway, the XRI must be enabled for the Connect Plus SIP Telephony feature prior to uploading the file.

b Check to verify that the correct Key File was uploaded.

c Check to verify that the IP Address & SIP Gateway device information provided to Motorola Solutions Customer Service was correct.

6.3.3
Launching the Feature Status Window

When and where to use: The Feature Status window shows the purchasable feature(s) for the connected device, and whether or not any feature on the list is presently enabled. It can also be used to enable additional features for the device.

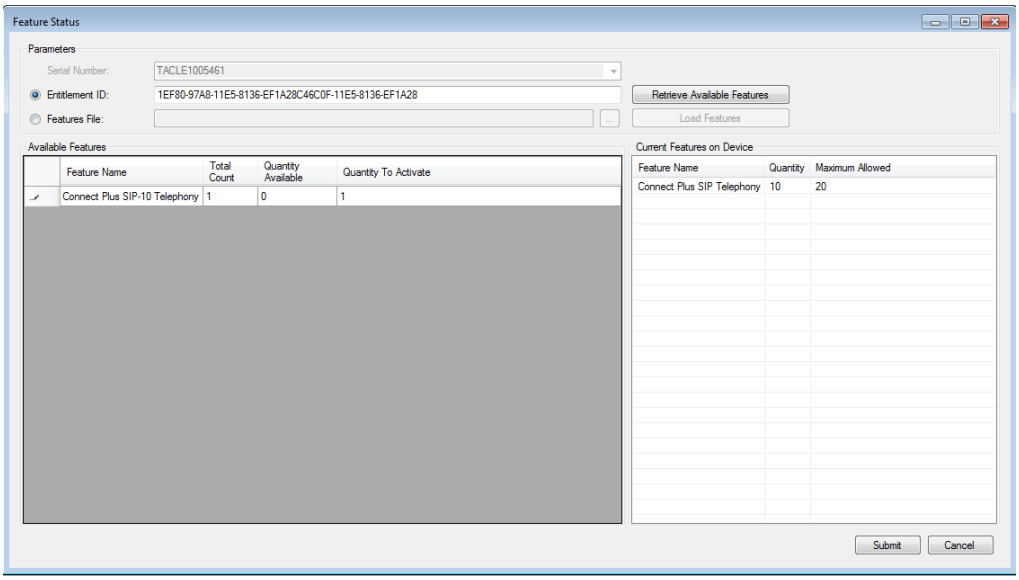
Procedure:

1 Click on **Settings** in the Menu Bar.

2 Click on **Features** within the menu.

The **Feature Status** window appears. The following image shows the **Feature Status** window with full application connectivity after retrieving available features from a valid Entitlement ID.

See Enabling Features with Full Application Connectivity on page 82 for further information.



3 When finished, click **X** or **Cancel** to exit the **Feature Status** window.

6.3.3.1
Feature Status Window Overview

The Feature Status window contains three sections.

Section	Description
Parameters	Displays the Serial Number for the connected device (or allows Serial Number Input when not connected to the device). It also contains fields and buttons used when enabling new features for the device. See Enabling Features with Full Application Connectivity on page 82 and Partial Application Connectivity on page 83 for more information.
Available Features	A grid that displays available features, based on the Entitlement ID displayed in the Parameters section. The grid is labeled **Features in File** if the features are loaded from a previously saved features file. See Partial Application Connectivity on page 83 for more information. There are four fields under **Available Features**: **Feature Name** The name of the feature for which other data on the same row applies. **Total Count** The number of licenses originally secured for the named feature on this Entitlement ID.

Table continued…

	Quantity Available The number of licenses that are still available for the named feature on this Entitlement ID. **Quantity to Activate** Used to enter the number of licenses that you wish to activate for this feature on the connected device. If the Feature Name indicates that the license is a “pack”, or if the name uses other words or numbers to denote more than one, then each license will enable multiple instances of the feature.
Current Features	A grid that displays the status of features currently available for this device. The grid is labeled **Features currently registered to Serial Number** if the current feature list is obtained from the feature licensing server rather than from the device. See Partial Application Connectivity on page 83 for more information. This section consists of three fields: **Feature Name** The name of a device feature. The other columns on the same row provide information regarding the status of the named feature. The feature name displays in either black or blue text. See Enabling Features with Full Application Connectivity on page 82 for more information **Quantity** Shows the current status of the named feature. Zero (0) indicates the feature is not enabled for this device. One (or greater) indicates that some level of feature support is currently enabled. To determine whether the feature is enabled for its maximum allowed capacity, compare “Quantity” with “Maximum Allowed”, as described in the following field. **Maximum Allowed** Shows the maximum allowed capacity of the named feature. When “Maximum Allowed” is equal to “Quantity”, the feature is currently enabled for its maximum capacity. When “Maximum Allowed” is greater than “Quantity”, the feature is not currently enabled for its maximum capacity. The feature capacity can be increased after obtaining an Entitlement ID with available licenses.

