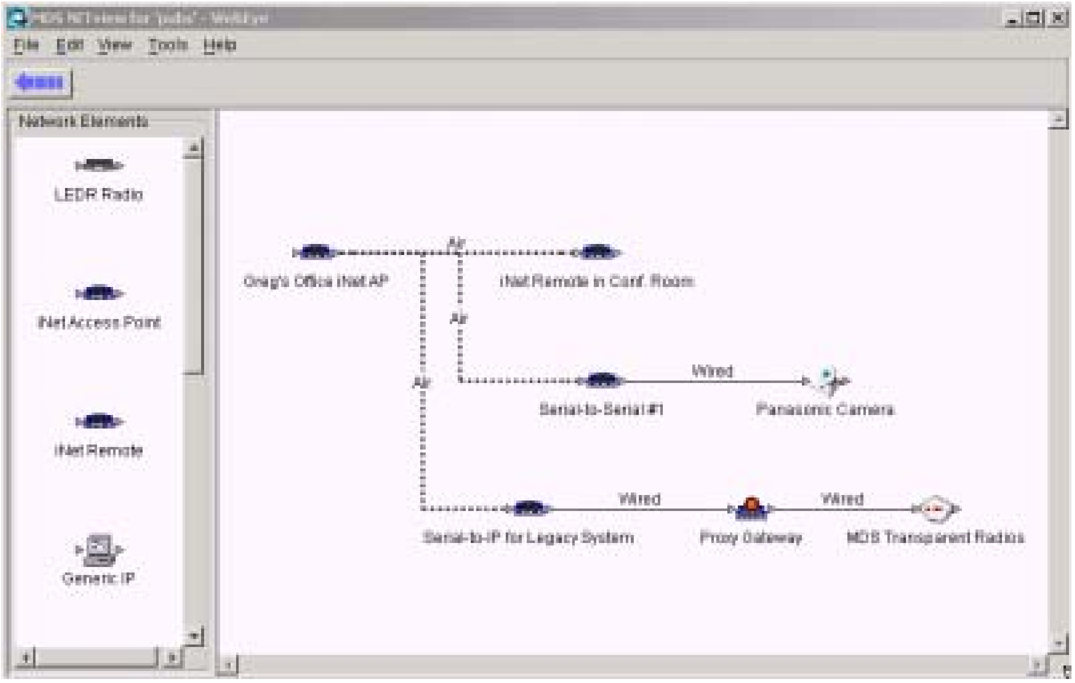
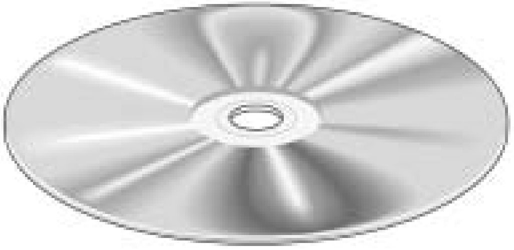
# Microwave Data Systems Inc.

# MDS NETview MS™





## NETWORK MANAGEMENT SOFTWARE

***Software Version 3.x***

MDS 05-2973A01, Rev. C
OCTOBER 2004

industrial/wireless/performance

MDS

Installation & Operation Guide

# *MDS NETview MS™ Quick Start*

MDS NETview software provides a central console from which an MDS radio network and associated IP-connected devices can be viewed in a hierarchal map perspective. NETview monitors the network for fault and performance information, and allows various maintenance tasks to be performed on MDS radios. Because NETview provides a client/server interface, multiple users can connect to the application simultaneously to perform network management.

Below are the basic steps for installing NETview and preparing it for usewith your network. Online help is also provided with the program. To access the online help file, simply select **Help** from the top menu bar.

## 1. Check computer and radio equipment for compatibility with NETview.

- The MDS NETview program is intended to operate on a Windows 2000, NT 4.0 or Windows XP platform. The entire NETview package can run on a single PC or multiple PCs using the client/ server interface.
- The NETview server and NETview client both require the Java Runtime Environment (JRE) to operate. (The JRE is provided on the NETview CD.)
- The program is designed primarily to service MDS IP-capable radios, such as the MDS iNET, entraNET and MDS LEDR Series. However, it is not limited to MDS products; any IP-based node may be monitored.

## 2. Install the software in the following order: 1) JRE, 2) the three servers, and 3) the two clients.

- A single CD is supplied that includes all necessary program files. (Prerequisite: JRE 1.3 and a TFTP Server must already be installed for executing the binaries and downloading/uploading configuration files to/from a device.)
- A CD browser guides the user through the installation process. Insert the disk and follow the on-screen prompts and dialog boxes to install the program elements in the desired directories. When installation is complete, the MDS NETview server and client programs appear on the **Start** menu.

## 3. Launch the program and create a system map.

- First time users will be prompted to create a system map following login. A network map is a graphical representation of the associated IP-connected devices in a hierarchal map perspective. Select a name for the map and ensure that you are in edit mode by verifying that **Lock Map** is displayed in the **File** menu.
- To add a Network element, simply click on an icon at the left side of the screen, and drag it over to the map area.
- You will be prompted for an IP address and SNMP community string password (optional) for the new element. After a connection to the new element is tested (automatically) , it is placed onto the map area. (If the connection fails, a dialog box allows you to delete it or keep it despite the connection failure.) Network elements can be “wired” together on the map to illustrate their position within the network. For MDS radios, enter “public” for the SNMP community string.

## 4. Select a system to monitor via the NETview screen.

- Device icons are highlighted with colors to indicate operating status as follows: **Clear** (no color)–No alarms detected; **Blue**–Information; **Green**–Warning; **Yellow**–Minor alarm; **Orange**–Major alarm; **Red**–Critical alarm.
- Click a device icon to view data for that unit. If the unit has associated devices, you can view their data also, by clicking the respective icons that will appear under the main radio.
- Many additional polling modes and viewing options are available. Consult online help for details.

# CONTENTS

## Copyright Notice

## MDS Quality Policy Statement

We, the employees of Microwave Data Systems, are committed to understanding and exceeding our customer's needs and expectations.

- We appreciate our customers' patronage. They are our business.
- We promise to serve them and anticipate their needs.
- We are committed to providing solutions that are cost effective, innovative and reliable, with consistently high levels of quality.

We are committed to the continuous improvement of all of our systems and processes, to improve product quality and increase customer satisfaction.

## ISO 9001 Registration

Microwave Data Systems adheres to the internationally-accepted ISO 9001 quality system standard.

## Manual Revisions

While every reasonable effort has been made to ensure the accuracy of this manual, product improvements may result in minor differences between the manual and the product shipped to you. If you have additional questions or need an exacs specification for a product, please contact our Customer Service Team using the information at the back of this guide. In addition, manual updates can often be found on the MDS Web site at www.microwavedata.com.

# 1.0 INTRODUCTION

MDS NETview MS™ is a Windows®-based program for remote management, control, and diagnosis of MDS wireless products and associated IP-connected devices. It provides a central console from which entire networks can be monitored for fault and performance information. It can also be used to perform various maintenance tasks, including downloads of new firmware or configuration files for MDS radios.

NETview is a client/server based program that allows multiple users (up to 10) to simultaneously connect to its server and perform network management. Figure 1 illustrates a typical multi-user layout. The program may be used from any location in a network, including authorized access via the Internet.

While the program is optimized for use with new-generation MDS products—such as the LEDR II, MDS iNET 900®, MDS entraNET®, it also supports other types of IP devices that communicate via industry-standard protocols including SNMP, TFTP, Telnet and Web server access.

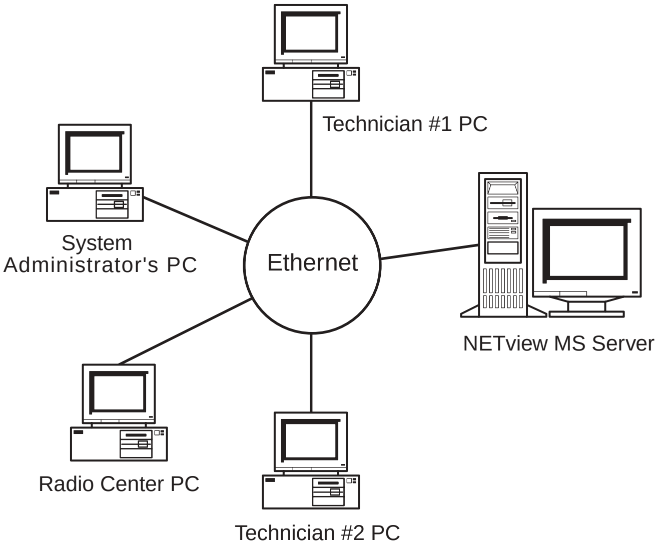


**Figure 1. NETview is a Client/Server based application. This allows multiple users to connect to its server for network management.**

## 1.1 Problem Detection & Logging

NETview helps users detect system problems and correct them before they become a threat to network operations. When problems are found, alerts are generated and displayed on the console screen. Alert messages can also be sent to remote maintenance personnel via e-mail or Internet-capable pagers. Should a trip to a field site become necessary, personnel will often know the likely cause of the problem and can prepare accordingly by bringing the correct service equipment or spares.

All SNMP traps from NETview are sent to the TrapTracker Viewer **Z?**[1] database (included with the NETview program suite) for historical archiving. Users can access this data at any time to examine the events leading up to a failure or change in network performance.

## 1.2 Types of Users

The NETview program is aimed at two primary users—SCADA/telemetry personnel at small to mid-sized organizations, and large-scale users in the Telecommunications industry. For SCADA/telemetry users, the program provides a stand-alone tool for essential, centralized network management functions with minimal cost and training requirements.

For large-scale users with hundreds, or even thousands of radios deployed, NETview offers a tool that can be integrated with existing network management products, such as HP Openview and TeMIP. In these cases, NETview will complement the generic functions of these products with MDS-specific applications.

For all users, NETview adds value by reducing network downtime and minimizing the need to send technicians out to the field. NETview also provides a rich set of tools specifically tailored for monitoring and controlling MDS radios.

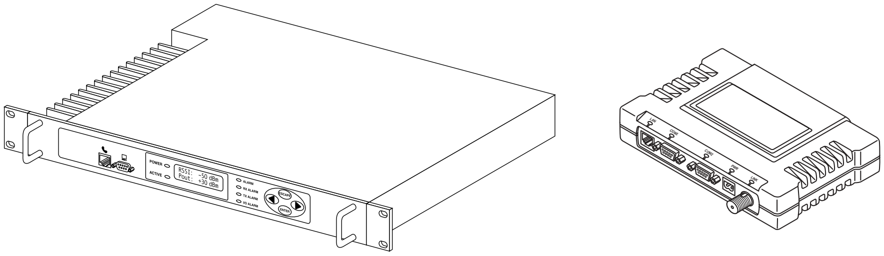


**Figure 2. Two examples of radios that are compatible with NETview—LEDR II (left) and MDS iNET 900 Transceiver. The program also functions with other IP-connected equipment.**

**NOTE:** While NETview provides valuable assistance in monitoring the performance of radio systems, it is not intended to be a substitute for calibrated test equipment.

[1]

## 1.3 Hierarchal Map Views

A key feature of NETview is its hierarchal map structure. Using realistic icons, routing lines and other symbols, the program displays the topology of a communications network in a graphical format. This allows users to gain a quick understanding of a system's layout at a glance. Figure 3 shows a typical network map created with the program. The appearance of maps is fully configurable using NETview's built-in tools.

**NOTE:** There may be slight differences between the screens shown here and those displayed in the NETview MS program, due to product changes made after the release of this publication.

Network maps can contain multiple layers of linked "submaps" represented by a unique icon on higher level maps. This hierarchal structure allows a virtually unlimited number of nodes (or radios) to be monitored through a single submap icon and is a very powerful feature of the program.

Submaps are opened by simply double-clicking the icon that represents them. By following the maps and submaps, users can navigate all the way down to individual radios or other IP nodes to obtain device-specific data.

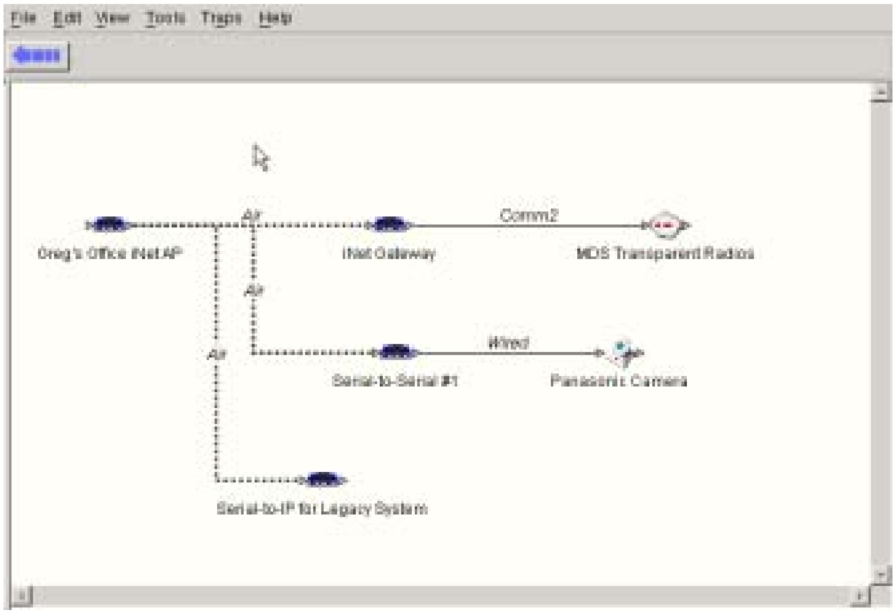


**Figure 3. Sample Network Map**

### Understanding NETview's "Layers"

For a better understanding of NETview's layering concept, it may be helpful to think of the various maps, sub-maps and individual icons as familiar geographic entities (World, continents, countries, states, and so on). A comparison of these terms in relation to the NETview program is offered in Table 1. While not all systems will require this many layers of mapping structure, NETview offers the scalability to accommodate a wide range of network architectures.

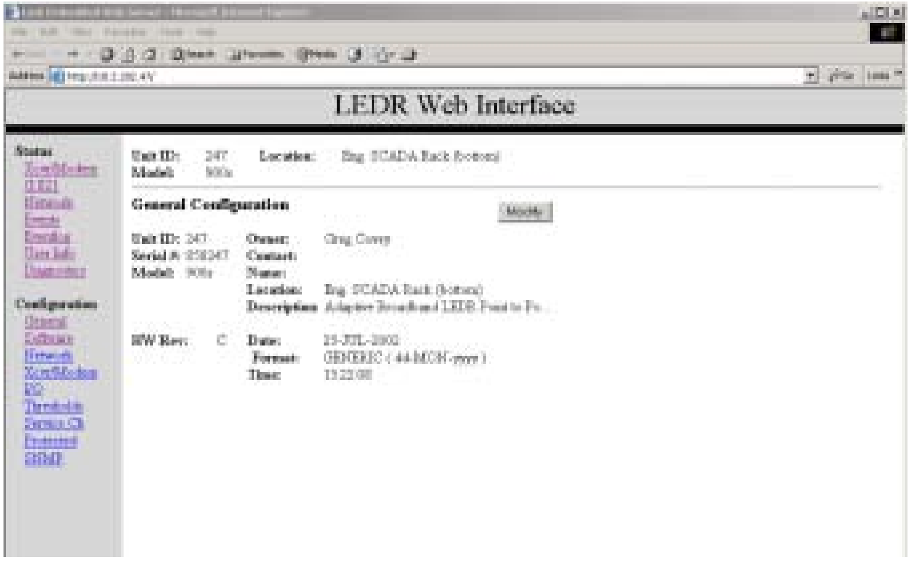
**Table 1. Comparison of NETview vs. Geographic Terms**

| NETview Item | Geographic Equivalent |
|---|---|
| Overall User Map | World |
| Individual Networks | Continents |
| Backbones | Countries |
| Spurs | States |
| Systems | Counties |
| Subsystems | Towns |
| Individual Radios/IP Devices | Houses |

## 1.4 Obtaining Device-Specific Data

NETview allows viewing key configuration and performance data for IP-reachable devices on a network, whether they be MDS radios or other "generic" IP devices. To access device information, you simply double-click the icon of interest.

In addition, the program supports new-generation MDS products such as the MDS LEDR II, MDS iNET 900 and MDS entraNET transceivers that include a built-in web server. The web server provides access to radio-specific data in a familiar web browser format, such as Internet Explorer or Netscape Navigator. A web browser can be launched from within NETview and provides a powerful management tool for network administrators and maintainers. Several radio parameters can be changed online by authorized users. For security, a password is required to make most changes. Figure 4 shows an example of a web browser screen containing data for an MDS LEDR radio.



Unit ID: 247 Location: Eng. SCADA Rack (bottom)
Model: 900x

General Configuration

Unit ID: 247 Owner: Greg Covey
Serial #: 258247 Contact:
Model: 900x Name:
Location: Eng. SCADA Rack (bottom)
Description: Adaptive Broadband LEDR Point to Po...

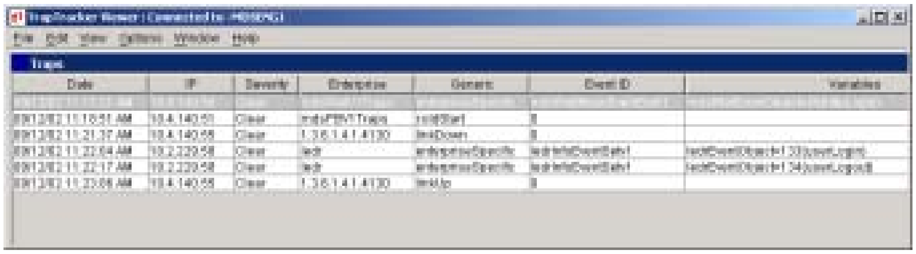
HW Rev: C Date: 25-JUL-2002
Format: GENERIC ( dd-MON-yyyy )
Time: 13:22:08

Figure 4. Typical Browser Screen

## 1.5 TrapTracker for Windows™ (TTW)

Working in conjunction with NETview, the TrapTracker for Windows program (included with the NETview program suite) has the capability to detect and store “traps” or “events” initiated by MDS radios. The traps are defined in an MDS enterprise-specific MIB (Management Information Base) file that provides a standard method for delivering alarms and permitting access to management information. Network events include alarms, logins, reboot commands and other information useful to administrators and maintainers who need to resolve system difficulties.

Prior to the release of NETview, users had to sort through hundreds, if not thousands, of SNMP codes from their radios to obtain the meaning of a trap. NETview simplifies this process by highlighting the node’s name field with an appropriate background color denoting the severity of an alarm. (See Viewing Alarms on Network Maps on Page 24.) Additionally, with TrapTracker Viewer, the alarm is displayed in a historical format that can be shared with other management systems using database tools such as ODBC. No knowledge of the raw SNMP codes is necessary to use this feature. Figure 5 shows a sample screen from the TrapTracker Viewer.



