System Release 7.17.x
ASTRO® 25
INTEGRATED VOICE AND DATA

InfoVista
User Guide

FEBRUARY 2020

MN005104A01-B

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

Contact Us

The Solutions Support Center (SSC) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions.

Service agreement customers should be sure to call the SSC in all situations listed under Customer Responsibilities in their agreement, such as:

- Before reloading software
- To confirm troubleshooting results and analysis before taking action

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response. However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

1. Enter motorolasolutions.com in your browser.
2. Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
3. Select "Support" on the motorolasolutions.com page.

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number or title of the section with the error
- A description of the error

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to https://learning.motorolasolutions.com to view the current course offerings and technology paths.

Document History

Version	Description	Date
MN005104A01-A	Original release of the *InfoVista User Guide*	July 2018
MN005104A01-B	Consolidated for the following releases: • 7.17.3 • 7.17.2 • 7.17 Sections updated: • Importing InfoVista Virtual Machine on page 24	February 2020

Contents

List of Figures

List of Tables

List of Processes

List of Procedures

About InfoVista User Guide

This manual describes InfoVista™. InfoVista is a customizable performance management application that is a part of the Transport Network Management (TNM) application suite.

InfoVista interfaces with, and obtains data from, multiple network devices supporting Simple Network Management Protocol (SNMP) including Master Site gateway, Ethernet LAN switches, and WAN switches/Cooperative WAN Routing. This data includes CPU utilization, memory utilization, buffer utilization, port characteristics, and traffic analysis.

What is Covered In the Infovista User Guide

This manual contains the following chapters:

- InfoVista Description on page 19 presents an overview of the information provided by the InfoVista Reports and lists the devices that can be monitored.
- InfoVista Installation on page 23 details installation procedures relating to the InfoVista client application software.
- InfoVista Configuration on page 38 details configuration procedures relating to the InfoVista application software.
- InfoVista Operation on page 40 details tasks that you perform once the InfoVista Reports is installed and operational on your system.
- InfoVista Troubleshooting on page 125 is for fault management and troubleshooting information relating to the InfoVista Report application.
- InfoVista Reference on page 127 contains supplemental reference information relating to InfoVista™.
- InfoVista Disaster Recovery on page 129 provides references and information that enables you to recover InfoVista in the event of a failure.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information about the current course offerings and technology paths, go to http://www.motorolasolutions.com/training.

Related Information

See the following documents for associated information about the radio system.

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as R56 manual. This document may be purchased by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
System Overview and Documentation Reference Guide	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.

Related Information	Purpose
Authentication Services Feature Guide	Provides information relating to the implementation and management of the Active Directory (AD) service, Remote Authentication Dial-In User Service (RADIUS), and Domain Name Service (DNS) in ASTRO® 25 systems.
Backup and Restore Services Feature Guide	Provides information relating to the implementation and management of centralized backup and restore services for supported devices in ASTRO® 25 systems. This manual addresses server and client functions required for these services.
Centralized Event Logging Feature Guide	Provides information relating to the implementation and management of the Centralized Event Logging feature available for ASTRO® 25 systems. This feature enables capturing operating system events generated by most devices in ASTRO® 25 systems. This manual includes information about the server and client function required for the feature.
Core Security Management Server Feature Guide	Provides information relating to the implementation and management of Core Security Management Server (CSMS). The CSMS hosts network security software components in ASTRO® 25 systems, including client and server functions supporting RADIUS authentication for remote access. This manual also includes information about managing system-wide threat prevention along with information associated with security manager user interface hosted on the CSMS.
GGM 8000 System Gateway Feature Guide	Provides information relating to the installation, configuration, and management of the GGM 8000 Gateway used in various network locations.
RF Site Technician Guide	Contains the installation, configuration, operation, and maintenance procedures of the RF Site equipment in ASTRO® 25 L and M Core Trunking sites, including Comparators, Site Controllers, Base Radios, Receivers, Reference and Transceiver Modules.
RF Site Technician Reference Guide	Describes the ASTRO® site components and tools used in their installation, configuration, and maintenance in ASTRO® 25 systems, and contains referential sections that provide additional information relevant when performing operations described in the RF Site Technician Guide, including feature descriptions, diagrams, and lists of parameters.
S6000 and S2500 Routers Feature Guide	Provides information relating to the installation, configuration, and management of the S6000 and S2500 routers used in various network locations.
Virtual Management Server Software User Guide	Provides procedures for implementing and managing VMware ESXi-based virtual server hosts on the common Hewlett-Packard hardware platform in ASTRO® 25 systems.
Windows Supplemental Configuration Setup Guide	Provides additional procedures for Windows-based devices in ASTRO® 25 systems.

Chapter 1

InfoVista Description

This chapter provides a high-level description of InfoVista and the functions it serves on your system.

1.1 InfoVista Overview

InfoVista is a customizable performance management application that is a part of the Transport Network Management (TNM) application suite. When installed, this application is accessible through the Transport Network Management menu or through the InfoVista server.

InfoVista interfaces with, and obtains data from, multiple network devices that support Simple Network Management Protocol (SNMP) including Master Site gateway, Ethernet LAN switches, and Cooperative WAN Routing (CWR). This data includes CPU utilization, memory utilization, buffer utilization, port characteristics, and traffic analysis.

In particular, InfoVista performs the following tasks:

- Collects Management Information Base (MIB) data at the specified time intervals
- Reports and graphs MIB data for single or multiple devices, spanning – daily, weekly, monthly, and yearly time periods
- Provides customized reports using pre-configured report templates for network transport devices in your Motorola radio system

The InfoVista client application is used to access server software and perform administrative tasks such as starting and stopping existing reports, adding an instance, or creating a report.

Network Time Protocol (NTP) is a service used to provide time and date information to devices in the network. The source time and date reference for the InfoVista server is default, that is a local Domain Controller.

1.2 InfoVista Reports

InfoVista performance management software reports can be used for the proactive troubleshooting of network performance and capacity planning.

You can perform the following tasks using InfoVista:

- View custom individual or group reports for the Motorola Network Resources (MNRs), LAN switch, Cooperative WAN Routing (CWR), and the Transport Network Performance Server (TNPS) using daily, weekly, monthly, and yearly report templates
- Filter (search) for a particular report
- Navigate folders organized by the system and zone
- Monitor the system for troubleshooting clues by viewing device activity and using that information to troubleshoot the device
- Use the traps sent to Unified Event Manager (UEM) and daily individual reports for troubleshooting purposes

InfoVista sends warnings and major traps to UEM for the key statistics that it collects. The traps sent to UEM are generated from the daily reports for the individual device, as group reports neither show

thresholds nor generate traps. Traps are only sent to the UEM collocated in the zone, in which the InfoVista server is located.

All key statistics have two thresholds:

- Tw = Threshold warning – If the statistic exceeds this value, a warning trap is sent.
- Tm = Threshold major – If the statistic exceeds this value, a major trap is sent.

The following table lists the different types of reports that can be viewed through InfoVista.

NOTICE: When using InfoVista reports with Conventional IV&D systems/subsystems, some statistics or values may be reported as zero if they are dedicated for the ASTRO® 25 system.

Table 1: InfoVista Report Features

Device	Reports
GCP 8000	• GCP 8000
GGM 8000	• MNR Performance • MNR CWR LMI Performance • MNR Interface Performance • MNR Group Top 10 Performance • MNR PVC Utilization • MNR PVC Queue Performance • MNR Group Top 10 PVC Utilization • MNR Group Top 10 PVC Performance (Queues 3 to 7) • MNR WAN Link Performance
HP LAN Switch	• HP LAN Switch Port Performance • HP LAN Switch Group Top 10 Port Performance
Motorola Network Resource	• MNR Performance • MNR CWR LMI Performance • MNR Interface Performance • MNR Group Top 10 Performance • MNR PVC Utilization • MNR PVC Queue Performance • MNR Group Top 10 PVC Utilization • MNR Group Top 10 PVC Performance (Queues 3 to 7) • MNR WAN Link Performance
Packet Data Router	• PDR Roaming and Registration Statistics • PDR ICMP Traffic • PDR Dropped Messages Statistics • PDR IP Bearer Service Statistics
Radio Network Gateway	• RNG Context Activation

Device	Reports
	• RNG HPD Packet Data Service - UP Connect Information • RNG HPD Packet Data Service - SDU Transmissions • RNG Mobility • RNG Channel Resources • RNG Inbound and Outbound Data Profile
System Wide Devices	• Device Reachability • InfoVista SNMP Traffic Analysis

1.3

User Input and Variable Requirements

The following table contains a list of information that you must obtain before beginning the installation process, to avoid time-consuming delays. Required user input or variable information is indicated by *text in italic font* in the procedures.

NOTICE: Motorola Solutions provides the confidential passwords to approved users. Contact your Motorola Solutions Solutions Support Center (SSC) Representative for additional information. For detailed configuration information, see the System Manual delivered with the system.

Table 2: User Input Requirements

User Input Required	Notes
<TNPS IP address>	IP address **NOTICE:** Contact your network administrator to obtain the IP address.
<Subnet mask>	IP address
<TNPS Default Gateway>	IP address
<Windows Server 2012 administrator password>	Motorola Solutions internal password for the administrator user
<InfoVista administrator password>	Motorola Solutions internal password for the administrator user
<InfoVista ivadmin password>	InfoVista administrator
<InfoVista ivviewer password>	InfoVista End-User
<Unified Event Manager IP Address >	IP address
<Preferred DNS Server IP Address>	IP address
<Alternate DNS Server IP Address >	IP address
NOTICE: DNS Server IP Addresses are required only if your organization uses Centralized Authentication.	

User Input Required	Notes
<Windows Server 2012 Product Key>	Virtual Product/License key associated with the Microsoft Windows Server 2012 media. It may be on a sticker that came with the media or it may be attached to the hardware. **NOTICE:** You can use the same Product/License Key for up to four virtual machines that reside on the same physical Virtual Server. Register the Product/License Key with Microsoft using the standard procedure required by Microsoft (for instructions, click the **Keys** icon that appears in the system tray).

1.4 Required License Keys

The following license keys are required for the InfoVista installation process:

- Windows Server 2012 license key, on a sticker on the *Microsoft Windows Server 2012 Getting Started* book
- InfoVista license key

NOTICE: If you do not have the necessary license keys, contact the Motorola Solutions Support Center (SSC).

1.5 Other InfoVista Reference Sources

The InfoVista Documentation Guide is available in PDF format in the InfoVista Help menu. Infovista Administration Guide, Infovista Development Guide or Infovista Installation Guide can be accessed from the Windows Start menu of the server or client workstation. From the Start menu, go to: **Apps → Infovista**

Chapter 2

InfoVista Installation

This chapter details the installation procedures relating to InfoVista.

2.1 Software Installation Options

This section contains two types of software installation procedures:

- Full software installation procedures
- Software re-installation procedures

Motorola pre-installs all the required software before the system installation. This booklet provides procedures to install all the required software and configure the server in the event of equipment failure.

2.2 Full Software Installation

Full software installation procedures typically represent those procedures that are conducted before product shipment and usually represent a full installation of operating system software and application software.

While full software installation activities are often accomplished before product shipment, some situations call for full software installation procedures in the field (such as when a boot hard drive fails).

2.3 Software Re-Installation

Software re-installation procedures typically represent an installation of application software employing the same software or software version used during an initial software installation.

You perform software re-installation procedures after the system installation, to load new equipment with software or to perform system configuration changes.

2.4 Installation Scenarios

The following table explains the frequently occurring installation scenarios.

Table 3: Installation Scenarios

Installation Scenario	Audience
To configure a Transport Network Performance Server (TNPS) that already has the software loaded.	Motorola Solutions staff who configure the system. Where to begin: *Installing the Plug-in and Completing the Installation*.
To re-install all software on the TNPS.	Use this scenario if you re-install all software under advice from the Motorola Solutions Support Center (SSC). Where to begin: Software Pre-Installation Requirements and Considerations on page 24.

Installation Scenario	Audience
Received new TNPS.	Anyone who has to install software for a new TNPS server. Where to begin: Software Pre-Installation Requirements and Considerations on page 24.

2.5 Software Pre-Installation Requirements and Considerations

Review the following list of requirements and considerations before installing the software. If you do not have any of the following information, contact your system administrator or the local Motorola Solutions field representative.

- Make sure you have appropriate network administrative rights or privileges required to install the software.
- Make sure that all CD-ROMs and other software media are available before starting any software installation activity.
- Identify and review all appropriate installation procedures required to complete the software installation process being implemented before installation to become familiar with its characteristics and requirements.
- Obtain all required system information and configuration data (IP addresses, host names, and so forth) before installing any software.
- Make sure the software installation process will not negatively affect the operating condition of the system during critical or heavy system usage.
- Notify your regional support centre and your operations group prior to starting any procedures that would impact system performance.
- Notify your administration group that you are performing system maintenance and features will be affected and unavailable.

2.6 Setting up InfoVista Virtual Machine

Perform the procedures in this section to set up an InfoVista as a virtual machine on a virtual server.

2.6.1 Importing InfoVista Virtual Machine

Use this procedure to set up an InfoVista Virtual Machine

Prerequisites: From your system administrator, obtain:

- Motorola Virtual Appliance DVD (Contains the Windows 2012 InfoVista virtual machine files)
- Virtual Server Host (ESXi-based server) IP address
- ESXi-based server administrator account name and password

NOTICE: Before performing this procedure, connect the virtual machine to the DVD drive where the software media is inserted. See the ASTRO® 25 system *Virtual Management Server Software User Guide* for information about connecting DVD drives to virtual machines in the ASTRO® 25 system.

Procedure:

1. Launch the **VMware vSphere Client** from the Windows-based device where it resides (a desktop shortcut was created during installation).

   A dialog box appears prompting for an IP address, user name, and password.

2. Type the ESXi server IP address, then type the user name `root`, and the ESXi server root user password. Then, click **Log in**.

   The vSphere Client Inventory screen appears.

3. In the DVD drive of the Windows server where the vSphere Client resides, insert the *Virtual Appliance – InfoVista* DVD.

4. For optimal speed during the import process, copy the following InfoVista virtual machine folder from the DVD to any location on the hard drive of the Windows device that you are using for this import:

   `IV-Astro-`***`<RR.RR.RR>.<XX-XX>`***

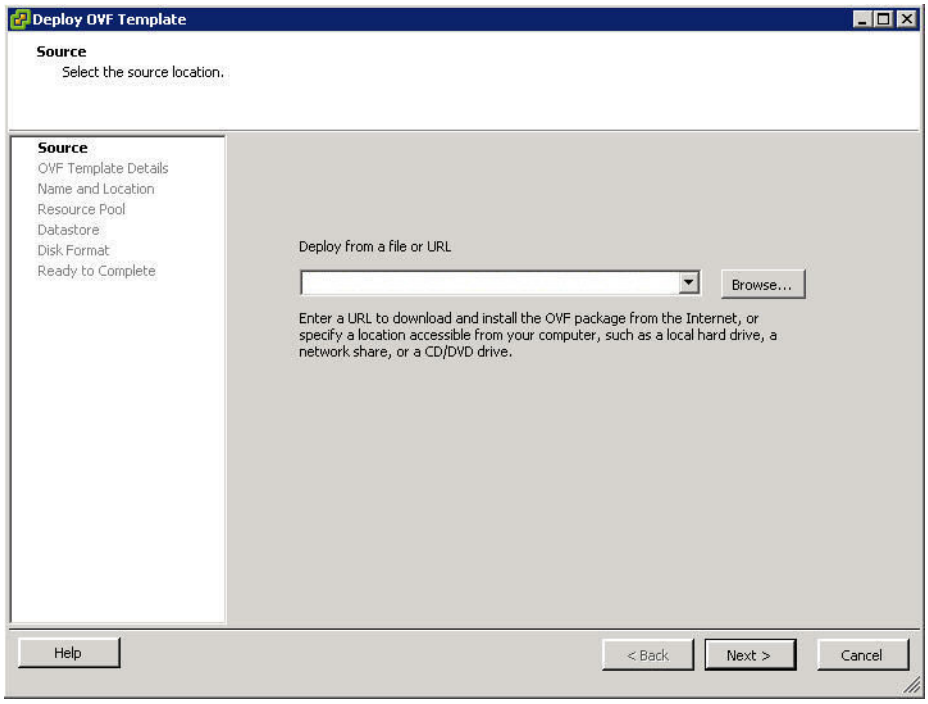
   At this time, you can copy the folders for all the virtual machines that you plan to import using this Windows server.

   NOTICE: In the version number, ***`<RR.RR.RR>`*** represents the release information, and ***`<XX-XX>`*** represents the OVF image version.

5. From the **File** menu in the vSphere Client, select **Deploy OVF Template**.

   The following window appears.

   Figure 1: Deploy OVF Template Window – Source



6. Click **Browse**.

   A window displays file directories.

7 Navigate to the virtual machine files on the DVD, or if you copied them to the hard drive, navigate to the directory where you pasted them. Select the following file: `IV-Astro-<RR.RR.RR>.<XX-XX>` and click **Open**.

NOTICE: In the version number, ***<RR.RR.RR>*** represents the release information, and ***<XX-XX>*** represents the OVF image version.

The file name and path for the virtual machine you selected appear on the Deploy OVF Template window.

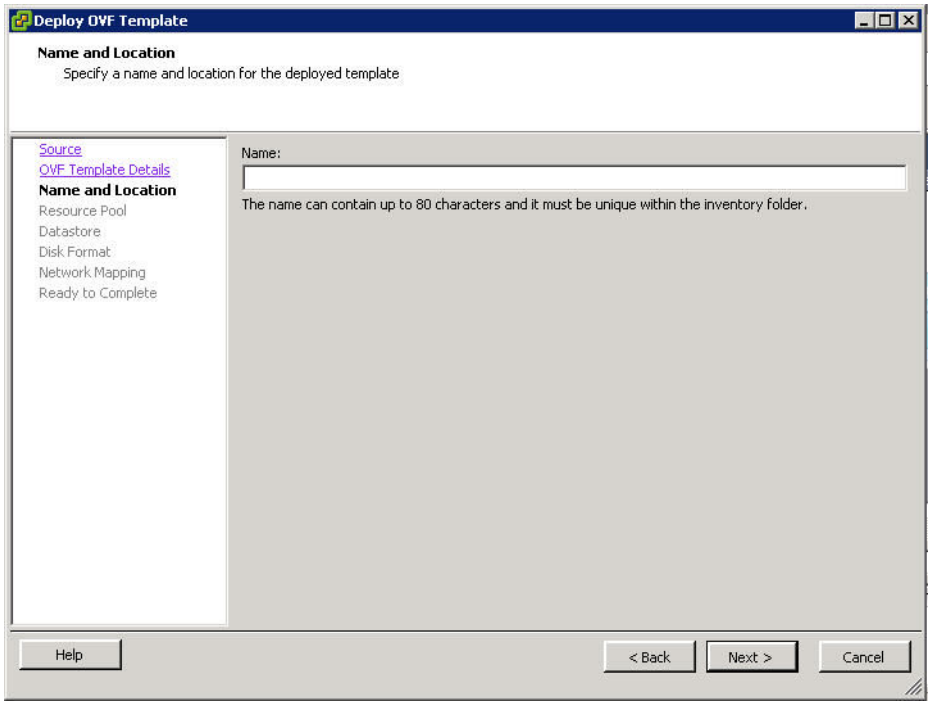
8 Click **Next**.

The OVF Template Details screen appears in the Deploy OVF Template window.

9 Click **Next**.

The following screen appears.

Figure 2: Deploy OVF Template Window – Name and Location



10 In the **Name** field, the name `InfoVista` can already be pre-populated. Change it to the appropriate hostname of the InfoVista Server (infovi1). Click **Next**.

NOTICE: For a system implementing a Dynamic System Resilience feature, use the `infovi2` hostname for the InfoVista in the backup core.

11 In the DataStore list, perform one of the following actions:

If…	Then…
If a 4524 / 4525 DAS or a 4124 / 4125 expansion enclosure is used,	select datastore1.
If a 3520 DAS is used in a regular core,	select datastore2.
If a 3520 DAS is used in a High Capacity UNC core,	select datastore3.

IMPORTANT: DataStore for InfoVista should be DAS1 or DAS2. So, select DAS1 or DAS2 DataStore. It is important to make sure that InfoVista VM resides on DAS1 or DAS2 DataStore.

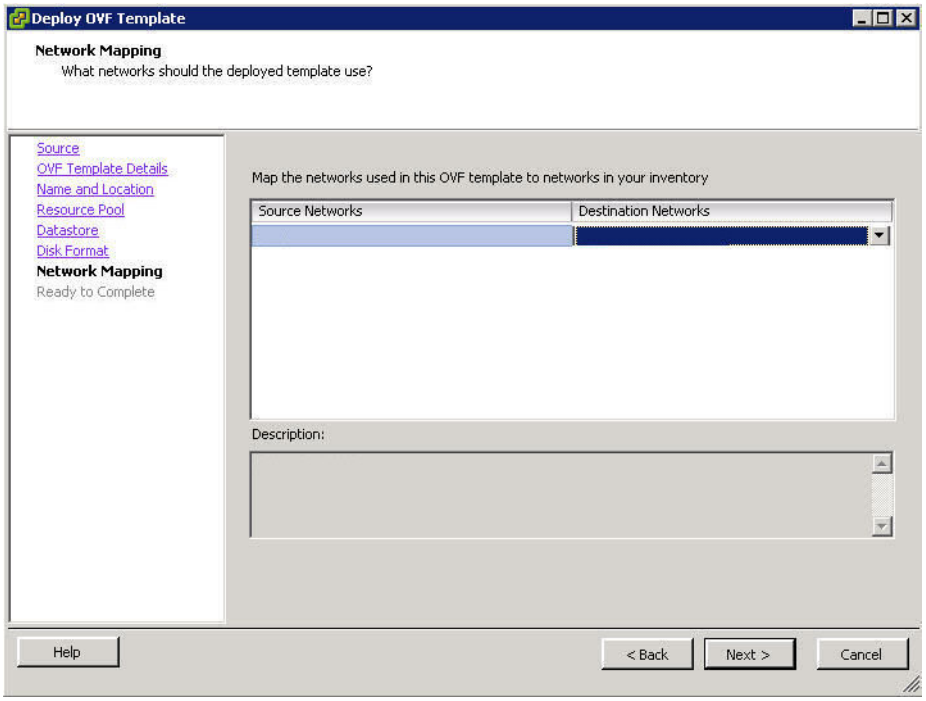
12 Click **Next**.

The Disk Format screen appears in the **Deploy OVF Template** window.

13 Leave the default option, that is **Thick Provisioned Lazy Zeroed**. Click **Next**.

The following screen appears.

Figure 3: Deploy OVF Template Window – Network Mapping



14 Select the UCS network for the InfoVista virtual machine from the **Destination Networks** drop-down list. Click **Next**.

NOTICE:
The Destination Networks in the drop-down list correspond to the Network Labels entered in the properties for the virtual switches on the Hardware: Networking screen in vSphere Client.

The Source Networks column lists the networks specified in the OVF file.

If the appropriate network label does not appear in the **Destination Networks** drop-down list, review the procedure for configuring Virtual Networking in the ASTRO® 25 system *Virtual Management Server Software User Guide* to determine what steps were missed.

The **Ready to Complete** screen appears in the **Deploy OVF Template** window.

15 In the **Ready to Complete** window, verify the information that is displayed is correct. Click **Finish**.

The **Deploying...** window appears showing the progress of the deployment. It takes 10 to 20 minutes.

16 Once the InfoVista Server virtual machine is imported, the `Completed successfully` message appears. Click **Close**.

The InfoVista Server virtual machine import is completed.

17 Verify that the left pane of the vSphere Client main window displays the InfoVista server virtual machine name that you entered in step 10.

NOTICE: You may need to expand the list in the left pane to locate the virtual machine name.

18 Remove the media from the drive.

2.6.2
Connecting and Powering On Virtual Machine

When and where to use: This procedure contains the detailed instructions to connect to and power on the virtual machine that was imported in the Importing InfoVista Virtual Machine on page 24 procedure.

NOTICE: The name of the appropriate zone network for the server you are setting up as a virtual machine is the same as the Destination Network that you selected in Importing InfoVista Virtual Machine on page 24, step 14.

Procedure:

1 Edit the configuration settings for the virtual machine import. Right-click the virtual machine in the navigation pane and select **Edit Settings** from the pop-up menu.

The **Virtual Machine Properties** window appears.

2 For each Network Adapter listed in the left pane, select the **Network Adapter** and then select the **Connect at power on** check box. Ensure that the correct zone network connection displays for Network Label.

NOTICE: For information about Network Adapters, Network Labels and other virtual networking settings, see the Virtual Networking sections in the configuration chapter of the *Virtual Management Server Software User Guide*.

3 Click the **Options** tab and select **CPU/MMU virtualization** option from the left pane.

4 Select **Intel VT-x/AMD-V for instruction set virtualization and Intel EPT/AMD RVI for MMU Virtualization** radio button.

5 Click **OK**.

6 Turn on power to the virtual machine. Right-click each virtual machine imported and select **Power → Power On**.

The selected virtual machine powers on. The icon of the virtual machine turns green in the left pane and displays a green triangle.

2.6.3
Configuring the vCenter for the Newly Deployed VM

For newly deployed virtual machines to run properly in an existing vCenter environment, you must override the default High Availability (HA) cluster settings and modify the restart priority for the new virtual machines. After a Virtual Management Server (VMS) host fails, the virtual machines are restarted in the relative order determined by their restart priority.

When and where to use:

- This procedure applies only to systems where the vCenter application is installed.

- Perform this procedure only if an Open Virtualization Format (OVF) virtual machine was deployed after the vCenter was originally configured.

Procedure:

1. Launch the Internet Explorer from a Windows-based device, such as the Network Management (NM) Client, or a service computer or laptop.
   - In the address field of the browser, enter the address in the following format: `https://<vCenter_IP_address>/vsphere-client`
   - Ignore or accept any warnings about the connection security or self-signed certificates.
2. In the dialog box, perform the following actions:
   a. Enter the user name in the following format:

      `administrator@z00<Z>vcs<H>.zone<Z>`
      <Z> is the zone number

      <H> is the vCenter instance number

   b. Enter the password for the administrator account.
   c. Click **Login**.

   The vSphere Web Client homepage appears.
3. In the left pane, click **Hosts and Clusters**.
4. Expand the tree and right-click the **Zone***<X>* HA cluster

   where *<X>* is the zone number.
5. Select **Settings**.
6. In the **Settings** window, click **VM Overrides**.
7. Click **Add**.
8. Click the plus (**+**) button.
9. Select the check box for the virtual machine you are configuring. Click **OK**.
10. Depending on the virtual machine you are configuring, select the appropriate value for **VM Restart Priority**.
    - For the vCenter virtual machine, select **Medium**.
    - For virtual machines that are monitored under Fault Tolerance, select **High**.
    - For virtual machines that are not monitored under Fault Tolerance or HA, select **Disabled**.
11. Click **OK**.
12. Optional: **If you are recovering the virtual machine after a failure and the virtual machine is not monitored under Fault Tolerance:** Perform the following actions:
    a. In the **Settings** window, click **VM/Host Groups**.
    b. Select the group for the VMS host where the virtual machine resides. Click **Edit**.
    c. Click **Add**.
    d. Select the check box next to the virtual machine. Click **OK**.

       For information about the locations of virtual machines on the VMS and their configurations with regard to vCenter, see "Virtual Machine Locations for vCenter Configs" in the *ASTRO 25 vCenter Application Setup and Operations Guide*.
    e. Click **OK**.

    The restart priority setting for the newly deployed virtual machine is configured.

2.6.4
Setting Startup and Shutdown Order

In an ASTRO® 25 system, virtual machines hosted on a Virtual Management Server (VMS) are configured to boot automatically with the system in a prescribed order. When you install a virtual machine on a VMS, change the VMS settings to ensure that the new virtual machine boots in the correct order with respect to the other virtual machines hosted on the VMS.

Procedure:

1. From a Windows-based device, launch the **VMware vSphere Client**.

   A desktop shortcut was created during installation.
2. Log on to the server as `root`.
3. On the upper left side of the **vSphere Client Inventory** window, select the ESXi server.
4. On the right side of the window, select the **Configuration** tab.

   The window displays information about the configuration of the ESXi server.
5. In the **Software** section, select **Virtual Machine Startup/Shutdown**.
6. On the right side of the main window, select **Properties**.
7. In the **System Settings** area, select **Allow virtual machines to start and stop automatically with the system**.
8. In the **Default Startup Delay** area, select **Continue immediately if the VMware Tools start**.
9. In the **Default Shutdown Delay** area, from the **Shutdown Action** drop-down list, select **Guest Shutdown**.
10. Put the virtual machines hosted on the ESXi server in the correct boot order:
    a. In the **Startup Order** area, from the **Automatic Startup** list, select a virtual machine.
    b. By using the **Move Up** and **Move Down** buttons, move the virtual machine to the correct ordered slot.

       NOTICE:
       Zone Core Virtual Machine Boot Order on page 31 outlines the boot order for the virtual machines that can reside on an ESXi-based Virtual Management Server (VMS).

       See the boot order table to determine the correct ordered slot for each virtual machine hosted on the ESXi server that you are configuring.
    c. Repeat steps 10a and 10b until the boot order for the virtual machines is correct.
11. Click **OK**.

    The **Properties** window closes.

2.6.4.1

Zone Core Virtual Machine Boot Order

NOTICE:
Up to two instances of the Graphical Master Computer (GMC) for MOSCAD Network Fault Management (NFM) can be on the server.

If the Unified Network Configurator Device Server (UNCDS) is present, three instances of the UNCDS are on the server.

Table 4: Zone Core Virtual Machine Boot Order

Order		Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
Automatic Startup						
	1	ZC	Enabled	Use Default	Use Default	Use Default
	2	Transcoder	Enabled	Use Default	Use Default	Use Default
	3	ISGW	Enabled	Use Default	Use Default	Use Default
	4	PDG-Conv	Enabled	Use Default	Use Default	Use Default
	5	PDG-HPD	Enabled	Use Default	Use Default	Use Default
	6	PDG-IV&D	Enabled	Use Default	Use Default	Use Default
	7	License Manager	Enabled	Use Default	Use Default	Use Default
	8	ATR	Enabled	Use Default	Use Default	Use Default
	9	DC-System	Enabled	Use Default	Use Default	Use Default
	10	Intermediate CA	Enabled	Use Default	Use Default	Use Default
	11	CWES	Enabled	Use Default	Use Default	Use Default
	12	DC-Zone	Enabled	Use Default	Use Default	Use Default
	13	IPCAP	Enabled	Use Default	Use Default	Use Default
Any Order		AuC	Enabled	Use Default	Use Default	Use Default
		BAR	Enabled	Use Default	Use Default	Use Default
		CSMS	Enabled	Use Default	Use Default	Use Default
		ESS DB Server	Enabled	Use Default	Use Default	Use Default
		InfoVista	Enabled	Use Default	Use Default	Use Default
		FMS – Fortinet	Enabled	Use Default	Use Default	Use Default
		GDG	Enabled	Use Default	Use Default	Use Default
		GMC	Enabled	Use Default	Use Default	Use Default
		LMP	Enabled	Use Default	Use Default	Use Default
		NM Client	Enabled	Use Default	Use Default	Use Default
		UCS	Enabled	Use Default	Use Default	Use Default
		SSS	Enabled	Use Default	Use Default	Use Default
		Syslog	Enabled	Use Default	Use Default	Use Default
		UEM	Enabled	Use Default	Use Default	Use Default
		UNC	Enabled	Use Default	Use Default	Use Default

Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
	UNCDS	Enabled	Use Default	Use Default	Use Default
	vCenter App	Enabled	Use Default	Use Default	Use Default
	ZDS	Enabled	Use Default	Use Default	Use Default
	ZSS	Enabled	Use Default	Use Default	Use Default
Manual Startup	DESU Waypoint	Disabled	Use Default	Use Default	Use Default

2.6.5
Configuring InfoVista Virtual Machine

Use this procedure to configure InfoVista Virtual Machine.