6.3.3.2
Viewing Features

Procedure:

1 Launch the **Feature Status** window while connected to the device.

2 View the Current Features pane.

Each populated row of Current Features displays the status of one available feature for the connected device. Refer to Feature Status Window Overview on page 80 for more information.

6.3.3.3

Full Application Connectivity

Full application connectivity is the recommended method to enable features. This method enables features when the application is simultaneously connected to both the device and the feature licensing server and it is recommended because it allows the application to perform important checks that reduce the possibility of user input error.

Whenever the **Feature Status** is screen is launched from the **Menu Bar** while connected to a device, the application attempts to establish communication with the feature licensing server.

If the application detects that there is no connection to the feature licensing server (or some other problem), it displays a message that explains the problem and provides three buttons (**Yes**, **No**, and **Cancel**). Please read the message carefully before clicking the most appropriate button to continue.

If the application cannot connect to the feature licensing server, you can view current features, but you cannot enable new features unless you have previously completed the steps outlined in the first sub-section of Partial Application Connectivity on page 83.

IMPORTANT: It is strongly recommended to enable features when there is full application connectivity to both the device and the feature licensing server. If a temporary network problem prevents connection to the feature licensing server, investigate and resolve the connectivity issue. After resolving the connectivity issue, follow the steps outlined in Enabling Features with Full Application Connectivity on page 82.

6.3.3.3.1

Enabling Features with Full Application Connectivity

Prerequisites:

- Obtain an Entitlement ID that contains one or more licenses for the desired feature(s).
- Connect to the desired device with Administrator Role login. The Network Manager must be able to access the internet while connected to the desired device.

When and where to use:

WARNING: Submitting features as described in this section causes the device to reboot.

Procedure:

1 Launch the **Feature Status** window.

2 Click the **Entitlement ID** field, if not already selected.

3 Copy the Entitlement ID from the source document and paste it into the **Entitlement ID** field.

4 Click the **Retrieve Available Features** button.

This requires an internet connection and may take a few seconds.

If the application is able to retrieve information on available features, it loads this information into the **Available Features** pane.
If the application is not able to retrieve this information, it displays an error message.

5 View the **Available Features** pane.

Each populated row contains information on a feature available with this Entitlement ID.

6 In **Quantity to Activate**, enter the number of licenses (for the named feature) that you wish to activate for this device. If the Feature Name indicates that the license is a “pack”, or if the name uses other words or numbers to denote more than one, then each license will enable multiple instances of the feature. Take this into account when entering the number of licenses to activate.

IMPORTANT: If the Feature Name is displayed with black text in the **Current Features** pane, then the number of feature instances activated via the **Available Features** pane is added to the number of feature instances displayed in the **Current Features** pane (after submitting the change and completing the operation). If the Feature Name is displayed with blue text in the **Current Features** pane, then the number of feature instances activated via the **Available Features** pane replaces the number of feature instances displayed in the **Current Features** pane (after submitting the change and completing the operation).

NOTICE: If the application detects a problem with the number entered into **Quantity to Activate**, it displays an exclamation point icon next to the feature name in the **Available Features** pane. Place the cursor over the icon to view a message with information about the problem.

If you are enabling multiple features for the connected device from the same Entitlement ID, repeat this step for each desired feature.

7 Click the **Submit** button.

All submitted changes must be accepted for any change to be applied

If a change cannot be accepted, the application displays an error message with information about the problem

If the changes in the **Quantity to Activate** column are accepted, the application provides a reboot warning message. Perform one of the following actions:

- Click **Yes** to apply the changes and reboot the device.
- Click **No** or **Cancel** to abort the operation.

6.3.3.4
Partial Application Connectivity

This is another alternative method to enable features. However, whenever possible, it is strongly recommended to enable features while the application has full, simultaneous connectivity to both the device and the feature licensing server and by following the steps described in Enabling Features with Full Application Connectivity on page 82.