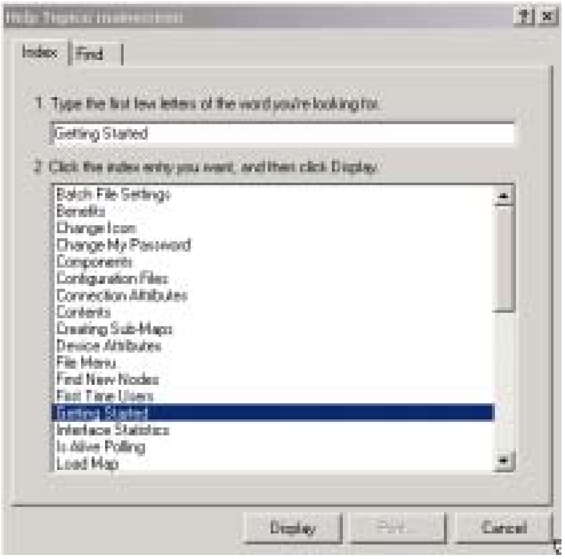
TrapTracker Viewer | Connected to: MDSNG1
File Edit View Options Window Help
Traps

| Date | IP | Severity | Enterprise | Generic | Event ID | Variables |
|---|---|---|---|---|---|---|
| [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] |
| 08/12/02 11:18:51 AM | 10.4.140.51 | Clear | mdsPBV1Traps | coldStart | 0 | |
| 08/12/02 11:21:37 AM | 10.4.140.55 | Clear | 1.3.6.1.4.1.4130 | linkDown | 0 | |
| 08/12/02 11:22:04 AM | 10.2.220.58 | Clear | iedr | enterpriseSpecific | iedrInfoEventSet1 | iedrEventObject.1.33(userLogin) |
| 08/12/02 11:22:17 AM | 10.2.220.58 | Clear | iedr | enterpriseSpecific | iedrInfoEventSet1 | iedrEventObject.1.34(userLogout) |
| 08/12/02 11:23:08 AM | 10.4.140.55 | Clear | 1.3.6.1.4.1.4130 | linkUp | 0 | |

**Figure 5. TrapTracker for Windows (TTW) Viewer Screen**

## 1.6 Online Help

NETview includes built-in help to assist you in understanding the functions of various menu buttons and screen items. The help files may be accessed from most screens by selecting **Help** from the top menu bar or by clicking the rectangular **Help** button at the bottom of a screen, as applicable. The main help files include an index tool (Figure 6) to assist you in finding a specific help topics.



1. Type the first few letters of the word you're looking for.

Getting Started

2. Click the index entry you want, and then click Display.

Batch File Settings
Benefits
Change Icon
Change My Password
Components
Configuration Files
Connection Attributes
Contents
Creating Sub-Maps
Device Attributes
File Menu
Find New Nodes
First Time Users
Getting Started
Interface Statistics
Is Alive Polling
Load Map

**Figure 6. Help File Index**

# 2.0 INSTALLATION

## 2.1 Computer Requirements

NETview's software elements are designed to run on the **Windows**® **2000** or **NT 4.0** operating systems. The computer must include adequate resources for running and storing the programs and their associated data files.

### NETview Server's PC

The server PC is where the NETview Server program resources are stored and "served up" to client users. The requirements for this PC are more demanding than for the NETview Client's PC because the server is doing the work of running the core application and handling requests from client users. Table 2 summarizes the server PC requirements.

Note that their are *three* server application programs that must be run on the server PC; TFTP Server, SNMP Server, and MDSnv (NETview) Server.

**Table 2. PC System Requirements for NETview Server**

| System Item | Preferred | Minimum |
|---|---|---|
| **Processor** | 600 MHz or faster Pentium® processor | 400 MHz Pentium® processor |
| **Operating System** | <——— Microsoft® Windows® 2000, or NT 4.0 ———> | |
| **Memory (RAM)** | 256 Megabytes (MB) | 128 MB |
| **Video** | 1024 x 768<br>24-bit high color | SVGA (800 x 600)<br>high-color 16-bit display |
| **Sound** | Sound card desirable (for alert sounds) | The program may be run without a sound card |
| **Hard Drive Space** | <———— 400 MB for program operation ————> | |
| **CD-ROM Drive** | Required for initial installation of the server program. | |
| **Network Connection** | Connection to network (direct, or via web) | |

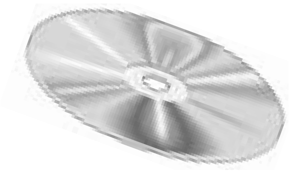
### NETview Client's PC

The NETview Client PCs require only a subset of the full NETview program suite to be installed. The requirements for this computer are not as demanding as those given for the NETview Server PC above. Table 3 lists the operating requirements for client computers running NETview.

**Table 3. PC System Requirements for NETview Client**

| System Item | Preferred | Minimum |
|---|---|---|
| Processor | 333 MHz or faster Pentium® processor | 166 MHz Pentium® processor |
| Operating System | Microsoft® Windows® 2000, NT 4.0, or XP | |
| Memory (RAM) | 64 Megabytes (MB) | 32 MB |
| Video | SVGA (800 x 600) high-color 16-bit display | 256 colors—Some degradation in display quality will result |
| Sound | Sound card desirable (for alert sounds) | The program may be run without a sound card |
| Hard Drive Space | <————— 100 MB for program operation —————> | |
| CD-ROM Drive | Required for initial installation of the client program. | |
| Network Connection | Connection to network (direct, or via web) | |

## 2.2 Software Included on the CD



The factory-supplied NETview CD contains all files necessary for installing the program on server and client PCs. The files consist of several software elements, some of which are *only* used when installing on a server PC. Below is a list of all program elements included on the disk:

- **Java Runtime Environment (JRE)—***Needed to run the program on both server and client PCs.*
- **SNMP TrapTracker for Windows—**Used to install the Simple Network Management Protocol (SNMP) TrapTracker for Windows Manager and Viewer programs. *Both elements are required for server PCs, but only the viewer is optionally required for client PCs.*
- **NETview Server—***Required only on the server PC.*
- **NETview Client—***For installation on any PC that requires the NETview console, including the server PC, if desired.*
- **MDS TFTP Server—**Trivial File Transfer Protocol server. *Required only on the server PC.*

## 2.3 Installing NETview

This section explains how to install the NETview program resources on server and client PCs. The software resources to be installed will depend on the type of PC on which the program is installed. The only decision you will need to make is choosing whether to install either the client or server packages, or both.

It is also possible to install the full NETview MS program on a single PC that will act as *both* a client and server. This common arrangement provides full NETview MS functionality, including the ability to serve the application to additional client PCs, either now or in the future.

**NOTE:** If re-installing or upgrading to a newer version of NETview, the program's installer utility will sense a previous installation and perform an uninstall routine, asking if you wish to keep the current map database.

In order for the server's database to be preserved when upgrading or re-installing NETview, Microsoft Access 2000 or later, must be installed on the host computer.

### Installation Steps

In the steps below, you will determine which software elements are required for a particular installation depending on whether it is for a client or server PC.

Follow these steps to install the NETview program:

a. Start Windows and close any applications that may be running on your PC.

b. Insert the NETview CD into the computer's CD-ROM drive. After a short time, the disk should begin to run automatically.

   If it does not, choose **Run** from the computer's **Start** menu, type the letter of the CD drive you are using, followed by a colon, backslash (\), and the word "setup." Example: **d:\setup**.

c. When NETview MS Installer's opening screen appears (Figure 7), click on **INSTALL SOFTWARE**.

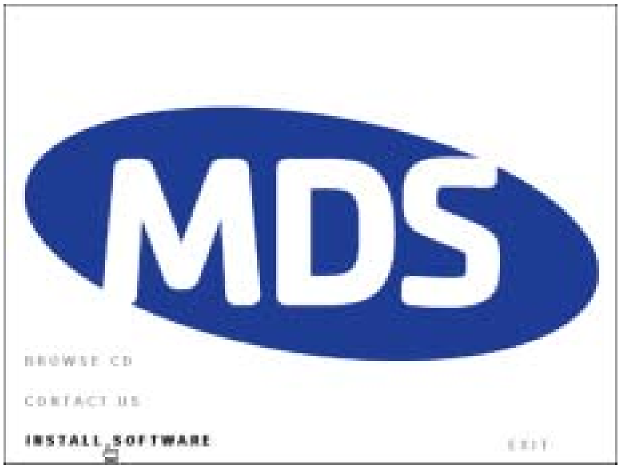
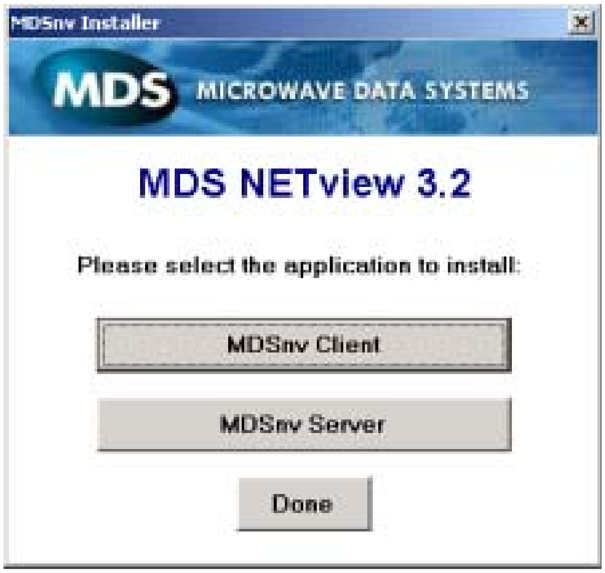


**Figure 7. NETview Opening Screen**

d. The installation screen (Figure 8) appears with a choice of two software applications to install; **MDSnv Client**, or **MDSnv Server.** Click once on the desired title to begin the installation.

- The first title, **MDSnv Client**, installs the Java Runtime Engine (JRE)—unless JRE is already installed, TrapTracker for Windows, and the core NETview MS client application.
- The second title, **MDSnv Server**, installs the Java Runtime Engine (JRE)—unless JRE is already installed, MDS NETview Server application, MDS Trivial File Transfer Protocol (TFTP) server, NETview MS client application, and TrapTracker for Windows (Manager and Viewer).



Please select the application to install:

**Figure 8. NETview Installation Screen**

e. Follow the remaining prompts and dialog boxes to finish the installation. During the installation process, various software elements will be automatically installed depending on whether the installation is for a client or a server.

f. When the installation is complete, click **Done** on the installation screen. The NETview MS program will appear on the computer’s **Start** menu. Optionally, you may create a shortcut for the program by right-clicking on the program name and selecting **Create Shortcut.**

**NOTE:** When the program resources are first installed, a **README** file appears on the screen. This file contains important release notes and other data, including information about the initial username and password. This file should be reviewed before using the program.

## 2.4 Connecting the PC to the Radio Network

With the NETview software installed on the computer, you are ready to connect the PC to the radio network so that it can be used to manage the enterprise. This is typically a straightforward process, requiring only an Ethernet cable connection between the rear panel of the PC and the LAN connector on the radio or gateway device (i.e., MDS gateNET). Figure 9 shows a typical cabling arrangement.

Additional detail/verification to be supplied.

**Figure 9. Typical Cabling Arrangement for NETview PC**

# 3.0 LAUNCHING THE SOFTWARE

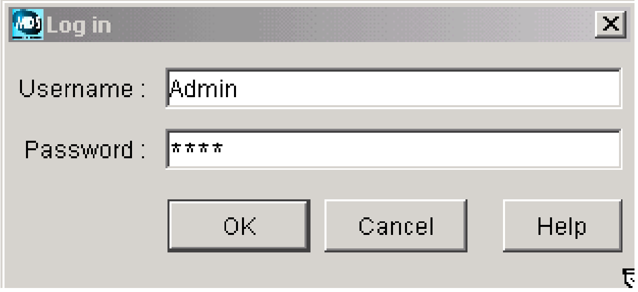
Launch the NETview MS program by selecting it from the Windows **Start** menu, or by double-clicking a shortcut icon. Follow the instructions below to log into the program and create a user account.

## 3.1 Initial Login—Required for First Time Users

NETview requires a login/authentication process before any program functions can be accessed. This provides security against unauthorized users, and allows individual privilege levels to be set in a multi-user environment.

When the program is first launched, the Login screen (Figure 10) appears, with entry boxes for a username and password. Enter the factory default username (**Admin**) and password (**Admin**) into each box. (Passwords and usernames are case sensitive.)

These default credentials are intended for initial login only and should be changed before leaving the computer. See *Establishing a User Account* below for instructions on how to do this.



Log in

Username : Admin

Password : ****

**Figure 10. User Login Screen**

Click **OK** to log in. A new NETview window opens with a menu bar at the top of the screen.

If this is the first time you are accessing the program, a message appears stating that “No default map is found” and you are asked to define one to use. See “Building a Network Map” on Page 15 to create a network map and define it as your default selection. Even if you are not yet ready to build a map, you must select some map (even a new, blank one) in order to edit users or perform other program functions.

## 3.2 Establishing a User Account

**NOTE:** After the creation of a personal user account and password, it is strongly recommended that the password for the **Admin** user account be changed, or the account deleted altogether. This prevents unauthorized users from gaining access to the program.

Follow the steps below to create a user account for yourself and any other users that require access to the NETview program.

a. Select **File>>User Maintenance>>Add New User** from the top menu bar as shown in Figure 11).

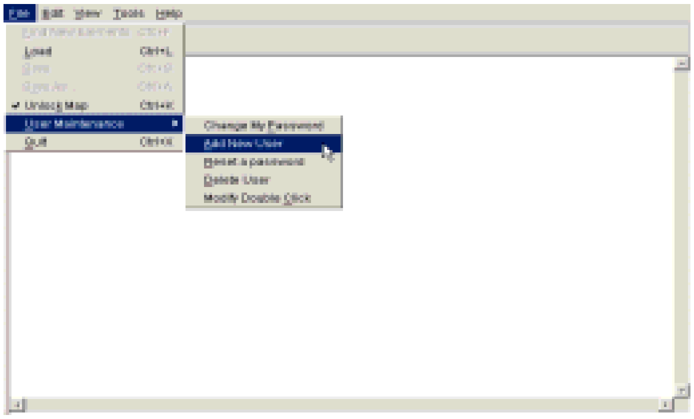


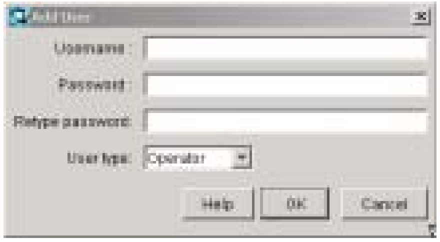
**Figure 11. Add New User Menu Selection**

b. When the **Add User** screen appears (Figure 12), enter a desired user name (up to 64 characters) and password (up to 16 characters). *Remember, passwords and usernames are case sensitive*.

---

**TIP:** For enhanced security, consider using a *misspelled* word for your password. This helps guard against sophisticated hackers who may use a database of common words (e.g., a dictionary file) to determine a password. Making your password as long as possible (up to 16 characters), and including one or more numbers will further improve its security.

---



User type: Operator

**Figure 12. Add New User Screen**

c. Open the drop-down **User Type** list, and highlight the privilege level that will be assigned to the new account as listed below:

- **Administrator—**All user privileges and features are granted.
- **Operator—**Has privilege to perform any NETview server operation on existing network elements, but may *not* modify network maps or user accounts other than their own.
- **Read-only User—**This is the most restrictive setting. The user may view network management data, but cannot change maps or object properties, upgrade firmware, or perform any other program modifications.

d. Click **OK**. A confirmation message appears indicating that the new account has been added to the list of users. Repeat the above steps for any additional user accounts that need to be created.

# 4.0 BUILDING A NETWORK MAP

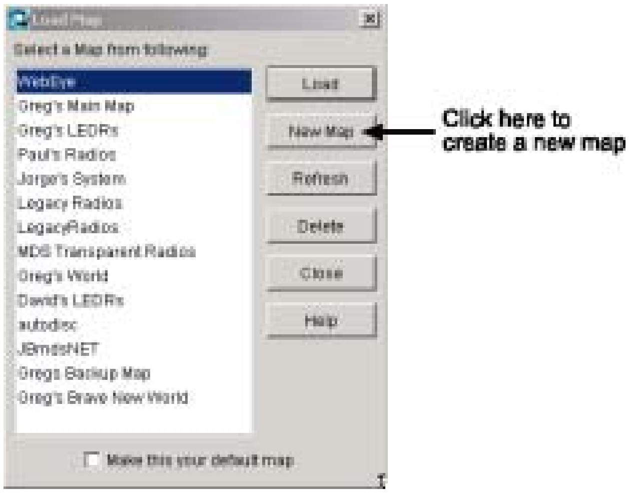
This section explains how to create a network map of your system using NETview's built-in tools. Network maps provide a graphical overview of the system being monitored, and are essential to the operation of the program. *No control or monitoring can be performed without first creating a network map.*

**HINT:** Prior to creating a network map in the NETview program, it is recommended that the layout of the system be drawn on paper for use as a planning aid—especially if it is a large system that includes sub-networks or links to other systems. The drawing should clearly identify all units in the network, their IP addresses and their relation to other pieces of equipment.

a. Verify that the map is unlocked. To do this, select **File** from the top menu bar and view the lock status. If the **Lock Map** command appears, the map is currently unlocked. If **Unlock Map** is displayed, select it (or enter Ctrl-K on the keyboard) to unlock the map.

b. With the map unlocked, select **File>>Load** to display the Load Map screen (Figure 13).

c. Click **New Map**. A dialog box appears for entering a name for the new map. Enter the desired name and click **OK**.



Select a Map from following:

WebEye
Greg's Main Map
Greg's LEDRs
Paul's Radios
Jorge's System
Legacy Radios
LegacyRadios
MDS Transparent Radios
Greg's World
David's LEDRs
autodisc
JBmdsNET
Gregs Backup Map
Greg's Brave New World

☐ Make this your default map

Click here to create a new map

**Figure 13. Load Map Screen**

d. A new screen appears that is ready for map building (see Figure 14). Note that the left side of the screen contains a palette of network elements (icons). These icons are used to represent the types of equipment that can be monitored with the program, and they provide useful symbols for building new network maps.

Table 4 shows a sampling of available icons and explains their meanings. You can view the complete set of images in the **Icons** folder of the Server directory. A small "thumbnail" view of each image may be seen by clicking once on a filename. Image files supplied with the NETview program have the prefix"**builtin**" in their filenames.

In addition to the images supplied with NETview, you may also install customized icons for display on maps. Custom image files must first be installed in the **Icons** folder of the Server directory. Then, from within the map screen, you can right-click an existing icon and select a new image. (**Edit>>Change Icon** on the top menu bar may also be used for this purpose.)