Prerequisites:

- The new InfoVista virtual machine must already be powered on. See Connecting and Powering On Virtual Machine on page 28.
- The Windows Server 2012 Product Key must be obtained from the system administrator.
- The administrator password must be obtained from the system administrator.

NOTICE: For details, see User Input and Variable Requirements on page 21.

Procedure:

1. After powering on the InfoVista virtual machine, as described in the Connecting and Powering On Virtual Machine on page 28 section, click the InfoVista virtual machine in the navigation pane on the left side of the screen.
2. Click the **Console** tab on the right side of the screen.

   The Console tab for the InfoVista displays the Settings Wizard.
3. Select the appropriate **Country or region**, **App language**, and **Keyboard layout** in the Settings Wizard. Click **Next**.

   The window for entering the Windows Server 2012 Product Key is displayed.
4. Enter the `Windows Server 2012 Product Key`. Click **Next**.

   The **License Agreement** window appears.
5. Click **I accept**.

   A message appears stating that a password for the built-in administrator account must be typed.
6. Type the new `administrator password` twice and press FINISH.

   The login screen appears.
7. Set your time zone.
   a. In the bottom-right corner of the taskbar, click on the Date/Time settings and click **Change date and time settings...**

      The **Date and Time** window appears.

b Click on **Change Time Zone**.

The **Time Zone Settings** window appears.

c Select your timezone and click **OK**.

The selected timezone is set.

8 Proceed to the Primary/Backup InfoVista Server Configuration on page 33 process.

2.7 InfoVista Software Media

This section contains the list of elements required for the InfoVista software installation.

The contents of the following media exist on the InfoVista image that was imported:

- Microsoft Windows Server 2012 Embedded Standard Edition
- InfoVista 5.0 media
- Transport Network Performance Plug-in CD
- *Windows Supplemental* media

The InfoVista software is pre-installed in the InfoVista image that was imported.

2.8 Primary/Backup InfoVista Server Configuration

This section provides details about the primary and backup InfoVista server configuration process flow.

2.8.1 Primary InfoVista Server Configuration Process Flow

Process:

1 Upgrade the VMware Tools. See “Upgrading VMware Tools on Windows-Based Virtual Machine" in the *Virtual Management Server Software User Guide*.

2 Configure the primary InfoVista server. See Configuring the Primary InfoVista Server on page 33.

3 Verify the MAC address. See Verifying the MAC Address on page 39.

4 Configure InfoVista License Key. See Configuring the InfoVista License Key on page 38.

5 Join InfoVista Server to the Active Directory Domain. See the *Windows Supplemental Configuration Setup Guide*.

6 Install the McAfee Agent Software. See the *Core Security Management Server Feature Guide*.

2.8.1.1 Configuring the Primary InfoVista Server

Use this procedure to configure the Primary InfoVista Server.

Prerequisites: From the system administrator, obtain:

- Transport Network Performance Plug-in CD
- *Windows Supplemental* media
- Co-located Zone ID
- WAN Link type

- Time Zone information
- SNMP Authentication and Privacy passwords (If System is configured for SNMP Secure Mode)

Procedure:

1. Log on to the Windows-based device using the credentials for your administrator account that is maintained locally on the Windows-based device.

   For Windows Server 2012-based devices, the account name set up by Motorola Solutions is Motosec.

   NOTICE: Ensure that the local hostname is selected in the **Log on to** field.

2. From the **vSphere Client**, click the **CD/DVD**  icon.
3. From the drop-down menu, select **CD/DVD drive** → **Connect to E**.
4. Insert the *InfoVista Plug-In* media to the CD/DVD drive.
5. Navigate to `E:\` and double-click `infoVista_scripts.msi`

   Installation scripts are copied to `C:\Program Files\Motorola\AstroIV\scripts`

6. Remove the *InfoVista Plug-In* from the CD/DVD drive.
7. From the **vSphere Client**, click the **CD/DVD**  icon.
8. From the drop-down menu, select **CD/DVD drive** → **Connect to E**.
9. Insert the *Windows Supplemental* media to the CD/DVD drive.
10. From the **Start** menu, select **All Programs** → **Accessories** → **Windows PowerShell**.
11. Right-click **Windows PowerShell** and select **Run as Administrator**.
12. Change directory to `C:\Program Files\Motorola\AstroIV\scripts` and run the command `.\InstallIV.ps1`
13. After the message `Enter the hostname of this InfoVista Server (infovi1/infovi2):` appears, perform one of the following:

If…	Then…
If InfoVista Server is installed in Primary Core,	type `infovi1` and press ENTER.
If InfoVista Server is installed in Backup (DSR) Core,	type `infovi2` and press ENTER.

14. After the message `Enter the local administrator password:` appears, type the local administrator password twice and press ENTER.
15. After the message `Enter the Co-located Zone ID [1-7]:` appears, type the appropriate Co-located Zone ID and press ENTER.
16. In the prompt asking for the time zone, select the appropriate and click **OK**.
17. After the message `Enter the WAN Link type (DS1/E1):` appears, type `DS1` and press ENTER.
18. After the message `Motorola Windows BAR Client should be installed (yes/no):` appears, type `yes` or `no` and press ENTER.

19 After the message `Motorola Windows Logging Client should be installed (yes/no):` appears, type `yes` or `no` and press ENTER.

20 After the message `Please Enter the SNMP Mode of this System (secure/clear):` appears, type `Secure` or `Clear` and press ENTER.

21 If you typed `Secure`, type SNMPv3 Authentication and SNMPv3 Privacy passwords twice and confirm by pressing ENTER.

22 When the **WIF execution log window** appears with `Installation finished.` message, click **OK**.

IMPORTANT:
Installation is complete and InfoVista Discovery process is automatically initiated as a background task via Task Scheduler. Depending on the number of zones in the system, InfoVista discovery may take 2-3 hours (per zone) to complete. Log on to IVReports after this time to view all the discovered devices and their corresponding performance-related reports.

2.8.2
Backup InfoVista Server Configuration Process Flow

Prerequisites: The Primary InfoVista Server is already configured.

When and where to use: Use this process to configure the Backup InfoVista Server.

Process:

1 Upgrade the VMware Tools. See “Upgrading VMware Tools on Windows-Based Virtual Machine" in the *Virtual Management Server Software User Guide*.

2 Configure the backup InfoVista server. See Configuring the Backup InfoVista Server on page 35.

3 Verify the MAC address. See Verifying the MAC Address on page 39.

4 Configure InfoVista License Key. See Configuring the InfoVista License Key on page 38.

5 Join InfoVista Server to the Active Directory Domain. See the *Windows Supplemental Configuration Setup Guide* for instructions.

6 Install the McAfee Client Software. See the *Core Security Management Server Feature Guide*.

2.8.2.1
Configuring the Backup InfoVista Server

Use this procedure to configure the Backup InfoVista Server.

Prerequisites:

- The Transport Network Performance Plug-in CD has been obtained from the system administrator.
- The Primary InfoVista Server has already been configured.
- The Windows Supplemental media has been obtained from the system administrator.
- The Co-located Zone ID has been obtained from the system administrator.
- The WAN Link type has been obtained from the system administrator.
- The Time Zone information has been obtained from the system administrator.
- The SNMP Authentication and Privacy passwords (If System is configured for SNMP Secure Mode) have been obtained from the system administrator.

Procedure:

1. Log on to the Windows-based device using the credentials for your administrator account that is maintained locally on the Windows-based device.

   For Windows Server 2012-based devices, the account name set up by Motorola Solutions is Motosec.

   NOTICE: Ensure that the local hostname is selected in the **Log on to** field.

2. Use the procedure: Configuring the Primary InfoVista Server on page 33.

2.9 Configuring Trap Receiver Address

Prerequisites: Log on to the InfoVista server by using the local administrator account.

NOTICE: When using Active Directory credentials, make sure that the Active Directory domain is selected in the **Log on to** field. If your Active Directory account fails, enter the credentials for a Windows user account that is maintained locally on this Windows-based device, and make sure that the local hostname is selected in the **Log on to** field. If you are logging on with a local account, and you must perform operations requiring Windows administrator privileges, log on with a local Windows administrator account (the account name set up by Motorola is Motosec for Windows Server 2012-based devices).

When and where to use: Use this procedure to configure the trap receiver address.

Procedure:

1. Right-click **IVreport** icon and select **Run as Administrator**.

   The **InfoVista** login window opens.

   NOTICE: If the error `Communication failure` appears, reboot the InfoVista Server twice and redo this procedure starting with step 1.

2. In the Login window:
   - Type the appropriate user name in the **User name** field
   - Type the appropriate password in the **Password** field
   - Leave the **Server name** field blank
   - Click **OK**.

   The **InfoVista–local** window appears.

3. In the **InfoVista–local** window, click the **System** tab.

   The content of the System tab displays.

4. In the **System** tab expand **Setup Families**, click **Network**, and then expand **Network**.

   The right pane shows the properties of the network.

5. In the right pane double-click **SNMP trap receiver (auxiliary)**.

   The property value window opens.

6. In the **Value** section, type the IP address of UEM, which is co-located in the same Zone as this InfoVista server. Click **OK**.
7. Close the **InfoVista-local** window.

   The window disappears.

2.10 Running the Discovery Script Manually

Prerequisites:
Ensure that the Discovery Script is not already running in the background. It is automatically started after the installation process, or launched weekly via a Task Scheduler.

When and where to use: Use this procedure to manually run the discovery script.

Procedure:

1. Launch Task Manager
2. Open the **Processes** tab
3. Check for any "Perl Interpreter" tasks in the Background processes list. If there is any present, it means that the Discovery Script is already running.
4. Open a command prompt and navigate to the `D:\IV-Customizations\Discovery` directory.
5. Enter: `ivdisc.pl`

   NOTICE: A blank cursor is blinking as the script executes. Do not open the log files until the script completes. On a large system, running this discovery script manually can take 2-3 hours per each zone.

   The script completes and the command prompt appears.
6. Close the command prompt window.

2.11 The AntiVirus Software Installation

For installation procedures, see “CSMS – Deploying McAfee Client Software to Anti-Malware Clients” procedure in the *Core Security Management Server Feature Guide*.

Chapter 3

InfoVista Configuration

This chapter details the configuration procedures relating to InfoVista.

3.1 Configuring the InfoVista License Key

When and where to use: Use this procedure to configure an InfoVista License Key if you are using an evaluation license key.

Procedure:

1. Log on to the Windows-based device using the credentials for your account that is a member of the Active Directory group for logging in to this device (for example, “all-windows-login” is the group for logging in to the InfoVista Client).

   NOTICE: When using Active Directory credentials, make sure that the Active Directory domain is selected in the **Log on to** field. If your Active Directory account fails, enter the credentials for a Windows user account that is maintained locally on this Windows-based device, and make sure that the local hostname is selected in the **Log on to** field. If you are logging on with a local account, and performing operations that require Windows administrator privileges, log on with a local Windows administrator account (the account name set up by Motorola is motosec for Windows Server 2012-based devices).

2. Right-click on the Windows Start Button and select **Run** option.

   The **Run** dialog box appears.

3. In the **Open:** field, type **`ivconfiggui.exe`** and click **OK**.

   The **InfoVista Server Configuration** window appears.

4. In the **Key** field, replace "EVAL" with the full production license Key. Then, click **Save and Close**

   The full license is applied and the **InfoVista Server Configuration** window closes.

   NOTICE:
   Keys from previous versions of Infovista Server do not work with Infovista Server 5.0. Contact your Infovista Representative to obtain a valid license key for the latest version.

   The InfoVista Server Configuration window contains System Id information, which is required to generate the license key.

3.2 The Windows Server 2012 Server OS Configuration

This section contains the following procedures:

- Verifying the MAC Address
- Verifying the Windows Server 2012 User Logons

3.2.1
Verifying the MAC Address

When and where to use: Use this procedure to verify the MAC address and obtain the physical address.

Procedure:

1. Log on to the Windows-based device using the credentials for your account that is a member of the Active Directory group for logging in to this device (for example, “all-windows-login” is the group for logging in to the InfoVista Client).

   NOTICE: When using Active Directory credentials, make sure that the Active Directory domain is selected in the **Log on to** field. If your Active Directory account fails, enter the credentials for a Windows user account that is maintained locally on this Windows-based device, and make sure that the local hostname is selected in the **Log on to** field. If you are logging on with a local account, and you need to perform operations requiring Windows administrator privileges, log on with a local Windows administrator account (the account name set up by Motorola is Motosec for Windows Server 2012-based devices).

2. To verify the TCP/IP configuration, from the **Start** menu, select **Programs** → **Accessories** → **Command Prompt**, and enter `ipconfig /all`

   A display shows the configuration information that you entered.

3. Note the **Physical Address** information. The physical address is the MAC address you need to obtain the license key for InfoVista.

4. Test the link by pinging the gateway router. Enter:
   `ping` ***`<IP address>`***

   NOTICE: Ping and get results before continuing the installation.

   You should get four replies from the client.

5. Close the command prompt window.

6. Continue to the next procedure.

3.3
Discovering the InfoVista/TNPS Server in Unified Event Manager

The InfoVista/TNPS server must be discovered in the Unified Event Manager (UEM) server application co-located in the same zone as the InfoVista/TNPS server. Traps and events from InfoVista are viewable in UEM only after this procedure is complete. It is accomplished in UEM as part of the subnet or IP node (individual device) discovery. For details, see *Unified Event Manager Online Help*.

Chapter 4

InfoVista Operation

This chapter contains the optimization procedures and recommended settings relating to InfoVista.

4.1 Managing Network Transport Equipment Performance

Managing Network Transport Equipment Performance explains:

- How to navigate, use, and interpret the Motorola custom-designed reports, and to understand the custom-designed trap generation feature
- How to use the applications and access the reports using the client software web interface
- How to manage the Transport Network Performance Server (TNPS)

4.2 Ways to Access InfoVista

InfoVista resides on the Transport Network Performance Server. You can access InfoVista from the TNPS, a Network Management (NM) client, or a Transport Network Management (TNM) client.

4.2.1 Supported Features Overview

InfoVista interfaces with network devices supporting Simple Network Management Protocol (SNMP). By importing Management Information Base (MIB) files, InfoVista can report and graph a wide variety of data from multiple devices such as routers, GGM 8000, Ethernet LAN switches, and CWR.

InfoVista performs the following performance management tasks:

- Collects MIB data at any specified time interval
- Displays the collected data in daily, weekly, monthly, and yearly reports
- Reports and graphs single and multiple device information
- Provides customized reports using pre-configured standardized report templates for network transport devices in your Motorola Solutions radio system

4.2.1.1 Accessing the InfoVista Documentation

When and where to use: Use this procedure to access InfoVista documentation for more details on terminology and general use.

NOTICE: InfoVista documentation is available from the TNPS or the client workstations.

Procedure:

To access InfoVista documentation, perform one of the following:

If…	Then…
If you are accessing the documentation from Windows,	Open the start screen and go to the Apps list. Select one of the following: • Infovista Administration Guide • Infovista Development Guide • Infovista Installation Guide
If you are accessing the documentation from the InfoVista client software menu bar,	select **Help** to open the *Documentation Guide* with a full list of documentation provided with InfoVista.

4.2.2
User Rights for Windows 2012 and InfoVista

NOTICE: Motorola Solutions provides the confidential passwords to approved users. Contact the Motorola Solution Support Center (SSC) for additional information.

4.2.2.1
InfoVista Client User Account Rights

NOTICE: The InfoVista Runtime license prevents you from modifying or adding any library. You can only import a new library.

Table 5: User Logons for InfoVista Client

Users	User Rights and Tasks
ivviewer	Has the viewer profile in InfoVista. Can perform the following tasks: • View reports through InfoVista • Find reports and print them • Save reports from the Schedule dialog box or from the Report Viewer • Query the MIB variables from the MIB Browser
ivadmin	Has the writer profile in InfoVista. Can do all the tasks listed for ivviewer, plus these additional tasks: • Add new instances and create reports for them • Start or suspend any report instance • View contents of the Motorola libraries

4.2.3
Choosing How to Access InfoVista

You can access the InfoVista client from either the client workstation or from the Transport Network Performance Server.

4.2.3.1
Using the Client Workstation

Use the client workstation only if you have to view the reports. Most of the activity (90%) takes place using the client workstation.

Some tasks cannot be performed at the client workstations because the client does not have the same Motorola Solutions customized utilities installed for the TNPS server.

4.2.3.2
Using the TNPS

You can log on to the TNPS, which is a Windows 2012 server, to perform administrative task. From the server, you can access the customized InfoVista menu and perform tasks from that menu. The mechanism for opening InfoVista is different, but the same user accounts are used to access both.

4.2.4
Accessing the InfoVista Client from a Client Workstation

You can use the NM client or the TNM client workstations to access InfoVista.

The client application is used to access the server software and to provide an online connection to the server to perform administrative tasks, such as, starting and stopping existing reports, adding an instance, or creating a new report.

4.2.4.1
Accessing the InfoVista Client on the Client Workstation

This section provides information on:

- Access points for the InfoVista client on the TNM client workstation
- Access points for the InfoVista client on the NM client workstation
- Launching the InfoVista client on the client workstation

4.2.4.2
Access Points for the InfoVista Client on the TNM Client Workstation

Prerequisites: Log on with a user account belonging to both “secadm” and “confgaud” groups in Active Directory.

When and where to use: Use this procedure to access the InfoVista Client on the TNM Client Workstation.

Procedure:

1. From the **Start** screen, go to **Apps list** and start **IVreport**.
2. Right-click **IVreport** icon and select **Run as Administrator**.

   The **InfoVista** login window opens.

   Figure 4: InfoVista Report Desktop Icon

4.2.4.3
Access Points for the InfoVista Client on the NM Client Workstation

Prerequisites: Log on with a user account belonging to both “secadm” and “confgaud” groups in Active Directory.

When and where to use: Use this procedure to access the InfoVista client from two places on the NM client workstation.

Procedure:

1. From the **Start** screen, go to **Apps list** and start **IVreport**
2. Right-click **IVreport** icon and select **Run as Administrator**.

   Figure 5: InfoVista Report Desktop Icon

3. Enter the username and password. Click **OK**.

   InfoVista IV-Report Window opens.

4.2.4.4
Launching the InfoVista Client on the Client Workstation

Prerequisites: Log on to the client workstation with a user account belonging to both “secadm” and “confgaud” groups in Active Directory.

When and where to use: Use this procedure to access the InfoVista client application. The appearance of the InfoVista interface depends on the user login that you use.

NOTICE: If you need help on the InfoVista interface, see Accessing the InfoVista Documentation on page 40.

Procedure:

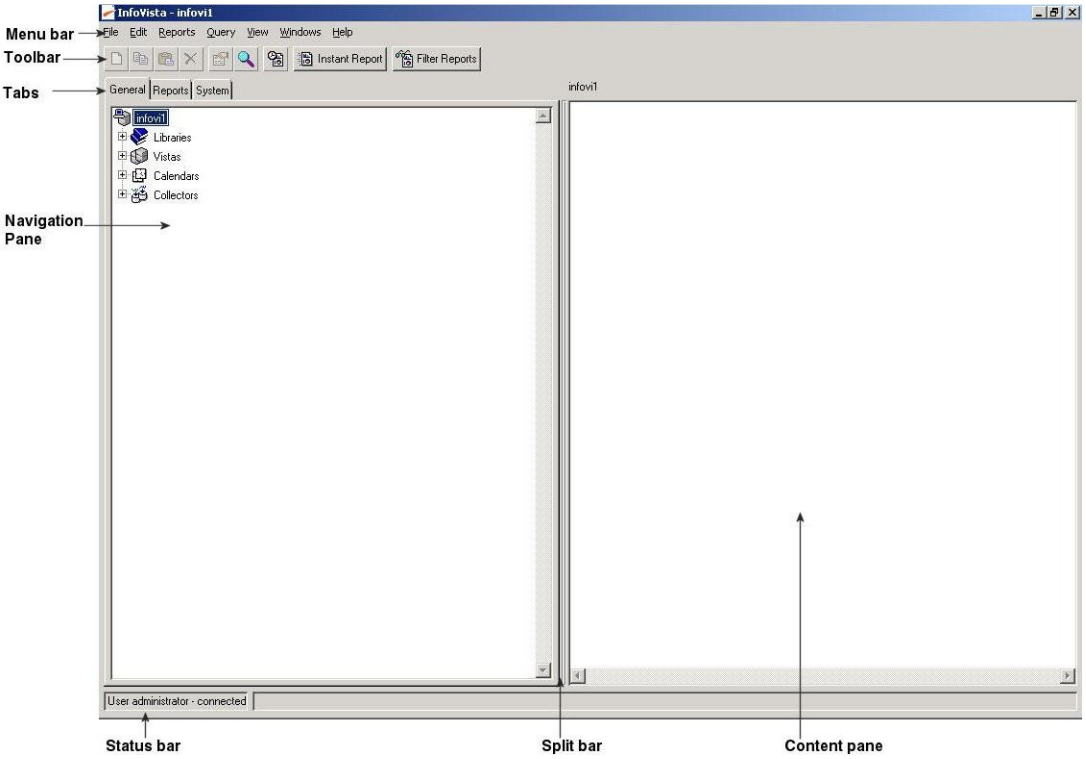
1. Open the InfoVista application.

   Step example: Right-click **IVreport** and select **Run as Administrator**. Enter the username and password. Click **OK**.
   The **InfoVista server connection** login window appears.

Figure 6: InfoVista Server Connection Login Window

2 Log on as the administrator or viewer, and type the password to log in to InfoVista. Click **OK**.

Figure 7: InfoVista Window (General Tab)



The InfoVista window appears.

3 Choose from the following key elements of the window:

- Menu bar or Toolbar. If you need additional information about options, see the Accessing the InfoVista Documentation on page 40 section.

- Tabs:
  General
  Shows the Motorola libraries.

  Reports
  Shows the objects that are used to classify and search for reports.

  System
  Shows administration and configuration objects.

- Navigation Pane – Displays the object tree. The root of the tree (at the top) is the InfoVista server system. The top-level node in the tree-directory could be the TNPS server name, for example, INFOVI1, the IP address of the TNPS, or localhost.
- Contents pane – Shows the objects located under the object selected in the navigation pane.

4.2.5
Setting Up Access Points to the InfoVista Client in a Different Zone

When and where to use: Use this procedure to set up access points to launch InfoVista from other zones. InfoVista access points are installed on the NM or TNM client for applications running in the current zone only. Perform this procedure if you have to launch InfoVista running in zone 2 from a client located in zone 1.

NOTICE: This procedure is intended for creating the access points on the desktop area only, not for the **Start** menu.

Procedure:

1. Log on to the client workstation.
2. From the desktop, double-click the launching point, and specify the InfoVista server IP address in the **Server Name** field to launch the InfoVista application from a different zone.

4.2.6
Accessing the InfoVista Client from the TNPS

This section provides information on:

- Accessing the TNPS
- Accessing InfoVista on the TNPS

4.2.6.1
Accessing the TNPS

When and where to use: Use this procedure to access the TNPS, where InfoVista resides.

Procedure:

1. Power on the server, if necessary.
2. Log on as the administrator or viewer, and type the password to log on to the TNPS server.

   The **Tray Notifier** dialog box appears.
3. Choose from one of the following:
   - If you only have to access InfoVista, move to the NM Client with the application installed. Most tasks are performed from the client workstation. See Choosing How to Access InfoVista on page 41.
   - If you have to perform an administrative task from the customized InfoVista menu, see InfoVista Operation on page 40 for the types of tasks that you can access.

4.2.6.2
Accessing InfoVista on the TNPS

This procedure explains how to access InfoVista on the TNPS. Use one of the following methods to access InfoVista from the server:

- From the **Start** menu, select **Programs** → **InfoVista** → **IVreport**.
- From the **Start** screen, go to **Apps list** and start **IVreport**

Figure 8: TNPS Desktop Icon for InfoVista

4.3
Report Design, Navigation, and Usage of InfoVista

This section provides information on:

- Report and Trap Generation design.
- Report navigation.
- Uses of InfoVista reports.

4.3.1
Report and Trap Generation Design

Traps are warning messages that let you know when a threshold has been exceeded for a managed device.

4.3.1.1
Report Design

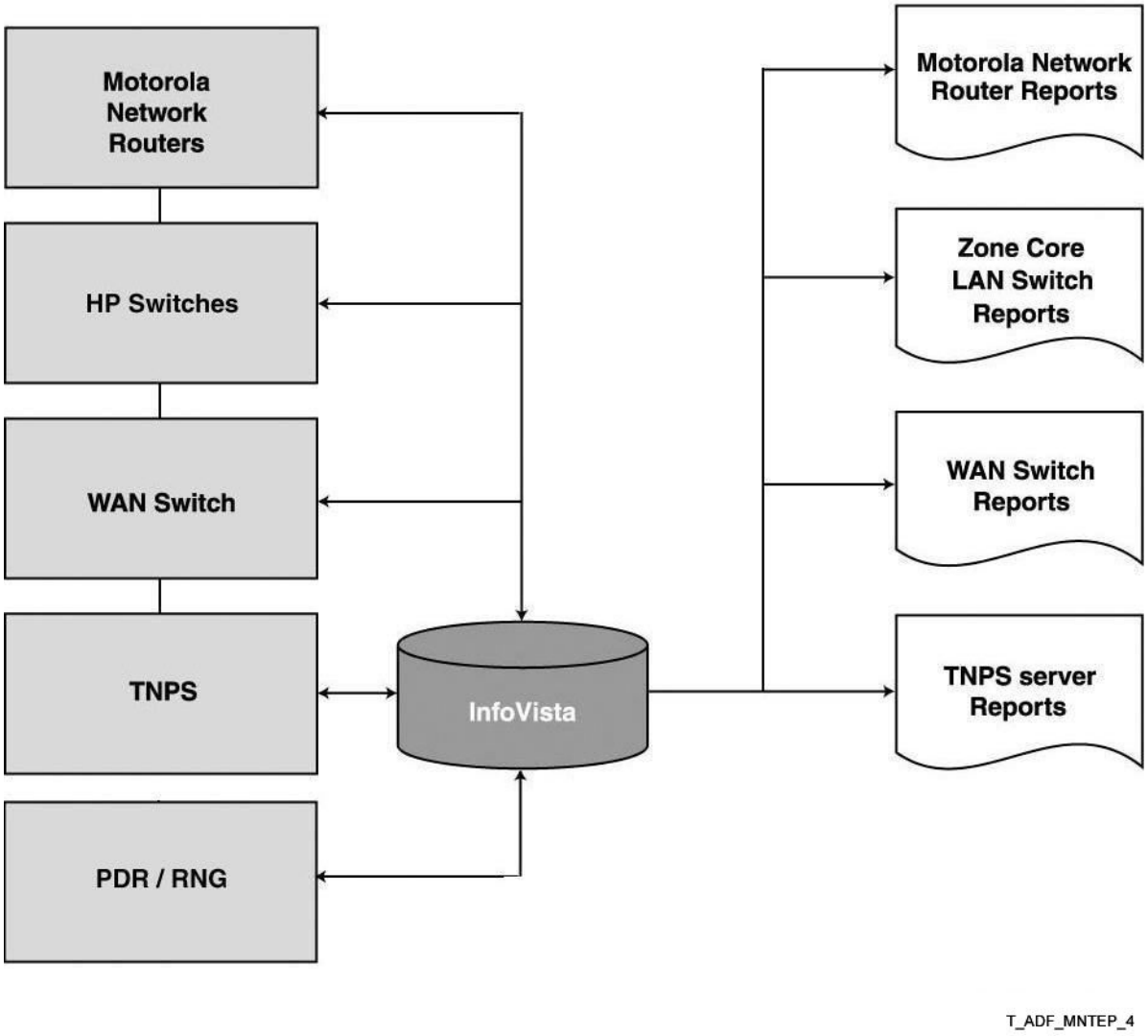
Report information is provided on:

- Report types
- Customized libraries (VistaViews)
- Vistas and instances
- Templates

4.3.1.2
Types of Reports

The following shows the devices polled by InfoVista to create the reports.

Figure 9: Types of Reports



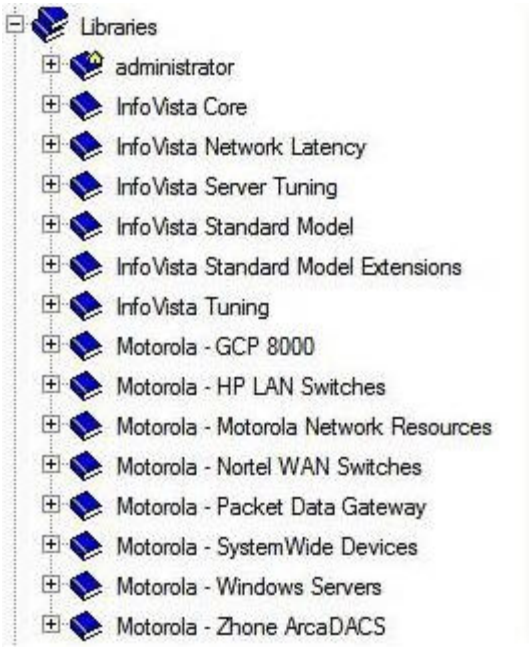
4.3.1.3

Customized Libraries (VistaViews)

Motorola Solutions develops customized libraries (VistaViews). Each library addresses the reporting for a specific vendor device type. See the following figure.

NOTICE: You cannot modify these libraries.

Figure 10: Motorola Libraries



Other required libraries are installed with InfoVista that must be present in order for the Motorola-customized libraries to work.