In some cases the network topology may not allow the application to simultaneously connect to the both the device and the feature licensing server. In this event, enabling features becomes a two part process as described in the following sub-sections. The first part of the process is to connect to the feature licensing server and to create a special features file. The second part is to connect to the desired device, to upload the file, and to submit the features to the device.

6.3.3.4.1
Connecting to the Features Server and Creating Features Files

The first part of the process is to connect the application to the feature licensing server and to create a special file that can be used to enable features for the device. For this first part of the process, the application must be able to connect to the public internet, but it does not need to connect to the device.

Prerequisites:

- Obtain an Entitlement ID that contains one or more licenses for the desired feature(s).

- Know the Serial Number of the device for which you are enabling the feature.
- Know the type of device for which you are enabling the feature (e.g. XRI, XRC or XRT). Not every device type supports every feature.
- The PC should be running the current release version of the MOTOTRBO Connect Plus Network Manager.
- The application must be able to access the internet.

Procedure:

1. Open the **Feature Status** screen when the Network Manager application is running, but not connected to a device.

   Recommended method for launching the application: Locate and double-click the shortcut called **Offline Mode - MOTOTRBO Connect Plus Network Manager**. The shortcut can be accessed via **Start Menu**>**All Programs**>**Motorola Solutions**. The Network Manager launches in offline mode.

2. Click on **Settings>Features**.

   The application attempts to automatically connect to the feature licensing server. If the application cannot connect to the feature licensing server, a message is displayed. In that event, the steps described in this sub-section cannot be performed until the connectivity problem is resolved.

3. In the **Serial Number** field, enter the Serial Number of the device on which the features should be enabled.

   IMPORTANT: Enter the Serial Number carefully. The application is not able to perform validation on the entered number. Entering a Serial Number (and then subsequently saving to a features file) incorrectly will require Customer Service to correct the license.

   When entering a Serial Number from the keyboard, alpha characters should be entered as upper case. As an alternative, select the desired serial number from the drop down list, if applicable. (If this copy of the application has previously connected to a device, its serial number is displayed in a drop-down list.)

4. Click **Get Currently Registered Features**.

   If there are any features currently registered in the feature licensing server for the inputted serial number, they will be displayed in the in the panel called **Features currently registered to Serial Number**. For more information on the columns in this panel, see Viewing Features on page 81.

   Any features activated on the device associated with this serial number prior to Connect Plus System Release 1.6 (and not recorded on the Feature Licensing server) will not display in Features currently registered to Serial Number.

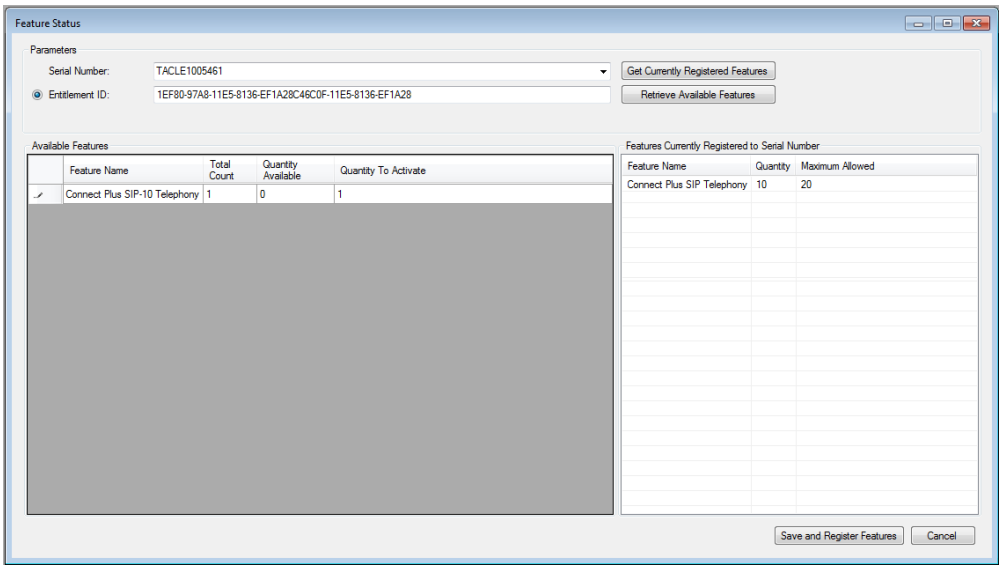
5. Perform one of the following actions:
   - If using an Entitlement ID to add new features, proceed to step 6.
   - If creating a file that can be used to restore the currently registered features of the device only, proceed to step 9.
6. Copy the Entitlement ID from the source document and paste it into the **Entitlement ID** field.
7. Click **Retrieve Available Features**.