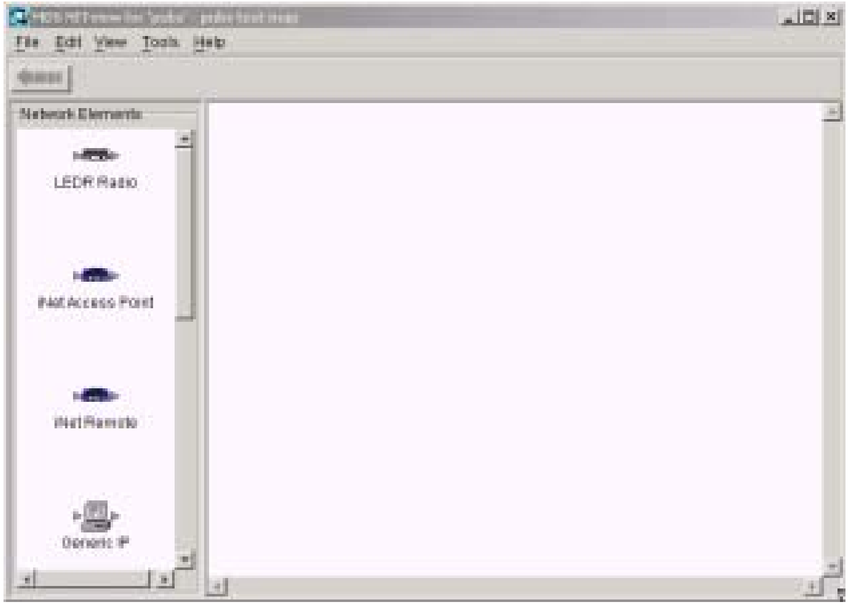


**Figure 14. Map Building Screen**

### Table 4. Available Network Elements

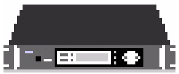
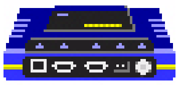
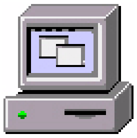
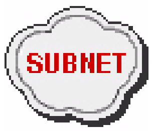
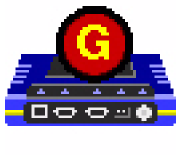
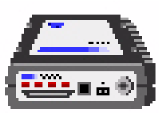
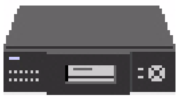
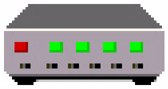
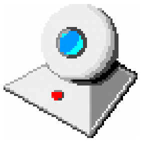
| Network Element Symbol | Explanation of Symbol |
|---|---|
|  | MDS LEDR II radio. These units are typically used in point-to-point voice and data networks. |
|  | MDS iNET or MDS entraNET Series transceiver. These units are typically used in wireless IP/Ethernet applications, but also support serial I/O data. (Two types of symbols are available—one for Access Points (APs), and another for Remote units.) |
|  | Generic IP element. This icon is available for identifying IP-connected devices that are not represented by a product-specific icon. This could be a Remote Telemetry Unit (RTU), networked PC, printer, or any other IP device not represented by a unique NETview icon. |
|  | Submap icon. Indicates a link to subordinate network map that has been created with the program. |
|  | MDS gateNET IP Proxy. This device is used to link a non-IP radio device or system, such as an MDS serial-based SCADA network, to the NETview MS program. It provides cross-platform compatibility between IP-based and serial-based wireless networks. *For more information on the MDS gateNET product, refer to publication 05-6083A01, the instruction manual for this product.*<br>NETview offers a “Discover Radios” feature that automatically finds radios connected to a gateNET device and places them on the map. For more information, see Auto-Discovery of Radios (MDS gateNET) on Page 20 of this manual. |
|  | MDS transparent (serial-based, non-IP) remote transceiver, such as MDS x710, MDS 9810 or TransNET 900 radio. This icon works in conjunction with the gateNET device mentioned above. |
| Insert MUX icon | Digital Multiplexer, such as the MDS MX-2100. |
| Insert MDS 5800/AB Full Access icon | MDS 5800 or AB Full Access point-to-point radio operating on 5.8 GHz. |
| Insert Network Junction icon | Network Junction device. |
|  | MDS transparent master station, such as an MDS 4790 or 9790 series radio. This icon works in conjunction with the gateNET device mentioned above. |

Table 4. Available Network Elements (Continued)

| Network Element Symbol | Explanation of Symbol |
|---|---|
|  | Router Hub. This device interfaces with other networks, acting as a gateway for moving traffic from one IP network to another. |
|  | IP-based “webcam” camera. These devices are commonly used with MDS radios to convey IP-based video traffic. |
| ▬▬▬▬ | Wired link. Represents a hardwire (cabled) link between pieces of equipment on the map. This pictorial image is used only to document the network layout. |
| ▪ ▪ ▪ ▪ ▪ | Wireless link. Indicates a wireless (over-the-air) link between pieces of equipment on the map. This pictorial image is used only to document the network layout. |

e. There are two ways to add network elements (icons) to the blank map area—**Manual** and **Automatic**. These procedures are described below:

***Manual Entry of Network Elements***

You can manually add elements by dragging the desired icons from the left side of the screen to the blank map area. As each item is dragged to the map, a dialog box (Figure 15) appears requesting entry of the unit’s IP address and SNMP Read Community String. The Community String is an optional entry. When used, the typical entries for MDS radios are **Read: public**, **Write: private**, **Trap: public**. Enter the requested information and click **OK**.

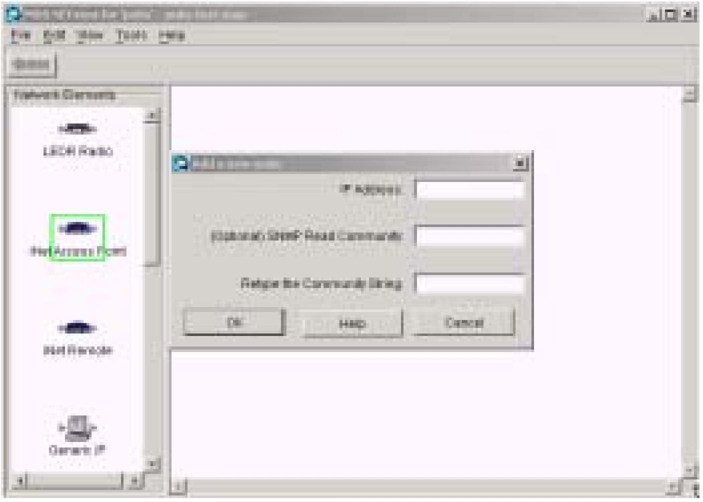
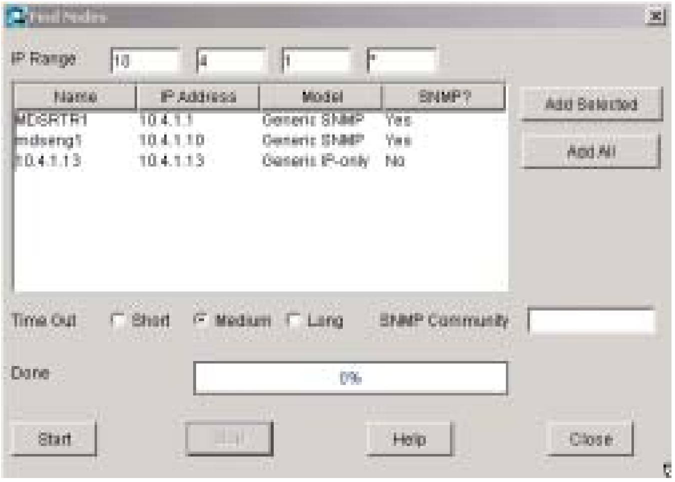


Figure 15. IP Address Entry Screen

The connection to the new element is tested, and if successful, it is placed onto the map area. If the connection fails, a dialog box asks whether you wish to delete the item or keep it despite a connection failure.

### *Automatic Entry of Network Elements*

You can automatically scan the network for available radios and other IP devices to place on the map. To do this, you must first unlock the map (**File>>Unlock Map**), then select **File>>Find New Elements**. The Find Nodes screen (Figure 16) appears.



Find Nodes

IP Range: 10 . 4 . 1 . *

| Name | IP Address | Model | SNMP? |
|---|---|---|---|
| MDSRTR1 | 10.4.1.1 | Generic SNMP | Yes |
| mdseng1 | 10.4.1.10 | Generic SNMP | Yes |
| 10.4.1.13 | 10.4.1.13 | Generic IP-only | No |

Time Out: ○ Short ● Medium ○ Long

SNMP Community:

Done: 0%

**Figure 16. Find Nodes Screen**

Enter the IP range to be scanned, the SNMP community string (if applicable), the desired timeout setting (short, medium, long) and click the **Start** button. The program begins searching the network for available devices and lists them on the screen as they are found. A progress bar shows the percentage of the search completed. The search may take a considerable amount of time, depending on the size of your network.

When the search is finished, you may either select the devices you wish to add and click **Add Selected**, or add *all* listed elements by clicking **Add All**. Icons for the selected units are immediately placed on the screen.

---

**NOTE:** An asterisk (*) may be used as a “wild card” in the IP range to scan an entire subnet, or a smaller range can be scanned by using a syntax such as **1-10**.

---

f. Arrange the network elements as desired and connect the units together using the dashed line icon for over-the-air links or the solid line icon for hardwired links. Figure 17 shows an example of a completed network map.

g. Select **File>>Lock Map** when you are finished building the network map. This hides the palette of icons at the left side of the screen and allows the map to occupy the full screen space.

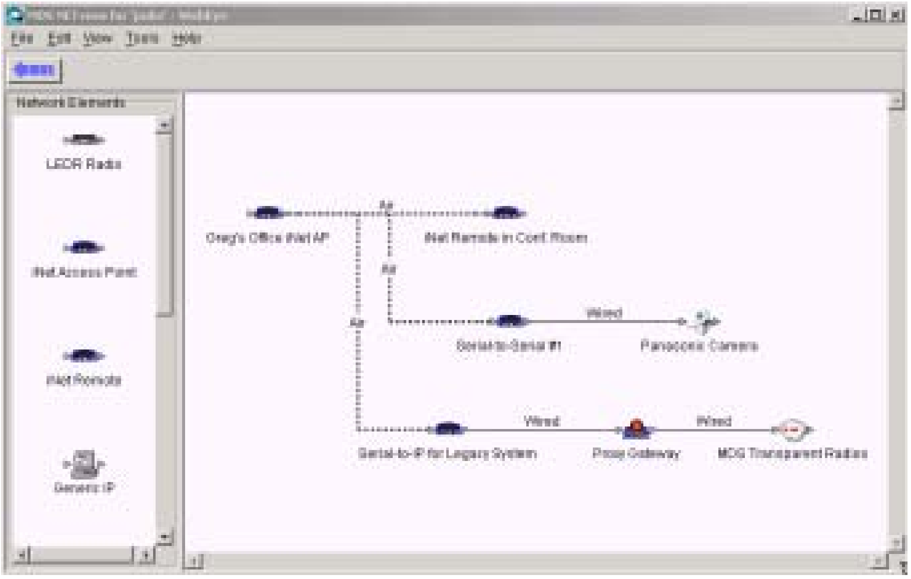


**Figure 17. Example of a Completed Network Map**

***Auto-Discovery of Radios (MDS gateNET)***

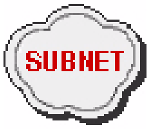
MDS gateNET devices typically have several radios connected to them. Once a gateNET icon has been placed on the map (with the map unlocked), you can perform an automatic scan of the device to see what radios are connected and add them to the map. Do this by selecting the gateNET icon and choosing **Edit>>Discover Radios** from the top menu bar. The program searches for connected radios and places them on the map as shown in Figure 18.

For more information on the MDS gateNET product, refer to publication 05-6083A01, the instruction manual for this product.

TO BE SUPPLIED

**Figure 18. Auto-Discovery Results for MDS gateNET Device**

## 4.1 Creating Submaps



A submap is used to represent an associated network that is linked to a higher level map icon. This might be required if your main network includes secondary or tertiary layers (“spurs”) that carry data on a separate wireless network.

For example, suppose you have a top-level network of several MDS iNET radios exchanging telemetry and control data in a utility application. One of these radios is linked to a LEDR point-to-point radio that carries the data to a distant location for processing. In this case, the LEDR radios would be properly represented by a submap in NETview’s hierarchy.

A submap is simply another network map that you create with the program and associate to a specific submap icon. Double-clicking a submap icon brings the new map to the forefront, and makes it the active NETview screen. A virtually unlimited number of sub-networks may be created by placing additional submap links into existing map frames.

To create a submap and link it to a higher level map, proceed as follows:

a. Create and save a network map that illustrates the sub-network. (Section 4.0 gives map building instructions.) Lock the newly created map.

a. Return to the top level map (the map that will contain the link to the submap) and drag a Submap icon onto the current frame. You will be prompted to associate an existing map name to this new element.

b. Select the map that you created in Step a and click the **Load** button.

c. A dialog box appears requesting a name for the submap icon. Enter the desired name and click **OK**. The submap icon is then placed on the screen and may be positioned and wired to other equipment as desired.

   Double-clicking the icon opens up the submap for viewing or editing.

## 4.2 Exporting Existing Maps

Existing maps may be exported from the NETview program. For more information, see Exporting Existing Maps on Page 22 of this manual.

# 5.0 USING NETVIEW SOFTWARE

This section describes how NETview can be used for monitoring and configuring the devices on your network. It covers the most common tasks performed with the program and provides guidance on tailoring NETview to meet the needs of your system.

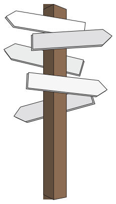
**NOTE:** The following assumes that the software has been properly installed, a valid user account has been established, and at least one network map has been created and saved with the program. Procedures for installation and setup of the program are given in Sections 2.0 through 4.0 of this manual.

## 5.1 Launching the Program

a. Select **MDS NETview** from the computer's **Start** menu and log in with your username and password.

b. If you've previously defined a default map for viewing, it will be presented on the screen. If not, select **File>>Load** and highlight the name of the desired map. Click **Load** to view the map.

c. With a network map displayed on the screen, you may proceed in one of several directions, depending on the task(s) you wish to perform. Section 5.2 describes the use of common NETview features and directs you to the pages in this manual where more detailed information can be found.



***With a network map displayed, you can proceed in one of several directions. Table 5 on Page 24 lists common program tasks.***

## 5.2 NETview Tasks

This section is organized in a task-oriented format. Table 5 lists common tasks that NETview users need to perform, and references the appropriate headings where you will find step-by-step instructions.

### Online Help

The NETview program includes built-in help files to assist users in understanding the functions of various buttons and screen items. The help files are accessible from most screens by selecting **Help** from the top menu bar or by clicking the **Help** button at the bottom of a screen, as applicable.

**Table 5. NETview Program Functions**

| | Program Task or Function | Refer to... |
|---|---|---|
| Network/Node Checks and Operations | View alarms on Network Maps | Page 24 |
| | View Event Logs | Page 26 |
| | Poll a selected node/device for IP and SNMP connectivity | Page 27 |
| | Enable “Is Alive” Polling (periodic connectivity check) | Page 28 |
| | Open a Telnet session with a device | Page 30 |
| | Open a web server session with a device | Page 31 |
| | View Performance Statistics (Radio & Interface) | Page 32 |
| | Download new firmware to a radio | Page 37 |
| | Upload/Download configuration files to a radio | Page 39 |
| | Managing Traps | Page 47 |
| | Check the status of transparent radios connected to an MDS gateNET proxy | Page 36 |
| | | |
| Program Settings & Configuration | Changing your password | Page 40 |
| | Loading maps, defining default map, creating new maps | Page 41 |
| | Set viewing options | Page 43 |
| | Right-click features | Page 44 |
| | Modifying double-click action | Page 47 |
| | Managing Traps | Page 47 |

## Viewing Alarms on Network Maps

One of the most common tasks performed with the program is simply viewing a network map for alarm indications. This section explains how to detect, interpret and investigate alarms reported by the program.

In addition to viewing alarms, Netview allows you to view Event information (SNMP traps) via the **Tools>>Get Event Log** menu, or by launching the TrapTracker viewer program accessible from the **Traps** menu. Event information is displayed in a plain language format and does not require any knowledge of the “raw” SNMP codes issued by the radio or device. For more information, refer to Viewing Event Logs on Page 26.

**NOTE:** Old alarms are not retained when a new NETview client is launched on another PC. Rather, the *current state* of the network is displayed. Each time you log on or change to a new map view, the program checks to see whether the nodes in the current map are responding. Unresponsive nodes are flagged with a critical alarm. This provides an instant view of network status when logging in.

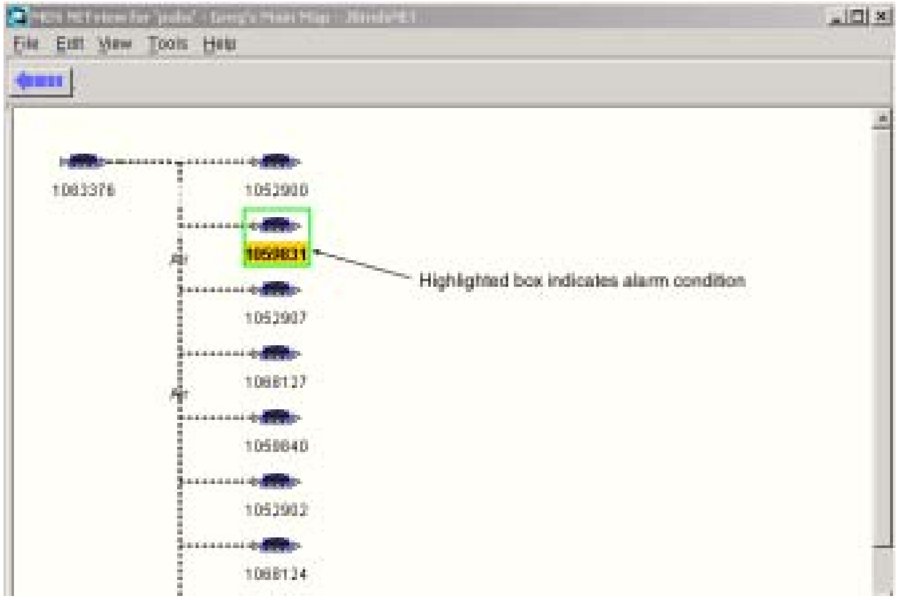
### *Alarm Indications*

The first indication of trouble on the network will be a color change on a network element name (see Figure 37) and an alert sound emitted by the PC (if sound is enabled on your computer). No highlighting (clear) indicates no detected problems, or that a problem was later matched by a "Clear" trap of the same severity, indicating that the problem was resolved.

When NETview receives an SNMP trap from the TrapTracker Manager, it converts it to a color change on the appropriate node's text label. If the alarmed node resides on a submap the color change is "propagated up" the network hierarchy so that it is visible on the top-level map.