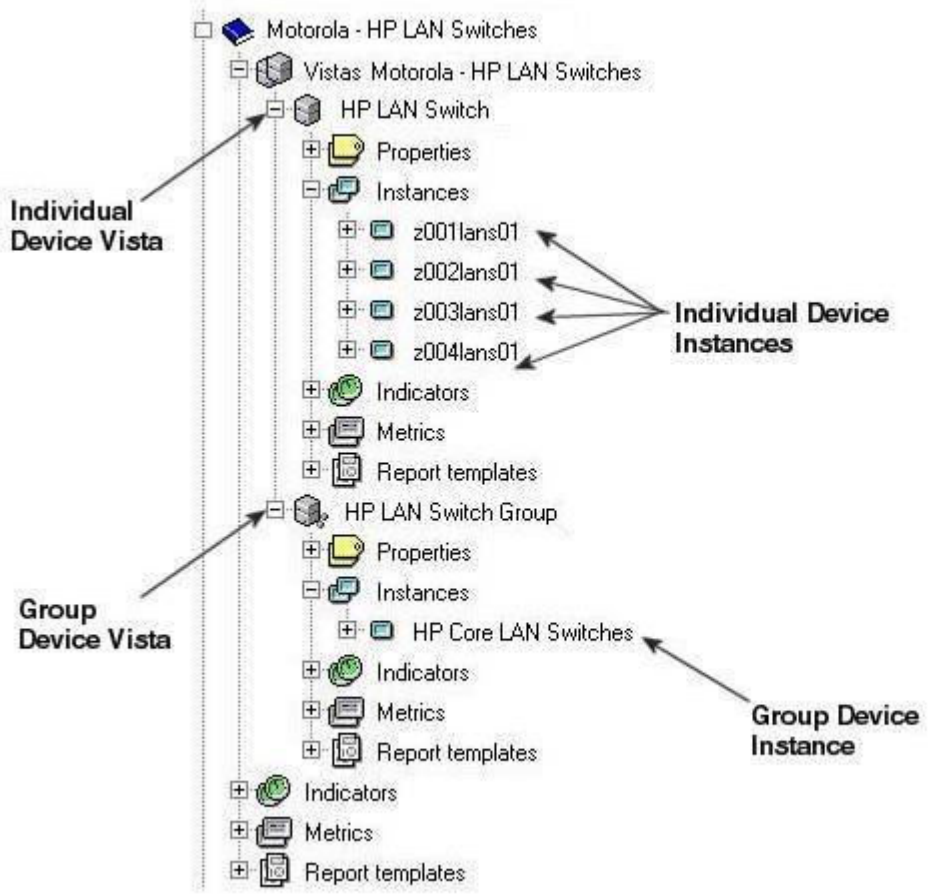
Motorola does not support the creation of reports using the report templates in these libraries.

4.3.1.4
Vistas and Instances

A Vista is an object that is used to model a type of resource. The two kinds of Vistas created in the Motorola libraries are basic and group.

The following figure shows an example of these two Vista types defined in the **Motorola - HP LAN Switches** library. **HP LAN Switch** is a basic Vista that models a single switch, and the **HP LAN Switch Group** is a group Vista that models a group of switches.

Figure 11: Vistas and Instances



The Vista contains the following associated with an instance type:

Properties

Characteristics of a resource, such as an IP address of a switch instance or a threshold for a statistic. Major and Warning threshold properties are created in the individual device Vistas. For more information, see Trap Generation on page 51.

Instances

Each instance is derived from a Vista. An instance represents a specific monitored resource in InfoVista. An instance can be any logical or physical resource such as a switch, a switch port, or a group of switches. The Motorola Solutions libraries use both single instances, which represent a single physical resource, and group instances, which represent a group of homogeneous instances. The Motorola Network Resource libraries have both single and group instances. The instance name is defined by using the **sysname** of the device, for example: **z001lan01**.

Indicators

A measurement that tells us something about the operation of the resource. An indicator contains formulae that use MIB variables, properties, or other indicators. Usually, one or more indicators are used to calculate a statistic.

Metrics

A group of one or more indicators that have the same parameters.

Report templates

A graphical layout tool for reports. See Report Templates on page 50.

4.3.1.5
Report Templates

The Report template represents the graphical layout that is used to create a report. It consists of graph templates and such elements as text and graphics. A graph template is added for each metric that is defined in the report template. The graph template defines the layout of the graph and the display rate, acquisition rate, and the time span for the graphs it defines.

Each type of report has four report templates (Daily, Weekly, Monthly, and Yearly). For various report types, see Report Type Overview on page 63. The naming scheme for the report templates is the type of report - Daily, Weekly, Monthly, or Yearly. For example, the names of the four report templates for a Motorola Network Resource Performance Report are as follows:

- MNR Performance - Daily
- MNR Performance - Weekly
- MNR Performance - Monthly
- MNR Performance - Yearly

The name of the reports generated from an instance-report template pair is the instance name with the report template name in parentheses.

Example: A report template named MNR Performance - Daily instantiated with an instance named *z001core01* would generate a report named *z001core01 (MNR Performance - Daily)*

4.3.1.6
Report Template Title Information

Figure 12: Report Template Title Information

Table 6: Report Template Title Descriptions

Title Information	Description
Instance	A single device or group of devices.
End Date	The date of the last data point displayed on the graph.
End Time	The time of the last data point displayed on the graph. **NOTICE:** All time information appears in Greenwich Mean Time (GMT). GMT is a 24-hour clock that uses one universal time zone.
Time Span	The span of time on the x-axis.
Display Rate	How often a data point is displayed on the graph.

4.3.1.7
Report Template Times

The following descriptions apply to the tables that follow:

- Acquisition rate: The time interval between two data polls of the monitored device.

- Display rate: The time interval between how often a data point is displayed on the graph. For a graph with a time span on the x-axis, this is the time between each point. The display rate must be greater than or equal to the acquisition rate.
- Time Span: The period over which the graph must display data.
- Lifetime: The length of time that InfoVista stores the data for the report.
- Time Span in Title: The period over which the graph must display the data.

4.3.1.8
Individual Report Templates

The following table shows the report templates correlated to the time span of the x-axis on the graphs.

Table 7: Individual Report Templates

Report Templates	Display Rate	Acquisition Rate	Time Span	Lifetime	Time Span in Title
Daily	15 minutes*	15 minutes*	24 hours	3 months	24 hours
Weekly	4 hours	15 minutes*	7 days	6 months	7 days
Monthly	12 hours	15 minutes*	1 month	1 year	1 month
Yearly	1 day	6 hours*	1 year	3 years	1 year

*Two reports have different values from these rates. The MNR Interface Performance and Nortel WAN Switch HSSI Port Performance reports have a display rate of 10 minutes for their Daily report templates and an acquisition rate of 5 minutes for their Daily, Weekly, Monthly, and Yearly report templates.

4.3.1.9
Group Report Templates

The following table shows the group report templates correlated to the frequency in the display of the data. The x-axis of group report templates does not span over time. They are a single point in time.

Table 8: Group Report Templates

Report Templates	Display Rate	Acquisition Rate	Time Span	Lifetime	Time Span in Title
Daily	1 day	15 minutes	1 day	6 months	1 day
Weekly	1 week	15 minutes	1 week	1 year	1 week
Monthly	1 month	15 minutes	1 month	3 years	1 month
Yearly	1 year	1 day	1 year	5 years	1 year

4.3.1.10
Trap Generation

InfoVista sends warnings and major traps to the Unified Event Manager (UEM) server for the key statistics that it collects. Traps are sent only to the UEM server colocated in the same zone as the InfoVista/TNPS server. Most key statistics have two thresholds:

- Tw = Threshold warning. If the statistic exceeds this value, a warning trap is sent.

- Tm = Threshold major. If the statistic exceeds this value, a major trap is sent.

Traps sent to UEM are generated from the individual device daily reports. The threshold values are defined on the report templates. For example, if a CPU Utilization graph shows that the Tw = 80, a trap is sent only when the CPU Utilization reaches 80%. Group reports do not show thresholds or generate traps.

A trap is generated using the highest value in either the IN (receive) or OUT (transmit) direction for router interfaces and switch ports.

4.3.1.11
Trap Generation Design

Motorola Solutions has developed a customized trap generation functionality that minimizes the number of traps that InfoVista sends. This functionality cannot be found in out-of-the-box InfoVista reports that generate traps. Using the trap operator directly in a formula would generate a trap on every poll if the value of the statistic exceeds the threshold.

4.3.1.12
Scenario when a Warning and Major Threshold Is Exceeded and Relieved

The following scenario is an example of what could occur when a warning and major threshold is exceeded and relieved:

1. When the value of a statistic *x* is greater than the warning threshold (Tw) but less than the major threshold (Tm), a Warning trap is sent.
2. If on the next poll, *x* is still greater than Tw, but less than Tm, no trap is sent.
3. If on the next poll, the value of *x* jumps above the major threshold (Tm), both a Major trap and a Warning Clear trap are sent.
4. If on the next poll, the value of *x* falls below the major threshold (Tm), but is greater than the warning threshold (Tw), both a Major Clear trap and a Warning trap are sent.
5. If on the next poll, the value of *x* falls below the warning threshold (Tw), a Warning Clear trap is sent.

4.3.1.13
Scenario when a Warning and Major Threshold Is Exceeded

The following scenario is an example of what could occur when a warning and major threshold is exceeded and relieved:

1. When the value of a statistic *x* is greater than the warning threshold (Tw) but less than the major threshold (Tm), a Warning trap is sent.
2. If on the next poll, *x* is still greater than Tw, but less than Tm, no trap is sent.
3. If on the next poll, the value of *x* jumps above the major threshold (Tm), both a Major trap and a Warning Clear trap are sent.
4. If on the next poll, the value of *x* falls below the major threshold (Tm) but is greater than the warning threshold (Tw), both a Major Clear trap and a Warning trap are sent.
5. If on the next poll, the value of *x* falls below the warning threshold (Tw), a Warning Clear trap is sent.

4.3.1.14
Trap Destinations

InfoVista collects fault events and traps from network devices in all zones are reported to the Unified Event Manager (UEM) server located in the same zone as the InfoVista server.

4.3.2
Report Navigation

This section provides information on:

- Report folders
- Filter types to search the Motorola Solutions custom-designed reports
- Drill downs
- Displaying formula descriptions

4.3.2.1
Report Folders

Report folders are a way to organize the reports for easy access. The folders are organized by system and zone.

- System-level folder: One system-level folder. The system-level folder contains all group reports for the system-level groups and an InfoVista reports folder that contains reports specific to InfoVista and its polling of all devices in the system.

4.3.2.2
LAN Sharing

Reports are placed into report folders based on the IP address of the instance. In a LAN sharing configuration, the Network Management router has an IP address for three zones. In this design, the reports for this router can show up in any of the three zone report folders.

4.3.2.3
Navigating the Reports Using the InfoVista Client

When and where to use: Use this procedure to navigate the report folders to find a report and to use the Report Viewer window to view or print a report.

NOTICE: The InfoVista Find dialog box can also be used to search for a specific report. For additional information about common tasks performed in InfoVista, such as finding reports, see InfoVista Troubleshooting on page 125.

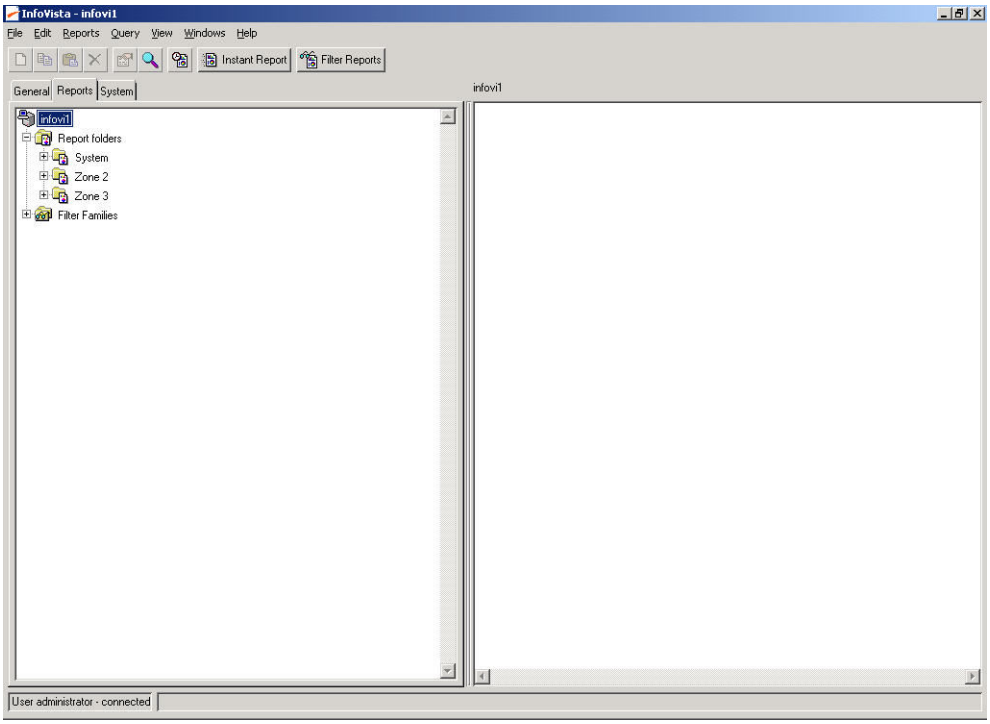
Procedure:

1. Access the InfoVista client using the method described in Launching the InfoVista Client on the Client Workstation on page 43. (You can log on as **ivadmin** or **ivviewer**).

   The **InfoVista** window appears.

2. To view reports, in the **InfoVista** window, select the **Reports** tab and expand the **Report folders** node.

Figure 13: InfoVista Window (Reports Tab)

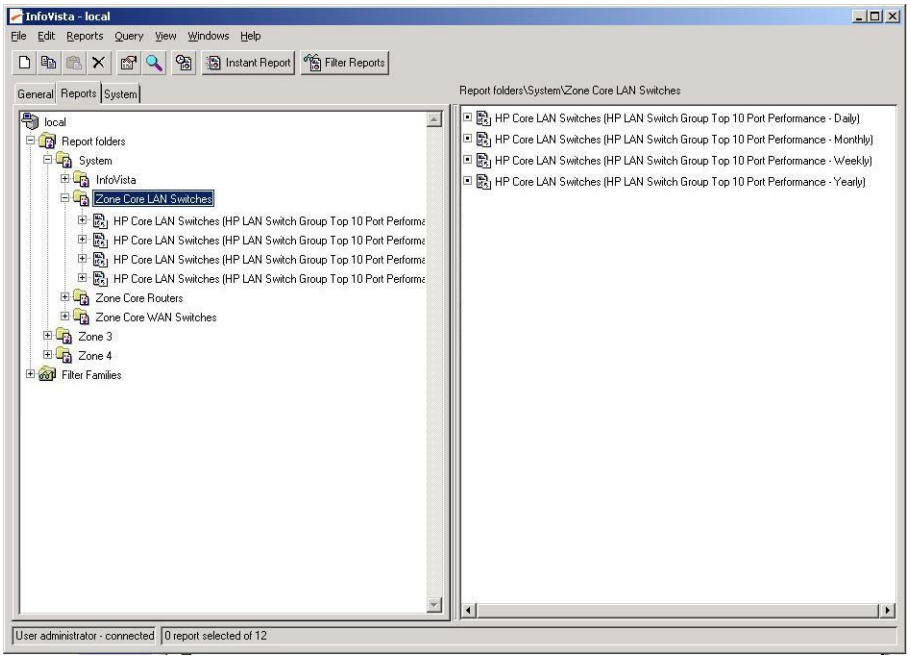


The folders appear.

3 Expand the System and Zone Core LAN Switches, for example, and left-click the **Zone Core LAN Switches** folder.

NOTICE: Because you may have hundreds of individual device reports running on your system, you may want to start your viewing with the group reports. From there, you can determine at a higher level which devices out of a certain group has a problem. Drill down for additional information on a single device.

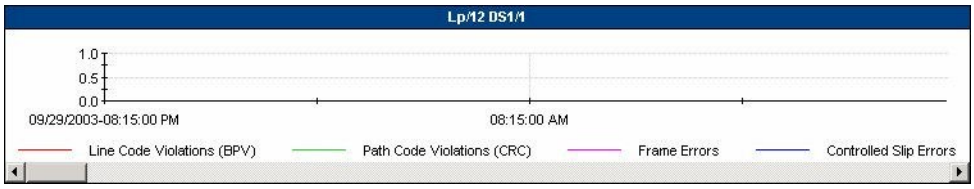
Figure 14: System Level Folders



The group reports for all Zone Core LAN Switches in the Cluster appear in the right window pane.

4 To open a report, double-click a running report instance. Running reports show a color icon. Suspended reports appear dimmed.

Figure 15: Report Viewer Window



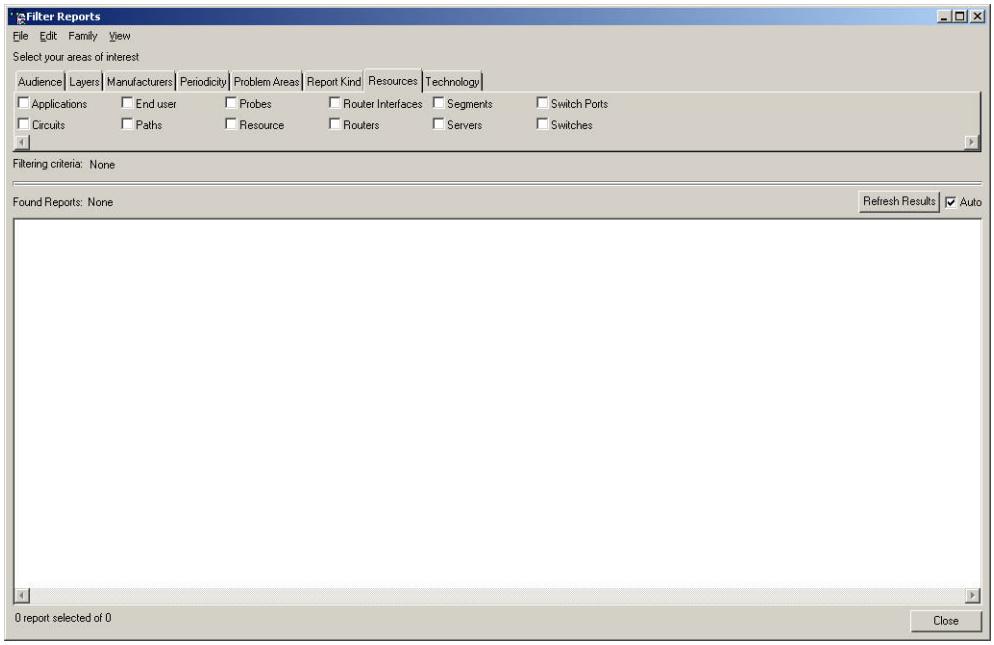
The report appears in the Report Viewer window. The title bar contains the instance name with the report template name in parentheses. The menu bar contains menu options specific to the report viewer window, and the drill downs list drills down to related reports.

4.3.2.4

Filter Types to Search the Motorola Custom-Designed Reports

The following shows the **Filter Reports** dialog box. On the **Filter Reports** window, five tabs represent the filter types, then you can use selections on the tabs to narrow the search.

Figure 16: Filter Reports Dialog Box



4.3.2.5

Filter Types

The following table shows five of the eight possible filter types that you can use to search the Motorola Solutions custom-designed reports. The other three filters are not used in your system.

Table 9: Filters Window Options

Filter Type (Tab)	Filtering Criteria
Layers	Every report appears using the **network** filter. This filter was implemented for future design considerations and is not useful at this time.
Manufacturers	Choose from the following to narrow the search by the manufacturer: • **Motorola** produces all reports in Motorola - Motorola Network Resource and Motorola - Packet Data Gateway library. • **Nortel** produces all reports in Motorola - Nortel WAN Switch library. • **Motorola - HP LAN Switches** produces all reports in Motorola - HP LAN Switches library.
Resources	Choose from switches, routers, router interfaces, switch ports, and circuits: • **Routers** produce all reports in Motorola - Motorola Network Resources library. • **Router Interfaces** produce reports of a type: MNR Interface Performance. • **Switch Ports** produce all reports of type: Nortel WAN Switch HSSI Port Performance.

Filter Type (Tab)	Filtering Criteria
	• **Circuits** produce all reports of type: MNR Group Top 10 PVC Performance, MNR PVC Queue Performance, and MNR PVC Traffic Performance. • **Group** produces all reports of type: HP LAN Switch Group Top 10 Port Performance, Nortel WAN Switch DS1 Group Top 10, Nortel WAN Switch InterZone DS1 Performance, and Nortel WAN Switch Intra-zone DS1 Performance.
Periodicity	Choose from **Daily**, **Weekly**, **Monthly**, and **Yearly**. For example, filtering on **Daily** produces reports in all libraries with daily periodicity.
Report Kind	Choose from Group or Individual. • **Group** produces reports of the following vistas: Motorola Network Resource Group InfoVista Tuning (for the InfoVista SNMP Traffic Analysis report). • **Individual** produces reports of the following vistas: Motorola Network Resource, Nortel WAN Switch, and IpNode (for the Device Reachability report).

4.3.2.6
Filtering Reports

When and where to use: Use this procedure to search for reports.

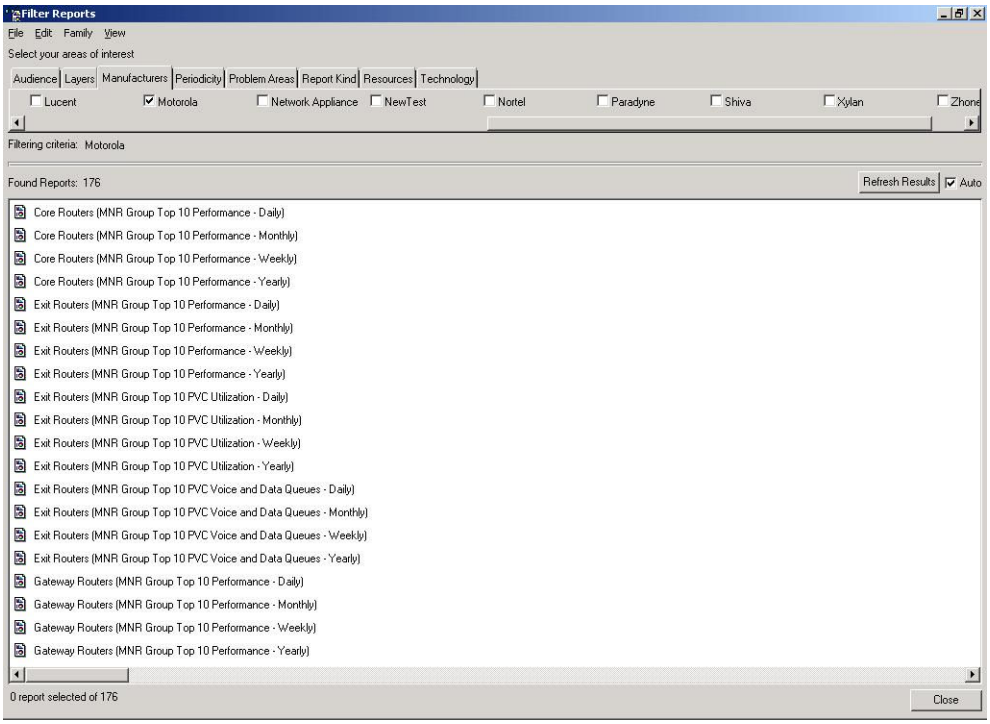
Procedure:

1 From the **Reports** menu, select **Filter**.

The **Filter Reports** window appears.

2 Select the **Manufacturers** tab, then **Motorola**.

Figure 17: Filter Reports Results



All reports in the Motorola - Motorola Network Resource library appear.

3 On the **Report Kind** tab, select **Router Interfaces**.

All reports for the Motorola - Motorola Network Resources that report specifically on router interfaces appear.

4.3.2.7
Drill Downs

Drill downs have been designed to allow you to quickly open different reports for the same instance without having to go back to the InfoVista main window to find them. All reports for an individual instance can be accessed through a drill-down and all reports have drill downs to all four InfoVista SNMP Traffic Analysis reports.

- At the top of all reports, a Drill-Down list allows you to explore other reports.
- For individual reports, by right-clicking on any graph in the report and selecting Drill Downs, you can navigate to other reports of an instance.
- For group reports, by right-clicking on the bar graph for an instance and selecting Drill Downs, all reports for that instance are shown and can be opened.

4.3.2.8
Drilling Down on Reports

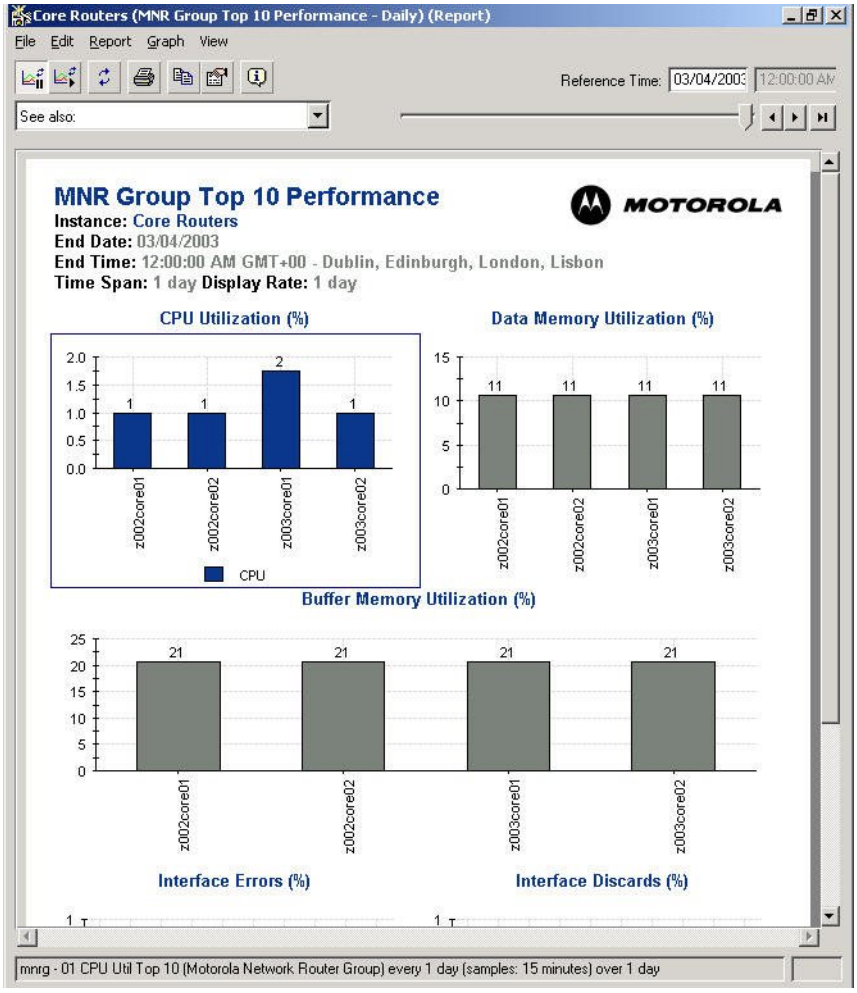
When and where to use: Use this procedure to drill down from a group report to an individual report on an instance in a graph.

Procedure:

1 Open a report.

This example shows core routers (MNR Group Top 10 Performances - Daily). Assume for this example that **z002core02** shows a CPU utilization that is noticeably higher than that of the other routers, and you can see the CPU utilization over a time for this instance to determine when and how long the CPU was at this level.

Figure 18: Core Routers (MNR Group Top 10 Performance - Daily)

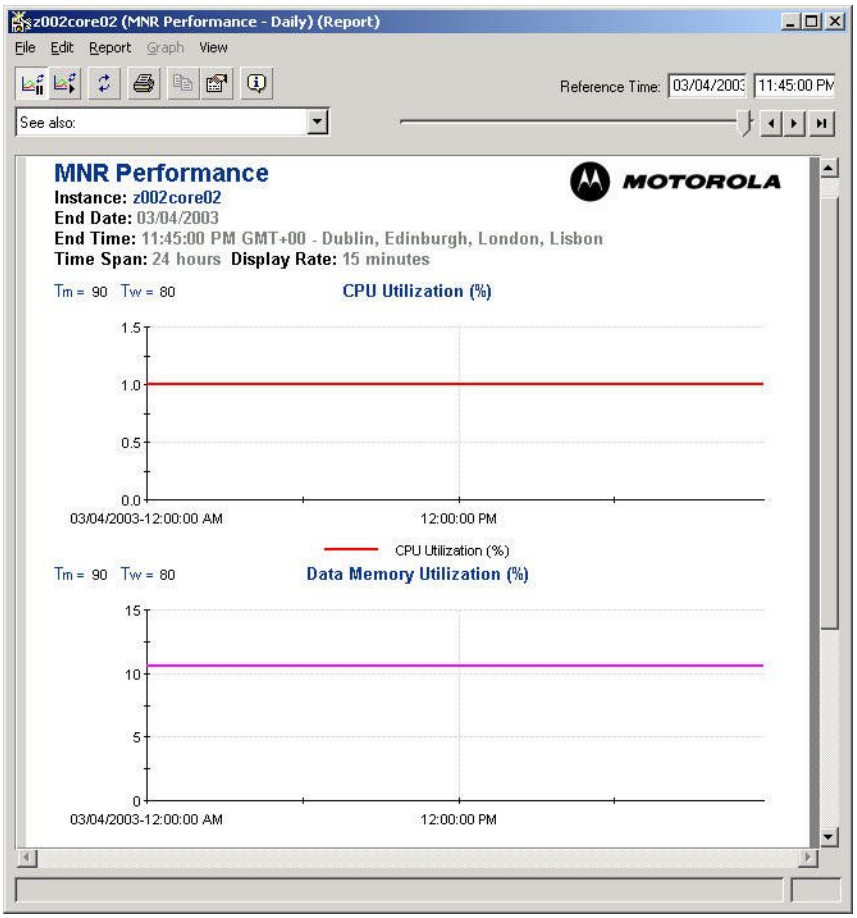


2 In the CPU Utilization graph, right-click the **z002core02** instance and select **Drill Downs**.

The Drill Down submenu appears.

3 Select the **z002core02** (MNR Performance - Daily) report to view a graph of the CPU utilization over time.

Figure 19: MNR Performance – Daily Report



The MNR Performance - Daily report appears in a new **Report Viewer** window.

4.3.2.9
Displaying Formula Descriptions

When and where to use: Use this procedure to obtain formula descriptions.

Procedure:

1. Right-click the graph to obtain a pop-up menu.
2. Select **Formulas**, and then select one of the indicators listed in the submenu.

   NOTICE: If the Description pane does not show the formula in the **Expression** dialog box, click **View**, and then click **Description**.

   The **Expression** dialog box appears, displaying the formula for that indicator in the **Description** pane.

4.3.3
Uses of InfoVista Reports

You can use InfoVista reports for proactive network performance, troubleshooting, and network capacity planning.

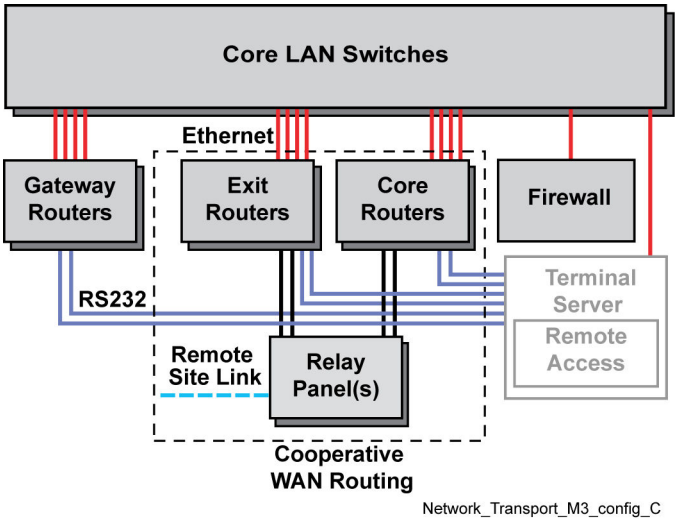
4.3.3.1

System Devices Monitored by InfoVista

The following shows an example of the devices monitored by InfoVista. Motorola Solutions provides customized reports for all HP LAN switches, Radio Network Gateways (RNGs), Packet Data Routers (PDRs), GCP 8000 Site Controller switches, GGM 8000s, and all Motorola Network Resources (MNRs) in the system.