   This requires an internet connection and may take a few seconds.

   The application will retrieve information on available features. If the application is able to retrieve information on available features, it loads this information into the **Available Features** pane. If

the application is not able to retrieve this information, it displays an error message. The following image shows the **Feature Status** screen in offline mode after retrieving available features. Each populated row of Available Features contains information on a feature available with this Entitlement ID.

Figure 28: Features Screen in Offline Mode



8 In **Quantity to Activate**, enter the number of licenses (for the named feature) that you wish to activate for the device that corresponds to the entered Serial Number.

If the Feature Name indicates that the license is a “pack”, or if the name uses other words or numbers to denote more than one, then each license will convert to multiple instances of the feature when creating the features file (as described in a subsequent step). Take this into account when entering the number of licenses to activate.

If the application detects a problem with the number entered into Quantity to Activate, it displays an exclamation point icon next to the feature name in the **Available Features** pane. Place the cursor over the icon to view a message with information about the problem.

9 Click **Save and Register Features**.

This launches the **Save As** file dialogue, with a default file name and directory. It is recommended to use these defaults, but the file name and/or directory can be changed if necessary.

10 Make a record of the file name and directory (for future reference).

The saved file will be used to activate features on the device, as described in the next sub-section.

11 Click the **Save** button in the file dialogue.

The application conducts some checks. If the application does not encounter any problems, it displays a message advising that the features will be activated on the server.

12 Perform one of the following actions:

- To proceed, click **Yes**.
- To abort the operation, click **No** or **Cancel**.

13 When finished, click the **X** to close the application.

6.3.3.4.2

Connecting to the Device and Uploading the Features File

The second part of the process is to connect the application to the desired device, to upload the features file, and to submit (activate) the features.

Prerequisites:

- Obtain the features file that was created in the process described in the previous sub-section. The file can only be used with that the device whose Serial Number matches the Serial Number that was inputted when the file was created.
- Connect to the desired device with Administrator Role login.
- Launch the **Feature Status** window.

When and where to use:

WARNING: Submitting features as described in this section causes the device to reboot.

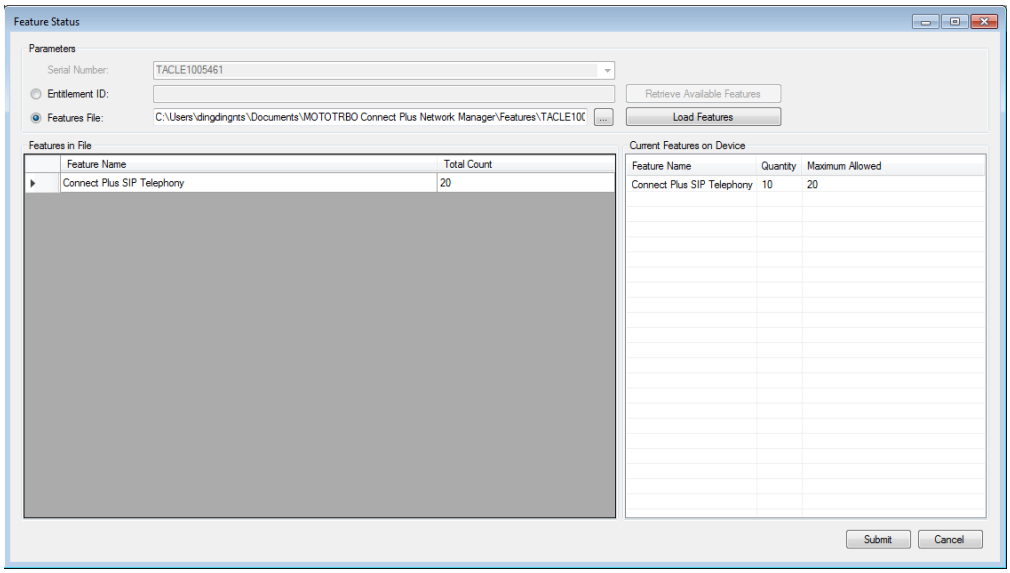
Procedure:

1. Click the **Features File** bullet, if not already selected.
2. Click the **Browse** icon to launch the **Select a Features File** file dialogue.
3. Locate and select the previously saved features file (that was created for the Serial Number that matches the connected device) and click **Open**.

   The path and file name displays in the **Features File** field.

4. Click **Load Features**.

   The features listed in the saved file are displayed in the **Features in File** pane as shown in the following image.