Alarm indications are color-coded in accordance with the MIB definitions of the particular radio or device. Refer to the manual for the device for more information on a particular alarm or event indication. NETview's color indications and their meanings are as follows:

- Red (Critical Alarm)—Device inoperative/Link down.
- Orange (Major Alarm)—Degraded unit performance, but operation may still be possible.
- Yellow (Minor Alarm)—Reports an anomaly that usually does not affect unit operation but should be investigated.
- Green (Warning)—Early notice of a potential problem that should be investigated.
- Blue (Information)— Reports routine events, such as user log-in, command assertion, or result from a device self-test.
- Clear (no color)—No alarms detected.



Highlighted box indicates alarm condition

**Figure 19. Example of Alarmed Device**

### *Checking for alarms*

To view a particular network map for alarms, proceed as follows:

a. **Select File>>Load** and highlight the map that you wish to view. Click the **Load** button and the map will appear.

b. Observe the network elements shown on the map. Normally, these icons will appear without any highlighting color just as they appear in the icon palette used to construct maps. However, if an alarm occurs for a particular device, the icon becomes highlighted with a color and a sound is played (if sound is enabled). NETview's color indications are listed on Page 25.

c. For more information on an alarm, simply double click a color-highlighted icon. This allows you to navigate further into the network to locate the device that is alarmed and determine the cause for the alarm. Several double-clicks may be required to reach submaps that are nested far below the top-level map.

***Alarm Precedence***

The color of the highest-severity event always takes precedence in NETview. For example, if an Information, Minor Alarm and a Critical Alarm all came in for a node, its color would be red (Critical). Likewise, if various elements in a submap were reporting Critical, Minor and Information level events, the submap icon at the higher level map would be red.

If a later "Information" trap (blue) came in, it would *not* affect the display—the node/submap would still be red. The color indicates the highest *severity* among all the events in that area, not the severity of the most *recent* event.

"Clear" events clear the color changes for the specified severity of an event *and lower*. That is, if an Information trap is pending on a node, and a Minor-Clear event comes in for that node, it will clear the Information event. Likewise, a Critical-Clear event clears everything.

## Viewing Event Logs

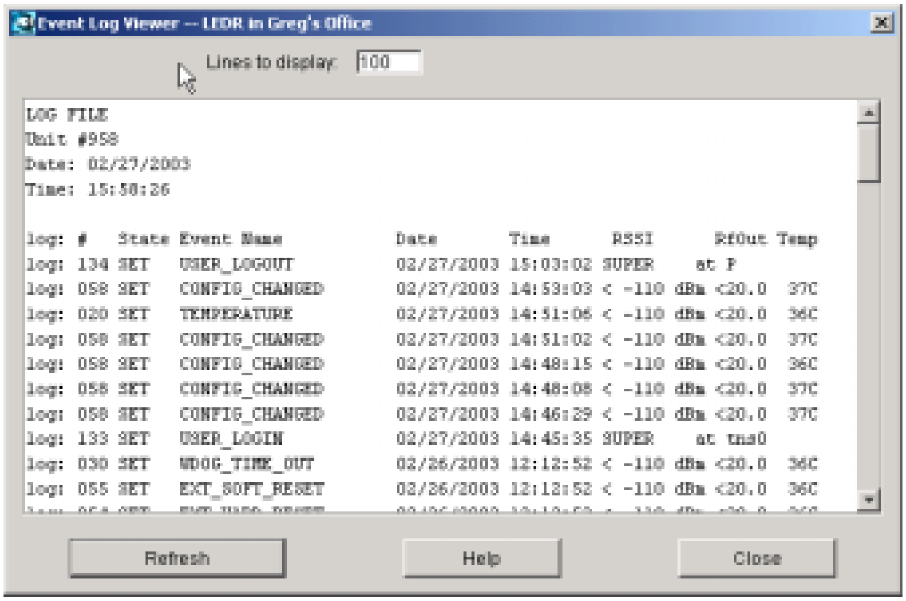
Network events are logged by NETview, allowing you to review them at any time. This may be helpful in understanding the events that led up to a malfunction or other network difficulty. Follow these steps to view the Event Log for a node or device:

a. Highlight the node of interest by single-clicking its icon.

b. Select **Tools>>Get Event Log** from the top menu bar.

c. The Event Log Screen (Figure 20) displays a history of radio events, including user actions, alarms, logins, and re-boots.

**HINT:** You may also view an Event Log by highlighting a node and entering the keyboard shortcut **Ctrl+Alt+E**.



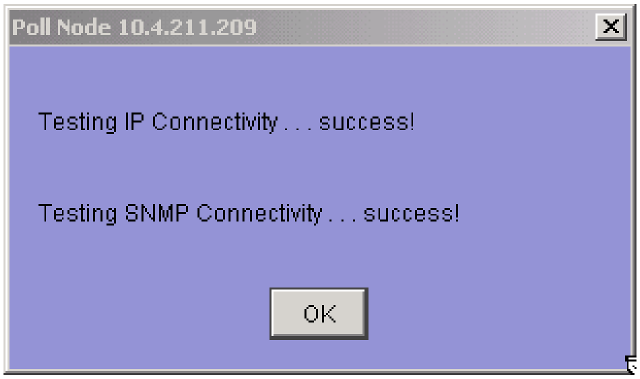
```
LOG FILE
Unit #958
Date: 02/27/2003
Time: 15:58:26

log: #   State Event Name           Date       Time     RSSI       RfOut Temp
log: 134 SET   USER_LOGOUT          02/27/2003 15:03:02 SUPER     at P
log: 058 SET   CONFIG_CHANGED       02/27/2003 14:53:03 < -110 dBm <20.0  37C
log: 020 SET   TEMPERATURE          02/27/2003 14:51:06 < -110 dBm <20.0  36C
log: 058 SET   CONFIG_CHANGED       02/27/2003 14:51:02 < -110 dBm <20.0  37C
log: 058 SET   CONFIG_CHANGED       02/27/2003 14:48:15 < -110 dBm <20.0  36C
log: 058 SET   CONFIG_CHANGED       02/27/2003 14:48:08 < -110 dBm <20.0  37C
log: 058 SET   CONFIG_CHANGED       02/27/2003 14:46:29 < -110 dBm <20.0  37C
log: 133 SET   USER_LOGIN           02/27/2003 14:45:35 SUPER     at tns0
log: 030 SET   WDOG_TIME_OUT        02/26/2003 12:12:52 < -110 dBm <20.0  36C
log: 055 SET   EXT_SOFT_RESET       02/26/2003 12:12:52 < -110 dBm <20.0  36C
```

**Figure 20. Sample Event Log Screen**

**NOTE:** Old traps are not retained when a new NETview client is launched on another PC. Rather, the *current state* of network traps is displayed. Each time you log on or change to a new map view, the program checks to see whether the nodes in the current map are responding. Unresponsive nodes are flagged with a critical trap. This provides an instant view of network status upon log-in.

## Polling a Selected Node/Device for Connectivity

To test a specific node or device for IP and SNMP connectivity, highlight it by clicking once on its icon, and then select **Tools>>Poll Selected Node**. A results screen appears (Figure 21) showing whether or not the poll was successful. Click **OK** to acknowledge the results.



Testing IP Connectivity . . . success!

Testing SNMP Connectivity . . . success!

**Figure 21. Poll Node Results Screen**

## “Is Alive Polling” Feature (Periodic Connectivity Check)

NETview’s *Is Alive Polling* feature takes the worry out of having an unresponsive node go undiscovered for an extended time. It automatically performs a connectivity check for each desired node at user-defined intervals. The default polling interval is 60,000 milliseconds (1 minute). A new Multi-Ping feature allows for efficient polling checks on networks with a very large number of operating nodes.

To enable Is Alive Polling for a node, proceed as follows:

a. Highlight a desired node on the network map and perform a right mouse click. The pop-up screen shown in Page 28 appears.

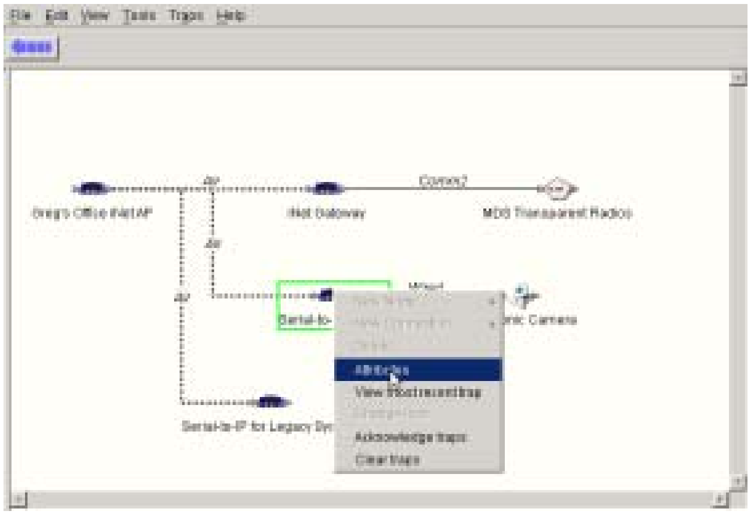
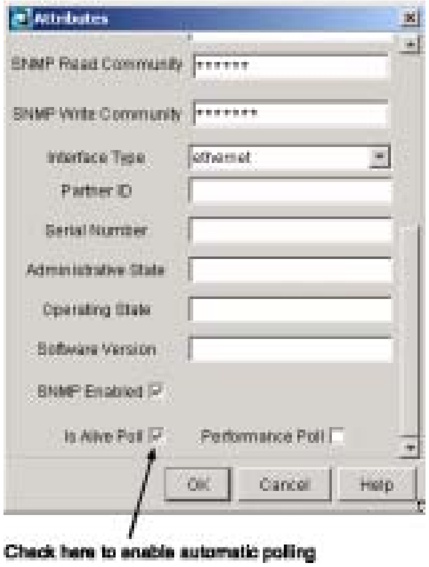


Figure 22. Right-Click Pop-Up Screen

b. Select **Attributes** from the menu. When the Attributes screen appears, click the **Is Alive Poll** box at the bottom of the screen to activate polling (see Figure 23).



SNMP Read Community ******

SNMP Write Community ********

Interface Type ethernet

Partner ID

Serial Number

Administrative State

Operating State

Software Version

SNMP Enabled ☑

Is Alive Poll ☑ Performance Poll □

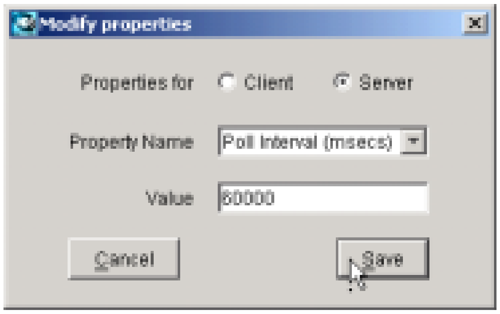
Check here to enable automatic polling

**Figure 23. Attributes Screen with "Is Alive" Polling Enabled**

c. Determine the polling interval you wish to use. The default setting is 60,000 milliseconds (1 minute) designed to suit most networks. If desired, the setting may be changed on the server as follows:

- On NETview version 2.2 and higher, the polling interval may be changed using the **File>>Modify Properties** menu (keyboard shortcut: Ctrl + P). Page 29 shows a sample of the Modify Properties screen.

  Select **Poll Interval (msecs)** in the server's Property Name list and enter the desired poll interval in the **Value** box. The value must be expressed in milliseconds. Click **Save**.



Properties for ○ Client ● Server

Property Name Poll Interval (msecs)

Value 60000

**Figure 24. Modify Properties Screen**

- On pre-version 2.2 programs, the polling interval may changed by accessing the **<KeepAlivePollInterval>** parameter in the **<mdsserver>** file of the server's application directory.

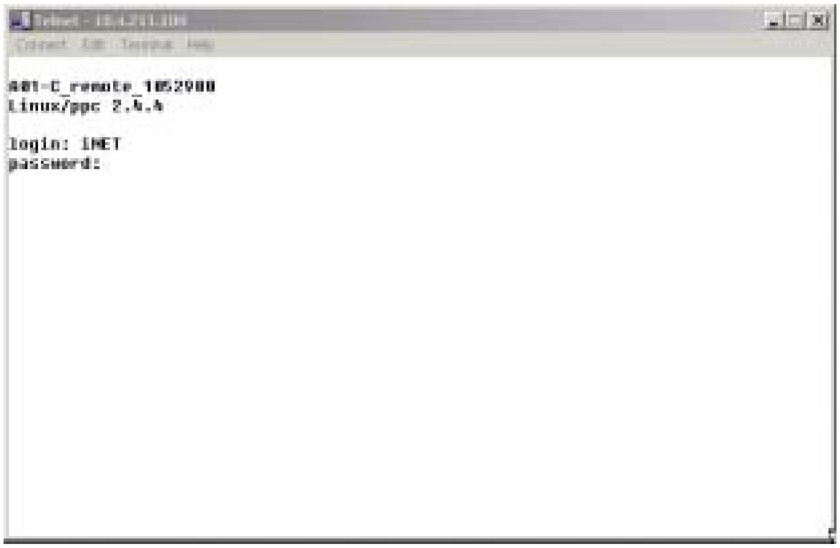
## Opening a Telnet Session with a Device

MDS radios, such as the MDS iNET, entraNET and LEDR Series, can be interrogated and controlled via a Telnet session. Once logged in, specific commands contained in the transceiver manuals may be issued. This method of control—also known as a Command Line Interface (CLI)—is not as graphically oriented as a web server connection, however, it offers a powerful tool for advanced users and maintenance personnel who need to communicate remotely with a radio and issue specific commands.

Follow these steps to establish a Telnet session with an MDS radio via NETview:

a. Highlight the device that you wish to connect with by clicking once on its icon.

b. Select **Tools>>Telnet** to bring up the Telnet login screen as shown in Figure 25.

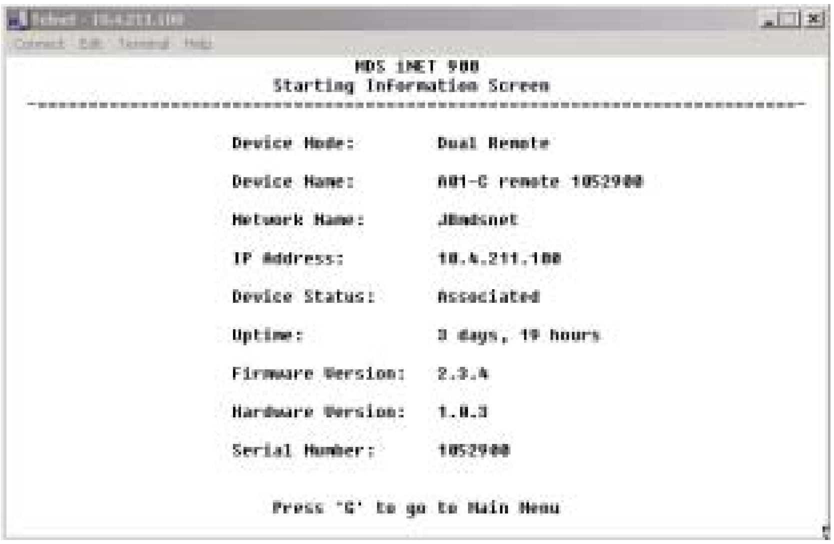


```
401-C_remote_1052900
Linux/ppc 2.4.4

login: iNET
password:
```

**Figure 25. Telnet Login Screen**

c. Enter your password. The Telnet Session screen shown in Figure 26 appears.

**NOTE:** If the wrong password is entered three times in a row, a 5-minute penalty lockout occurs, after which time the password may be entered again.



```
                          MDS iNET 900
                   Starting Information Screen
-------------------------------------------------------------------------

            Device Mode:        Dual Remote

            Device Name:        A01-C remote 1052900

            Network Name:       JBmdsnet

            IP Address:         10.4.211.100

            Device Status:      Associated

            Uptime:             3 days, 19 hours

            Firmware Version:   2.3.4

            Hardware Version:   1.0.3

            Serial Number:      1052900

                   Press 'G' to go to Main Menu
```

**Figure 26. Telnet Session Screen**

d. At the command prompt, you may enter a radio command from those listed in the radio’s instruction manual. Press ENTER to invoke the command.

e. The Telnet screen displays a response to each command.

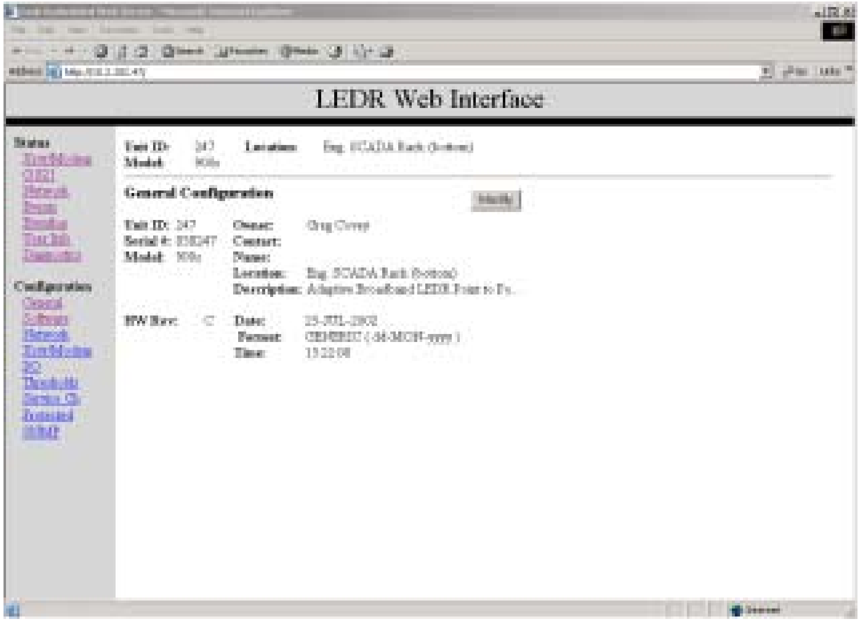
## Opening a Web Server Session with a Device

Many MDS radios, including the MDS iNET, entraNET and LEDR Series, contain a built-in web server that provides a convenient way to interact with the radio using a familiar web browser such as Internet Explorer or Netscape Navigator. Some non-MDS devices may also support this capability. Follow the steps below to launch a web browser session with a connected device.

a. Double-click the network element (or highlight it and select **Tools>>Connect To WebServer**). You will be prompted to enter your username and password for login.

b. Enter your login information and click **OK**. Upon successful entry, a browser screen similar to Figure 27 appears with information specific to the device you are monitoring.

The screen presents detailed status and configuration data for the connected device. For MDS radios, the type of information displayed depends on the selection made at the left side of the screen. Simply click on a title to display its information.