In a system with the Dynamic System Resilience feature, reports are available on the primary InfoVista server only. If the primary fails and the backup server is set up to run as the primary, reports are available.

Figure 20: Devices Monitored by InfoVista (Example)



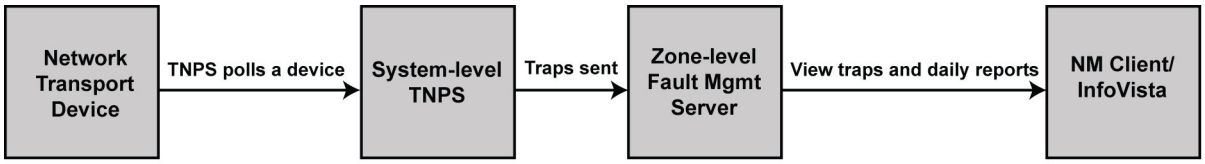
4.3.3.2

Performance Management Troubleshooting

Traps and daily individual reports provide a useful, proactive performance management troubleshooting tool.

The following figure shows how data flows from the devices to the TNPS server and how traps are sent from the TNPS server to the Unified Event Manager (UEM) server, which houses the zone-level fault management application. Using the NM client, you can view the traps sent to the UEM server and then use the InfoVista client to view the daily reports generated by the traps.

Figure 21: Performance Data and Trap Flows



4.3.3.3

Capacity Planning

After the installation of your system, you can collect information that can be used as a baseline for how the system runs initially. Each month, you can compare the data to determine if the system is functioning better or worse and if the changes are major or minor.

Periodically and after major additions, view the reports with large time-spans such as weekly and monthly to determine the effect of adding new radios/devices to the system and when to add more network resources.

Use the individual weekly, monthly, and yearly reports for the capacity planning of an instance. Use the group reports for system capacity planning to compare device instances and look at traffic at the zone or system level.

4.3.3.4
Recommended Viewing Frequency

View reports as needed according to the following suggestions.

4.3.3.5
Recommendations for Individual Reports

The individual report types and the associated recommendations are:

- Daily Reports - View the daily reports to do a day-to-day analysis. The daily reports generate the threshold traps, which are sent to the Unified Event Manager (UEM). In this way, there is no need to monitor all reports all the time. If a trap is sent to the UEM that means a problem has been detected and the report that generated the trap should be examined. Use daily reports to compare in the performance of like devices.
- Weekly Reports - Use for the historical trending of week-to-week comparison.
- Monthly Reports - Use for the historical trending of month-to-month comparison. Look for steady increases or spikes that can be correlated to an event. For example, you can compare the reports from June and July.
- Yearly Reports - Use for historical trending for year-to-year comparison.

4.3.3.6
Recommendations for Group Reports

The group report types and associated recommendations are:

- Daily – Use as an initial baseline to compare the performance of like devices.
- Weekly – Use for capacity planning and trending. For example, compare the Weekly group reports against another week to see if the same devices are still in the Top 10. Before a large change, such as adding many new radios, look at weekly (or daily) group reports for a baseline. Change and then compare the baseline with the new report to view any changes that may have occurred in the network performance. A few days later, look at the Daily group reports to see if devices of like types have changed substantially.
- Monthly – Use for historical trending month-to-month comparison.
- Yearly – Use for historical trending year-to-year comparison.

4.4
Interpreting the InfoVista Report Types

The reports monitor the performance of critical devices that make up the IP network infrastructure.

4.4.1
Report Type Overview

This section discusses in detail, individual, and group report types provided by Motorola Solutions in detail. Each of the report types has four templates to provide – daily, weekly, monthly, and yearly reports.

4.4.1.1
Information Provided for Each Report Template

The following is provided under the sections for interpreting each report type:

- The use of the report
- A table describing each graph on the report and its key variables in detail
- A report example that captures one of the running reports for that report type
- Where no traps for the statistics are sent, the Threshold major (Tm) and Threshold warning (Tw) columns show not applicable (N/A).

4.4.2
Interpreting Motorola Network Resource Reports

This section covers reports for the Motorola Network Resources (MNRs).

4.4.2.1
Types of Reports for the Routers

The Motorola Network Resource reports collect information for the routers that are used in your system.

4.4.2.2
Types of Motorola Network Resources

Table 10: Types of Resources

Router Model	Function
GGM 8000	All, except T1/E1 Core, T1/E1 Exit, T1/E1 Access, Peripheral
S6000	All, except Distributed Conventional Subsystem, and L core
S2500	RF Site, IP Simulcast Subsite, Dispatch Site

All transport devices providing support for IntraZone (zone-to-site) network traffic (Core router/gateway) and InterZone (zone-to-zone) network traffic (Exit router/gateway) may be deployed as combined (Core and Exit router/gateway) or standalone devices. If T1/E1 site links are needed to support intra-zone, or inter-zone traffic then combining the Core and Exit functions is not allowed and therefore separate Core and Exit transport devices must be used. For more details, see *S6000 and S2500 Routers Feature Guide*, and *GGM 8000 System Gateway Feature Guide*.

4.4.2.3
Reports and the Router Types

The following table lists the reports and the routers for which they collect information.

Table 11: Reports and the Router Types

Report	Collects Performance Information for the following routers:
MNR Performance	Site, core, exit, and gateway
MNR CWR LMI Performance	Site, core, exit, and gateway
MNR Interface Performance	Site, core, exit, and gateway
MNR Group Top 10 Performance	• Zone-level router groups: site, core, exit, and gateway • System-level router groups: site, core, exit, and gateway
MNR PVC Utilization	Site, core, and exit
MNR PVC Queue Performance	Site, core, and exit
MNR Group Top 10 PVC Utilization	• Zone-level group: Intra-zone routers (includes both core and site gateways) • System-level group: exit routers
MNR Group Top 10 PVC Performance (Queues 3 to 7)	• Zone-level group: Intra-zone routers (includes both core and site gateways) • System-level group: exit routers
MNR WAN Link Performance	Site, core, exit, GGSN, and CBR

NOTICE: Some NM/Dispatch sites can be colocated at the Zone Master site. The gateway router at the Zone Master site functions as the site gateway. In this case, the gateway router is listed as one of the site gateways. If there is more than one colocated site, the gateway router at the Zone Master site acts as the site gateway for all the colocated sites. The gateway router is listed only once under the site gateway category.

4.4.2.4
MNR Performance

MNR Performance is an individual report that is created for each Motorola Network Resource (MNR) in the system. It collects CPU and memory utilization on the MNR.

For the types of routers in your system, see Types of Reports for the Routers on page 63.

Thresholds are defined for CPU, data memory, and buffer memory utilization.

View the daily report template when a trap is generated to aid with more in-depth problem determination. View the weekly, monthly, and yearly reports to assist with capacity planning.

4.4.2.5
MNR Performance Report Description

Thresholds are defined for the graphs on this report as follows:

- **Tm** = Threshold major. If the statistic exceeds this value, a major trap is sent to Unified Event Manager (UEM).

- **Tw** = Threshold warning. If the statistic exceeds this value, for example, if the CPU Utilization (%) reaches 80%, a warning trap is sent to UEM.

Table 12: MNR Performance Report Description

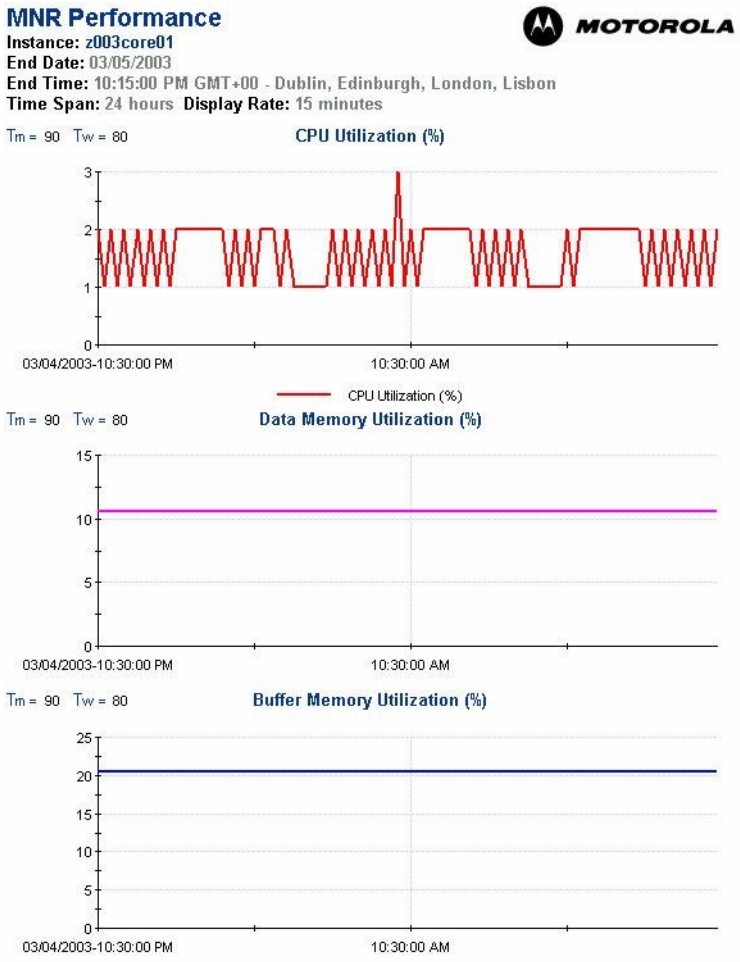
Graph/Table	Tm	Tw	Description
CPU Utilization (%) CoCPU Utilization (%) where available	90	80	**CPU Utilization (%)**: Provides a measure of the current utilization of the CPU on the device. **CoCPU Utilization (%)**: Provides a measure of the current utilization of the CoCPU on the device. The current router types do not have a second CPU, but this has been added for the future routers.
Data Memory Utilization (%)	90	80	Percentage of Data memory utilized in the system. The fragment memory is used first. Fragment memory comprises the number and sizes of free and allocated memory within the dynamic memory pools. The fragment memory represents the approximate 10% of memory that is shown as the % used on the graph. Once this memory is used, the router uses the remaining data memory. Having a steady value of used memory that is 10% means that the fragment memory has not been used up yet. For example, the graph shows the current value, near 10%, which is the normal, baseline value. A Tw trap will not be sent until the value reaches 80%.
Buffer Memory Utilization (%)	90	80	Percentage of buffer memory utilized in the system. The buffer memory that is allocated to specific buffer sizes is used first. The total memory for all buffer sizes represents the approximate 20% of memory that is shown as the % used on the graph. Once this memory is used, the router uses the remaining buffer memory. Having a steady value of used memory that is 20% means that the buffer memory allocated for the buffer sizes has not been used up yet.

4.4.2.6
MNR Performance Report

The following information explains how to use the report.

- For definitions of the report template title elements (such as instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. The maximum value for graphs that show percentages (%) is 100%. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the span of time.

Figure 22: MNR Performance Report



4.4.2.7

MNR CWR LMI Performance

MNR Cooperative WAN Routing Local Management Interface Performance report collects LMI errors and timeouts.

View the daily report template when a trap has been generated to aid with more in-depth problem determination. View the weekly, monthly, and yearly reports to assist with capacity planning.

4.4.2.8

MNR CWR LMI Performance Report Description

Table 13: MNR CWR LMI Performance Report Description

Graph/Table	Tm	Tw	Description
LMI Sequence Errors	N/A	N/A	• **DCE Sequence Errors** enables you to read the DCE LMI Sequence Errors. • **DTE Sequence Errors** enables you to read the DTE LMI Sequence Errors.

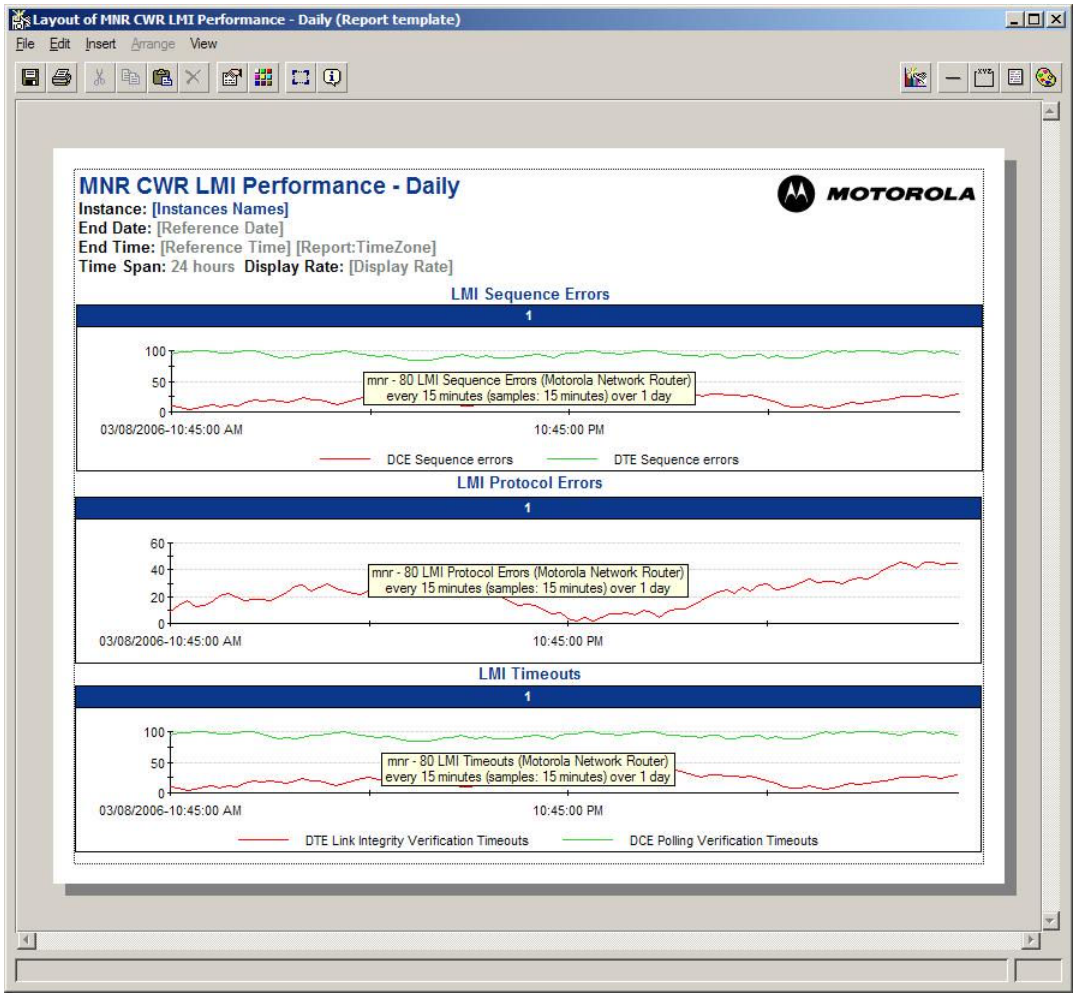
Graph/Table	Tm	Tw	Description
LMI Protocol Errors	N/A	N/A	• Provides the ability to read DCE LMI Protocol Errors.
LMI Timeouts	N/A	N/A	• **DTE Link Integrity Verification Timeouts** enables you to read the DTE LMI LIV Timeouts. • **DCE Polling Verification Timeouts** enables you to read the DCE LMI Polling Verify Timeouts.

4.4.2.9
MNR CWR LMI Performance Report

The following information explains how to use the report.

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. This report shows two types of graphs, one shows % value, the other shows milliseconds (ms). The maximum value for graphs that show percentages (%) is 100%. For graphs that show a count, the maximum varies. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the span of time.

Figure 23: MNR CWR LMI Performance Report



4.4.2.10

MNR Interface Performance

MNR Interface Performance is an individual report that is created for each Motorola Network Resource (MNR) in the system. It collects errors and discards on every interface of the MNRs. For the types of routers in your system, see Types of Reports for the Routers on page 63.

Thresholds are defined for both the errors and discards. Traps are sent for these statistics using the maximum of the IN and OUT values.

View the daily report template when a trap has been generated to aid with more in-depth problem determination. View the weekly, monthly, and yearly reports to assist with capacity planning.

4.4.2.11

MNR Performance Report Description

Thresholds are defined for the graphs on this report as follows:

- **Tm** = Threshold major. If the statistic exceeds this value, a major trap is sent to Unified Event Manager (UEM).

- **Tw** = Threshold warning. If the statistic exceeds this value, for example, if the CPU Utilization (%) reaches 80%, a warning trap is sent to UEM.

Table 14: MNR Performance Report Description

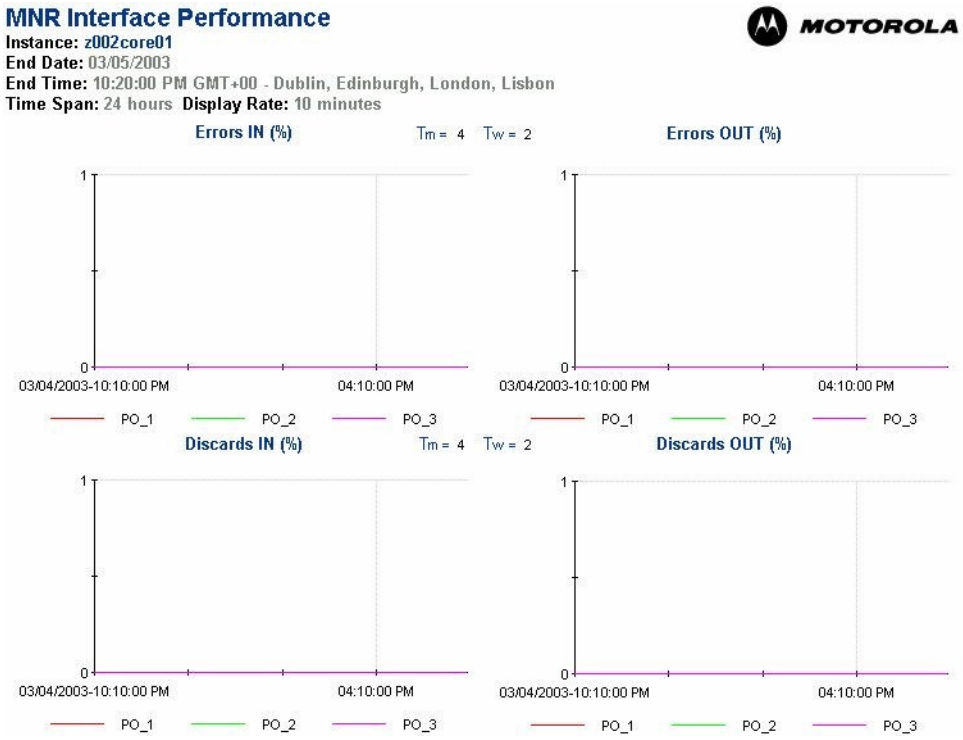
Graph/Table	Tm	Tw	Description
CPU Utilization (%) CoCPU Utilization (%) where available	90	80	**CPU Utilization (%)**: Provides a measure of the current utilization of the CPU on the device. **CoCPU Utilization (%)**: Provides a measure of the current utilization of the CoCPU on the device. The current router types do not have a second CPU, but this has been added for the future routers.
Data Memory Utilization (%)	90	80	Percentage of Data memory utilized in the system. The fragment memory is used first. Fragment memory comprises the number and sizes of free and allocated memory within the dynamic memory pools. The fragment memory represents the approximate 10% of memory that is shown as the % used on the graph. Once this memory is used, the router uses the remaining data memory. Having a steady value of used memory that is 10% means that the fragment memory has not been used up yet. For example, the graph shows the current value, near 10%, which is the normal, baseline value. A Tw trap will not be sent until the value reaches 80%.
Buffer Memory Utilization (%)	90	80	Percentage of buffer memory utilized in the system. The buffer memory that is allocated to specific buffer sizes is used first. The total memory for all buffer sizes represents the approximate 20% of memory that is shown as the % used on the graph. Once this memory is used, the router uses the remaining buffer memory. Having a steady value of used memory that is 20% means that the buffer memory allocated for the buffer sizes has not been used up yet.

4.4.2.12
MNR Interface Performance Report

The following information explains how to use the report:

- For definitions of the report template title elements (such as instance or time span), see Types of Reports for the Routers on page 63.
- The y-axis (vertical axis) represents the values of the statistic. The maximum value for graphs that show percentages (%) is 100%. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the span of time.

Figure 24: MNR Interface Performance Report



4.4.2.13

MNR Group Top 10 Performance

MNR Group Top 10 Performance is a group report that is created for the groups of Motorola Network Resources (MNRs) in the system. For the types of routers in your system, see Types of Reports for the Routers on page 63.

It shows the Top **N** (up to 10) routers with the highest values for all statistics in the MNR Performance and MNR Interface Performance reports. It reports on CPU and data and buffer memory utilization. It also shows interface errors and discards.

View the reports to assist with capacity planning. You can drill down to individual reports from this group report.

4.4.2.14

MNR Group Top 10 Performance Report Description

NOTICE: Group reports do not generate threshold traps.

Table 15: MNR Group Top 10 Performance Report Description

Graph/Table	Description
CPU Utilization (%) CoCPU Utilization (%) where applicable	**CPU Utilization (%)**: The top 10 routers that have the highest CPU Utilization. **CoCPU Utilization (%)**: The top 10 routers that have the highest CoCPU Utilization.
Data Memory Utilization (%)	The top 10 routers that have the highest Data Memory Utilization.

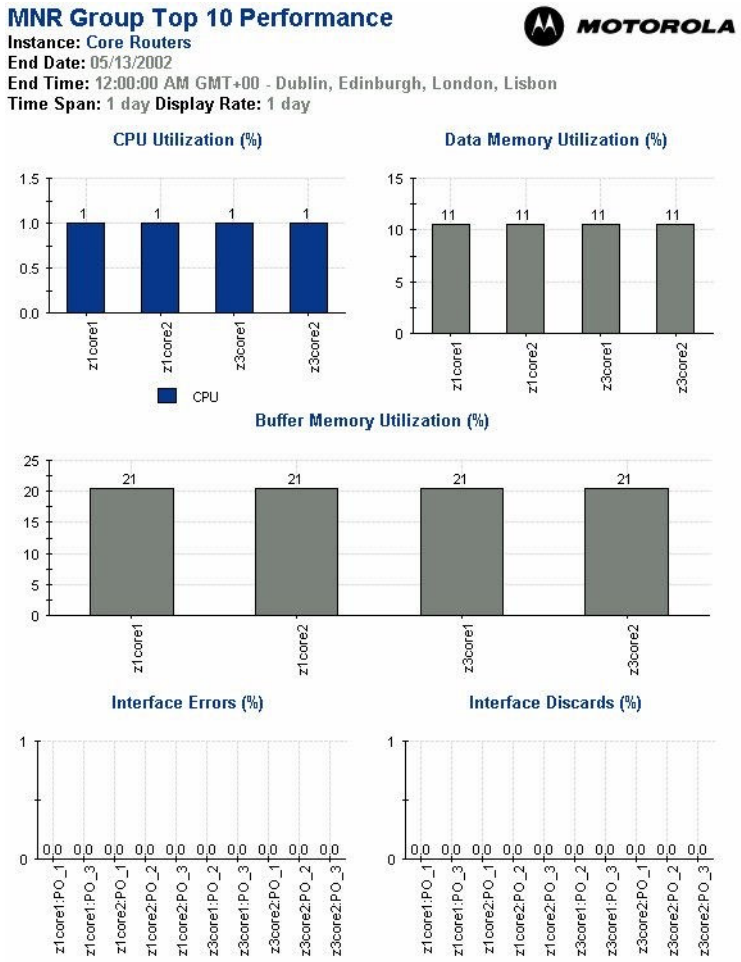
Graph/Table	Description
Buffer Memory Utilization (%)	The top 10 routers that have the highest Buffer Memory Utilization.
Interface Errors (%)	The top 10 routers that have the highest Port Errors (Port Errors are calculated using the maximum of IN and OUT Port Errors).
Interface Discards (%)	The top 10 routers that have the highest Port Discards (Port Discards are calculated using the maximum of IN and OUT Port Discards).

4.4.2.15
MNR Group Top 10 Performance Report

The following information explains how to use the report:

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. The maximum value for graphs that show percentages (%) is 100%. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the top ten routers.
- The bars of a graph show the value of the statistic to the nearest value on the y-axis. For example, if the value is between 20 and 25, and the number 21 appears above the bar, this indicates that the actual value is closer to 21.

Figure 25: MNR Group Top 10 Performance Report



4.4.2.16

MNR WAN Link Performance

Ethernet WAN Interface performance report includes statistics for each Ethernet site link in the router. Ethernet WAN link is a logical link connected between 2 routers using IP-IP protocol on the Ethernet interfaces. In the ASTRO® 25 system, it could be between a core and site gateway, exit to exit routers, GGSN to CBR routers, and so on. All statistics are measured only when the link is operative (up). Measurement frequency varies for each statistics and they are collected for the configured interval (which can be 15, 30, 45, or 60 minutes) and obtained by Ethernet WAN link Performance report at end of collection interval.

NOTICE: This report does not generate traps to Unified Event Manager (UEM).

4.4.2.17

MNR WAN Link Performance Description

The report displays collected data in a form of six graphs. This section presents MNR WAN Link Performance usage in each of the graphs.

Table 16: IPLR Packets

MIB Object Name	Report Object Name	Description
mnrEthWanIfPer-fIPLRPktNotRcvd	Lost Packets	Number of packets that were not received by the receiving end-point for last interval.
mnrEthWanIfPer-fIPLRTxPktNum	Transmit Packets	Number of packets transmitted by the source end-point in successful IPLR measurement attempts for last interval.

Table 17: Packet Loss Rate (in Hundredths of a (%))

MIB Object Name	Report Object Name	Description
mnrEthWanIfPerfIPLR-LossRate		IP packet loss rate (that is, number of packets not received divided by number of packets transmitted) for last interval.

Table 18: IPTD Round Trip (in milliseconds)

MIB Object Name	Report Object Name	Description
mnrEthWanIfPerfIPTD-Max	Maximum	Maximum round-trip IPTD measurement for last interval.
mnrEthWanIfPerfIPT-DAvg	Average	Average value of the round-trip IPTD measurements for last interval.
mnrEthWanIfPerfIPTDMin	Minimum	Minimum round-trip IPTD measurement for last interval.

Table 19: Number of Successful Measurements

MIB Object Name	Report Object Name	Description
mnrEthWanIfPerfIPDV99Per-centNum	IPDV99 Percent	Number of successful measurements of the 99th percentile IPDV for last interval.
mnrEthWanIfPerfIPDVNum	IPDV	Number of successful IPDVmeasurements for last interval.
mnrEthWanIfPerfIPTDNum	IPTD	Number of successful round-tripIPTD measurements for last interval. Value zero (0) indicates that link is inoperative throughout the measurement interval.

Table 20: IPDV (in milliseconds)

MIB Object Name	Report Object Name	Description
mnrEthWanIfPerfIPDVSum	Sum	Sum of the IPDV measurements for last interval.
mnrEthWanIfPerfIPDV-SumSq	Sum of Squares	Sum of squares of the IPDVmeasurements for last interval.
mnrEthWanIfPerfIPDVAvg	Average	Average value of the IPDV measurements for last interval.

Table 21: IPDV 99 Percent (in milliseconds)

MIB Object Name	Report Object Name	Description
mnrEthWanIfPerfIPDV99PercentSum	Sum	Sum of the measurements of the 99th percentile IPDV for last interval.
mnrEthWanIfPerfIPDV99PercentAvg	Average	Average value of the 99th percentile IPDV measurements for last interval.
mnrEthWanIfPerfIPDV99PercentMax	Maximum	Maximum 99th percentile IPDV-measurements for last interval.
mnrEthWanIfPerfIPDV99PercentMin	Minimum	Minimum 99th percentile IPDV-measurements for last interval.

4.4.2.18
MNR WAN Link Performance Report

The following information explains how to use the report.

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. This report shows two types of graphs, one shows % value, the other shows milliseconds (ms). The maximum value for graphs that show percentages (%) is 100%. For graphs that show a count, the maximum varies. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the span of time.

4.4.2.19
DS1/E1 Interface Performance

This section provides information on the DS1/E1 Interface Performance report.

4.4.2.20
DS1/E1 Interface Performance Report Description

Table 22: DS1/E1 Interface Performance Report Description

Graph/Table	Description
Total Number of Bursty Errored Seconds	The total number of Bursty Errored Seconds (BES) encountered by a DS1/E1 interface. This is applicable only for ESF frame mode. A second with fewer than 320 and more than 1 Path Coding Violations error events, no severely errored frame defects, and no detected incoming AIS defects.
Controlled Slip Seconds	The total number of Controlled Slip Seconds (CSS) encountered by a DS1/E1 interface. This is a one-second interval containing one or more controlled slips.
Errored Seconds	The total number of Errored Seconds (ES) encountered by a DS1/E1 interface. An ES is the second with one or more OOF, one or more Path Code Violations (BPV or CRC), one or more controlled slip or AIS defect events.
Line Errored Seconds	The total number of Line Errored Seconds (LES) encountered by a DS1/E1 interface. This is a one-second interval containing one or more line errors. Line errors include BPV, EXZ (Excessive Zeros), and LOS defects.
Severely Errored Framing Seconds	The total number of Severely Errored Framing Seconds (SEFS) encountered by a DS1/E1 interface. A SEFS is the second with one or more out of frame (OOF) events.
Severely Errored Seconds	The total number of Severely Errored Seconds (SES) encountered by a DS1/E1 interface. For ESF Frame mode, a SES is a second with 320 or more Path Code Violations (BPV or CRC) or one or more OOF events or a detected AIS event. For E1-CRC frame mode, a SES is a second with 832 or more Path Code Violations (BPV or CRC) or one or more OOF events or a detected AIS event. For E1-noCRC frame mode, a SES is a second with 2048 Line Code Violations (LCVs) or more. For D4 (SF) signals, a SES is a second with OOF or framing error events.
Unavailable Seconds	The total number of Unavailable Seconds (UAS) encountered by a DS1/E1 interface. An UAS is the seconds that interface is in an unavailable signal state. An unavailable signal state occurs at the onset of 10 consecutive SESs. The state is cleared at the onset of 10 seconds with no SESs.
Degraded Minutes	The number of Degraded Minutes (DM) errors encountered by a DS1/E1 interface. A degraded minute is one in which the estimated error rate exceeds 1E-6, but does not exceed 1E-3. This is the total minutes that this condition occurs since the last time when the port was not in this condition. These are contiguous minutes.
Controlled Slip	The total number of Controlled Slip (CS) errors encountered by a DS1/E1 interface. This statistics is directly reported from the 8370 chipset in performance monitoring registers (register 0x06).