Each populated row displays information on a feature:

Feature Name
The name of the feature for which other data on the same row applies.

Total Count
The total number of instances of the named feature that will be enabled in the device after submitting the change.

5 Click **Submit**.

6 Perform one of the following actions:

- To apply the changes and reboot the device, click **Yes**.
- To abort the operation, click **No** or **Cancel**.

6.4 Logs

This section explains the viewing and management of event logs.

6.4.1 Downloading Call Logs

Procedure:

1 Click on **Logs** in the Menu Bar.

2 Select **Call Log** from the Logs menu.

3 Select **Download Call Log** from the sub-menu.

The Save As window displays.

4 Use the Save As window to select the location where the Call Log should be saved.

5 In the **File Name** field, enter a name for the Call Log, if desired (or accept the default file name created by the XRI).

6 To proceed with the download, click **Save** or to cancel the download, click **Cancel**.

If you select Save, the Network Manager displays a progress bar during the download.

6.4.2 Clearing Call Logs

Procedure:

1 Click on **Logs** in the Menu Bar.

2 Select **Call Log** from the Logs menu.

3 Select **Clear Call Log** from the sub-menu.

The Network Manager displays a warning message that you are about to clear the Call Logs on the XRI.

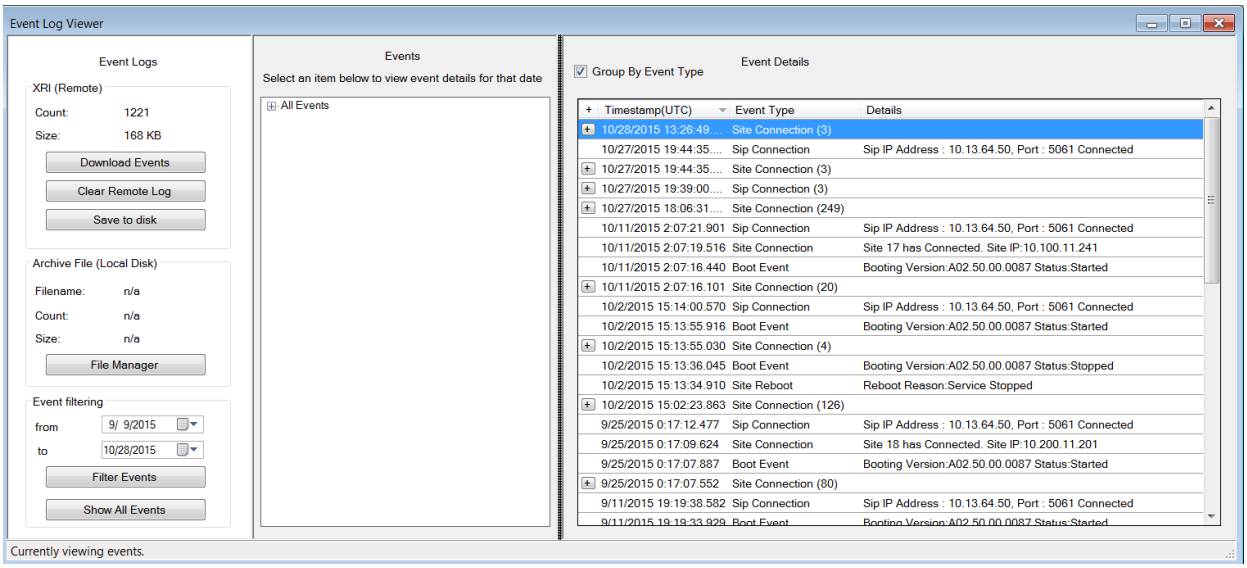
4 Perform one of the following actions:

- To clear the Call Logs, click **Yes**.
- To cancel the operation, click **No** or **Cancel**.

6.4.3
Event Log Viewer

The event log viewer has three panels namely Event Logs, Events and Event Details.

Figure 29: Event Log Viewer Window



Event Logs

On the Left hand side of the Event Log Viewer is the Event Logs panel. Within this panel, event logs are loaded from the device or local PC. Event filtering is also available to aid searching large event logs.

XRI (Remote)

Count: Displays the number of events currently on the device.

Size: Displays the Event Log file size on the device in Bytes.

NOTICE: When the Event Log archive exceeds the maximum allowed size (which can vary by device type and release) the oldest entries are automatically purged. For this reason, it is recommended to: (a) download events on a regular schedule and (b) clear the Log after downloading events.