LEDR Web Interface

Unit ID: 247 Location: Eng. SCADA Rack (bottom)
Model: 900s

General Configuration

Unit ID: 247 Owner: Greg Covey
Serial #: [illegible]
Model: 900s
Contact:
Name:
Location: Eng. SCADA Rack (bottom)
Description: Adaptive Broadband LEDR Point to Pt...

HW Rev: C Date: 25-JUL-2002
Format: GENERIC ( dd-MON-yyyy )
Time: 13:22:08

Figure 27. Sample Web Browser Screen (MDS LEDR Radio Shown)

c. To modify data shown on the screen (authorization required), click the **Modify** button and enter your username and password.

d. Upon successful entry, you may highlight the information field(s) to be changed and enter new information. Consult the radio manual for guidance on setting radio parameters.

---

**NOTE:** As a security precaution, the browser screen should be closed immediately after you finish your session. This prevents unauthorized access to the radio network.

---

## Viewing Performance Statistics

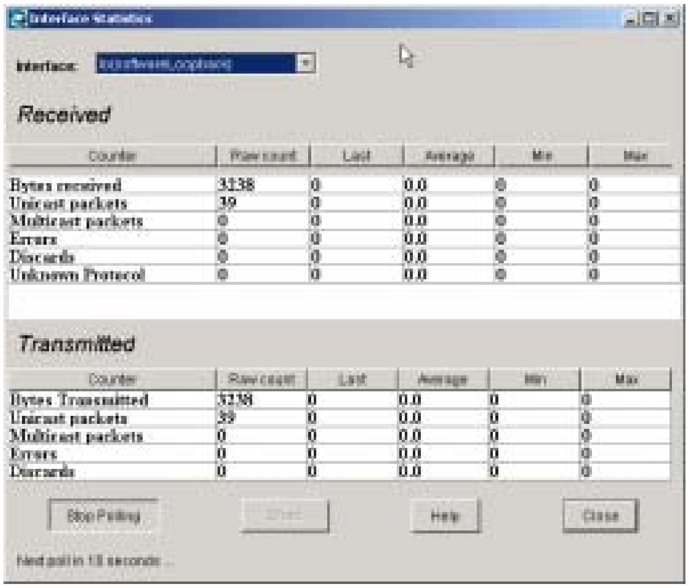
The NETview program can collect and display statistical quality data for a monitored radio and its data interface. When selected, this function polls the specified radio and presents the data in a table format for easy review.

### *Interface Statistics*

To view interface statistics, highlight a node on the network map, and select **Tools>>Performance>>Interface Statistics** from the menu bar.

When the Statistics screen appears (Figure 30), choose the type of interface you wish to monitor from the drop-down menu at the top left of the screen, then click the **Start Polling** button to begin data collection. The screen displays packet statistics on a continually updated basis for both Received and Transmitted data. Click the **Stop Polling** button to end polling.

Optionally, you may generate a graphical chart of the interface statistics by clicking the **Chart** button at the bottom of the screen. This changes the appearance of the screen to a view similar to the one shown in Figure 29. Charting is an effective, visual way to show trends in data performance.



Interface: lo(software Loopback)

Received

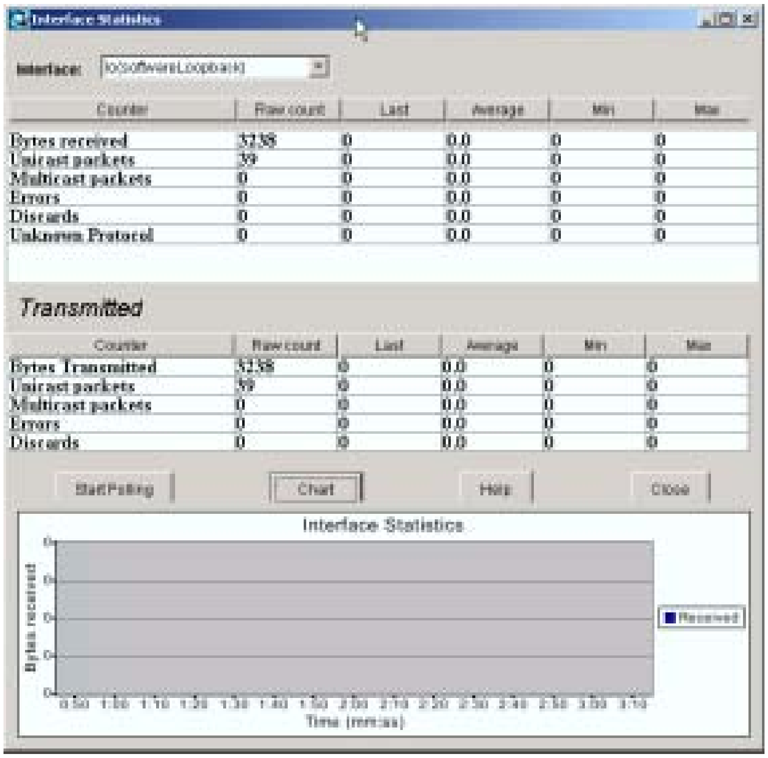
| Counter | Raw count | Last | Average | Min | Max |
|---|---|---|---|---|---|
| Bytes received | 3238 | 0 | 0.0 | 0 | 0 |
| Unicast packets | 39 | 0 | 0.0 | 0 | 0 |
| Multicast packets | 0 | 0 | 0.0 | 0 | 0 |
| Errors | 0 | 0 | 0.0 | 0 | 0 |
| Discards | 0 | 0 | 0.0 | 0 | 0 |
| Unknown Protocol | 0 | 0 | 0.0 | 0 | 0 |

Transmitted

| Counter | Raw count | Last | Average | Min | Max |
|---|---|---|---|---|---|
| Bytes Transmitted | 3238 | 0 | 0.0 | 0 | 0 |
| Unicast packets | 39 | 0 | 0.0 | 0 | 0 |
| Multicast packets | 0 | 0 | 0.0 | 0 | 0 |
| Errors | 0 | 0 | 0.0 | 0 | 0 |
| Discards | 0 | 0 | 0.0 | 0 | 0 |

Next poll in 18 seconds ...

**Figure 28. Interface Statistics Screen**



Interface: lo(software,Loopback)

| Counter | Raw count | Last | Average | Min | Max |
|---|---|---|---|---|---|
| Bytes received | 3238 | 0 | 0.0 | 0 | 0 |
| Unicast packets | 39 | 0 | 0.0 | 0 | 0 |
| Multicast packets | 0 | 0 | 0.0 | 0 | 0 |
| Errors | 0 | 0 | 0.0 | 0 | 0 |
| Discards | 0 | 0 | 0.0 | 0 | 0 |
| Unknown Protocol | 0 | 0 | 0.0 | 0 | 0 |

Transmitted

| Counter | Raw count | Last | Average | Min | Max |
|---|---|---|---|---|---|
| Bytes Transmitted | 3238 | 0 | 0.0 | 0 | 0 |
| Unicast packets | 39 | 0 | 0.0 | 0 | 0 |
| Multicast packets | 0 | 0 | 0.0 | 0 | 0 |
| Errors | 0 | 0 | 0.0 | 0 | 0 |
| Discards | 0 | 0 | 0.0 | 0 | 0 |

**Figure 29. Interface Statistics Screen—with Chart View**

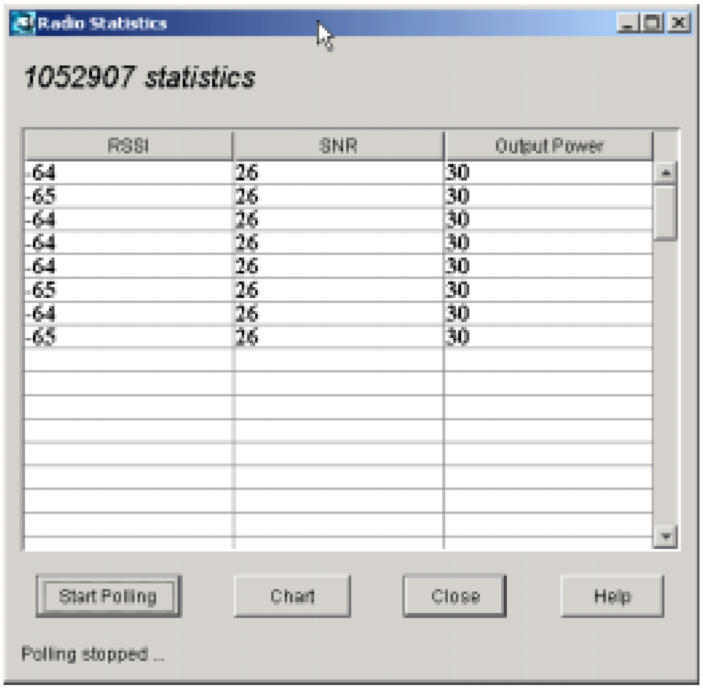
**TIP:** You may also view Interface Statistics by highlighting a node and entering the keyboard shortcut **Ctrl+Alt+C**.

### *Radio Statistics*

To view radio statistics, highlight a node on the network map, and select **Tools>>Performance>>Radio Statistics** from the menu bar.

When the Radio Statistics screen appears (Figure 30), click the **Start Polling** button to begin data collection. The screen lists key operating parameters on a continually updated basis, including: received signal strength indication (RSSI) in dBm, signal-to-noise ratio (SNR) in decibels, and RF power output in dBm. Some radio models will also display their internal chassis temperature. Click the **Stop Polling** button to end polling.

**TIP:** You may also view Radio Statistics by highlighting a node and entering the keyboard shortcut **Ctrl+Alt+R**.



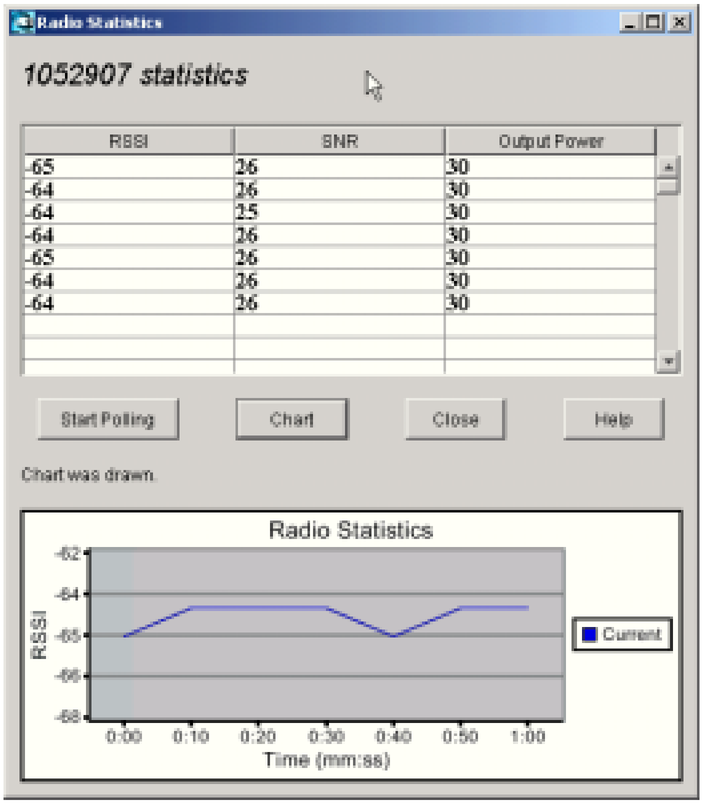
1052907 statistics

| RSSI | SNR | Output Power |
|---|---|---|
| -64 | 26 | 30 |
| -65 | 26 | 30 |
| -64 | 26 | 30 |
| -64 | 26 | 30 |
| -64 | 26 | 30 |
| -65 | 26 | 30 |
| -64 | 26 | 30 |
| -65 | 26 | 30 |

Polling stopped ...

**Figure 30. Radio Statistics Screen**

Optionally, you may generate a graphical chart of radio statistics by clicking the **Chart** button at the bottom of the screen. This changes the appearance of the screen to a view similar to Figure 31. Statistical charting is often an effective, visual way to show trends in radio performance.



1052907 statistics

| RSSI | SNR | Output Power |
|---|---|---|
| -65 | 26 | 30 |
| -64 | 26 | 30 |
| -64 | 25 | 30 |
| -64 | 26 | 30 |
| -65 | 26 | 30 |
| -64 | 26 | 30 |
| -64 | 26 | 30 |

Chart was drawn.

**Figure 31. Radio Statistics Screen—with Chart View**

### *Impact Graphing with NETview*

Critical parameters, such as RSSI, output power, and the temperatures of radios are recorded in a database and may be viewed as described above in *Viewing Performance Statistics*. These functions also allow for generating a small, basic chart at the bottom of the Statistics screens for easier viewing (see Figure 31).

In many cases, a larger graphical display of the data will provide a more useful format that is easier to interpret and share with others. Third party applications, such as Microsoft Access, Microsoft Excel and Crystal Reports may be used to extract the data from the database and display it in a variety of ways. While each of these tools offers graphing/charting capability, MDS has extensively tested Crystal Reports with NETview and it is recommended for graphing of performance data.

Figure 32 shows a sample chart produced with Crystal Reports using data from MDS NETview. This is one of many formats possible with the program. The documentation provided with your charting application will provide detailed instructions on importing database files and displaying them in the desired format.

NETview's online help file contains more information about charting with specific applications. In the help index, select one of the "Charting in..." entries to view this information. In addition, a supplemental file, *NETview Charting Instructions*, is included on the NETview CD, and will prove helpful in understanding how data may be extracted and used for charting in external applications.

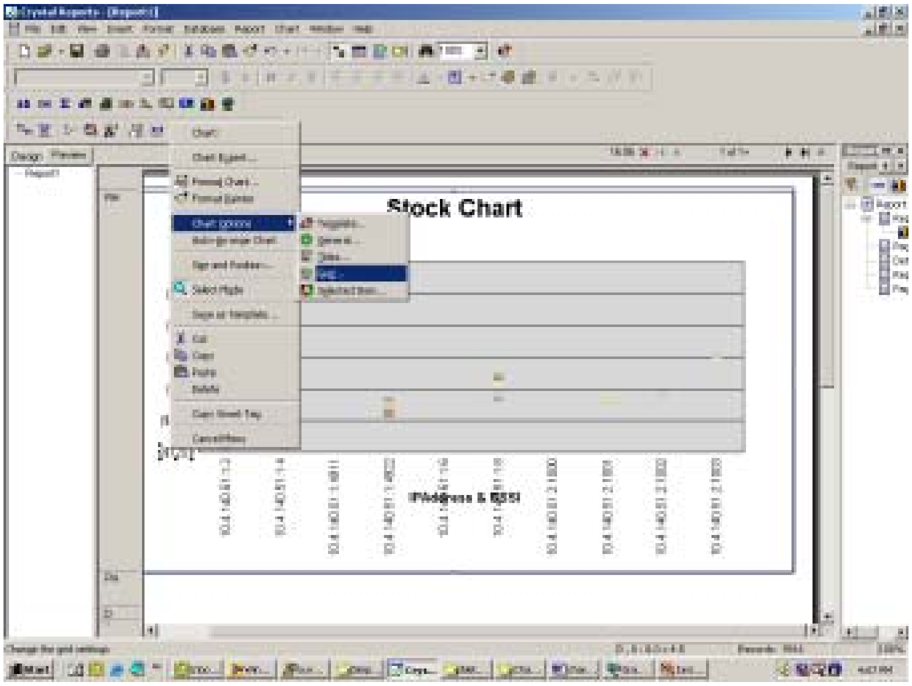


Figure 32. Sample Chart Created with Crystal Reports

## Transparent Radio Health Check (For radios connected to an MDS gateNET proxy)

Transparent radios are units that pass data over the air without altering it in any way. The data applied at the transmitting end is available at the receiving end in exactly the same format. These radios are designed to pass serial data (e.g. RS-232), as opposed to IP-based protocols used by some newer-generation MDS radios. Examples of MDS Transparent radios are the TransNET transceiver, MDS x710 transceiver, x790 master station or x810 spread spectrum transceiver.

NETview's Transparent Radio Health Check offers a quick way to check the status of these radios when they are connected to an MDS gateNET Proxy device. For more information on this device, refer to MDS publication 05-6083A01.

To perform a health check for radios connected via a gateNET proxy, proceed as follows:

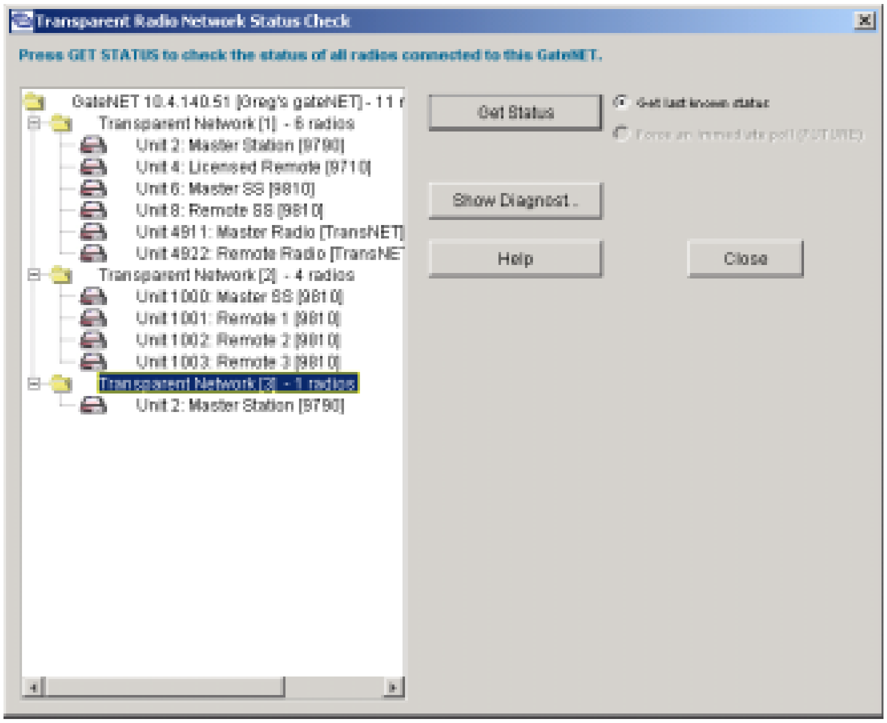
1. Click once on a gateNET Proxy device icon.

2. Choose **Tools>>Perfomance>>Transparent Radio Health Check** from the top menu bar. The Transparent Radio Network Status Check screen appears.

3. Press the **Get Status** button to check the status of all radios connected to the selected gateNET.

4. A screen similar to Figure 33 appears showing the networks/radios that were detected. Double-click folders to view the radios associated with a particular network.