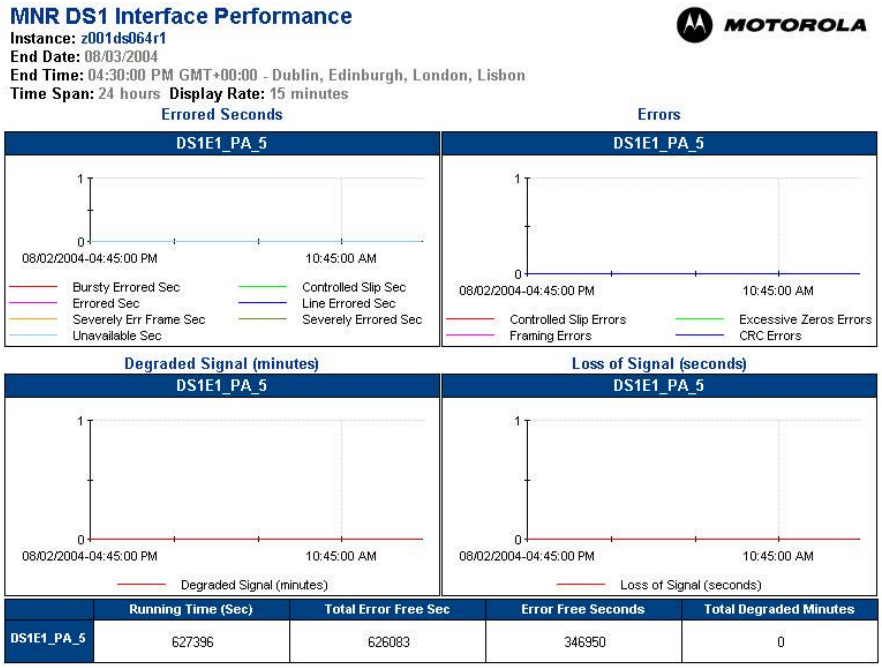
Graph/Table	Description
Excessive Zeros	The total number of Excessive Zeros (EXZ) errors encountered by a DS1/E1 interface. This statistics is directly reported from the 8370 chipset in the performance monitoring registers (register 0x54, 0x55). The registers 0x54 and 0x55 show the combined EXZ and BPV errors provided the EXZ_LCV bit is set in the register 0x45.
Framing Errors	The total number of Framing Errors encountered by a DS1/E1 interface. This statistics is directly reported from the 8370 chipset in the performance monitoring registers (registers 0x50 or 0x51).
CRC Errors	The total number of CRC Errors. This statistics is directly reported from the 8370 chipset in the performance monitoring registers (registers 0x052, 0x053).
Loss of Signal	The total number of times that the line lost signal. 8370 Alarm register (0x004) provides the statistics for the same. The DS1/E1 driver reads this register in a polling routine, which gets called every 250 milliseconds.
Running Time	The number of seconds since the DS1/E1 interface path was set to operational state.
Total Error Free Seconds	The number of Total Error Free Seconds (TEFS) encountered by a DS1/E1 interface. A TEFS is the total number of seconds in which the port is not in error state since it is operational. This counter is not contiguous, it is a cumulative one of all the seconds in which the ports state is error free.
Error Free Seconds	The number of Error Free Seconds (EFS) encountered by a DS1/E1 interface. This is the number of seconds in which the port is not in error state since the last errored second occurred.
Total Degraded Minutes	The number of Total Degraded Minutes (TDM) errors encountered by a DS1/E1 interface. A degraded minute is one in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3. This is the total number of minutes that this condition occurs even if they are not continuous.

4.4.2.21
DS1/E1 Interface Performance Report

The following information explains how to use the report:

- The y-axis (vertical axis) represents the values of the statistic. The maximum value for graphs that show percentages (%) is 100%. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the span of time.

Figure 26: DS1/E1 Interface Performance Report



4.4.2.22

MNR PVC Utilization

MNR PVC Utilization is an individual report that is created for each Motorola Network Resource (MNR) in the system to look at Permanent Virtual Circuit (PVC) traffic.

It collects bandwidth utilization IN and OUT on each Frame Relay PVC (shown in the legend using the Data Link Connection Identifier (DLCI) number). For the types of routers in your system, see Types of Reports for the Routers on page 63.

NOTICE: This report does not generate traps to Unified Event Manager (UEM).

View the daily report template when a trap has been generated to aid with more in-depth problem determination. View the daily, weekly, monthly, and yearly reports to assist with capacity planning.

4.4.2.23

MNR PVC Utilization Report Description

NOTICE: Where no traps for the statistics are sent, the Tm and Tw columns show Not Applicable (N/A).

Table 23: MNR PVC Utilization Report Description

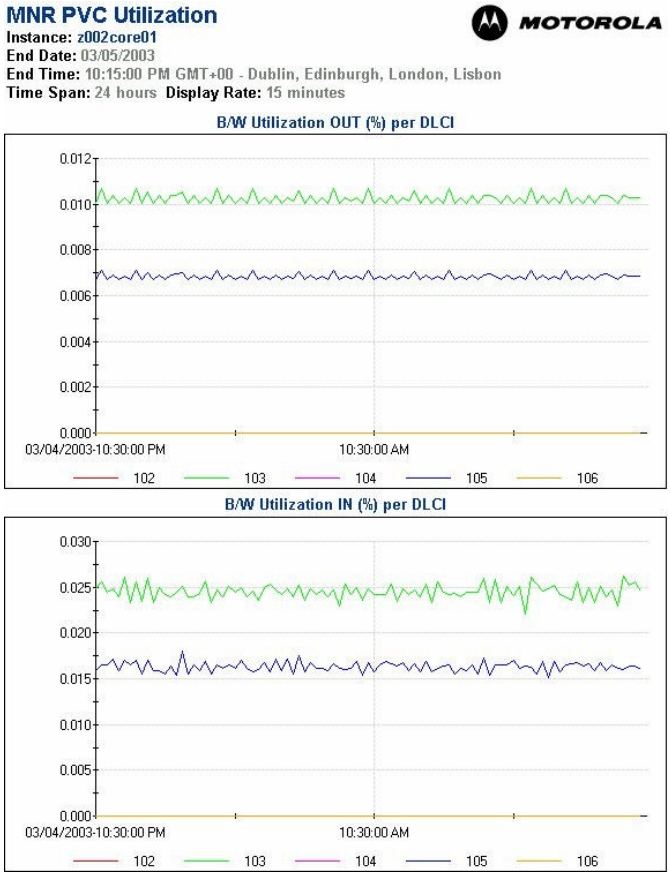
Graph/Table	Tm	Tw	Description
B/W Utilization OUT (%) per DLCI	N/A	N/A	The PVC utilization percentage is calculated using the total number of octets transmitted on the PVC to the PVC's Committed Burst Rate (CBR) in Kbps.
B/W Utilization IN (%) per DLCI	N/A	N/A	The PVC utilization percentage is calculated using the total number of octets received on the PVC to the PVC's Committed Burst Rate (CBR) in Kbps.

4.4.2.24
MNR PVC Utilization Report

The following information explains how to use the report.

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. The maximum value for graphs that show percentages (%) is 100%. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the span of time.

Figure 27: MNR PVC Utilization Report



4.4.2.25
MNR PVC Queue Performance

MNR PVC Queue Performance is a report that shows all of used router queues in each of the graphs. It also provides the name for the type of traffic and the queue number. For the types of routers in your system, see Types of Reports for the Routers on page 63.

Thresholds are defined, and traps are sent for voice packets dropped per DLCI due to the full queue.

View the daily report template when a trap has been generated to aid with more in-depth problem determination. View the weekly, monthly, and yearly reports to assist with capacity planning.

4.4.2.26
MNR PVC Queue Performance Report Description

Table 24: MNR PVC Queue Performance Report Description

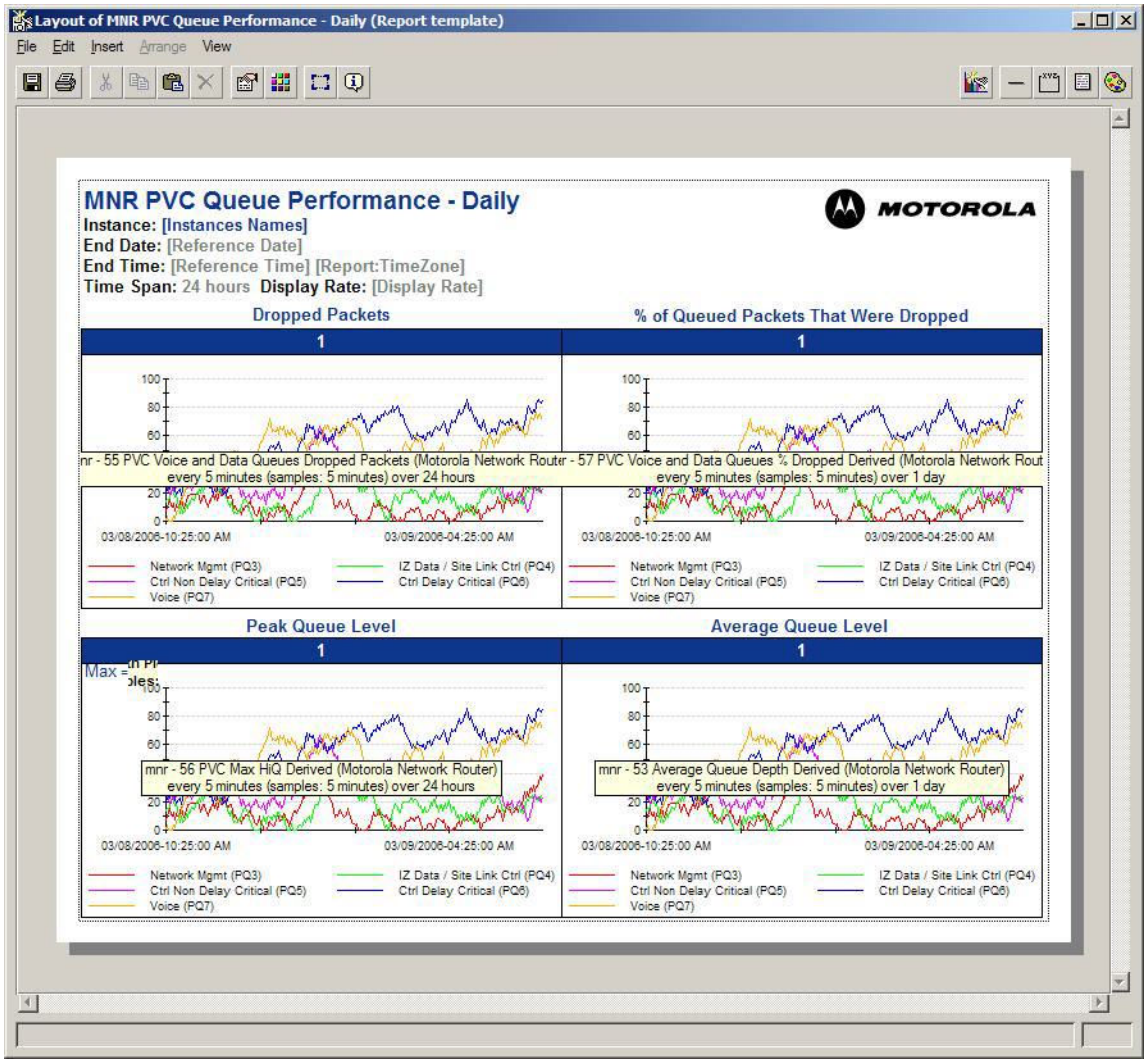
Graph/Table	Description
Dropped Packets	Dropped packets represent the number of packets that were dropped on that router for each queue (Each queue is listed individually for all graphs).
Percentage of Queued packets that were dropped	Percentage of Queued packets that were dropped is the number of packets that were placed in a queue and then dropped.
Peak Queue Level	Peak Queue Level is the highest level the queue reached during the previous polling cycle.
Average Queue Level	Average Queue level represents the average level of the queue over the last polling cycle.

4.4.2.27
MNR PVC Queue Performance Report

The following information explains how to use the report.

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- For **Graphs showing % values**:
  - The y-axis (vertical axis) represents the values of the statistic. The maximum value for graphs that show percentages (%) is 100%. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
  - The x-axis (horizontal axis) represents the span of time.
- For **Graphs showing number of packets dropped**:
  - The y-axis (vertical axis) represents the values of the statistic. For graphs that show a count, the maximum varies. For example, this graph shows the number of data packets dropped. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
  - The x-axis (horizontal axis) represents the span of time.

Figure 28: MNR PVC Queue Performance Report



4.4.2.28

MNR Group Top 10 PVC Utilization

MNR Group Top 10 PVC Utilization is a group report that is created for the Motorola Network Resources (MNRs) in the system. For the types of routers in your system, see Types of Reports for the Routers on page 63.

It shows the Top **N** (up to 10) PVCs (represented by DLCI numbers) of all routers in the group for all statistics in the MNR PVC Utilization report.

It shows two separate graphs for the Top **N** (up to 10) PVCs (represented by DLCI number) of all routers in the group that have the highest bandwidth utilization in the inbound and outbound directions.

View the daily, weekly, monthly, and yearly reports to assist with capacity planning by comparing the utilization for PVCs in a zone from the core to the sites or between zones on all exit routers in the system.

4.4.2.29
MNR Group Top 10 PVC Utilization Report Description

NOTICE: Group reports do not generate threshold traps.

Table 25: MNR Group Top 10 PVC Utilization Report Description

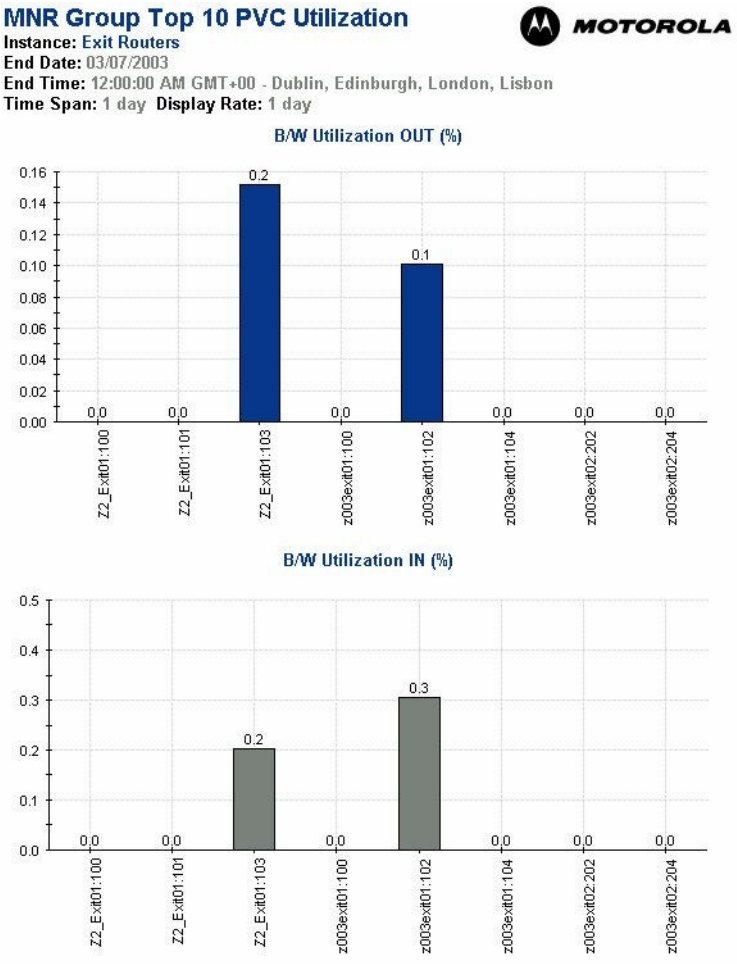
Graph/Table	Description
B/W Utilization OUT (%)	The top 10 PVCs (represented by DLCI numbers) of all routers in the group that have the highest bandwidth utilization in the out-bound direction.
B/W Utilization IN (%)	The top 10 PVCs (represented by DLCI numbers) of all routers in the group that have the highest bandwidth utilization in the inbound direction.

4.4.2.30
MNR Group Top 10 PVC Utilization Report

The following information explains how to use the report:

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. The maximum value for graphs that show percentages (%) is 100%. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the top 10 PVCs.
- The bars of a graph show the value of the statistic to the nearest value on the y-axis. For example, if the value is between 0.00 and 0.10, and the number 0.1 appears above the bar, this indicates that the actual value is closer to 0.10.

Figure 29: MNR Group Top 10 PVC Utilization Report



4.4.2.31

MNR Group Top 10 PVC Performance (Queues 3 to 7)

MNR Group Top 10 PVC Performance (Queues 3 to 7) is a group report that is created for the Motorola Network Resources (MNRs) in the system. For the types of routers in your system, see Types of Reports for the Routers on page 63.

It shows the Top **N** (up to 10) PVCs (represented by DLCI numbers) of all routers in the group for all statistics in the MNR PVC Queue Performance reports.

It shows four graphs for the Top **N** (up to 10) PVCs (represented by DLCI number) of all routers in the group that have the highest % of voice traffic queued, voice packets dropped, % of data traffic queued, and data packets dropped.

4.4.2.32

MNR Group Top 10 PVC Performance (Queues 3 to 7) Report Description

NOTICE: Group reports do not generate threshold traps.

Table 26: MNR Group Top 10 PVC Performance (Queues 3 to 7) Report Description

Graph/Table	Description
Dropped Packets for This Queue	The top 10 PVCs (represented by DLCI numbers) of packets that were dropped on that router for a particular queue.
% of Queued Packets that were dropped for this queue	The top 10 PVCs (represented by DLCI numbers) of all routers in the group that have the highest % of packets that were placed in queue and then dropped.
Peak Queue Level for this queue	The top 10 PVCs (represented by DLCI numbers) of all routers in the group that had the highest queue level during the previous polling cycle.
Average Queue level for this Queue	The top 10 PVCs (represented by DLCI numbers) of the average level of the queue over the last polling cycle.

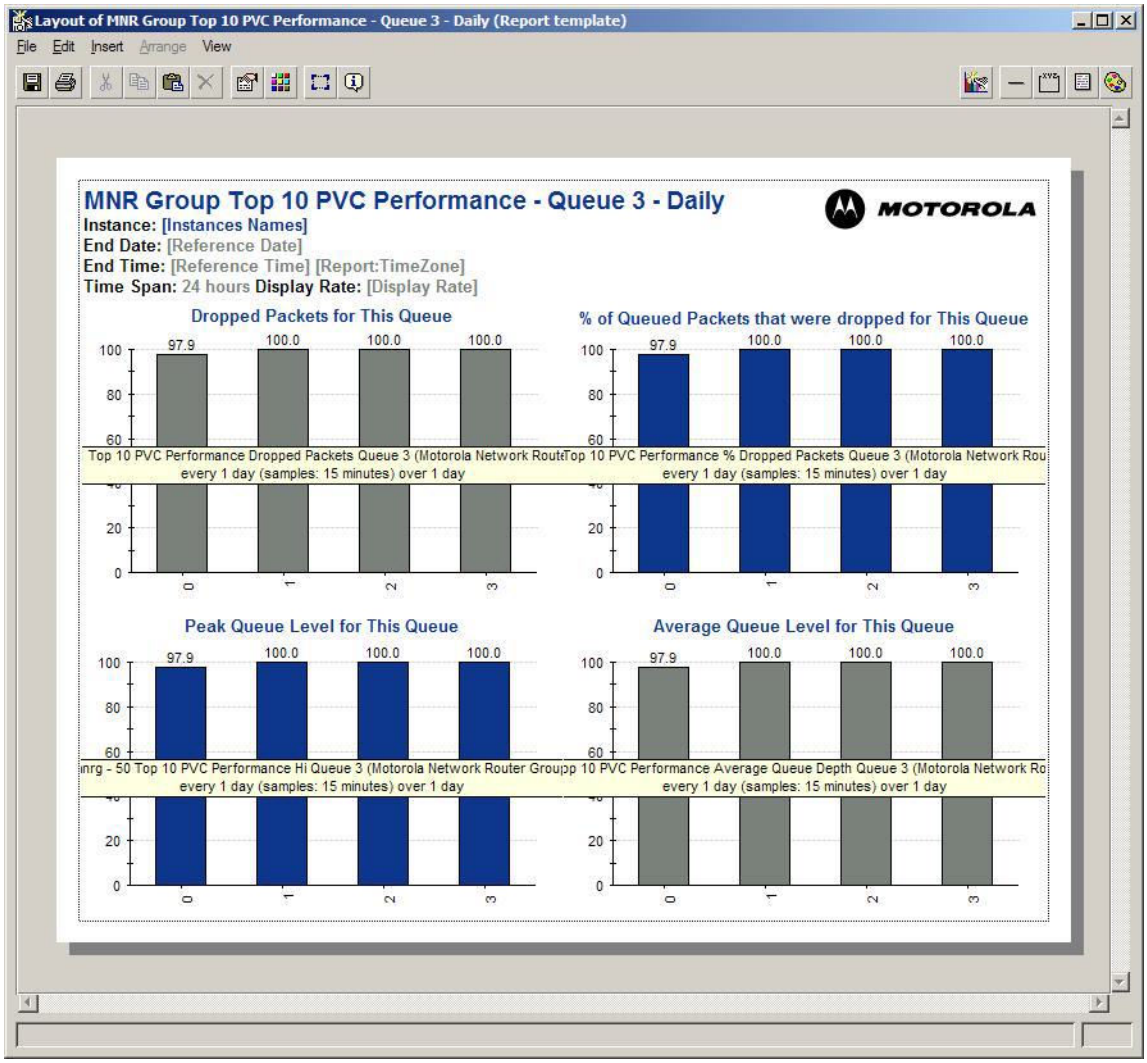
4.4.2.33

MNR Group Top 10 PVC Performance (Queues 3 to 7) Report

The following information explains how to use the report.

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- For **Graphs showing % values**:
  - The y-axis (vertical axis) represents the values of the statistic. The maximum value for graphs that show percentages (%) is 100%. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
  - The x-axis (horizontal axis) represents the top 10 PVCs.
- For **Graphs showing number of packets dropped**:
  - The y-axis (vertical axis) represents the values of the statistic. For graphs that show a count, the maximum varies. For example, this graph shows the number of packets dropped. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
  - The x-axis (horizontal axis) represents the top 10 PVCs.
  - The bars of a graph show the value of the statistic to the nearest value on the y-axis. For example, if the value is between 0 and 1, and the number 1 appears above the bar, this indicates that the actual value is closer to 1.

Figure 30: MNR Group Top 10 PVC Performance (Queues 3 to 7)



4.4.3
Interpreting HP LAN Switch Reports

This section provides information on:

- HP LAN switch port performance.
- HP LAN switch group top 10 port performance.
- HP LAN switch port Name/MIBIndexNo. report.

4.4.3.1
HP LAN Switch Port Performance

HP LAN Switch Port Performance is an individual report that is created for each port on a single HP LAN switch.

It collects bandwidth utilization IN and OUT for each port and total errors, total discards, and specific errors and discards IN and OUT for each port.

Thresholds are defined for bandwidth utilization IN and OUT. Traps are sent when the maximum of the two IN and OUT values exceeds the thresholds. Thresholds are also defined for total errors and total discards.

View the daily report template when a trap has been generated to aid with more in-depth problem determination. View the weekly, monthly, and yearly reports to assist with capacity planning.

4.4.3.2

HP LAN Switch Port Performance Report Description

Thresholds are defined for some graphs on this report, as follows:

- **Tm** = Threshold major. If the statistic exceeds this value, a major trap is sent to Unified Event Manager (UEM).
- **Tw** = Threshold warning. If the statistic exceeds this value, a warning trap is sent to UEM, for example, if the Bandwidth Utilization IN (%) reaches 95%.

Table 27: HP LAN Switch Port Performance Report Description

Graph/Table	Tm	Tw	Description
Bandwidth Utilization IN (%)	100	95	The port utilization percentage is calculated using the total number of octets received on the interface to the interface's current bandwidth in units of 1,000,000 bits per second.
Bandwidth Utilization OUT (%)	100	95	The port utilization percentage calculated using the total number of octets transmitted out on the interface to the interface's current bandwidth in units of 1,000,000 bits per second.
Total Errors (%)	4	2	**Errors IN (%)** If the number of inbound packets is greater than zero (0) and greater than total packets in errors, Port Errors Utilization is the (Number of Inbound Packets in Error)/(Total Inbound Packets). If the Number of Errors is greater than zero (0) and the Number of Errors is greater than Total Inbound Packets then Utilization is 100%, else it is 0%. **Errors OUT (%)** If the number of outbound packets is greater than zero (0) and less than total packets in errors, Port Errors Utilization is the (Number of Outbound Packets in Error)/(Total Outbound Packets). If the Number of Errors is greater than zero (0) and the Number of Errors is greater than Total Outbound Packets, then Utilization is 100%, else it is 0%.
Total Discards (%)	4	2	**Discards IN (%)** If the number of inbound packets is greater than zero (0) and greater than total packets discarded, Port Discards Utilization is the (Number of Inbound Packets Discarded)/(Total Inbound Packets). If the Number of Discards is greater than zero (0) and Number of Discards is greater than Total Inbound Packets then Utilization is 100%, else it is 0%. The number of inbound packets is chosen to be discarded though no errors have been detected to prevent it from being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

Graph/Table	Tm	Tw	Description
			Discards OUT (%) If the number of outbound packets is greater than zero and greater than total packets discarded, Port Discards Utilization is (Number of Outbound Packets Discarded)/(Total Outbound Packets). If Number of Discards is greater than zero (0) and Number of Discards is greater than Total Outbound Packets then Utilization is 100%, else it is 0%. The number of outbound packets is chosen to be discarded though no errors had been detected to prevent it being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Specific Errors and Discards IN	N/A	N/A	These errors do not represent all possible errors on the port. This means that if you see a % of errors or discards in the graph, you may not necessarily see any errors on this graph. **Alignment (frames)**: A count of frames received on a particular interface does not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the Media Access Control (MAC) service to the Logical Link Control (LLC) layer. **FCS (frames)**: A count of frames received on a particular interface does not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC layer. **Long Frame (frames)**: A count of frames received on a particular interface that exceeds the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC layer. **Mac Rx (frames)**: A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
Specific Errors and Discards OUT	N/A	N/A	These errors do not represent all possible errors on the port. This means that if you see a % of errors or discards in the graph, you may not necessarily see any errors on this graph. **Carrier Sense (errors)**: The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. **Excess Collsn (frames)**: A count of frames for which transmission on a particular interface fails due to excessive collisions. **Mac Tx (frames)**: A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.

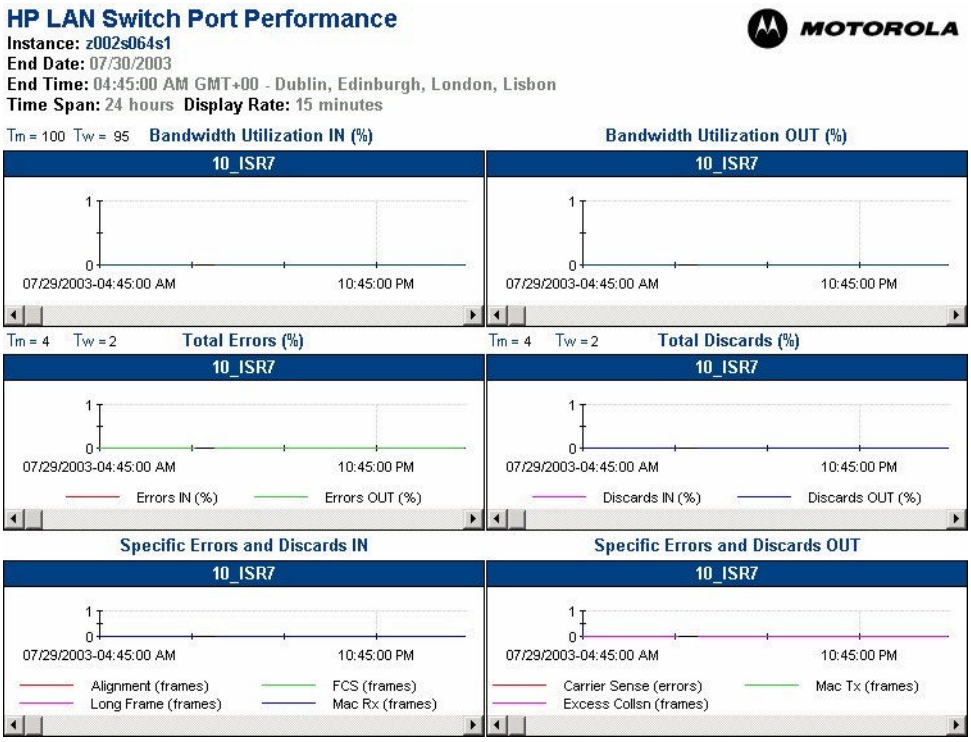
4.4.3.3
HP LAN Switch Port Performance Report

The following information explains how to use the report:

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.

- The port number followed by the name of the device connected to that port appears at the top of every graph on the report.
- For **Graphs showing % values**:
  - The y-axis (vertical axis) represents the values of the statistic. The maximum value for graphs that show percentages (%) is 100%. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
  - The x-axis (horizontal axis) represents the span of time.
- For **Graphs showing number of errors and discards**:
  - The y-axis (vertical axis) represents the values of the statistics either as a percentage or a number. The minimum value of the y-axis is always zero, and the maximum value shown varies depending on the value of the statistic. For example, if the value of a statistic is 0.5%, the y-axis may span from 0 to 1 or if the value is 32%, the y-axis may span from 0 to 40.
  - The x-axis (horizontal axis) represents the span of time.

Figure 31: HP LAN Switch Port Performance Report



4.4.3.4

HP LAN Switch Group Top 10 Port Performance

HP LAN Switch Group Top 10 Port Performance is a group report that is created for each port on a group of HP LAN switches. It is a system-level report.

It shows the Top **N** (up to 10) ports on the HP LAN switch with the highest values for all statistics in the HP LAN Switch Port Performance report. It collects bandwidth utilization, errors, and discards on the ports.

View the reports to assist with capacity planning. You can drill down to individual reports from this group report.

NOTICE: This report does not generate threshold traps to Unified Event Manager.