Events and Events Details

The **Events** panel is first populated with information in a collapsed form. Click the **+** next to **All Events** to see a list of one or more years in which the downloaded events were recorded. The next level will be the month(s) and then the day(s) of the month. The results are displayed in the **Event Details** panel as the different headings are selected.

The Event Details panel contains a checkbox called **Group By Event Type**. When the box is checked, consecutively listed events of the same Event Type are collapsed into a single entry. The number of events contained within the collapsed entry is shown in parenthesis next to the **Event Type**. Click **+** to the left of an entry to show all of the consecutively listed events of the same Event Type. To collapse the events into a single entry again, click the **-** to the left of an entry.

6.4.3.1
Launching the Event Log Viewer

Procedure:

1 Click on **Logs** in the Menu Bar.

2 Select **Event Log** from the Logs menu.

The Event Log Viewer displays as shown in Figure 30.

6.4.3.1.1
Downloading Events

Procedure:

1 Click on **Logs** in the Menu Bar.
2 Select **Event Log** from the Logs menu.
3 The Event Log Viewer displays.
4 In the Event Log panel click the **Download Events** button.
5 Event information displays on the Event and Event Detail panels.

6.4.3.1.2
Clearing Event Logs

Procedure:

1 Click on **Logs** in the Menu Bar.
2 Select **Event Log** from the Logs menu.

The Event Log Viewer displays.

3 In the Event Log panel click the **Clear Remote Log** button.
4 In the Warning! dialog box click **Yes** to clear all events.
5 Event information, if downloaded, will be cleared on the Event and Event Detail panels.

6.4.3.1.3
Saving to Disk

Procedure:

1 From the **Logs** menu bar, select **Event Log**.

The Event Log Viewer window appears.

2 In the Event Log panel click the **Download Events** button.

Event information is displayed on both the Event and Event Detail panels.

3 Click the **Save to disk** button.

The file is saved in the MOTOTRBO Connect Plus Network Manager folder in the following format: EAmm-dd-yy-hh.mm.ss, where mm-dd-yy is the date and hh.mm.ss is the time. The **Save to disk** button is grayed out until events are downloaded from the device.

6.4.3.1.4
Archive File (Local Disk)

This area allows access to saved event logs.

6.4.3.1.4.1
Loading Archive File

Procedure:

1. From the **Logs** menu bar, select the **Event Log Viewer** option.

   The Event Log Viewer window appears.

2. In the Event Log panel click the **File Manager** button.

   Event Archive File Manager window appears.

3. Click the file name of the event archive to be displayed.
4. Click the **Load Selected** button.

   Event information is displayed on both the Event and Event Detail panels.

6.4.3.1.4.2
Deleting Archived File

Procedure:

1. From the **Logs** menu bar, select the **Event Log Viewer** option.

   The Event Log Viewer window appears.

2. In the Event Log panel, click the **File Manager** button.

   The Event Archive File Manager window appears.

3. Click the file name of the event archive to be deleted.
4. Click the **Remove Selected** button.

   A message box asking to confirm the deletion appears.

5. Click **Yes** to delete the event archive.
6. To close the Event Archive File Manager dialog box, click the "X" in the upper right corner.

6.4.3.1.4.3
Filtering Events

Procedure:

1. Click on **Logs** in Menu Bar.
2. Click on **Event Log Viewer** in the menu.

   This displays the Event Log Viewer screen.

3. Do one of the following:
   - In the Event Log panel, click the **Download Events** button.
   - In the Event Log panel, click the **File Manager** button and load the saved archived file.

   Event information is displayed on the Event and Event Detail panels.

4. Select a beginning date from the "from" field.
5. Do one of the following:
   - Select an ending date for the "to" field and click on **Filter Events**.