5. To view diagnostics for a particular transceiver, select it, and the click the **Show Diagnost...** button.



Transparent Radio Network Status Check

Press GET STATUS to check the status of all radios connected to this GateNET.

```
GateNET 10.4.140.51 [Greg's gateNET] - 11 r
  Transparent Network [1] - 6 radios
    Unit 2: Master Station [9790]
    Unit 4: Licensed Remote [9710]
    Unit 6: Master SS [9810]
    Unit 8: Remote SS [9810]
    Unit 4911: Master Radio [TransNET]
    Unit 4922: Remote Radio [TransNET
  Transparent Network [2] - 4 radios
    Unit 1000: Master SS [9810]
    Unit 1001: Remote 1 [9810]
    Unit 1002: Remote 2 [9810]
    Unit 1003: Remote 3 [9810]
  Transparent Network [3] - 1 radios
    Unit 2: Master Station [9790]
```

Figure 33. Transparent Radio Health Check Sample Screen

## Downloading New Firmware for MDS Products

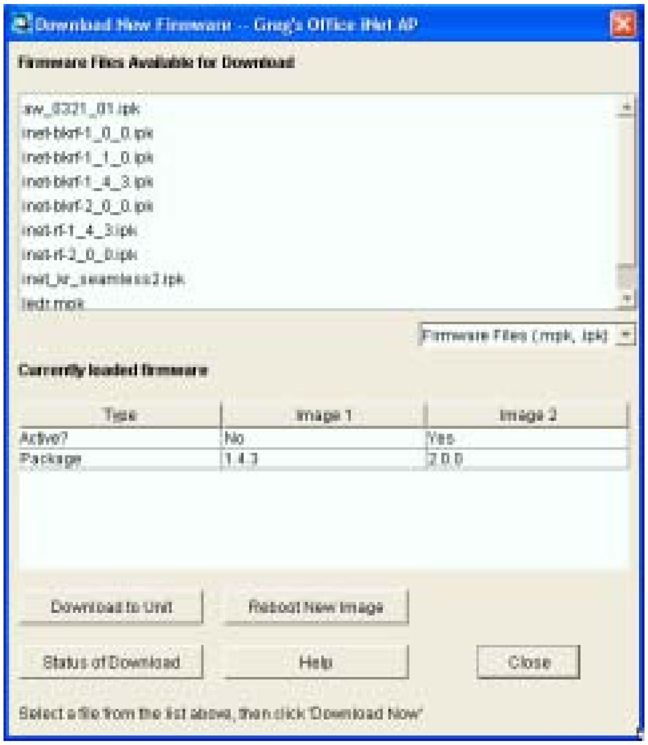
From time to time, Microwave Data Systems releases new software code for its products. This code can be downloaded into existing devices to take advantage of engineering improvements, or to add new functionality to equipment. The latest firmware for each product type may be downloaded free from the MDS web site at **www.microwavedata.com**.

This section describes the steps that an operator or system administrator can use to download new firmware code into an MDS product.

**NOTE:** MDS products keep two images of firmware in memory. This enables online downloads of firmware, without affecting current operation. Once the download is complete, you can make the new file active by clicking the **Reboot New Image** button on the Download screen.

a. Highlight the device that you wish to load with new firmware.

b. Select **Tools>>Configuration>>Update Firmware** from the top menu bar. The screen shown in Figure 34 appears, listing the firmware files available for download, and the currently loaded firmware.



Download New Firmware -- Greg's Office iNet AP

Firmware Files Available for Download

```
sw_0321_01.ipk
inet-bkrf-1_0_0.ipk
inet-bkrf-1_1_0.ipk
inet-bkrf-1_4_3.ipk
inet-bkrf-2_0_0.ipk
inet-rf-1_4_3.ipk
inet-rf-2_0_0.ipk
inet_kr_seamless2.ipk
ledr.mpk
```

Firmware Files (.mpk, .ipk)

Currently loaded firmware

| Type | Image 1 | Image 2 |
|---|---|---|
| Active? | No | Yes |
| Package | 1.4.3 | 2.0.0 |

Select a file from the list above, then click 'Download Now'

**Figure 34. Download New Firmware Screen**

- The **Firmware Files Available for Download** area lists files contained in the server application directory, **\tftp** folder. This location is typically defaulted to **C:\Program Files\Microwave Data Systems\MDSnv Server\tftp.**
- The **Currently loaded** firmware area displays the revision and active status of each firmware image in the radio.

c. Select a file from the list of available firmware files and click **Download to Unit.**

d. Click the **Status of Download** button to monitor the progress of the file transfer.

**NOTE:** The **Status of Download** button is not available on MDS LEDR radios. For these models, view the download status from the TFTP interface at the Server computer. Additionally, LEDR radios typically require a longer download time than other MDS models.

e. When the transfer is complete, you may proceed with one of two actions:

- Leave the new firmware stored in the unit, but in an inactive state.
- Invoke the new firmware immediately by clicking the **Reboot New Image** button.

## Uploading/Downloading Configuration Files

Configuration files determine how a unit operates when it is placed in service. Settable items such as carrier frequency, modulation type, data speed, and RF output level are all defined in a unit's configuration file. NETview allows you to upload or download configuration files for specific MDS models including the MDS iNET, entraNET and LEDR series. This section describes the steps that an operator or system administrator can use to transfer configuration files.

### *Benefits of Uploading a Configuration File*

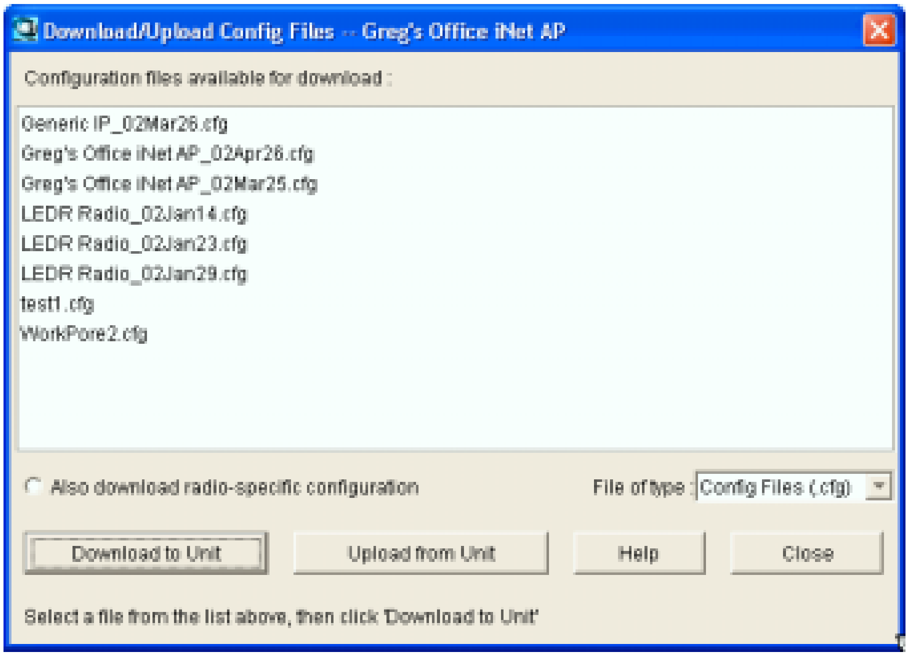
A configuration file from a known-working unit can be uploaded via NETview and stored for possible later re-use. In this way, inadvertent errors made during programming or troubleshooting can be corrected, and the unit can be returned to an operational state. This situation could occur if a number of changes have been made to the device and the operator is unsure which setting may have caused a problem. It is recommended that a configuration file be uploaded and stored for each unit operating in the network, in case it is needed later.

To download/upload configuration files proceed as follows:

a. Highlight the device that you wish to download/upload configuration files to.

b. Select **Tools>>Configuration>>Configuration Files** from the top menu bar. The screen shown in Figure 35 appears, listing the configuration files available for download to the unit.

- The **Configuration files available for download** area lists files contained in the server application directory \tftp folder. This location typically defaults to **C:\Program Files\Microwave Data Systems\MDSnv Server\tftp.**



Configuration files available for download :

Generic IP_02Mar26.cfg
Greg's Office iNet AP_02Apr26.cfg
Greg's Office iNet AP_02Mar25.cfg
LEDR Radio_02Jan14.cfg
LEDR Radio_02Jan23.cfg
LEDR Radio_02Jan29.cfg
test1.cfg
WorkPore2.cfg

○ Also download radio-specific configuration

File of type : Config Files (.cfg)

Select a file from the list above, then click 'Download to Unit'

**Figure 35. Download/Upload Configuration Files Screen**

c. To **download** a specific configuration file to the radio, select the file from the list and click **Download to Unit.**

To **upload** a configuration file from a radio, click **Upload from Unit**. The file will be saved under the name and directory you enter in the dialog box.

## Changing Your Password

Personal passwords are an important safeguard against network security breaches. It is highly recommended that you establish a unique password for your user account and change it periodically to protect the network from unauthorized access.

**TIP:** For enhanced security, consider using a *misspelled* word for your password. This helps guard against sophisticated hackers who may use a database of common words (e.g., a dictionary file) to determine a password. Making your password as long as possible (up to 16 characters), and including one or more numbers will further improve its security.

Follow these steps to change your password:

a. Select **File>>User Maintenance>>Change Password**. This brings up the Change Password screen (Figure 36).

b. Enter your existing password in the **Old password** field.

c. Enter your new password (16 characters max.) in the **New password** field, and re-enter it in the **Retype password** field for confirmation. *Note that passwords and usernames are case sensitive*.

d. Click **OK** to make the new password active.

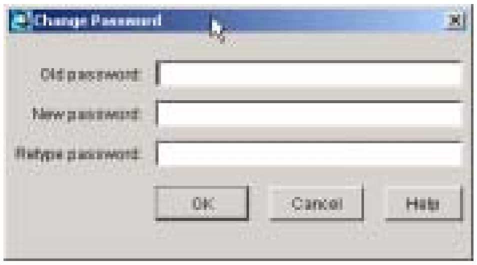


**Figure 36. Change Password Screen**

## Loading Maps

The NETview program can store numerous map configurations in its server database. This allows multiple systems to be represented, depending on which one is selected at the time of viewing. The steps below explain how to load an existing map, define a particular map as your default selection, create a new map, and export existing maps.

***Loading an existing map***

To load a map that has already been created and stored on the NETview server, proceed as follows:

a. Select **File>>Load** from the top menu bar. The **Load Map** screen appears with a list of available maps (Figure 37).

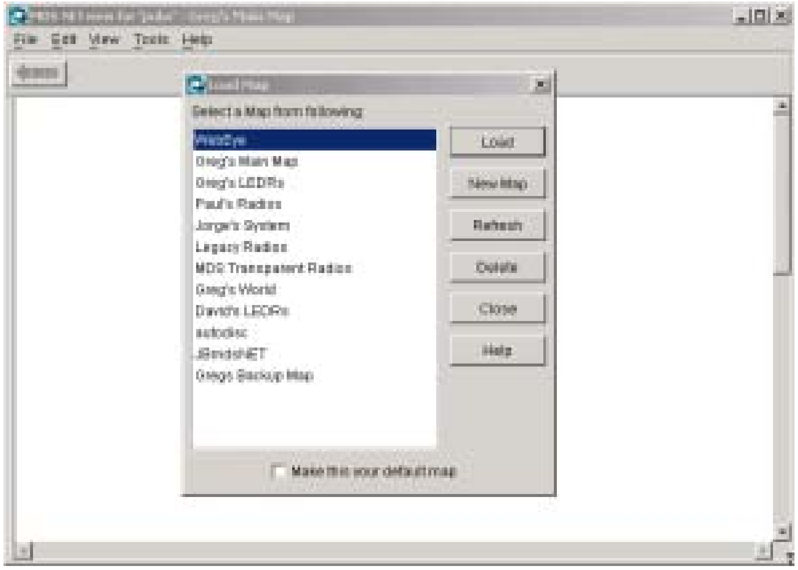


**Figure 37. Load Map Screen**

b. Select a map from the list by single-clicking it. The system saves the selected map to the user's configuration for auto-loading every time the NETview program is launched.

Optional: To define this map as your default selection, click the box at the bottom of the screen labeled **Make this your default map**.

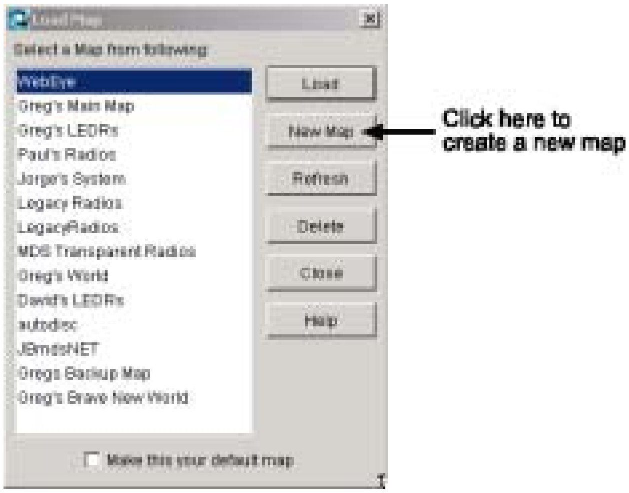
c. Click the **Load** button to load the selected map. The map will be brought up on the screen.

### *Creating a New Map*

Follow these steps to create a new map for use with NETview:

**NOTE:** Maps must be unlocked before they can be constructed. To check the lock status, select **File** from the top menu bar and view the selections. If the **Lock Map** command appears, the map is currently unlocked. If **Unlock Map** is displayed, select it (or enter Ctrl-K on the keyboard) to unlock the map.

a. Select **File>>Load** from the top menu bar. This brings the Load Map screen (Figure 38) to the forefront.



Click here to create a new map

**Figure 38. Load Map Screen**

b. Click **New Map**. A dialog box appears for entering a name for the new map. Enter the desired name and click **OK**. A new screen appears that is ready for map building (Figure 39).

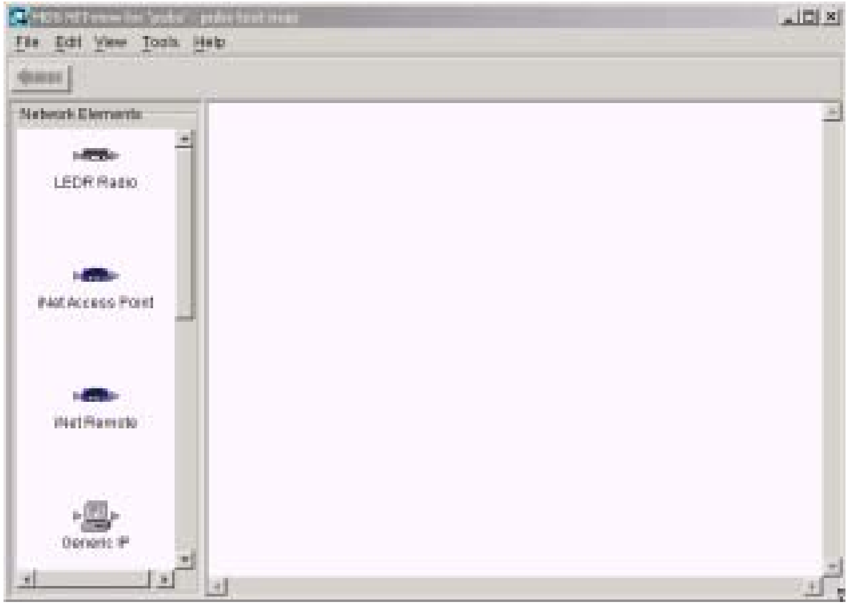


**Figure 39. Map Building Screen**

c. Drag the appropriate icons onto the screen from the palette at the left hand side. Detailed map building instructions are provided in Section 4.0, *Building a Network Map* (beginning on Page 15).

***Exporting Existing Maps***

Text to be supplied.

## Viewing Options

The **View** menu, accessible from the top menu bar, (see Figure 40) contains viewing options that may be selected with a mouse click, or by using keyboard function keys. Table 6 lists the available options and their keyboard equivalents.

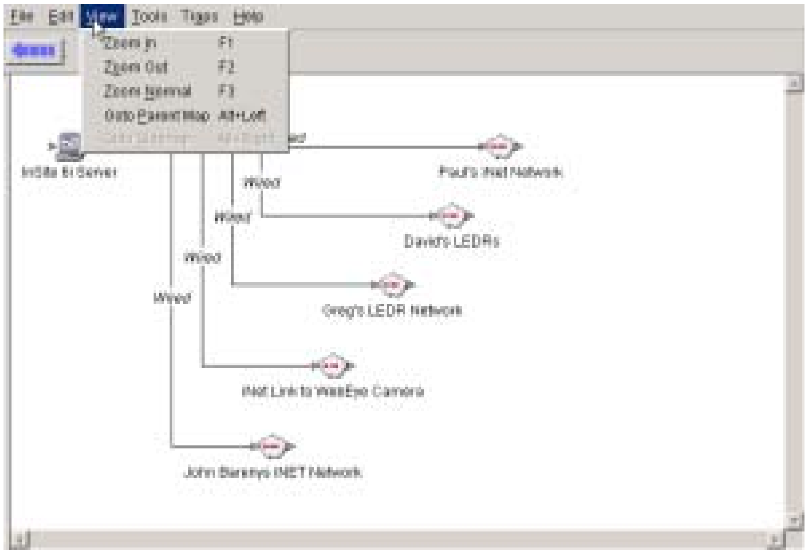


Figure 40. View Options Menu

Table 6. View Menu Options

| Menu Item | Description | Keyboard Shortcut |
|---|---|---|
| Zoom In | Enlarges the screen view | F1<br>or plus key (+) |
| Zoom Out | Shrinks the screen view, but may allow more items to be seen when working with larger maps | F2<br>or minus key (-) |
| Zoom Normal | Sets the screen size to the default setting | F3 |
| Goto Parent Map | Changes the view to the top level map | Alt + left arrow |
| Goto Submap | Changes the view to an underlying map which is subordinate to the parent map | Alt + right arrow |

## Right-Click Features

Right-clicking on an active network map brings up a the menu shown in Figure 41. The available menu items depend on where you click, and whether the map is locked or unlocked. Here is a breakdown of the functions:

- With the map unlocked, right-clicking on a node (IP device) gives access to all of the menu items.
- Right-clicking on a wireless connection line (dashed) or a wired connection line (solid) gives access to all menu items *except* **View most recent trap.**

- Right-clicking on a blank area of the screen provides access to two menu items: **New Node** and **New Connection**.