4.4.3.5
HP LAN Switch Group Top 10 Port Performance Report Description

Table 28: HP LAN Switch Group Top 10 Port Performance Report Description

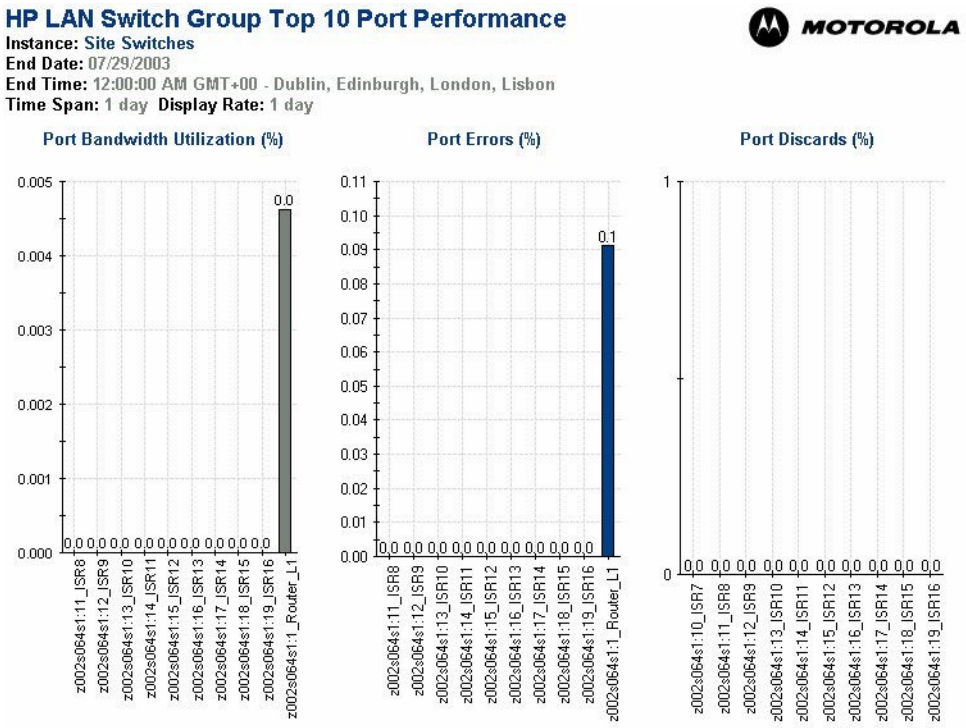
Graph/Table	Tm	Tw	Description
Port Bandwidth Utilization (%)	N/A	N/A	The top 10 switches that have the maximum Port Utilization. (Maximum Port Utilization is calculated using the maximum of IN and OUT Port Utilization.)
Port Errors (%)	N/A	N/A	The top 10 switches that have the highest Port Errors. (Port Errors is calculated using the maximum of the IN and OUT Port Errors.)
Port Discards (%)	N/A	N/A	The top 10 switches that have the highest Port Discards. (Port Discards is calculated using the maximum of IN and OUT Port Discards.)

4.4.3.6
HP LAN Switch Group Top 10 Port Performance Report

The following information explains how to use the report:

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. The maximum value for graphs that show percentages (%) is 100%. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the top ten switches.
- The bars of a graph show the value of the statistic to the nearest value on the y-axis. For example, if the value is between 0.18 and 0.20, and the number 0.2 appears above the bar, this indicates that the actual value is closer to 0.2.

Figure 32: HP LAN Switch Group Top 10 Port Performance Report



4.4.3.7

HP LAN Switch Port Name/MIB Index No. Report

The HP LAN Switch Port Name/MIB Index No. report should be viewed to obtain the MIB Index Numbers, the VLAN IDs, and the speed of the Port Names that appears in the HP LAN Switch Port Performance report. This report is only generated for the two HP LAN switches in the core and not the HP LAN Switches at the sites.

4.4.3.8

HP LAN Switch Port Name/MIB Index No. Report Description

Table 29: HP LAN Switch Port Name/MIB Index No. Port Performance Report Description

Graph/Table	Tm	Tw	Description
MIB Index Number	N/A	N/A	The MIB Index Number for each internal and external port on the switch. These MIB Index numbers show up in traps that are generated by the switch. This report can be used to determine which port sent the trap.
Port Name	N/A	N/A	The Port Name of each internal and external port on the switch. The first part of the Port Name contains the physical card/port number followed by the name of the device that is connected to the port.
Speed (Mbps)	N/A	N/A	The Speed in Megabits per second (Mbps) of each internal and external port on the switch. The possible values for this column are: • 1000 - this represents 1000 Mbps.

Graph/Table	Tm	Tw	Description
			• 100 - this represents 100 Mbps. • 10 - this represents 10 Mbps. • Auto-Detect - the switch port detect the speed of the device that is connected to the port and configure the port with the same speed.
VLAN ID	N/A	N/A	The VLAN ID of each internal and external port on the switch.
VLAN Name	N/A	N/A	The Name of each VLAN ID.

4.4.3.9
HP LAN Switch Port Name/MIB Index No. Report Example

The following figure shows the HP LAN Switch Port Name/MIB Index No. report.

Figure 33: HP LAN Switch Port Name/MIB Index No. Report

HP LAN Switch Port Info Table

MOTOROLA

Instance: z004lans01
End Date: 06/24/2004
End Time: 10:49:00 PM GMT+00:00 - Dublin, Edinburgh, London, Lisbon
Time Span: 1 hour **Display Rate:** 1 hour

MIB Index Number	Port Name	Speed (Mbps)	VLAN ID
1	a1-z004gtwy1-p2	100	251
2	a2-z004gtwy1-p1	100	1
3		10	1
4		10	1
5	a5-z004exit1-p1	100	251
6	a6-z004exit2-p1	100	251
7	a7-z004core1-p1	100	251
8	a8-z004core2-p1	100	251
9	a9-z004core3-p1	100	251
10	a10-z004core4-p1	100	251
11	a11-z004core5-p1	100	251
12	a12-z004core6-p1	100	251
13	a13-z004zc1-nic1	10	31
14	a14-z004zc2-nic1	10	31
15	a15-z004vlog1	10	36
16	a16-z004vlog2	10	36
17	a17-z004ggsn1-data	100	5
18	a18-z004sdr	10	5
19	a19-z004mgeg3	10	43
20	a20-z004mgeg1	10	41
21	a21-z004tig5	10	34
22	a22-z004tig7	10	34

VLAN ID	VLAN Name
1	DEFAULT_VLAN
5	z004_DATA
6	z004_DISPTCH
31	z004_CTRL1
33	z004_ZNM
34	z004_TIG1
36	z004_ATIA

4.4.4
Interpreting Radio Network Gateway Reports

This section provides information on:

- RNG Context Activation
- RNG HPD Packet Data Service – UP Connect Information
- RNG HPD Packet Data Service – SDU Transmissions
- RNG mobility
- RNG channel resources
- RNG inbound and outbound Data Profile
- RNG – Integrated Voice and Data

NOTICE: Not all statistics are supported for Conventional systems/subsystems. These statistics which are not supported are reported as 'zero' in Conventional statistics reports.

- The RNG instance ID (pdgPDRRNGProxyStatsRngInstanceID) appears in all RNG Reports.
- All RNG Reports shall display data in the following two ways:
  - Numbers since last statistics reset (pdgPDRRNGProxyStatsLastResetTime).
  - On a per-hour basis.

4.4.4.1
RNG Context Activation

RNG Context Activation is an individual report that is created for the RNG. It shows the rate at which mobile subscriber units are added and deleted from the RNG database.

Use this report to monitor and analyze mobile subscriber units that context activate/deactivate through a particular RNG.

NOTICE: This report does not generate traps to Unified Event Manager (UEM).

4.4.4.2
RNG Context Activation Report Description

Table 30: RNG Context Activation Report Description

MIB Object Name	Report Object Name	Object Description
pdgPDRRNGProxyStatsAddUsrCount	Add User Requests received from PDRs	Number of Add User Requests received from all Packet Data Routers.
pdgPDRRNGProxyStatsDelUsrCount	Delete User Requests received from PDRs	Number of Delete User Requests received from all Packet Data Routers.
pdgPDRRNGProxyStatsNewUsrResponseMsgCount	New User Responses received from PDRs	Number of New User Responses received from all Packet Data Routers.
pdgPDRRNGProxyStatsDeactUsrStbTimeoutMsgCount	Deactivate User Msgs sent to PDRs due to Standby Timer expiration	Number of Deactivate User Messages sent to all Packet Data Routers due to Standby Timer expiration.
pdgPDRRNGProxyStatsDeactUsrMobPushMsgCount	Deactivate User Msgs sent to PDRs due to Mobility Pushes	Number of Deactivate User Messages sent to all Packet Data Routers due to Mobility Pushes.
pdgPDRRNGProxyStatsFacilityMsgCount	Facility Indications sent to PDRs	Number of Facility Indications sent to all Packet Data Routers.

4.4.4.3
RNG Context Activation Report

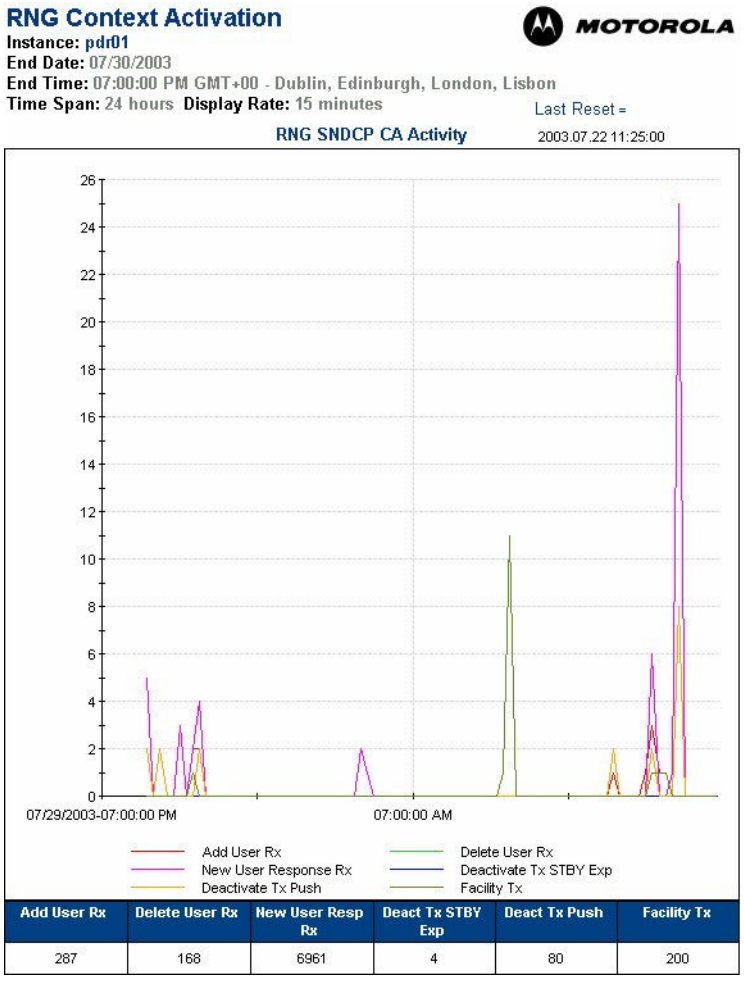
The following information explains how to use the report:

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. For graphs that show a count, the maximum varies. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the span of time.
- The **Last Reset** field shows the date and time of the last RNG reset.

NOTICE: The report object names in the graph are abbreviated.

- Add User Rx – Add User Requests received from PDRs
- Delete User Rx – Delete User Requests received from PDRs
- New User Response Rx – New User Responses received from PDRs
- Deactivate Tx STBY Exp – Deactivate User Msgs sent to PDRs due to Standby Timer expiration
- Deactivate Tx Push – Deactivate User Msgs sent to PDRs due to Mobility Pushes
- Facility Tx – Facility Indications sent to PDRs

Figure 34: RNG Context Activation Report



Add User Rx	Delete User Rx	New User Resp Rx	Deact Tx STBY Exp	Deact Tx Push	Facility Tx
287	168	6961	4	80	200

4.4.4.4

RNG – Integrated Voice and Data

Integrated Voice and Data service can support the following:

- Operation in the 700 MHz and 800 MHz, UHF-R2 (435 MHz to 524 MHz), and VHF (136 MHz to 174 MHz) frequency bands at 9600-baud
- Operation in up to seven zones. 100 sites per zone
- Up to 20,000 active data subscribers
- Support for up to three PDCHs per site (configurable) – a minimum of one PDCH per site
- One to 255 users per channel (configurable)
- Potential total capacity for 180 data capable subscriber radios per site – with 3 data channels at a site and 60 subscriber units per channel
- Industry standard protocols – Dynamic Host Control Protocol (DHCP), Point-to-Point Protocol (PPP), IPv4
- Industry standard services such as static and dynamic IP addressing, IP fragmentation, and Internet Control Message Protocol (ICMP) error reporting
- Network Address Translation (NAT) to coordinate Radio Network Infrastructure IP plans and outside network infrastructure IP plans
- Unicast transmissions only
- Confirmed delivery of messages
- General Packet Radio Service (GPRS) Tunneling Protocol (GTP)

4.4.4.5

Packet Data Channel Access

RNG HPD Packet Data Service – SDU Transmissions is an individual report that is created for the RNG. It presents RNG Packet Data Channel Access SDU transmission information.

NOTICE: This report does not generate traps to Unified Event Manager (UEM).

Table 31: Trunked Data Service – Packet Data Channel Access

MIB Object Name	Report Object Name	Object Description
pdgPDRRNGProxyStatsPDPgReqSentCount	PD Page Request Msgs sent to Sites	Number of Packet Data Page Request messages sent to all Sites.
pdgPDRRNGProxyStatsPDAccessRecvSuccessCount	PD Access Info Success Msgs received from Sites	Number of Packet Data Access Info Success messages received from all Sites.
pdgPDRRNGProxyStatsPDAccessFailCount	PD Access Info Failure Msgs received from Sites	Number of Packet Data Access Info Failure messages received from all Sites.
pdgPDRRNGProxyStatsMsuNotRegCount	PD Access Info – MSU Not Registered	Number of Packet Data Access Info messages received from all Sites with a response code of “MSU Not Registered.”

MIB Object Name	Report Object Name	Object Description
pdgPDRRNGProxyStatsPDAccessRecvSuccessMsuNotInRngCount	PD Access Info – MSU Not In RNG	Number of Packet Data Access Info messages received from all Sites where MSU is not registered in RNG.
pdgPDRRNGProxyStatsPDEndOfDataReqSentCount	PD End Of Data Requests sent to Sites	Number of Packet Data End Of Data Requests sent to all Sites.
pdgPDRRNGProxyStatsPDEndOfDataRecvTCHCount	PD End Of Data Indications received from Sites	Number of Packet Data End Of Data Indications received from all Sites.

4.4.4.6
SDU Transmissions

RNG – SDU Transmissions is an individual report that is created for the RNG. It presents RNG Packet Data Channel Access SDU transmission information.

NOTICE: This report does not generate traps to Unified Event Manager (UEM).

Table 32: Trunked Data Service – SDU Transmissions Report Description

MIB Object Name	Report Object Name	Object Description
pdgPDRRNGProxyStats1TLCount	Tx and Rx Of 1 SDU Per PDCH Access	Number of transmissions and receptions of exactly 1 SDU per PDCH Access.
pdgPDRRNGProxyStats2TLCount	Tx and Rx Of 2 SDUs Per PDCH Access	Number of transmissions and receptions of exactly 2 SDUs per PDCH Access.
pdgPDRRNGProxyStats3TLCount	Tx and Rx Of 3 SDUs Per PDCH Access	Number of transmissions and receptions of exactly 3 SDUs per PDCH Access.
pdgPDRRNGProxyStats4GtTLCount	Tx and Rx Of 4 Or More SDUs Per PDCH Access	Number of transmissions and receptions of 4 or more SDUs per PDCH Access.

4.4.4.7
Mobility

RNG Mobility is an individual report that is created for the RNG. It shows the rate at which Mobility Management messages occur at the RNG.

Use this report to monitor and analyze the RNG's transactions with the zone controller to keep the mobile subscriber unit database updated.

NOTICE: This report does not generate traps to Unified Event Manager (UEM).

This table presents RNG Packet Data Channel Access information.

Table 33: Trunked Data Service – Mobility

MIB Object Name	Report Object Name	Object Description
pdgPDRRNGProxyStatsZCQueriesCount	Queries sent to zone controller	Number of Mobility Queries sent to the zone controller.

MIB Object Name	Report Object Name	Object Description
pdgPDRRNGProxyStatsZCResponseCount	Responses received from zone controller	Number of Mobility Responses received from the zone controller.
pdgPDRRNGProxyStatsZCQueriesFailedCount	Queries sent to the zone controller that failed since query succeeded	Number of Mobility Queries sent to the zone controller that failed since last query succeeded.
pdgPDRRNGProxyStatsPDReconnSentCount	Reconnect Requests received from Sites.	Number of Reconnect Requests received from Sites.
pdgPDRRNGProxyStatsPDReconnAccptSentCount	Reconnect Request Accepts sent to Sites	Number of Reconnect Request Accepts sent to all Sites.

4.4.4.8
RNG Channel Resources

RNG Channel Resources is an individual report that is created for the RNG. It shows the rate at which the RNG requests and is allowed to send CAI Data Blocks to the Data Site Controller (DSC) for transmission to the mobile subscriber units over-the-air.

Use this report to monitor DSC overload conditions and problems with transmission of data messages from the RNG to the DSC.

NOTICE: This report does not generate traps to Unified Event Manager (UEM).

4.4.4.9
RNG Channel Resources Report Description

The following table presents RNG PDCH Channel usage.

Table 34: Channel Resources

MIB Object Name	Report Object Name	Object Description
pdgPDRRNGProxyStatsSRPChReqSentCount	SRP Channel Requests sent to Sites	Number of SRP Channel Requests sent to all Sites.
pdgPDRRNGProxyStatsSRPSlotReqSentCount	Segments requested	Number of SRP Segments requested for transmission through SRP Channel Requests.
pdgPDRRNGProxyStatsSRPChGrantRecvCount	SRP Channel Grants received	Number of SRP Channel Grants received from all Sites.
pdgPDRRNGProxyStatsSRPSlotGrantRecvCount	Segments granted	Number of SRP Segments granted for transmission through SRP Channel Grants.
pdgPDRRNGProxyStatsSRPSlotCancReqSentCount	SRP Cancel Requests sent	Number of SRP Cancel Requests sent to all Sites.

4.4.4.10
RNG Channel Resources Report

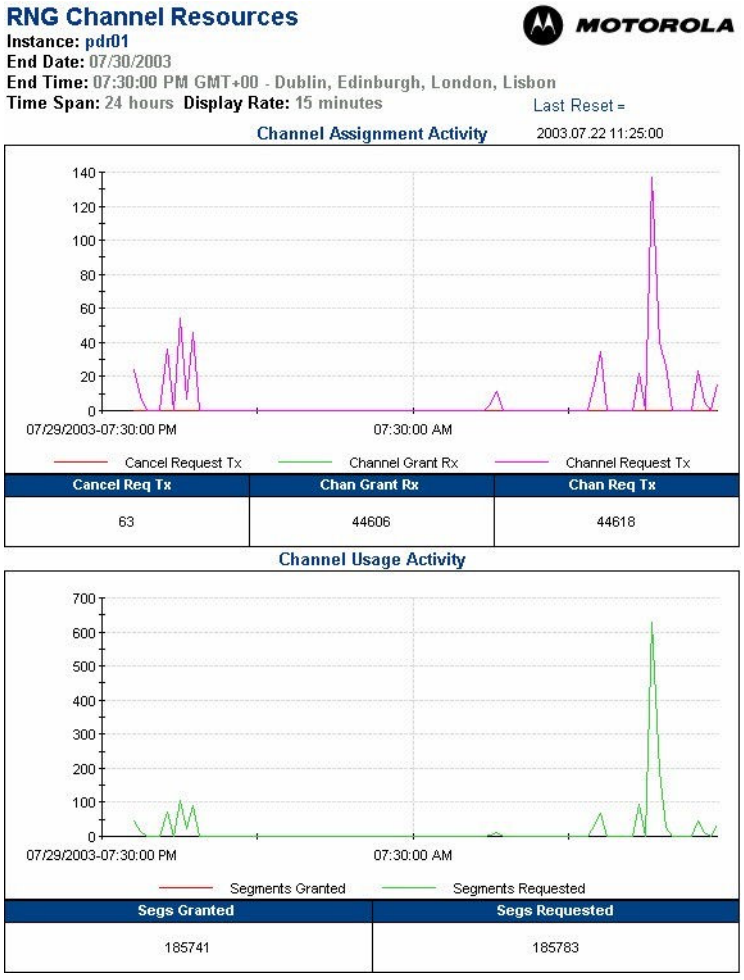
The following figure shows the RNG Channel Resources report. The following information explains how to use this report:

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. For graphs that show a count, the maximum varies. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the span of time.
- The **Last Reset** field shows the date and time of the last RNG reset.

NOTICE: The report object names in the graph are abbreviated.

- Cancel Request Tx – SRP Cancel Requests sent
- Channel Grant Rx – SRP Channel Grants received
- Channel Request Tx – SRP Channel Requests sent to Sites

Figure 35: RNG Channel Resources Report



4.4.4.11
RNG Inbound and Outbound Data Profile

RNG Inbound and Outbound Data Profile is an individual report that is created for the RNG. It shows RNG message loads.

Use this report to monitor inbound and outbound message transmission activities. Use it to detect potential over-the-air transmission problems by monitoring message retry count and response timeouts.

NOTICE: This report does not generate traps to Unified Event Manager (UEM).

4.4.4.12
RNG Inbound and Outbound Data Profile Report Description

Table 35: Outbound Data

MIB Object Name	Report Object Name	Object Description
pdgPDRRNGProxyStatsALOBSegCount	CAI PDUs transmitted to MSUs	Number of CAI PDUs transmitted to all Mobile Subscriber Units.
pdgPDRRNGProxyStatsALReTransOBSegCount	CAI PDUs retransmitted to MSUs	Number of CAI PDUs retransmitted to Mobile Subscriber Units.
pdgPDRRNGProxyStatsALAckIBCount	CAI ACKs received from MSUs	Number of CAI Response Messages (ACKs/NACKs/Selective ACKs) received from all Mobile Subscriber Units.
pdgPDRRNGProxyStatsALAckTimeoutCount	CAI ACK Timeouts	Number of CAI Response Message Timeouts in the RNG.
pdgPDRRNGProxyStatsTLSDUOBCount	PDGP SDUs transmitted to MSUs	Number of confirmed PDGP SDUs transmitted to all Mobile Subscriber Units.
pdgPDRRNGProxyStatsUnCnfOBCount	Unconfirmed Messages sent to MSUs	Number of unconfirmed messages sent to all Mobile Subscriber Units.
pdgPDRRNGProxyStatsBcastOBCount	Broadcast Messages sent to the Sites	The number of Broadcast Outbound PDGP messages forwarded by the RNG to the site controllers listening on the multicast IP address for broadcast data.

Table 36: Inbound Data

MIB Object Name	Report Object Name	Object Description
pdgPDRRNGProxyStatsALIBSegCount	CAI PDUs received from MSUs	Number of CAI PDUs received from all Mobile Subscriber Units.
pdgPDRRNGProxyStatsALReTransIBSegCount	CAI PDUs retransmitted by MSUs	Number of CAI PDUs retransmitted by all Mobile Subscriber Units.

MIB Object Name	Report Object Name	Object Description
pdgPDRRNGProxyStatsALAckOBCount	CAI ACKs transmitted to MSUs	Number of CAI Response Messages (ACKs/NACKs/Selective ACKs) transmitted to all Mobile Subscriber Units.
pdgPDRRNGProxyStatsTLSDUIBCount	PDGP SDUs received from MSUs	Number of confirmed PDGP SDUs received from all Mobile Subscriber Units.
pdgPDRRNGProxyStatsUnCnflBCount	Unconfirmed Messages received from MSUs	Number of unconfirmed messages received from all Mobile Subscriber Units.

4.4.4.13
RNG Inbound and Outbound Data Profile Report

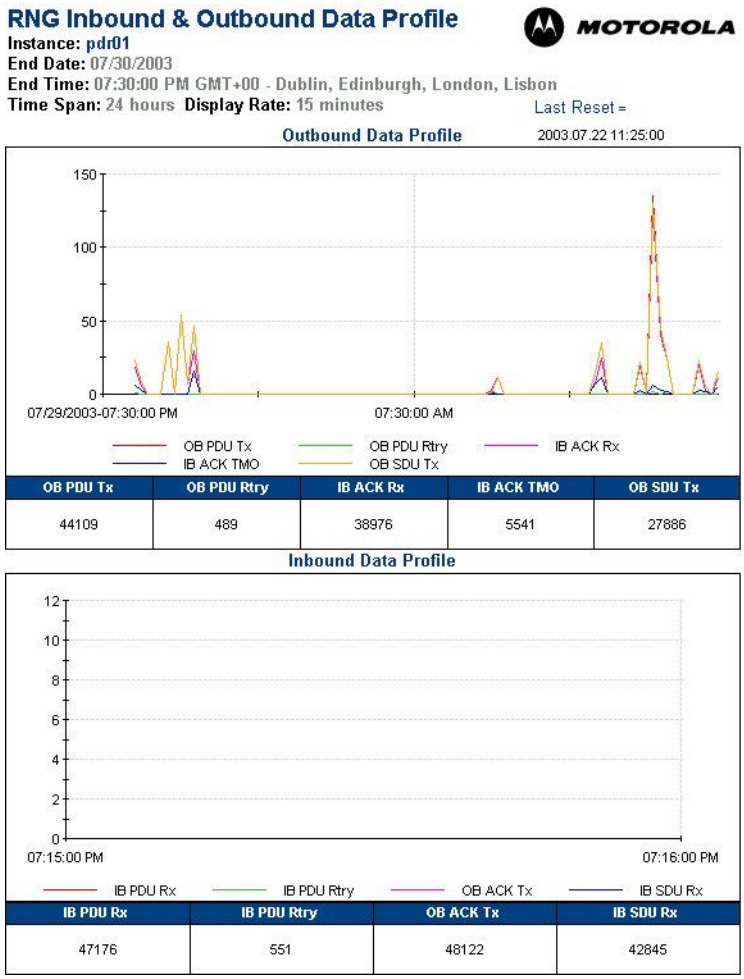
The following information explains how to use the report:

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. For graphs that show a count, the maximum varies. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the span of time.
- The **Last Reset** field shows the date and time of the last RNG reset.

NOTICE: The report object names in the graph are abbreviated.

- OB PDU Tx – CAI PDUs transmitted to MSUs
- OB PDU Rtry – CAI PDUs retransmitted to MSUs
- IB ACK Rx – CAI ACKs received from MSUs
- IB ACK TMO – CAI ACK Timeouts
- OB SDU Tx – PDGP SDUs transmitted to MSUs
- IB PDU Rx – CAI PDUs received from MSUs
- IB PDU Rtry – CAI PDUs retransmitted by MSUs
- OB ACK Tx – CAI ACKs transmitted to MSUs
- IB SDU Rx – PDGP SDUs received from MSUs

Figure 36: RNG Inbound and Outbound Data Profile Report



4.4.4.14

RNG HPD Packet Data Service – UP Connect Information

RNG HPD Packet Data Service – UP Connect Information an individual report that is created for the RNG. It presents Radio Network Gateway Up Connect Information.

NOTICE: This report does not generate traps to Unified Event Manager (UEM).

4.4.4.15

RNG HPD Packet Data Service – UP Connect Information Description

Table 37: RNG HPD Packet Data Service – UP Connect Information Description

Graph/Table	Description
Normal UP Connect Activity	Includes a graph and a table: • The graph shows the difference between the last poll and current one. • The table shows a running sum from the last time the RNG was reset. **UP Connects**: The number of successful UP Connects across all MSUs. **UP Connects Rx**: The number of UP Connects received from all MSUs.

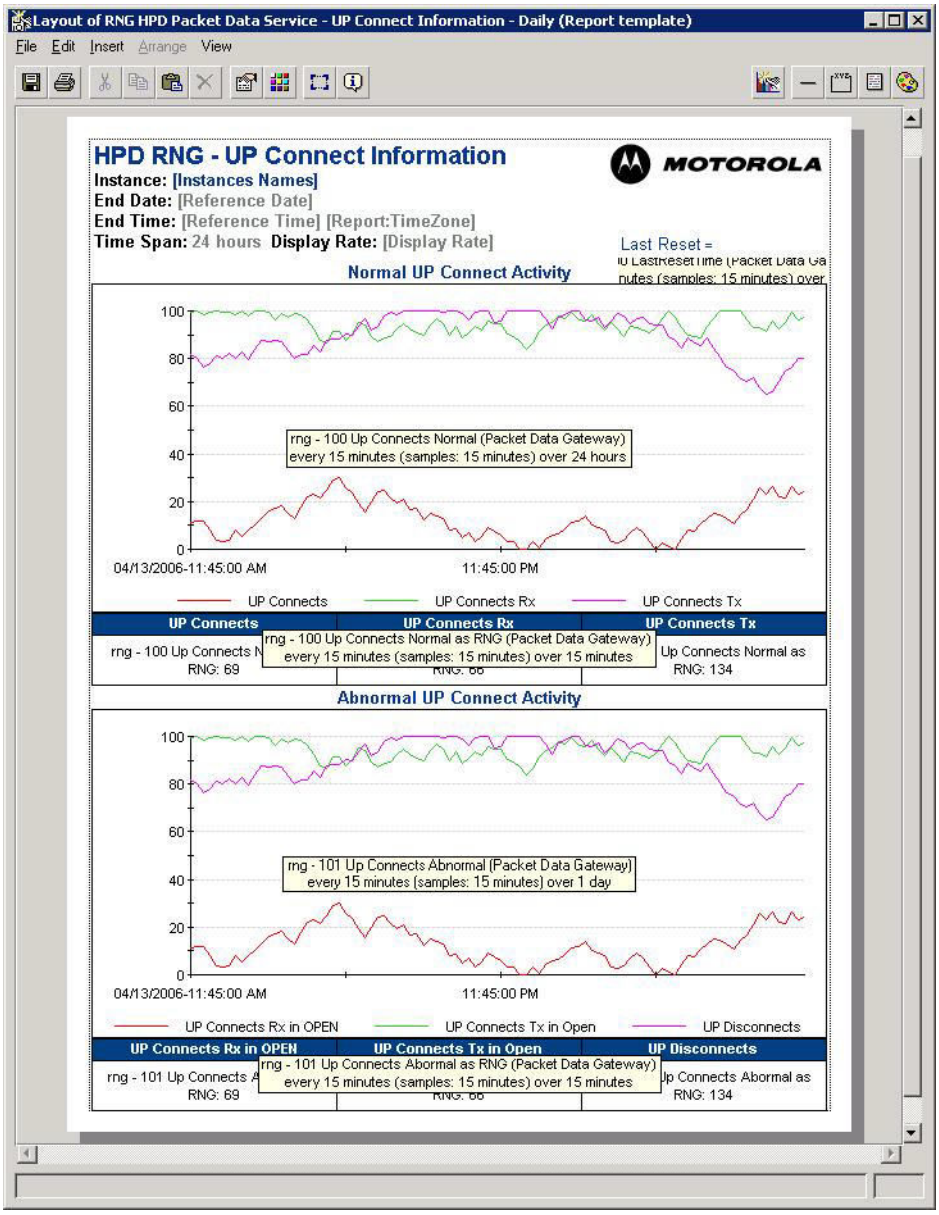
Graph/Table	Description
	UP Connects Tx: The number of UP Connects sent to all MSUs.
Abnormal UP Connect Activity	Includes a graph and a table: • The graph shows the difference between the last poll and current one. • The table shows a running sum from the last time the RNG was reset. **UP Connects Rx in OPEN**: The number of UP Connects received from all MSUs in OPEN state. **UP Connects Tx in OPEN**: The number of UP Connects sent to all MSUs in OPEN state. **UP Disconnects**: The number of UP Disconnects sent to all MSUs .

4.4.4.16
RNG HPD Packet Data Service – UP Connect Information Report

The following information explains how to use the report:

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. For graphs that show a count, the maximum varies. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the span of time.
- The **Last Reset** shows the date and time of the last RNG reset.