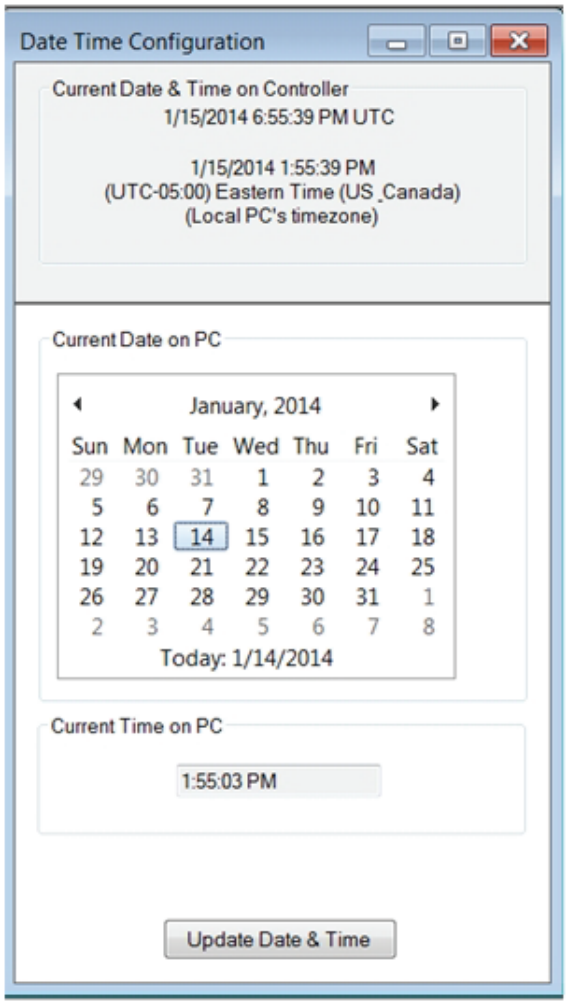
- Click on the **Show All Events** button to see all events.

The selected range of events are shown in the Event Details panel.

6.5 Date Time Configuration

It is necessary to set the time on the XRI because entries in the XRI Call Log and the XRI Event Log include the time and date.

Figure 30: Date Time Configuration Screen



The top (gray) portion of the screen shows the current date and time on the connected device. The device does not use local time. Instead, it uses Coordinated Universal Time (UTC), an international standard that correlates with time at the Royal Observatory in Greenwich, England. This is the time displayed on the top line in the gray box. On the second line in the gray box, the device software adjusts the hour to reflect the hour and time zone on the PC's clock at time of connection. The minutes and seconds are derived form the current time of the device

The bottom (white) part of the screen shows the current date and time for the PC running the device software. This portion of the screen allows the user to transfer the PC's date and time to the device. If this device is set as the NTP Server, updating the date and time on the device will also affect all sites that are programmed to look at this site as the NTP Server. Those sites will receive the updated date and time the next time they request a time update. Due to the normal operation of the NTP Protocol, it may require multiple updates to bring the Server and Client into synch if the two clocks are far apart to

begin with. For this reason, it is advisable to set the time on the NTP Client during initial set-up as described in the next section. Although the NTP Client's time will be adjusted by the NTP Server, the time synchronization will occur more quickly if the time on the two clocks is within a few minutes of one another to begin with.

IMPORTANT: When transferring the PC's date and time to the device (by following the procedure described in the next section), the device software will correctly adjust the PC's date and time to UTC provided that:

1. the date and time settings of the PC are accurate for the time zone that is configured for on the PC **Date and Time Properties** screen and
2. the **Automatically adjust clock for daylight savings changes** box is also configured correctly on the PC's **Date and Time Properties** screen.

If it should become necessary to modify either of these settings (time zone and/or daylight savings checkbox) on the PC, make the PC adjustments and then reconnect to the device prior to updating the time.

6.5.1
Enabling Confirmed Transmission

When Generic Data Call is enabled, this box determines whether the controller utilizes the confirmed or unconfirmed transmission method when sending Generic Data Call packets to this subscriber radio.

Procedure:

Do one of the following:

- Check this box to instruct the controller to utilize confirmed data transmission.
- Uncheck this box to instruct the controller to utilize unconfirmed data transmission.

6.5.2
Updating Date & Time Using PC Time

This operation will transfer the date and time of the PC to the device, and will initiate device reboot. The application will adjust the date and time of the PC to UTC prior to sending it to the device.

Prerequisites:

- Verify that the date and time settings of the PC are accurate for the time zone that the PC is configured for on the PC's "Date and Time Properties" screen.
- Verify that "Automatically adjust clock for daylight savings changes" is configured correctly on the "Date and Time Properties" screen of the PC.

When and where to use:

NOTICE: This setting is necessary for the application to accurately translate the date and time of the PC to UTC. However, it is important to understand that the device does not adjust its UTC time for Daylight Savings Time changes.

Procedure:

1. Click on **Settings** in Menu Bar.
2. Select **Date & Time** from the Settings menu.

   The Date & Time Configuration screen displays.
3. Click on the **Update Date & Time** button on the lower portion of the screen.