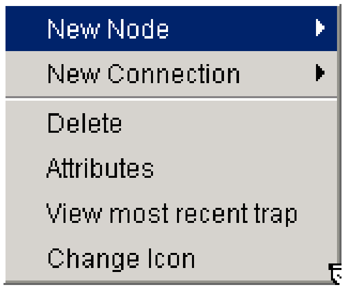


**Figure 41. Right-Click Menu**

***New Node***

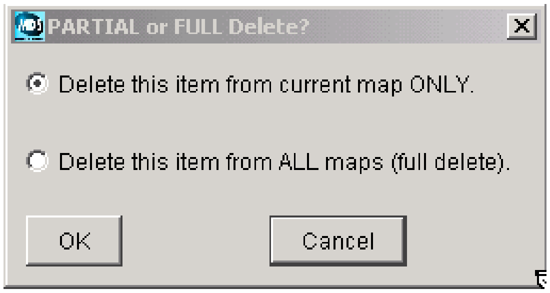
The **New Node** selection provides a convenient way to add a new IP device to an existing network map. A drop-down list of node types appears, from which you can select the appropriate entry. After making a selection, you will be prompted for an IP address and optional Community String. This prompt screen is identical to the one shown in Section 4.0, *Building a Network Map* (beginning on Page 15). Refer to this section for complete entry information.

***New Connection***

This item allows you to add a new wired or wireless connection to the network map.

***Delete***

This item allows you to delete a network element from the map. Before deletion, a dialog box appears (Figure 42) asking if you wish to delete the item from the *current map only*, or delete it from *all maps* (full delete). Choose the desired action and then click **OK**.



● Delete this item from current map ONLY.

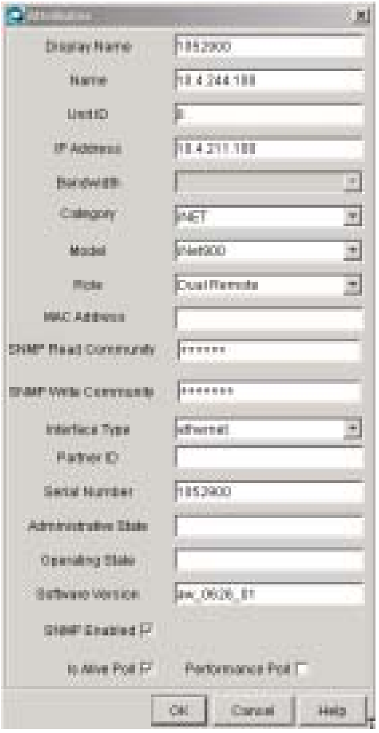
○ Delete this item from ALL maps (full delete).

**Figure 42. Delete Action Dialog Box**

***Attributes***

The Attributes screen (Figure 43) is available when you right-click on a network map device or connection line. It lists a variety of device/line specific items, many of which can be edited by clicking into an entry field and entering new information, or by selecting from a drop-down list.

The figure shows the typical information presented for an MDS iNET radio. The attributes displayed for a connection line are: **Display Name**, **Name**, **Type**, **Speed**, **Protocol**.



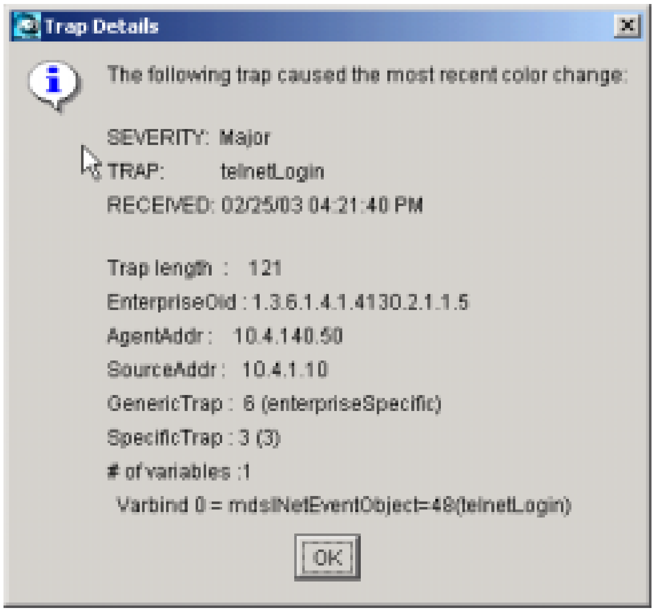
Attributes

Display Name: 1852900
Name: 10.4.244.188
Unit ID: 0
IP Address: 10.4.211.188
Bandwidth:
Category: iNET
Model: iNet900
Role: Dual Remote
MAC Address:
SNMP Read Community: ******
SNMP Write Community: *******
Interface Type: ethernet
Partner ID:
Serial Number: 1852900
Administrative State:
Operating State:
Software Version: sw_0626_01
SNMP Enabled ☑
Is Alive Poll ☑ Performance Poll ☐

**Figure 43. Attributes Screen for MDS Radio**

***View most recent trap***

This selection is used to query a device for its most recent trap information. It is useful for determining what caused a color change on a device and learning the specifics of the trap. Figure 44 shows a sample Trap Details screen.



Trap Details

The following trap caused the most recent color change:

SEVERITY: Major
TRAP: telnetLogin
RECEIVED: 02/25/03 04:21:40 PM

Trap length : 121
EnterpriseOid : 1.3.6.1.4.1.4130.2.1.1.5
AgentAddr : 10.4.140.50
SourceAddr : 10.4.1.10
GenericTrap : 6 (enterpriseSpecific)
SpecificTrap : 3 (3)
# of variables :1
Varbind 0 = mdsINetEventObject=48(telnetLogin)

**Figure 44. Trap Details Screen**

***Change Icon***

The **Change Icon** selection provides a convenient way to select a new image for a device or node on the network map. The available icons are presented in a scrollable list and include images for MDS radios and other IP equipment, plus symbols (arrows, rectangles and circles) that can be used on the map.

## Modify Double-Click Action

Using the **File>>User Maintenance>>Modify Double Click** menu, you may specify what action will be performed when double-clicking on a network element (icon). The default setting for a double-click is **Connect to Webserver**, but a variety of other actions may be set, if desired. See Figure 45 for a view of the Double-Click Action screen.

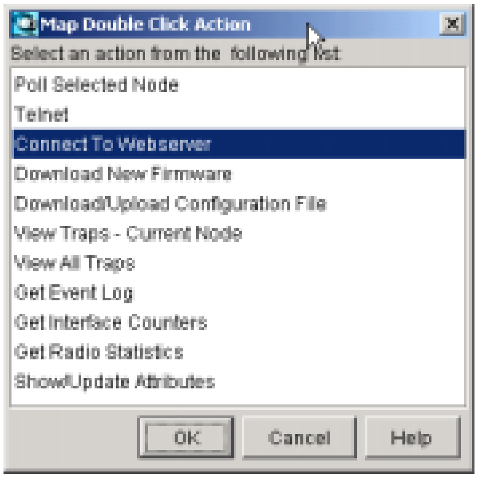


**Figure 45. Modify Double-Click Screen**

## Trap Management

NETview provides a variety of trap handling options that can be defined from the **Traps** menu on the top menu bar (see Figure 46). The following is a description of each selection on the **Traps** menu:

- **View most recent trap** brings up a new screen with details about the most recent trap received, including the trap name, time received, severity and other parameters.
- The **Stop receiving traps** selection shuts off all trap processing. When selected, the title of this selection changes to **Activate trap processing.** Click on this new title to restore trap processing
- **Acknowledge traps** brings up a submenu where you can choose to acknowledge traps for the selected node(s), or *all* nodes.
- The **Clear traps** selection brings up a submenu where you can choose to clear traps for the selected node(s), or *all* nodes.
- **Launch TrapTracker** brings up a submenu where you can choose to launch TrapTracker for the selected node(s), or *all* nodes.

- The **Trap Sounds** selection brings up a submenu where you can choose to play an alert sound for *every* trap received, play a sound *only* if a color change occurs, or turn sound off altogether.

For more information on trap handling between NETview and the TrapTracker program, refer to the paragraph titled TRAPTRACKER PROGRAM on Page 49.

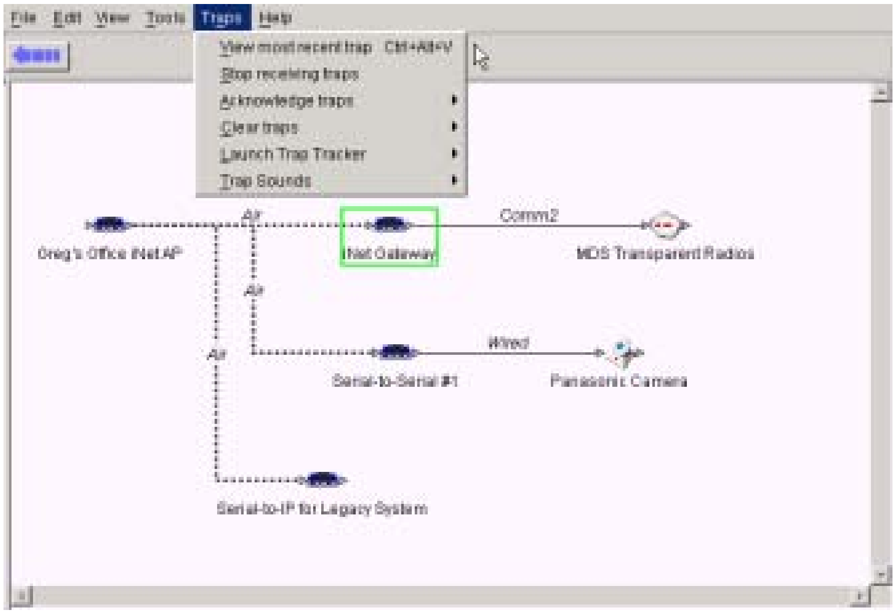


**Figure 46. Trap Management Menu**

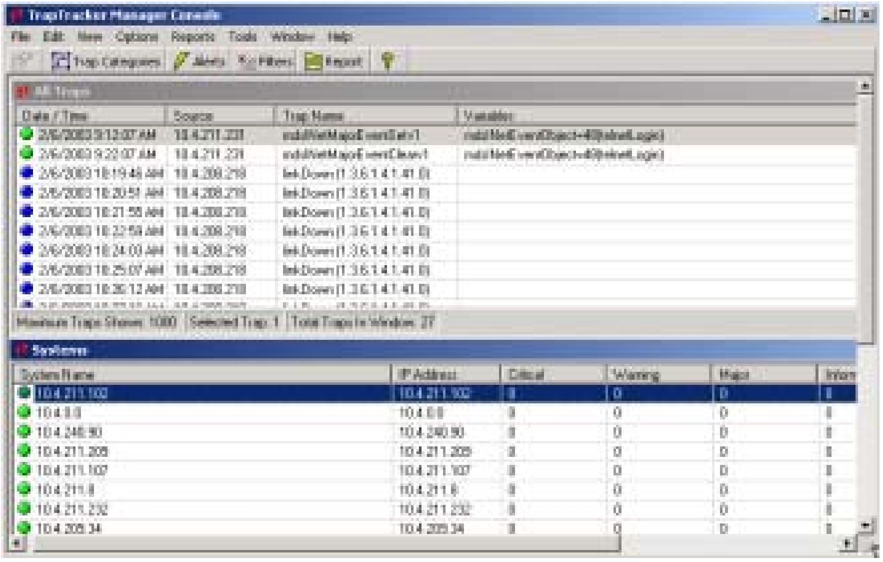
# 6.0 TRAPTRACKER PROGRAM

The NETview CD includes a separate application called TrapTracker. This program is a software-only solution for managing and logging critical events reported by network devices. The multi-threaded architecture of the program guarantees consistent performance and the ability to receive hundreds of thousands of SNMP traps without loss. NETview registers with the TrapTracker Server to exchange trap and alert information.

**NOTE:** Additional details on TrapTracker's features and capabilities are contained in the online documentation provided with the program.

## 6.1 TrapTracker Components

TrapTracker consists of two main elements—a Manager (or Server) and a Viewer. The **Manager** receives and logs all SNMP trap information from network devices and logs them into the TrapTracker database via its built-in Manager Service (called *TTReceiver*). It also includes a console that can be used to monitor events in real time and configure user preferences (alert types and trap severity, for example). A sample console screen is shown in Figure 47.


TrapTracker Manager Console
File Edit View Options Reports Tools Window Help
Trap Categories
Alerts
Filters
Report
All Traps
Systems

| Date / Time | Source | Trap Name | Variables |
|---|---|---|---|
| 2/6/2003 9:12:07 AM | 10.4.211.231 | mdsNetMajorEventSet v1 | mdsNetEventObject=40(mdsnetLogin) |
| 2/6/2003 9:22:07 AM | 10.4.211.231 | mdsNetMajorEventClear v1 | mdsNetEventObject=40(mdsnetLogin) |
| 2/6/2003 10:19:46 AM | 10.4.208.218 | linkDown (1.3.6.1.4.1.41.0) | |
| 2/6/2003 10:20:51 AM | 10.4.208.218 | linkDown (1.3.6.1.4.1.41.0) | |
| 2/6/2003 10:21:55 AM | 10.4.208.218 | linkDown (1.3.6.1.4.1.41.0) | |
| 2/6/2003 10:22:59 AM | 10.4.208.218 | linkDown (1.3.6.1.4.1.41.0) | |
| 2/6/2003 10:24:03 AM | 10.4.208.218 | linkDown (1.3.6.1.4.1.41.0) | |
| 2/6/2003 10:25:07 AM | 10.4.208.218 | linkDown (1.3.6.1.4.1.41.0) | |
| 2/6/2003 10:26:12 AM | 10.4.208.218 | linkDown (1.3.6.1.4.1.41.0) | |

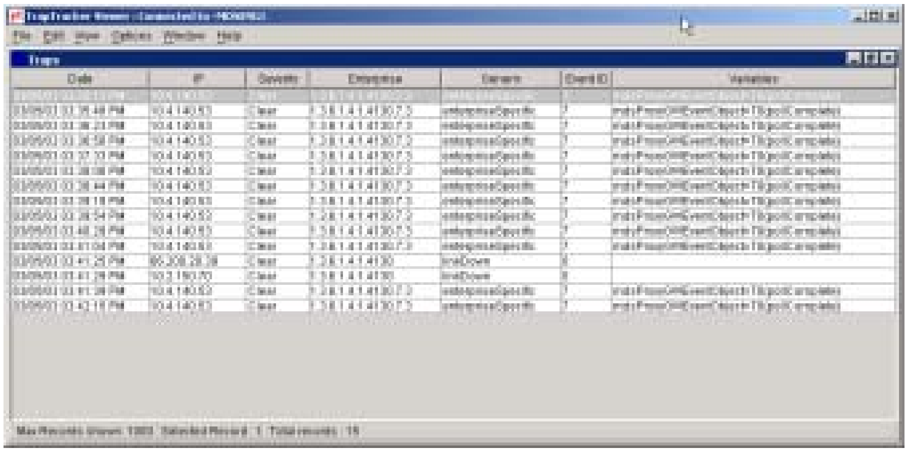
Maximum Traps Shown: 1000 | Selected Trap: 1 | Total Traps in Window: 27

| System Name | IP Address | Critical | Warning | Major | Inform |
|---|---|---|---|---|---|
| 10.4.211.102 | 10.4.211.102 | 0 | 0 | 0 | 0 |
| 10.4.0.0 | 10.4.0.0 | 0 | 0 | 0 | 0 |
| 10.4.240.90 | 10.4.240.90 | 0 | 0 | 0 | 0 |
| 10.4.211.205 | 10.4.211.205 | 0 | 0 | 0 | 0 |
| 10.4.211.107 | 10.4.211.107 | 0 | 0 | 0 | 0 |
| 10.4.211.8 | 10.4.211.8 | 0 | 0 | 0 | 0 |
| 10.4.211.232 | 10.4.211.232 | 0 | 0 | 0 | 0 |
| 10.4.205.34 | 10.4.205.34 | 0 | 0 | 0 | 0 |

**Figure 47. Sample TrapTracker Console Screen**

**NOTE:** The TrapTracker Manager program must be installed prior to installing the NETview application.

The TrapTracker **Viewer** is a Java-based component that is linked to the TrapTracker Manager. It displays real-time or historical SNMP events in a user-friendly environment. The viewer allows selecting devices and creating reports on demand, and provides the option of local or remote monitoring. Figure 48 shows a sample TrapTracker Viewer screen.


TrapTracker Viewer - Connected to - [illegible]
File Edit View Options Window Help
Traps

| Date | IP | Severity | Enterprise | Generic | Event ID | Variables |
|---|---|---|---|---|---|---|
| [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] |
| 03/09/01 03:35:48 PM | 10.4.140.53 | Clear | 1.3.6.1.4.1.4130.7.3 | enterpriseSpecific | 7 | [illegible] |
| 03/09/01 03:36:23 PM | 10.4.140.53 | Clear | 1.3.6.1.4.1.4130.7.3 | enterpriseSpecific | 7 | [illegible] |
| 03/09/01 03:36:58 PM | 10.4.140.53 | Clear | 1.3.6.1.4.1.4130.7.3 | enterpriseSpecific | 7 | [illegible] |
| 03/09/01 03:37:33 PM | 10.4.140.53 | Clear | 1.3.6.1.4.1.4130.7.3 | enterpriseSpecific | 7 | [illegible] |
| 03/09/01 03:38:08 PM | 10.4.140.53 | Clear | 1.3.6.1.4.1.4130.7.3 | enterpriseSpecific | 7 | [illegible] |
| 03/09/01 03:38:44 PM | 10.4.140.53 | Clear | 1.3.6.1.4.1.4130.7.3 | enterpriseSpecific | 7 | [illegible] |
| 03/09/01 03:39:19 PM | 10.4.140.53 | Clear | 1.3.6.1.4.1.4130.7.3 | enterpriseSpecific | 7 | [illegible] |
| 03/09/01 03:39:54 PM | 10.4.140.53 | Clear | 1.3.6.1.4.1.4130.7.3 | enterpriseSpecific | 7 | [illegible] |
| 03/09/01 03:40:29 PM | 10.4.140.53 | Clear | 1.3.6.1.4.1.4130.7.3 | enterpriseSpecific | 7 | [illegible] |
| 03/09/01 03:41:04 PM | 10.4.140.53 | Clear | 1.3.6.1.4.1.4130.7.3 | enterpriseSpecific | 7 | [illegible] |
| 03/09/01 03:41:25 PM | 65.208.28.28 | Clear | 1.3.6.1.4.1.4130 | linkDown | 3 | |
| 03/09/01 03:41:29 PM | 10.2.150.70 | Clear | 1.3.6.1.4.1.4130 | linkDown | 3 | |
| 03/09/01 03:41:39 PM | 10.4.140.53 | Clear | 1.3.6.1.4.1.4130.7.3 | enterpriseSpecific | 7 | [illegible] |
| 03/09/01 03:42:15 PM | 10.4.140.53 | Clear | 1.3.6.1.4.1.4130.7.3 | enterpriseSpecific | 7 | [illegible] |

Max Records Shown: 1000 Selected Record: 1 Total records: 15

**Figure 48. Sample TrapTracker Viewer Screen**

## 6.2 Managing TrapTracker Functions

### Exporting Traps to Non-SNMP Host Programs

TrapTracker's Open Database Connectivity (ODBC) compliance allows for retrieving alarm trap information for SCADA Host programs that do not support SNMP functionality. This retrieval is possible because the TrapTracker database uses a standard Microsoft Access format.