Figure 37: RNG HPD Packet Data Service – UP Connect Information Report



4.4.5
Interpreting Packet Data Router Reports

This section provides the following information:

- PDR Roaming and Registration Statistics.
- PDR ICMP Traffic.
- PDR IP Bearer Service Statistics.
- PDR Dropped Messages Statistics.

NOTICE:

- All PDR Reports shall display data in the following two ways:
  - Numbers since last statistics reset.
  - Rate for every 15 minutes interval.
- All PDR Reports shall display the last statistics reset time at the top of each report

4.4.5.1
PDR Roaming and Registration Statistics

PDR Roaming and Registration Statistics is an individual report that is created for each Packet Data Router (PDR). It shows the rate at which the PDR is receiving packet data registration and mobility events.

Use this report to troubleshoot message overload conditions and problems with the mobility interface between the PDR and the zone controller.

NOTICE: This report does not generate traps to Unified Event Manager (UEM).

4.4.5.2
PDR Roaming and Registration Statistics Report Description

Table 38: PDR Context Activation and Roaming Statistics

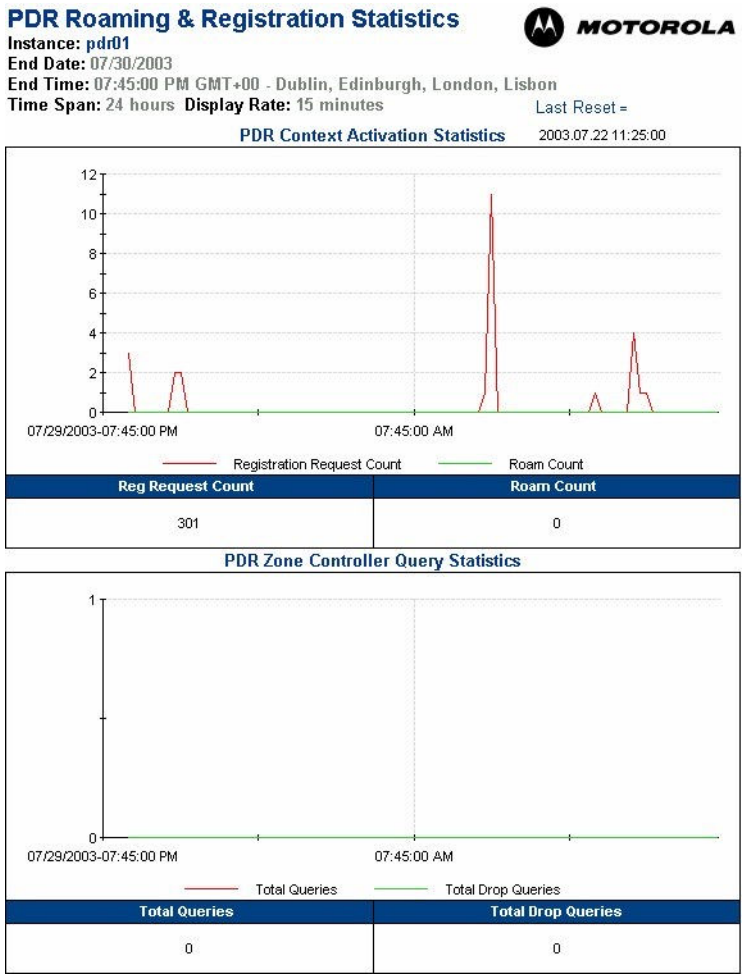
MIB Object Name	Report Object Name	Object Description
pdgPDRStats RegReqCount	SNDCP Registration Requests received by the PDR.	Number of SNDCP Registration Requests received by the PDR.
pdgPDRZCLinkStatsTotal-QueriesCnt	Queries sent to zone controller from the PDR	Number of Mobility Queries sent to zone controller from the PDR.
pdgPDRZCLinkStatsTotal-DropQueriesCnt	Queries sent to zone controller with no response	Queries sent to the Zone controller from PDR with no response.
pdgPDRStats RoamCount	Number of subscriber InterZone roams	Number of the subscriber InterZone roams handled by the PDR.

4.4.5.3
PDR Roaming and Registration Statistics Report

The following information explains how to use the report:

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. For graphs that show a count, the maximum varies. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the span of time.
- The **Last Reset** shows the date and time of the last PDR reset.

Figure 38: PDR Roaming Registration and Statistics Report



4.4.5.4

PDR ICMP Traffic

PDR ICMP Traffic is an individual report that is created for each PDR. It shows the rate at which Internet Control Message Protocol (ICMP) messages are received or generated by the PDR. The rate that ICMPs are generated correlates to the rate that the PDR is unable to deliver outbound messages due to buffer overflows or problems delivering downstream. A high rate of outbound ICMPs received may be an indication of network routing problems in the Customer Enterprise Network (CEN). Both ICMP messages generated and ICMP messages received contribute to the load on the PDR.

NOTICE: This report does not generate traps to Unified Event Manager (UEM).

4.4.5.5
PDR ICMP Traffic Report Description

The following table presents PDR ICMP data traffic.

Table 39: ICMP Traffic

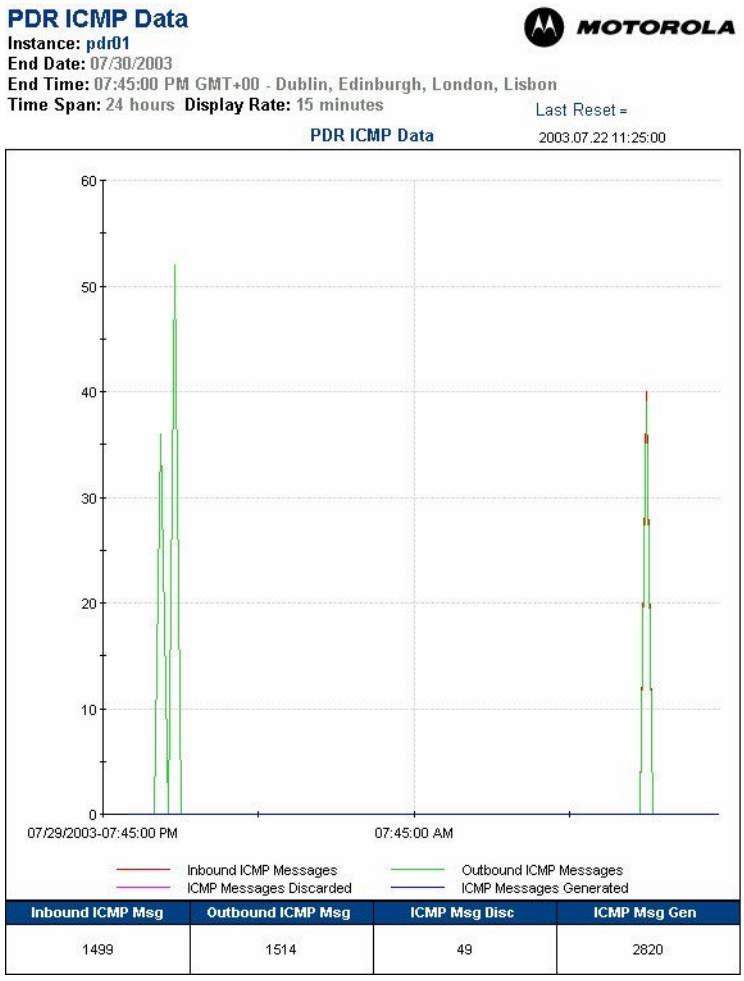
MIB Object Name	Report Object Name	Object Description
pdgPDRStat-sICMPMs-gRecvRFCount	Inbound ICMP messages	Number of ICMP messages from subscribers forwarded by the PDR.
pdgPDRStat-sICMPMsgRecv-LANCount	Outbound ICMP messages	Number of ICMP messages forwarded to subscribers by the PDR.
pdgPDRStat-sICMPMsgDisc-Count	ICMP messages discarded	Number of ICMP messages discarded.
pdgPDRStat-sICMPPckGen-Count	ICMP messages generated	Number of ICMP messages generated by the PDR.

4.4.5.6
PDR ICMP Traffic Report

The following information explains how to use the report:

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. For graphs that show a count, the maximum varies. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the span of time.
- The **Last Reset** shows the date and time of the last PDR reset.

Figure 39: PDR ICMP Traffic Report



4.4.5.7

PDR IP Bearer Service Statistics

PDR IP Bearer Service Statistics is an individual report that is created for each PDR. It shows the rate at which various user data message events occur at the PDR.

Use this report to troubleshoot overload conditions and problems with delivering outbound data through the PDR

NOTICE: This report does not generate traps to Unified Event Manager (UEM).

4.4.5.8
PDR IP Bearer Service Statistics Report Description

The following table presents PDR IP bearer service data traffic.

Table 40: IP Bearer Service Statistics

MIB Object Name	Report Object Name	Object Description
pdgPDRStat-sIPPckObCount	Outbound IP Packets	Subscriber destined IP Packets forwarded by the PDR.
pdgPDRStat-sIPPckIbCount	Inbound IP Packets	Subscriber sourced IP Packets forwarded by the PDR.
pdgPDRStat-sIPPckDiscCount	IP Packets discarded	Subscriber sourced and destined IP packets discarded due to ingress filtering, or bad IP header.
pdgPDRStatsRFC2507Err-Non-TCPHdrCmpCount	RFC2507 UDP/IP Header Decompression Errors	The number of subscriber-sourced non-TCP or UDP IP packets that were discarded due to RFC2507 header decompression failures.
pdgPDRStatsRFC2507IB-Non-TCPHdrCmpCount	RFC2507 Compressed UDP/IP Headers Received	The number of non-TCP or UDP IP packets with RFC2507 compressed headers received from a subscriber, and successfully decom-pressed.
pdgPDRStatsRFC2507OB-Non-TCPHdrCmpCount	RFC2507 Compressed UDP/IP Headers Sent	The number of non-TCP or UDP IP packets with RFC2507 compressed headers sent from PDR to a subscriber.
pdgPDRStatsBc-stIPPckCount	Broadcast IP Packets	The number of broadcast messages received by the PDR.
pdgPDRStatsBc-stIPPckDisc-Count	Broadcast Packets Dis-carded	The number of broadcast messages received by the PDR that were not deliverable (and were generated ICMP error messages).
pdgPDRStatsBcstDroppedCount	Broadcast Packets Drop-ped	The number of broadcast messages received by the PDR that were not deliverable, due to buffer overload (and were not generated ICMP error messages).

4.4.5.9
PDR IP Bearer Service Statistics Report

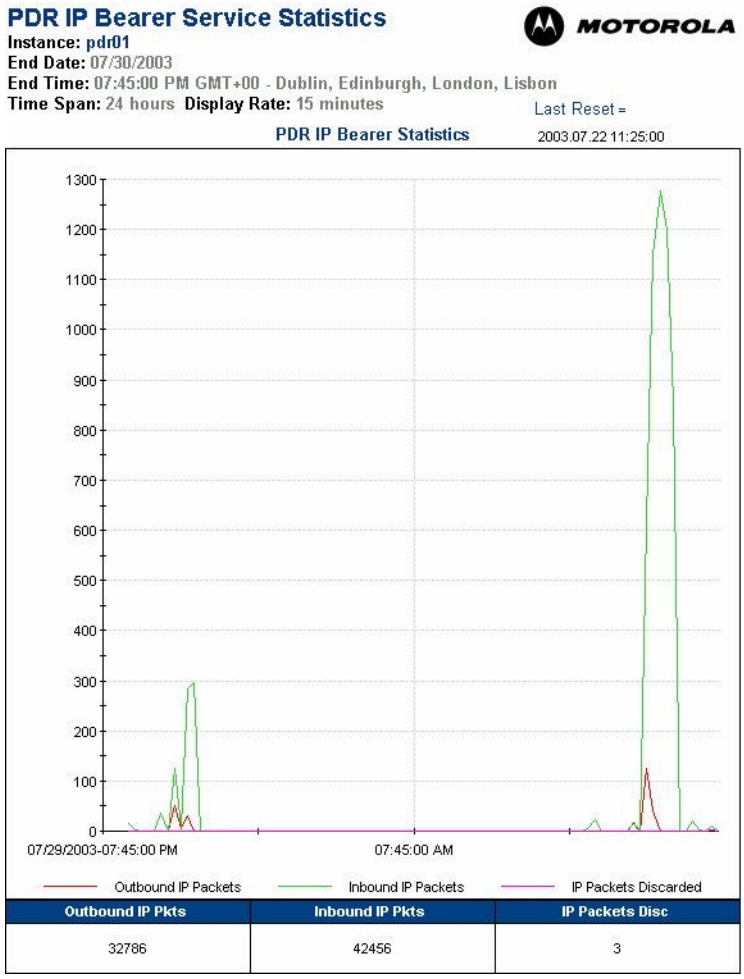
The following information explains how to use the report:

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. This report shows two types of graphs, one showing % value, and the other showing milliseconds (ms). The maximum value for graphs that show percentages (%) is 100%. For graphs that show a count, the maximum varies.

The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.

- The x-axis (horizontal axis) represents the span of time.
- The **Last Reset** shows the date and time of the last PDR reset.

Figure 40: PDR IP Bearer Service Statistics Report



4.4.5.10

PDR Dropped Messages Statistics

Dropped Messages Statistics is an individual report that is created for each PDR. This report presents PDR Message Overload Protection traffic.

NOTICE: This report does not generate traps to Unified Event Manager (UEM).

4.4.6

Interpreting System Wide Devices Reports

This section provides information on:

- Device Reachability
- InfoVista SNMP Traffic Analysis

4.4.6.1
Device Reachability

Device Reachability is an individual report that is created for every instance defined in InfoVista. It shows the % reachability of an Internet Control Message Protocol (ICMP) ping from the InfoVista server to the instance for that ping and response time in milliseconds.

Use this report for high-level problem determination to correlate a % reachability for a single IP node to blank spots in reports and for capacity planning by viewing a history of the response time.

4.4.6.2
Device Reachability Report Description

Table 41: Device Reachability Report Description

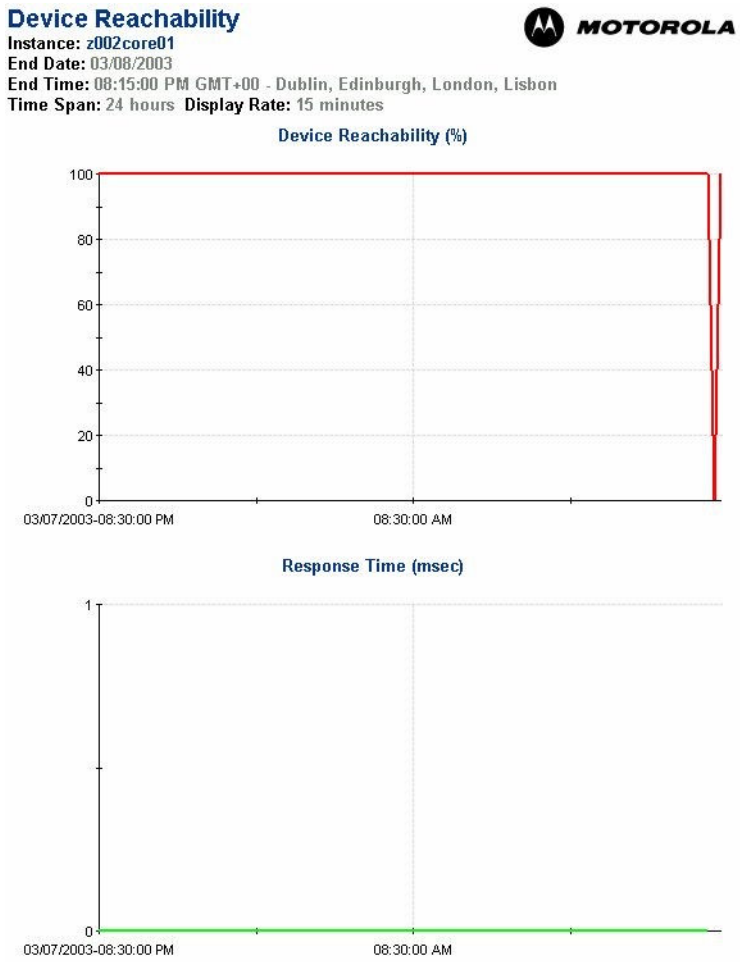
Graph/Table	Description
Device Reachability (%)	If the InfoVista server can ping the device at the time of the poll, the value on the graph shows 100%; otherwise it is 0. For Weekly, Monthly, and Yearly, it averages the polls to get the display rate value.
Response Time (msec)	The response time for the device to process one 32-byte packet. It times out after 1000 milliseconds (ms).

4.4.6.3
Device Reachability Report

The following information explains how to use the report.

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. This report shows two types of graphs, one showing % value, and the other showing milliseconds (ms). The maximum value for graphs that show percentages (%) is 100%. For graphs that show a count, the maximum varies. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the span of time.

Figure 41: Device Reachability Report



4.4.6.4

InfoVista SNMP Traffic Analysis

InfoVista SNMP Traffic Analysis is an individual report showing all SNMP traffic that flows to and from the InfoVista server in bytes and packets in a table and over time. It also shows the number of poll aborts and poll retries for each device that InfoVista manages. In short, this report shows why SNMP cannot reach a device. Use this report for a capacity planning of SNMP traffic on the network, to provide a traffic overview of the InfoVista server, and to correlate blank spots in reports with SNMP poll aborts and retries.

4.4.6.5

InfoVista SNMP Traffic Analysis Report Description

Table 42: InfoVista SNMP Traffic Analysis Report Description

Graph/Table	Description
Total IN/OUT (bytes/second)	Total IN: Total bytes received at the InfoVista server. Total OUT: Total number of bytes sent from the InfoVista server.

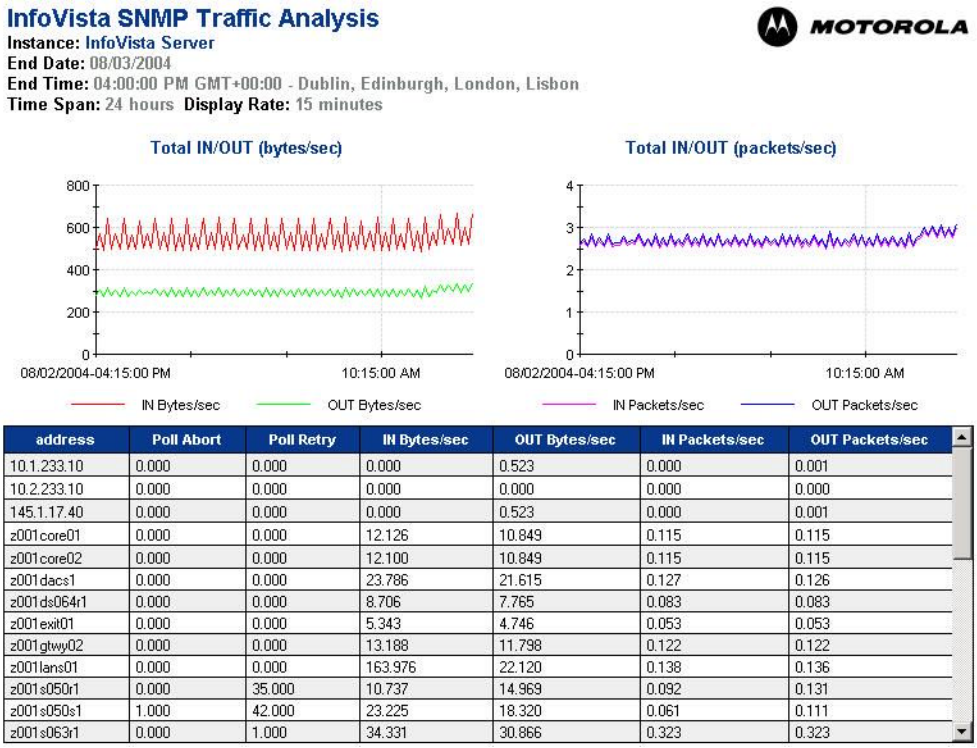
Graph/Table	Description
Total IN/OUT (packets/ second)	Total IN: Total number of packets received at the InfoVista server. Total Out: Total number of packets sent from the InfoVista server.
	Table of all instances showing SNMP information on each:
Poll Abort	Total number of aborts (that is, timeouts) representing the number of times the device timed out to SNMP requests from InfoVista.
Poll Retry	Total number of retries, representing the number of times InfoVista had to send the same SNMP request.
IN Bytes/ second	SNMP bytes/sec received by the InfoVista server from the device.
OUT Bytes/ second	SNMP bytes/sec sent from the InfoVista server to the device.
IN Packets/ second	SNMP packets/sec received by the InfoVista server from the device.
OUT Packets/ second	SNMP packets/sec sent from the InfoVista server to the device.

4.4.6.6
InfoVista SNMP Traffic Analysis Report

The following information explains how to use the report.

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The y-axis (vertical axis) represents the values of the statistic. For graphs that show a count, the maximum varies. For example, some graphs show the number of packets per second. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
- The x-axis (horizontal axis) represents the span of time.

Figure 42: InfoVista SNMP Traffic Analysis Report



InfoVista SNMP Traffic Analysis

Instance: InfoVista Server
End Date: 08/03/2004
End Time: 04:00:00 PM GMT+00:00 - Dublin, Edinburgh, London, Lisbon
Time Span: 24 hours Display Rate: 15 minutes

MOTOROLA

Total IN/OUT (bytes/sec)

800
600
400
200
0
08/02/2004-04:15:00 PM
10:15:00 AM
IN Bytes/sec
OUT Bytes/sec

Total IN/OUT (packets/sec)

4
3
2
1
0
08/02/2004-04:15:00 PM
10:15:00 AM
IN Packets/sec
OUT Packets/sec

address	Poll Abort	Poll Retry	IN Bytes/sec	OUT Bytes/sec	IN Packets/sec	OUT Packets/sec
10.1.233.10	0.000	0.000	0.000	0.523	0.000	0.001
10.2.233.10	0.000	0.000	0.000	0.000	0.000	0.000
145.1.17.40	0.000	0.000	0.000	0.523	0.000	0.001
z001core01	0.000	0.000	12.126	10.849	0.115	0.115
z001core02	0.000	0.000	12.100	10.849	0.115	0.115
z001dacs1	0.000	0.000	23.786	21.615	0.127	0.126
z001ds064r1	0.000	0.000	8.706	7.765	0.083	0.083
z001exit01	0.000	0.000	5.343	4.746	0.053	0.053
z001gtwy02	0.000	0.000	13.188	11.798	0.122	0.122
z001lans01	0.000	0.000	163.976	22.120	0.138	0.136
z001s050r1	0.000	35.000	10.737	14.969	0.092	0.131
z001s050s1	1.000	42.000	23.225	18.320	0.061	0.111
z001s063r1	0.000	1.000	34.331	30.866	0.323	0.323

4.4.7
Interpreting GCP 8000 Reports

GCP 8000 is an individual report that is created for each port on a single HP LAN switch.

It collects bandwidth utilization IN and OUT for each port and total errors, total discards, and specific errors and discards IN and OUT for each port.

Thresholds are defined for bandwidth utilization IN and OUT. Traps are sent when the maximum of the two IN and OUT values exceeds the thresholds. Thresholds are also defined for total errors and total discards.

View the daily report template when a trap has been generated to aid with more in-depth problem determination. View the weekly, monthly, and yearly reports to assist with capacity planning.

4.4.7.1
GCP 8000 Report Description

Table 43: GCP 8000 Report Description

Graph/Table	T m	T w	Description
Bandwidth Utilization IN (%)	100	95	The port utilization percentage is calculated using the total number of octets received on the interface to the interface's current bandwidth in units of 1,000,000 bits per second.
Bandwidth Utilization OUT (%)	100	95	The port utilization percentage calculated using the total number of octets transmitted out on the interface to the interface's current bandwidth in units of 1,000,000 bits per second.
Total Errors (%)	4	2	**Errors IN (%)**

Graph/Table	Tm	Tw	Description
			If the number of inbound packets is greater than zero (0) and greater than total packets in errors, Port Errors Utilization is the (Number of Inbound Packets in Error)/(Total Inbound Packets). If the Number of Errors is greater than zero (0) and the Number of Errors is greater than Total Inbound Packets then Utilization is 100%, else it is 0%. **Errors OUT (%)** If the number of outbound packets is greater than zero (0) and less than total packets in errors, Port Errors Utilization is the (Number of Outbound Packets in Error)/(Total Outbound Packets). If the Number of Errors is greater than zero (0) and the Number of Errors is greater than Total Outbound Packets, then Utilization is 100%, else it is 0%.
Total Discards (%)	4	2	**Discards IN (%)** If the number of inbound packets is greater than zero (0) and greater than total packets discarded, Port Discards Utilization is the (Number of Inbound Packets Discarded)/(Total Inbound Packets). If the Number of Discards is greater than zero (0) and Number of Discards is greater than Total Inbound Packets then Utilization is 100%, else it is 0%. The number of inbound packets is chosen to be discarded even though no errors have been detected to prevent from it being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. **Discards OUT (%)** If the number of outbound packets is greater than zero and greater than total packets discarded, Port Discards Utilization is (Number of Outbound Packets Discarded)/(Total Outbound Packets). If Number of Discards is greater than zero (0) and Number of Discards is greater than Total Outbound Packets then Utilization is 100%, else it is 0%. The number of outbound packets is chosen to be discarded even though no errors had been detected to prevent it from being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Specific Errors and Discards IN	N/A	N/A	These errors do not represent all possible errors on the port. This means that if you see a % of errors or discards in the graph, you may not necessarily see any errors on this graph. **Alignment (frames)**: A count of frames received on a particular interface does not pass the Frame Check Sequence (FCS) check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the Media Access Control (MAC) service to the Logical Link Control (LLC) layer. **FCS (frames)**: A count of frames received on a particular interface does not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC layer.

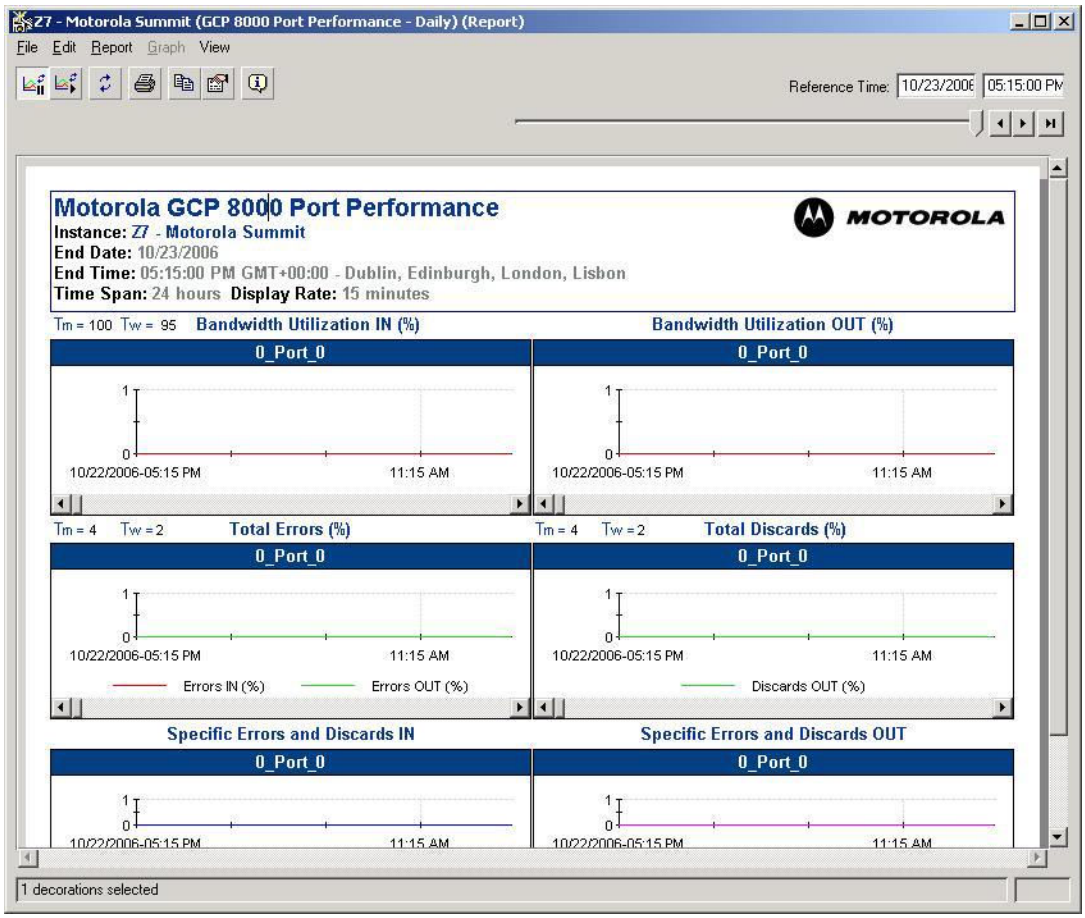
Graph/Table	Tm	Tw	Description
			Long Frame (frames): A count of frames received on a particular interface that exceeds the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC layer. **Mac Rx (frames)**: A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
Specific Errors and Discards OUT	N/A	N/A	These errors do not represent all possible errors on the port. This means that if you see a % of errors or discards in the graph, you may not necessarily see any errors on this graph. **Carrier Sense (errors)**: The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. **Excess Collsn (frames)**: A count of frames for which transmission on a particular interface fails due to excessive collisions. **Mac Tx (frames)**: A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.

4.4.7.2
GCP 8000 Report

The following information explains how to use the report:

- For definitions of the report template title elements (such as, instance or time span), see Report Template Title Information on page 50.
- The port number followed by the name of the device connected to that port appears at the top of every graph on the report.
- For **Graphs showing % values**:
  - The y-axis (vertical axis) represents the values of the statistic. The maximum value for graphs that show percentages (%) is 100%. The minimum value of the y-axis is set to 0. If the statistic value is 0, the graphs do not show data. If the statistic value is low, the graph appears truncated.
  - The x-axis (horizontal axis) represents the span of time.
- For **Graphs showing number of errors and discards**:
  - The y-axis (vertical axis) represents the values of the statistics either as a percentage or as a number. The minimum value of the y-axis is always zero, and the maximum value shown varies depending on the value of the statistic. For example, if the value of a statistic is 0.5%, the y-axis may span from 0 to 1 or if the value is 32%, the y-axis may span from 0 to 40.
  - The x-axis (horizontal axis) represents the span of time.

Figure 43: GCP 8000 Report



4.5

Managing InfoVista

This section provides information on:

- Accessing Motorola Custom-Designed Utilities on the TNPS
- Adding New Zones
- Adding and Removing SNMPv3 Users
- Changing Security Settings on an InfoVista Instance
- Discovering Devices and Verifying the Auto-Discovery
- Backing Up the InfoVista Database
- Manually Backing Up the InfoVista Databases
- Restore InfoVista Databases

4.5.1
Adding and Removing SNMPv3 Users

When and where to use: Use this procedure to add and remove SNMPv3 users.

Procedure:

1. Double-click the **IV-Report** icon on the desktop.

   InfoVista login dialog box appears.

2. Enter the username and password. Click **OK**.

   InfoVista IV-Report Window opens.

3. Click the **General** tab.

   The contents of the General tab are displayed.