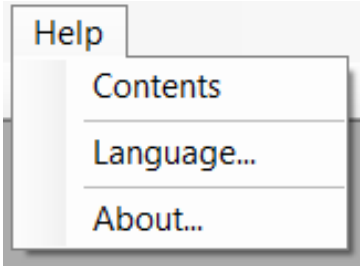
   The application automatically adjusts the hour to UTC when sending the time to the device.

6.6

Application Help Menu

This application comes with a Help file. The Help file is accessible from the **Help** menu.

Figure 31: Help Menu Drop Down Menu



6.6.1

Launching the Application Help File

Follow the procedure to launch the Application Help File.

Procedure:

1. Click on **Help** in the **Menu** Bar.
2. Click on **Contents …** within the menu.

   The default web browser displays the Help page in a new tab.

6.6.2

Selecting the Application Display Language

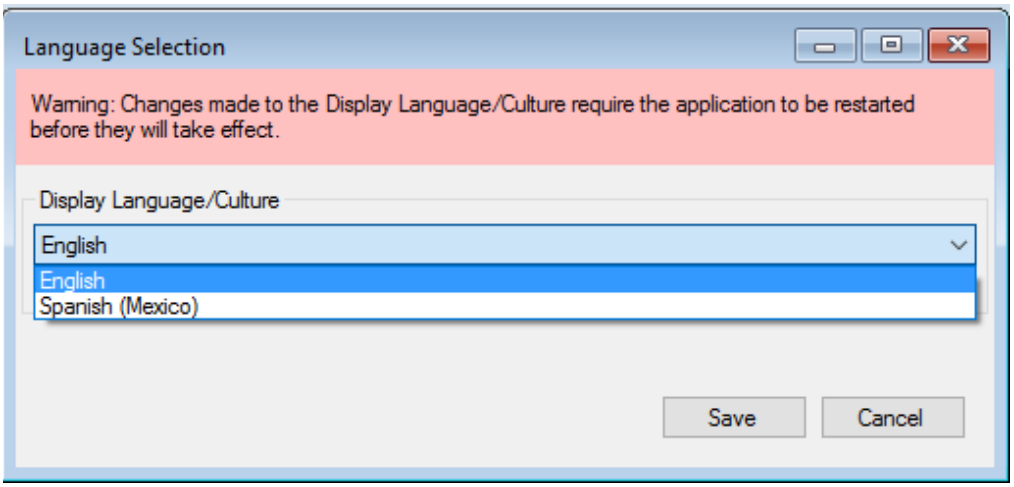
The application can be configured to display in English, or in the same language as the Operating System of the computer (if other than English and supported by the application).

Procedure:

1. Click **Help** in the **Menu** bar.
2. Click **Language ...** within the menu.

   The **Language Selection** screen displays.

Figure 32: Language Selection Screen



3 Click the arrow under **Display Language/Culture**.

The application displays a list of one or two languages.

NOTICE: For some computers, English is the only available language.

4 Select the desired Language/Culture from the list and click **Save**.

5 Manually close and then re-start the application to enforce the language change immediately.

NOTICE: The language change is automatically communicated to the Network Manager application the next time it is launched by the Network Manager Connection Tool.

Postrequisites: Changes to the Display Language/Culture require the application to be manually re-started before the changes take effect.

6.6.3
Launching the About Screen

Follow the procedure to launch the **About** screen.

Procedure:

1 Click **Help** in the **Menu** Bar.

2 Click **About…** within the menu.

The **About** window displays software version information and copyright information.

Chapter 7

Appendix A Determining the UPS Capacity

Procedure:

1. List all equipment to be protected by the UPS.
2. Write down the voltage and amperage for each device.
3. Multiply the voltage by the amperage of each device to calculate the Volt/Amps (VA).

   NOTICE: Some equipment may be marked with a power consumption measured in Watts. To convert Watts to VA, divide Watts by 0.65 (for a power factor of 0.65), or multiply by 1.54. The power factor refers to the relationship between the apparent power (volt-amps) required by the device and the actual power (watts) produced by the device.
4. Total the VA for all devices you want to protect with the UPS.
5. Multiply the subtotal found in Step 4 by 0.25. This number takes into account room for future growth. This growth factor allows for a 5% rate of growth for each year over a five-year period.
6. Add the results of steps 4 and 5 to get the Required VA. Now you can select the appropriate UPS model by choosing a model that has a VA rating at least as large as the Required VA that you calculated.

Motorola Solutions, Inc.
1303 East Algonquin Road
Schaumburg, Illinois 60196 U.S.A.

March 2016.

www.motorolasolutions.com/mototrbo

MN000960A01-BB