The table of all traps received can be accessed by navigating to: **Program Files\Prism Microsystems\Common\issdb.mdb**. You may also view the traps from TrapTracker's user interface by invoking the **Show Trap History** option. This selection provides a plain-text report.

### Setting Up a TrapTracker Alert

The MDS gateNET collects diagnostic data on its connected radios at a settable interval and stores this information in an internal memory buffer. The buffer needs to be periodically retrieved and cleared by the network management system.

NETview includes a Diagnostics Collection Process, which collects the performance data from a gateNET device and makes this data available to users. The collection process is triggered by the "Database Full" trap from the gateNET. This ensures that the data is collected as soon as the gateNET buffer is nearing its configured capacity, and before it is flushed out.

The Database Full trap triggers the collection process by means of an Alert configured in the TrapTracker application at the time of installation. TrapTracker for Windows (TTW) is a component of the NETview program, and is dedicated to processing, storing and viewing the SNMP traps generated throughout the managed network.

Follow the steps below to create an Alert in the TrapTracker application:

1. Start the TrapTracker Manager console by double-clicking the TrapTracker icon on the desktop, or by selecting **Start>>Programs>>iSMARTset>>TrapTracker>>TrapTracker Viewer.**
2. Click the **Alerts** button on TrapTracker's console toolbar. The Alert window appears.
3. On the Alert window, click **Add**. The Alert Configuration window appears.
4. On the **Alert Configuration** window, perform the following steps:
    a. Enter the **Alert Description** (e.g., **Poll gateNET**).

    b. Leave **Source IP Address** set to **All**.

    c. In the **Generic** field, select **enterpriseSpecific**.

    d. In the Enterprise field, select **mdsGateNETV1Traps**.

    e. In the Traps field, select **mdsGateNETInformEventSetV1**.

    f. In the **Match In VarBinds** field, enter the value **57**.

    g. In the **Actions** field, select **Custom**. The **Configure Action** window should appear. (If it does not, click on **Edit** and select **Custom Tab.**)

    h. In the **Configure Action** window, click **Browse** and navigate to the MDS NETview server installation directory (typically **C:\Program Files\Microwave Data Systems\MDSnv Server**). Select **MDSGateNet-PDC.exe**, click **Open** and then click **OK** on the **Configure Action** window.

    i. Click **OK** on the **Alert Configuration** window and then click **Close** on the **Alerts** window
5. Close the TrapTracker Manager console.

## Maintaining the TrapTracker Database

***Purging the Database***

NETview has an automatic database purge feature for SNMP traps, to prevent the database from growing too large. The default purge time is 30 days, but it can be set to occur at any number of days to suit your needs.

To set the number of days between purges, proceed as folows:

1. Select **File>>Modify Properties.**
2. Click the button for **Server.**
3. Click the drop-down arrow in the Property Name window and select **TTW Traps Table history size (days).**
4. Enter the number of days in the **Value** window and click **Save**.
5. A confirmation window appears. If you approve the displayed value, click **OK** to set the new parameter.

***Freeing Unused Memory Space***

In some cases, deleting old records from the database may not be enough to keep the mdb file size from growing too large. This is because the mdb file size does not decrease after records are deleted. The database retains the unused memory space in the mdb file, and the space is not available for re-use until the memory space is *manually* compacted. Follow these steps to manually compact the database memory:

1. Open the Windows Services control window and stop the **TTReceiver** service.
2. Go to **C:\Program Files\Prism Microsystems\Common** and open **issdbv3.mdb** in Microsoft Access.
3. In Microsoft Access, select **Tools>>Database Utilities>>Compact and Repair Database.**
4. Close Microsoft Access and restart the TTReceiver service.

**TIP:** As an alternative, you may also compact the database using the iSmartSet console. Do this by stopping the TTReceiver service and opening the iSmart program:

**Start>>Programs>>iSmartSet>>iSmartSet Console**

When the iSmart console opens, select **Tools>>Database Maintenance** from the top menu bar to compact the database. Be sure to restart the TTReceiver service when you are done.

# 7.0 APPENDIX A— PROPERTY SETTINGS FOR SERVER AND CLIENT

## 7.1 Server Property Settings

Open **mdsserver.properties** file from installation folder and define the following properties as appropriate:

**DataSource** –This is the name of the data source of Map JDBC database. This is the data source name you defined in previous section prefixed by **jdbc:odbc:**. (Example: **DataSource=jdbc:odbc:CMPDb;**)

**TopologyPort** – The Topology port is the port at which MDSServer receives MDSCMP Client requests for map based GUI actions.

**FileServerPort** – File server port is the port at which MDSServer receives MDSCMP Client requests for file-based requests, which will download/upload configuration files to/from the device.

**NodeDiscoveryPort** –This is the port at which MDSServer receives MDS Client requests for auto-discovery of nodes based on guessed IP addresses.

**PerformancePort** – The Performance Port is the port at which MDSServer receives MDS Client requests for performance statistics requests.

**TimeOut** – This is the timeout of connection channel between MDS Client and MDS Server. This should be chosen carefully, as it will affect how fast a node will be discovered. Too large a value increases response times and too short a value would return a failure notice. An optimal value should be chosen based on typical field response times.

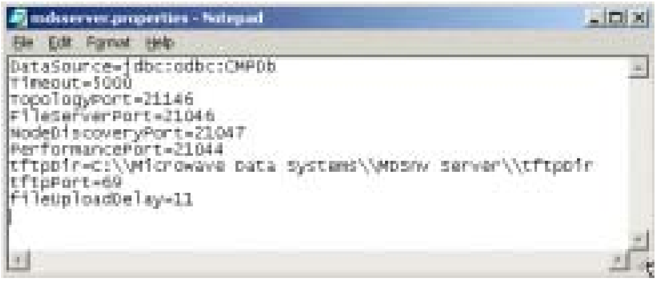
**tftpDir** – This is the folder on the server from which the TFTP server downloads files from and uploads files to a device.

**tftpPort** – The port on which the TFTP Server is “listening.” This port should not be changed normally unless your TFTP server is port configurable.

**fileUploadDelay** – This is a delay factor which controls how much time to wait while uploading an event log file. The proper setting depends on how large the file is.

**KeepAlivePollInterval** -The interval of polling for node connectivity is determined by this parameter in the <mdsserver> file in the server application directory. The default setting is 60,000 milli-seconds (1 minute).

A typical properties file is shown in Figure 49 below:



```
DataSource=jdbc:odbc:CMP06
Timeout=5000
TopologyPort=21146
FileServerPort=21046
NodeDiscoveryPort=21047
PerformancePort=21044
tftpDir=C:\\Microwave Data Systems\\MDSNV Server\\tftpDir
tftpPort=69
fileUploadDelay=11
```

**Figure 49. Typical Server Properties File**

## 7.2 Client Property Settings

Open **mdscmp.properties** file from installation folder and define the following properties as appropriate:

**MDSServer** –This should be equal to the DNS name of the server or IP address of the MDS Server.

**TopologyPort** – Topology port is the port at which the MDSServer receives MDSCMP Client requests for map based actions. This number should be same as **TopologyPort** setting in mdsserver.properties file.

**FileServerPort** – File server port is the port at which the MDSServer receives MDSCMP Client requests for file-based requests, which will download/upload configuration files to/from the device. This number should be same as **FileServerPort** setting in mdsserver.properties file.

**NodeDiscoveryPort** – is the port at which the MDSServer receives MDSCMP Client requests for auto discovery of nodes based on guessed IP addresses. This number should be same as **NodeDiscoveryPort** setting in mdsserver.properties file.

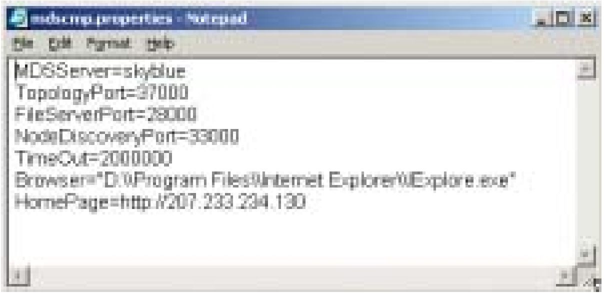
**PerformancePort** – is the port at which the MDSServer receives MDSCMP Client requests for performance statistics requests. This number should be same as **PerformancePort** setting in mdsserver.properties file.

**TimeOut** – This is the timeout of connection channel between MDSCMP Client and MDS CMP Server. This value should be chosen carefully, as it affects how fast a node will be discovered. Too large a value would increase response times and too short a value would return a failure notice. An optimal value should be chosen based on typical field response times.

**Browser** – This is the complete path along with file name to the folder containing the browser executable

**HomePage** – The default web page to display if user does not select a node.

Figure 50 shows a typical properties file:



```
MDSServer=skyblue
TopologyPort=37000
FileServerPort=28000
NodeDiscoveryPort=33000
TimeOut=2000000
Browser="D:\\Program Files\\Internet Explorer\\IExplore.exe"
HomePage=http://207.233.234.130
```

**Figure 50. CMP Properties File**

# 8.0 APPENDIX B— BATCH FILE SETTINGS FOR SERVER AND CLIENT

## 8.1 Server Batch File Settings

To open the MDSServer, launch the batch file **mdssvr.bat** in the NETview installation folder. This file sets several shell environment variables and loads the JVM supplied by the Java Runtime Environment (JRE) 1.3, which in turn loads MDSServer.

If you installed the MDS server in the recommended folder, you only need to modify **JAVA_HOME** variable.

With the **mdssvr.bat** file open, set the following as appropriate:

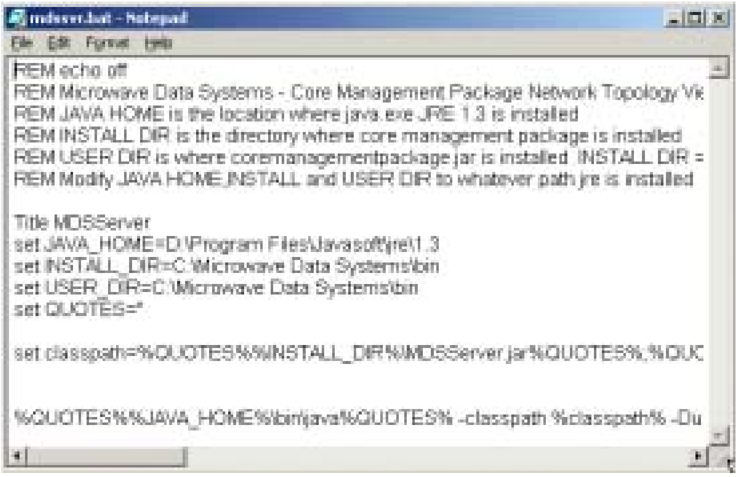
**JAVA_HOME** – This points to the JRE 1.3 full folder path, explained previously.

Example: **D:\Program Files\Javasoft\jre\1.3**

**INSTALL_DIR** – This points to the folder in which the MDS Server is installed. Typically, this is the folder in which this batch file is located.

**USER_DIR** – This is the folder, which the JVM executable will use as a default folder. Typically it is same as **INSTALL_DIR**.

Figure 51 shows a typical batch file:



```
REM echo off
REM Microwave Data Systems - Core Management Package Network Topology Vi
REM JAVA HOME is the location where java.exe JRE 1.3 is installed
REM INSTALL DIR is the directory where core management package is installed
REM USER DIR is where coremanagementpackage.jar is installed. INSTALL DIR =
REM Modify JAVA HOME,INSTALL and USER DIR to whatever path jre is installed

Title MDSServer
set JAVA_HOME=D:\Program Files\Javasoft\jre\1.3
set INSTALL_DIR=C:\Microwave Data Systems\bin
set USER_DIR=C:\Microwave Data Systems\bin
set QUOTES="

set classpath=%QUOTES%%INSTALL_DIR%\MDSServer.jar%QUOTES%;%QUC


%QUOTES%%JAVA_HOME%\bin\java%QUOTES% -classpath %classpath% -Du
```

Figure 51. Typical Batch File

## 8.2 Client Batch File Settings

To open the MDSClient, launch the batch file **mdscmp.bat** in the NETview installation folder. This file sets several shell environment variables and loads the JVM supplied by JRE 1.3. This, in turn, loads MDSClient.

If you installed MDS client in the recommended folder you need only modify the **JAVA_HOME** variable.

With the **mdscmp.bat** file open, set the following as appropriate:

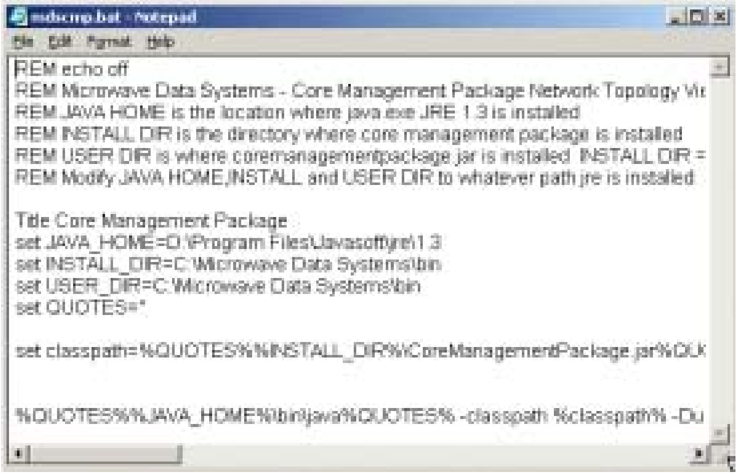
**JAVA_HOME** – This points to the JRE 1.3 full folder path, explained previously.

Example: **D:\Program Files\Javasoft\jre\1.3**

**INSTALL_DIR** – This points to the folder in which MDS Client is installed. Typically this is the folder in which this batch file is located.

**USER_DIR** – This is the folder which the JVM executable will use as a default folder. Typically, it is same as **INSTALL_DIR**.

Figure 52 shows a typical CMP batch file:



```
REM echo off
REM Microwave Data Systems - Core Management Package Network Topology Vi
REM JAVA HOME is the location where java.exe JRE 1.3 is installed
REM INSTALL DIR is the directory where core management package is installed
REM USER DIR is where coremanagementpackage.jar is installed. INSTALL DIR =
REM Modify JAVA HOME,INSTALL and USER DIR to whatever path jre is installed

Title Core Management Package
set JAVA_HOME=D:\Program Files\Javasoft\jre\1.3
set INSTALL_DIR=C:\Microwave Data Systems\bin
set USER_DIR=C:\Microwave Data Systems\bin
set QUOTES="

set classpath=%QUOTES%%INSTALL_DIR%\CoreManagementPackage.jar%QU


%QUOTES%%JAVA_HOME%\bin\java%QUOTES% -classpath %classpath% -Du
```

**Figure 52. Typical CMP Batch File**

# 9.0 APPENDIX C— TERMS AND ABBREVIATIONS

If you are new to IP-based network management tools, some of the terms used in this guide may be unfamiliar to you. The following glossary defines many of these terms, and will prove helpful in understanding the operation of NETview and its interaction with IP devices.

### BER

Bit-error rate. See also BERT.

### BERT

Bit-error rate test. The results of a BERT are normally expressed as a ratio (power of 10) of the number of bits received in error compared to the total number received.

### Bit

Binary digit. The smallest unit of digital data, usually represented by a one or a zero. Eight bits usually comprise a byte.

### bps

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

### CMP

Core Management Package. This refers to the essential elements of the NETview application. It is also the abbreviation used by the NETview server to report error conditions. CMP is equivalent to MDSnv.

### Console Port

The radio port used to manage, control and monitor a local radio through an ASCII-based protocol interface.

### dBm

Decibels relative to one milliwatt. An absolute unit used to measure signal power, as in received signal strength, or RF power output.

### Decibel

A measure of the ratio between two signal levels. Frequently used to express the gain or loss of a system.

### DRAM

Dynamic Random Access Memory.

### DSP

Digital Signal Processing. Advanced circuit technique used to optimize radio performance, primarily in the areas of modulation and demodulation.

### FPGA

Field-Programmable Gate Array

### G.821

The ITU standard by which data transmission quality is measured. The analysis considers available vs. unavailable time of a communications circuit.

### IP

Internet Protocol

### JDBC

Java Database Connectivity

### JRE

Java Runtime Environment

### JVM

Java Virtual Machine

### kbps

Kilobits-per-second

### MDSnv

An abbreviation used to designate the NETview server application.

### Mbps

Megabits-per-second

### MIB

Management Information Base. A database of objects that can be monitored by a network management system using SNMP.

### Network Element

A Network Element is a graphical representation of an IP device on the network map. The device can be an MDS radio, remote telemetry unit (RTU), or any other IP-based element.

### Network Map

A graphical representation of a communications network, showing all IP-connected devices. A network map may also include links to sub-networks or other related equipment.

### NMS

Network Management System

### ODBC

Open Database Connectivity standard

### OID

Object Identifier (SNMP)

### PSOS

Pioneer Server Operating System

### Raw Service Channel

The radio channel used to provide network management.

### RSSI

Received Signal Strength Indication. Expressed in dBm.

### SNMP

Simple Network Management Protocol

### SNR

Signal-to-noise ratio. Expressed in decibels (dB).

### SRAM

Static Random Access Memory

### TCP/IP

Transmission Control Protocol / Internet Protocol—A “guaranteed delivery” protocol used to set up a connection between two devices, with acknowledgement signals (ack/nack) and retries if the data is not received properly. Requires more overhead than UDP (see below) but is important for many mission-critial applications.

### Telnet

Part of the TCP/IP suite of Internet protocols. Enables a user to log on to a remote computer and enter commands as if using a text-based terminal. Also known as a Command-Line Interface (CLI).

## TFTP

Trivial File Transfer Protocol. A standard network protocol used to send and receive files between two devices.

## TMN

Telecommunications Managed Networks—A set of industry-wide standards for network management.

## Trap

An asynchronous event and alarm indication generated by means of SNMP. The trap is transmitted by a connection-less protocol called UDP.

## UDP

User Datagram Packets—A basic, connection-less protocol offering low overhead requirements, but no acknowledgemnent signals or retry capability. Operates in a “broadcast” mode, where a message is sent once to a recipient without regard to whether the message was received correctly. Incomplete messages are discarded by the recipient with no request for a resend.

# IN CASE OF DIFFICULTY...

If you have problems, comments or questions pertaining to the NETview MS program, please contact MDS using one of the methods listed below:

Phone: 585 241-5510
FAX: 585 242-8369

E-Mail: techsupport@microwavedata.com
Web: www.microwavedata.com

industrial/wireless/performance

MDS

Microwave Data Systems Inc.
175 Science Parkway
Rochester, NY 14620
General Business: +1 585 242-9600
FAX: +1 585 242-9620
Web: www.microwavedata.com

*A product of Microwave Data Systems Inc.*