4. Select a library, then select **Vistas** → ***<vistas>*** → **instance** → ***<instance>***.

   The right pane shows the properties of the instance.

5. Double-click **snmpv3** → **SecurityName =** ***<current SecurityName>***.

   The property value window opens.

6. Enter the Username in the **Value** section. Click **OK**.

   The window disappears.

4.5.2
Changing Security Settings on an InfoVista Instance

When and where to use: Use this procedure to change security settings on an InfoVista instance.

Procedure:

1. Double-click the **IV-Report** icon on the desktop.

   NOTICE: If for some reason you delete an instance or add a new device to the system, there should be no security settings on the device until after an InfoVista instance is created. Initial contact needs to be done in clear mode (no security settings). You can change the security settings on a device after the instance is created.

   InfoVista login dialog box appears.

2. Enter the username and password. Click **OK**.

   The **InfoVista IV-Report** window opens.

3. Select the **General** tab.

4. Expand the library of the device you wish to modify security configuration settings. Example: Select a library, and then select **Motorola – Motorola Network Resource** → **Vistas** → **Motorola Network Resource** → **Instances**.

   The list of all instances appears.

5. Click the selected instance.

   Right pane shows the properties of the instance.

6 Double-click the appropriate SNMPv3 parameter, such as **SNMPv3 – Authentication Password**.

The property value windows opens.

7 Type new data in the **Value** field. Click **OK**.

The window disappears.

8 Repeat step 4 through step 7 for all required devices and fields.

4.5.3
Discovering Devices and Verifying the Auto-Discovery

When and where to use: Use this process to discover devices and then verify the auto-discovery.

NOTICE: New devices on the system default to clear mode. The clear mode allows the discovery scripts to perform discovery tasks correctly. Remove any security setting on the SNMPv3 interface for the discovery script to create an instance of that device. For more details, see Changing Security Settings on an InfoVista Instance on page 115.

Process:

1 Routers and switches default to clear mode. The InfoVista discovery script needs that setting to operate correctly.

2 The initial invocation of the script attempts to contact IP addresses associated with certain routers/switches.

3 The discovery script adds records (instances) to the database for all the devices visible on the system.

4.5.3.1
Discovering Devices

If your system implements the Dynamic System Resilience feature, perform the discovery procedure on the primary and backup InfoVista servers to check their connectivity. However, do not set the discovery script as a scheduled task on the backup server. It results in both the primary and backup InfoVista servers polling devices and placing unnecessary network traffic on the system. For more information about executing the discovery script on the primary and backup InfoVista servers, see Running the Discovery Script Manually on page 37.
To set up the Auto-Discovery task on the primary Infovista server, see Scheduling the Auto-Discovery Task on page 119.

4.5.3.2
Verifying the Auto-Discovery

When and where to use: Use this procedure to verify the Auto-Discovery on the primary server.

NOTICE: Every week on Sunday at 1:00 AM Greenwich Mean Time (GMT), a Windows-scheduled task runs the Auto-Discovery script automatically. GMT is a 24-hour clock that uses one universal time zone.

If your system does not implement the Dynamic System Resilience feature, use this procedure to verify that the Auto-Discovery task discovered the new devices and created the report instances.

If the system implements the Dynamic System Resilience feature, see Verifying the Auto-Discovery on a Backup InfoVista Server on page 117.

Procedure:

1 From the **Start** screen, go to **Apps list** and start **IVreport**.

The **InfoVista server connection login** window appears.

2 Enter the InfoVista administrator user name and password to log on to the TNPS.

InfoVista appears.

3 Select the **Reports** tab.

The list of reports appears.

4 Click the **+** next to the Reports folder and locate the folder that should contain the new reports.

The new reports appear in the folder.

NOTICE: If the reports do not appear as expected, contact the Motorola Solutions Solutions Support Center (SSC).

4.5.3.3
Verifying the Auto-Discovery on a Backup InfoVista Server

When and where to use: Use this procedure to verify the Auto-Discovery on a Backup InfoVista Server.

NOTICE: Every night at 1:00 AM Greenwich Mean Time (GMT), a Windows-scheduled task runs the Auto-Discovery script automatically. GMT is a 24-hour clock that uses one universal time zone.

Procedure:

1 On the InfoVista client, browse to the following location: `D:\IV-Customizations\Discovery`

2 Open the file: `ivdisc-`***`<Day of the Month>`***`.log`

NOTICE: An example of the log file name is `ivdisc-07.log`. The example shows 07 as an example day of the month. Your day of the month could be different.

3 Scroll through the file to check with which devices InfoVista established connection.

NOTICE: If a device is discovered, a message appears stating that the given IP address has been found. If a device is not discovered, a message states that the IP address has not been found.

4.5.4
Scheduling Database Backup and Auto-Discovery Tasks

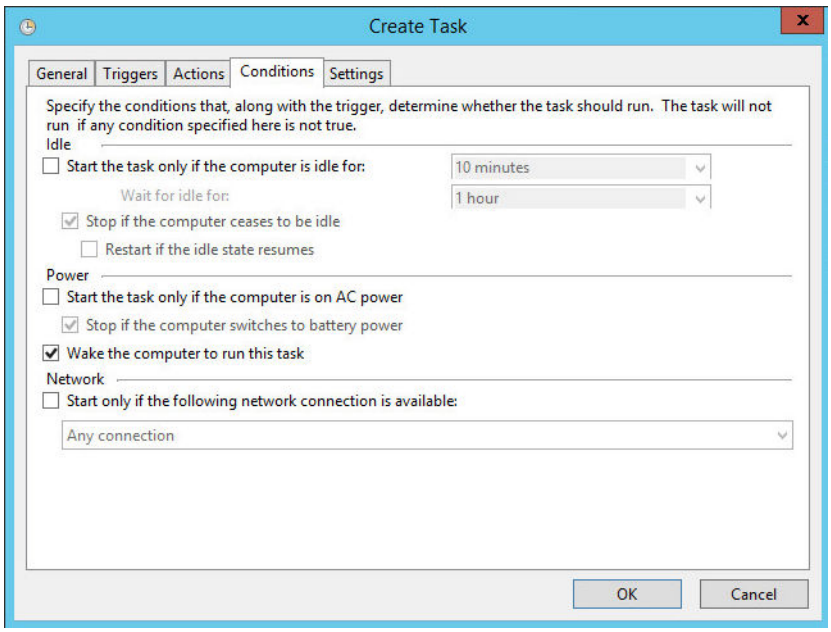
This section explains how to schedule two tasks: Database Backup (DB-Backup) and Auto-Discovery. Database Backup stores the flat files of the InfoVista databases to the hard drive. Auto-Discovery looks for new devices and adds them to InfoVista and creates the appropriate reports.

4.5.4.1
Scheduling the Backup Tasks

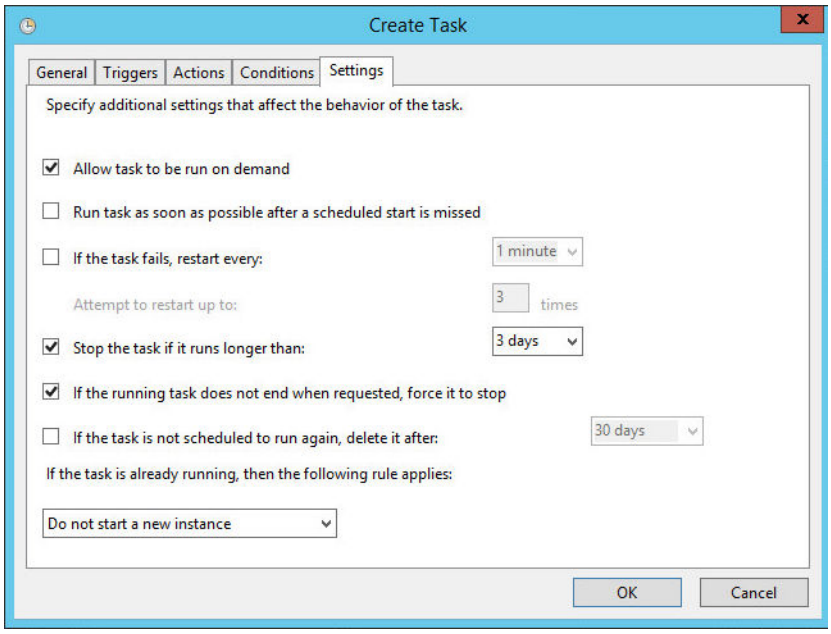
When and where to use: Use this procedure to schedule the backup tasks.

Procedure:

1. Start Task Scheduler
2. Select **New Task**
3. In the **General** tab, enter Name and Description
4. In The **Triggers** tab, create New Trigger
5. Set up the task to Begin On a Schedule, Daily, starting every Day at 1:00AM.
6. In the **Actions** tab, add a new action to Start a program: `D:\IV-Customizations\Backup\scripts\backup.pl Start in D:\IV-Customizations\Backup\scripts\ folder`
7. In **Conditions** tab, select options as per screenshot.



8. In **Settings** tab, select options as per screenshot.



9 In **General** tab, select to run this task as administrator. Change option to **Run whether user is logged on or not**. After pressing **OK**, you are prompted for an administrator password.

4.5.4.2
Verifying the Backup Task Schedule

When and where to use: Use this procedure to verify the backup task schedule.

Procedure:

1 Go to **Start** screen and launch **Task Scheduler**.

2 Go to **Active Tasks** list and open **DB Backup**.

3 From the **Actions** menu on the right, select **Run**.

4 Browse to the `D:\IV-Customizations\DB-Backup\Backup` directory.

The `db-backup`***<*>***`.gz` file appears, where ***<*>*** is a number from 1 to 7.

4.5.4.3
Scheduling the Auto-Discovery Task

When and where to use: Use this procedure to schedule the Auto-Discovery task.

NOTICE: When the Auto-Discovery is run, it outputs to a log file, `ivdisc-`***<Day of the Month>***`.log`. The log file is located in the `D:\IV-Customizations\Discovery` directory. A similar log file appears each time the Auto-Discovery is run.

Procedure:

1 Start Task Scheduler.

2 Select **New Task**.

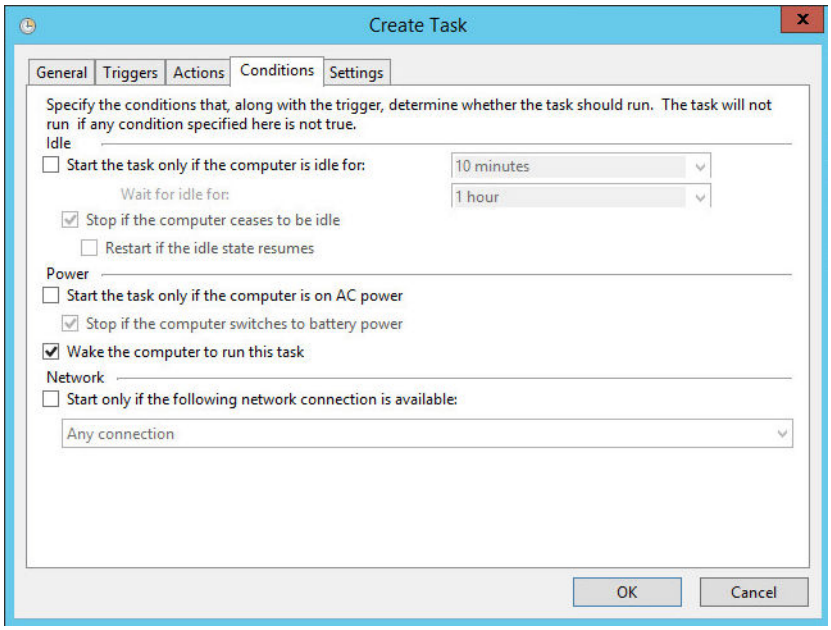
3 In the **General** tab, enter **Name** "Auto Discovery" and **Description** "Automatic task to discover network devices monitored by Infovista Server".

4 In The **Triggers** tab, create New Trigger, set up the task to Begin On a Schedule, Weekly, starting every Sunday at 1:00AM.

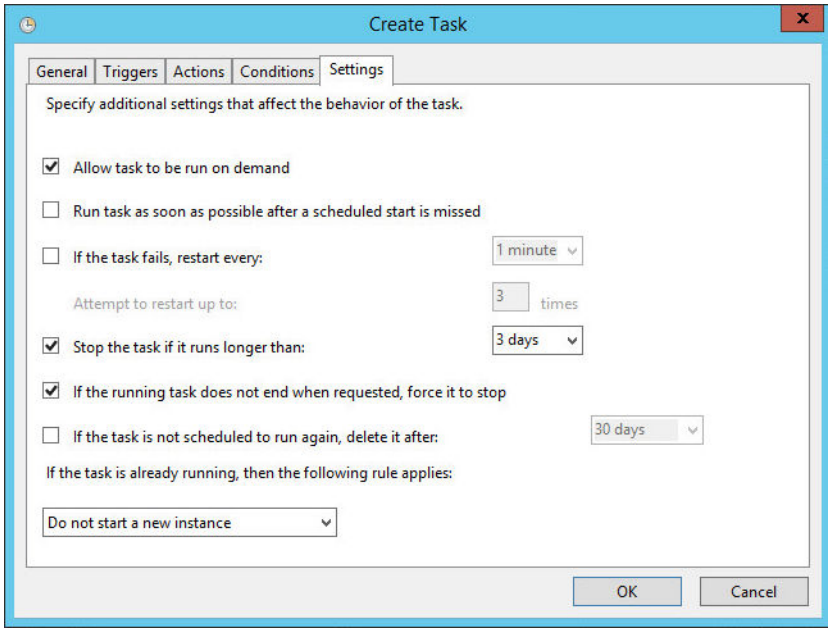
5 In the **Actions** tab, add a new action to start a program:

- Action `Start a program`
- Program/script `D:\IV-Customizations\Discovery\ivdisc.pl`
- Start in `D:\IV-Customizations\Discovery\ folder`

6 In the **Conditions** tab, modify settings as shown on the screenshot:



7 In the **Settings** tab, modify settings as shown on the screenshot:



8 In **General** tab, in **Security options** section, select **Run whether user is logged on or not**. After pressing **OK**, you are prompted for an administrator password.

4.5.5
InfoVista Database Backup

All backups are scheduled to be performed automatically. In addition, a manual backup mechanism is provided. For restores, see Restoring InfoVista Databases on page 122 in this manual or contact the Motorola Solutions Support Center (SSC).

There are the following types of backups:

- Automatic backup
  - The InfoVista databases are backed up to one flat file on the hard drive.
  - Flat file on hard drive can be then transferred by the user to an external storage media, depending on the internal backup policies.
- Manual backup
  - Manual backup of the InfoVista databases to one flat file on the hard drive.
  - Flat file on hard drive can be then transferred by the user to an external storage media, depending on the internal backup policies.
- For backing up the InfoVista database to the Backup and Restore (BAR), see the *Backup and Restore Services Feature Guide*.

The following table explains the naming convention of the backup file. The backup file is saved as `db-backup<*>.gz`, where **<*>** is a number from 1 to 7. The number in the filename corresponds to the date the file was saved.

Table 44: Filenames for the Backups

Filename #	Date
1	1, 8, 15, 22, 29
2	2, 9, 16, 23, 30
3	3, 10, 17, 14, 31
4	4, 11, 18, 25
5	5, 12, 19, 26
6	6, 13, 20, 27
7	7, 14, 21, 28

4.5.5.1
Automatic Backup Process During Installation and Configuration of TNPS

Motorola Solutions configures the Automatic backup schedules during installation and configuration of the TNPS.

NOTICE: Do not modify default schedules that are provided by Motorola Solutions.

The schedules are as follows:

- Flat file of InfoVista databases is backed up to the hard drive daily.
- Flat file on hard drive can be then transferred by the user to an external storage media, depending on the internal backup policies.

4.5.5.2
Setting up the Schedule

Schedules are created during installation and configuration of the software.

4.5.5.3
Manually Backing Up the InfoVista Databases

When and where to use: Use this procedure to back up the InfoVista databases to one file on the hard drive and move yesterday backup file to a new file name.

Procedure:

1. Check that the traffic monitor icon on the task bar is green before performing this procedure. Do not perform the procedure if the icon is red. Verify that the InfoVista services are started – for information see InfoVista Troubleshooting on page 125. If the services are not started, perform the troubleshooting procedure.
2. Open Command Prompt window (cmd) and browse to `d:\IV-Customizations\Backup \scripts\`
3. Type `backup.pl` and press **Enter**.

   The backup process is started.
4. Browse to `D:\IV-Customizations\DB-Backup\backup`, to verify the backup.

4.6
Restoring InfoVista Databases

When and where to use:
Use this procedure to restore the InfoVista databases.

NOTICE: See InfoVista Database Backup on page 121 for more information on what information the filenames of the database backups contain.

Procedure:

1. Ensure that a database backup file is available for you to run the database restore procedure.

   NOTICE: For more information, see InfoVista Database Backup on page 121.
2. Open the Start screen, type `ivconfiggui.exe` and press **Enter**.

   The **InfoVista Server Configuration** window opens.
3. Go to **Database** tab.
4. In Database Schemas section, click on **Restore...** button.
5. In the window that opens, browse to the `D:\IV-Customizations\DB-Backup\backup` directory and select the backup file you want to restore from. Click the **Restore** button.

   The restore process is now started. Wait for the process to complete and close **InfoVista Server Configuration** window.
6. Start IVreport and verify if the data is restored.

4.7

Running the InfoVista Auto-Discovery

When and where to use: Use this procedure to add instances and create reports automatically in InfoVista while simultaneously verifying the scheduled tasks that are completed in Scheduling the Auto-Discovery Task on page 119.

NOTICE: Every Sunday at 1:00 AM GMT, an Auto-Discovery task looks for new devices and adds them to InfoVista and creates the appropriate reports.

NOTICE: If your system implements the Dynamic System Resilience feature, perform the discovery procedure on the backup using the `ivdisc.pl -o backup` command. Perform the `ivdisc.pl -o` command on the primary and only set up a scheduled task on the primary. Run the discovery script on the backup InfoVista server (`ivdisc.pl -o backup`) initially and every time you add a new device on the system to check the connectivity. However, do not set the backup discovery script as a scheduled task on the backup server. It results in both the primary and backup InfoVista servers polling devices and placing unnecessary network traffic on the system.

Procedure:

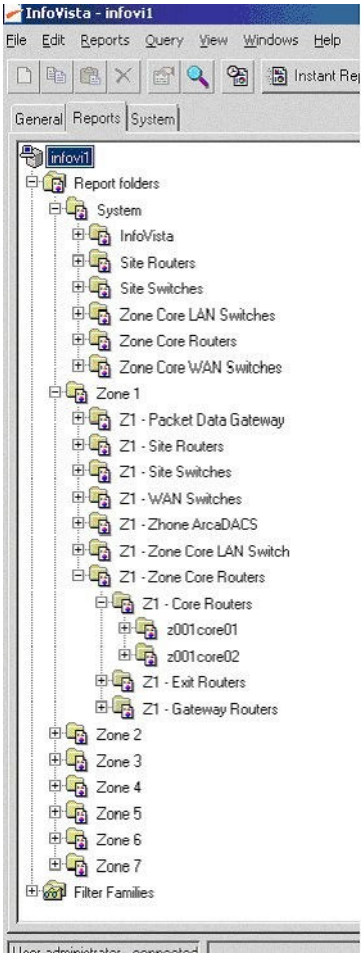
1. Open Command Prompt window (cmd) and browse to `d:\IV-Customizations\discovery\`.
2. Type `ivdisc.pl` and press **Enter**.

   NOTICE: When Auto-Discovery is run, it outputs to a log file, `ivdisc-<Day of the Month>.log`. The log file is located in `D:\IV-Customizations\Discovery`. A similar log file appears each time Auto-Discovery is run.
   Wait for the script to finish. The script takes approx. 2-3 hours per each zone in the system.
3. Browse to `D:\IV-Customizations\Discovery` and open `ivdisc-<Day of the Month>.log`. Scroll to the bottom of the file and look for the Success message.
4. Start **IVreport**, log into InfoVista and enter: `<InfoVista administrator password>`

   InfoVista appears.
5. Select the **Reports** tab.

   The list of reports appears.
6. Click the **+** next to the Reports folder.

Figure 44: Reports Tab



7 Verify if the given devices are added to the Report Folder.

For the data in the reports to show up, it takes another couple of hours, so make sure the sufficient amount of data is collected.

Chapter 5

InfoVista Troubleshooting

This chapter provides fault management and troubleshooting information relating to InfoVista.

5.1 Troubleshooting Overview

This section provides information on:

- Disaster Recovery
- Blank Spots on the Graphs
- Troubleshooting Server Status

5.1.1 Disaster Recovery

Contact the Motorola Solutions Support Center (SSC) for disaster recovery steps to restore the latest InfoVista databases from tape and then from the hard drive. A restore should only be performed under direction from the SSC, therefore no restore mechanism is provided in this booklet.

5.1.2 Blank Spots on the Graphs

To help diagnose why blank spots occur, look at the daily InfoVista SNMP Traffic Analysis and Device Reachability reports. Blank spots in a report indicate one of the following:

- The report is suspended, which means that InfoVista cannot collect statistics on the device.
- The TNPS is unable to reach the IP address defined in the IP Property for that instance. This may not mean that the device is down.InfoVista can only define one IP address used to contact a device. On many devices, the defined IP address is one of the redundant Ethernet interfaces. If the redundant interface goes down, it fails over to the backup interface and continues to work properly. However, InfoVista is not able to collect data from the IP address of the failed interface.

5.2 The InfoVista Server Fault Management

The InfoVista server is fault-managed using the SNMPv1 protocol by the zone-level fault management application, Unified Event Manager (UEM), situated in the same zone as the one in which the InfoVista Server is located. The InfoVista server periodically polls network transport devices in all zones on the ASTRO® 25 system (using the SNMPv3 protocol). When device statistics reported to InfoVista deviate from pre-established thresholds, InfoVista sends performance threshold traps (via SNMPv1) to the UEM server application located in the zone in which it resides. Threshold traps are not sent to UEM servers outside the zone in which the InfoVista server is located.

For more information on the use and interpretation of traps reported to the UEM application, see the *Unified Event Manager Online Help*.

5.3

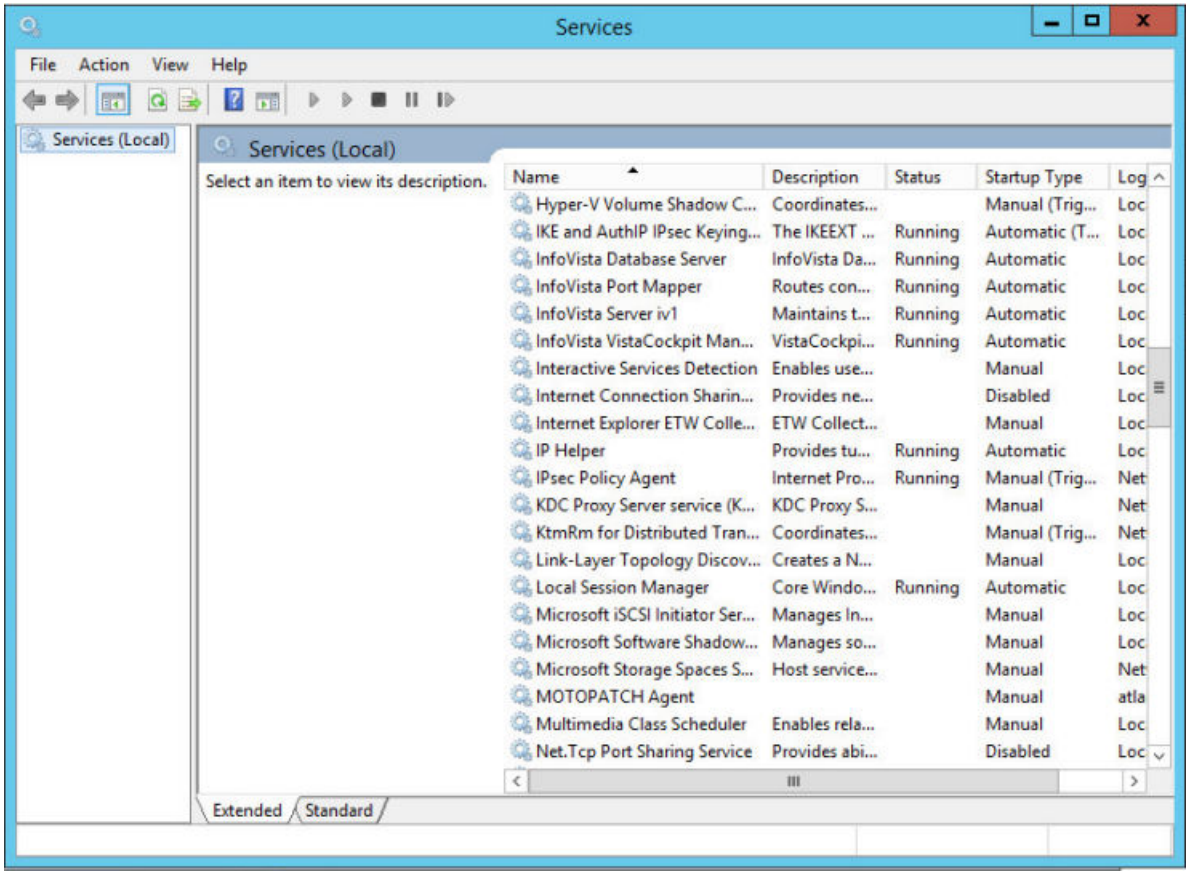
Troubleshooting InfoVista Services

When and where to use: Use this procedure to troubleshoot the installation if a service is not running.

Procedure:

1 From the **Start** menu, select **Administrative Tools** → **Services**.

Figure 45: Services Window



The Services window appears.

2 Ensure that the Status of the following services are **Started**: InfoVista Database Server, InfoVista Server iv1, InfoVista VistaCockpit Management Agent, and InfoVista Port Mapper.

NOTICE: Change the Time in the InfoVista Server. If the system time changes backwards, the service stops. The system cannot collect the statistics for times previous to what it had already collected. This only applies if the clock is rolled back. The system must wait for that time period to elapse before it can begin to obtain additional statistics. If the InfoVista services have not started, the system must wait for that time period to elapse before it can begin to obtain additional statistics.

Chapter 6

InfoVista Reference

This chapter contains supplemental reference information relating to InfoVista.

6.1 InfoVista Client User Accounts

The following table lists the InfoVista client user logons and describes the tasks that each user can perform.

Table 45: User Logons for InfoVista Client

User	User Rights and Tasks
ivviewer	Has the viewer profile in InfoVista. Can perform the following tasks: • View reports through InfoVistas • Find reports, print reports • Save reports from the Schedule dialog box or from the Report Viewer • Query the MIB variables from the MIB Browser
ivadmin	Has the writer profile in InfoVista. Can do all tasks listed for ivviewer, plus these additional tasks: • Add new instances and create reports for them • Start or suspend any report instance • View contents of the Motorola libraries **NOTICE:** The InfoVista Runtime license prevents you from modifying or adding to any library. You can only import a new library.

6.2 Installing InfoVista Client Application Software

When and where to use: Use this procedure to install InfoVista on the TNM client or NM client.

Procedure:

1. Insert *InfoVista Version 5.0* CD into the CD-ROM drive.
2. In the **InfoVista Welcome Screen**, click **Next**.
3. In the **License Agreement** screen, press PAGE DOWN until the end of screen, and click **Yes**.

   The Setup README file appears.
4. Press PAGE DOWN until the end of screen. Click **Next**.
5. In the **User Information** screen, enter your name and company. Click **Next**. For Name, use the Manager Windows 2012 client name. For Company, use Motorola. Leave the License Key field as the default.
6. In the **Evaluation screen**, click **Yes**.

7 In the **Select Components** screen, clear all check boxes. From the **Select Component** window, select the**Client Components** and**Online Documentation** components. Leave the Destination Folder unchanged. Click **Next**.

8 In the **Select Program Folder** selection screen, click **Next**.

9 In the **Start Copying Files** screen, click **Next**.

10 In the **Updating PATH** screen, click **Yes**.

The Perl Installation screen appears and the Setup Complete screen appears.

11 Select **No, I will restart my computer later**. Click **Finish**.

Software installation process continues until complete.

12 Remove the *InfoVista* CD.

Chapter 7

InfoVista Disaster Recovery

This chapter provides references and information that enables you to recover InfoVista in the event of a failure.

NOTICE: After the recovery operation is performed and completed, navigate to C:\ drive and permanently delete the **C:\restore** directory.

7.1 Recovery Sequence for InfoVista

When and where to use: Use this procedure to recover InfoVista.

Process:

1. Before you continue with step 2, make sure to delete the existing InfoVista virtual machine by right-clicking the virtual machine and selecting **Delete From Disk**.
2. Re-import the InfoVista Virtual Machine. See Importing InfoVista Virtual Machine on page 24.
3. Configure vCenter for newly deployed virtual machines. See Configuring the vCenter for the Newly Deployed VM on page 28.
4. Startup and shutdown the virtual machine. See Setting Startup and Shutdown Order on page 30.
5. Connect and Power On the Virtual Machine. See Connecting and Powering On Virtual Machine on page 28.
6. Configure the InfoVista virtual machine. See Configuring InfoVista Virtual Machine on page 32.
7. Configure the InfoVista License Key. See Configuring the InfoVista License Key on page 38.
8. Configure the Primary InfoVista Server. See Configuring the Primary InfoVista Server on page 33.
9. Configure the Backup InfoVista Server. See Configuring the Backup InfoVista Server on page 35.

   NOTICE: Perform this Procedure only if the system implements the Dynamic System Resilience feature.
10. Verify the MAC address. See Verifying the MAC Address on page 39.
11. Configure the Trap Receiver Address on InfoVista. See Configuring Trap Receiver Address on page 36.
12. Get the desired database (latest) backup file from your own external backup location or BAR server. See"Transferring Files to or from the BAR Server" in the *Backup and Restore Services Feature Guide*.
13. Restore the database backup file as described in Restoring InfoVista Databases on page 122.
14. Run the Discovery Script manually. See Running the Discovery Script Manually on page 37.
15. Discover InfoVista/TNPS Server in Unified Event Manager (UEM). The InfoVista/TNPS server must be discovered in the UEM server application co-located in the same zone as the InfoVista/TNPS server. Traps and events from InfoVista are viewable in UEM only after this procedure is complete. It is accomplished in UEM as part of the subnet or IP node (individual device) discovery. See the *Unified Event Manager Online Help* for details.

16 Set the Boot Order for the Workstation/Server.

For all Windows-based devices in the ASTRO® 25 system, do one of the following:

NOTICE: The boot order and configuration for a PC is found in the BIOS of the PC . See the PC manufacturer's documentation for instructions on how to set the boot order correctly.

- Remove the USB devices from the boot order. **OR**
- Ensure that USB devices do not appear before the hard drives in the PC boot order.

17 Join the active directory domain. See "Joining and Rejoining a Windows-Based Device to an Active Directory Domain with a Script" in the *Authentication Services Feature Guide*.

18 Installing the Antivirus Software. See "CSMS – Deploying McAfee Client Software to Anti-Malware Clients" in the *Core Security Management Server Feature Guide*.