System Release 2020.HS, 2020.1, 2019.x

ASTRO® 25

INTEGRATED VOICE AND DATA

InfoVista

User Guide

AUGUST 2022

© 2022 Motorola Solutions, Inc. All rights reserved

MN005959A01-G

Intellectual Property and Regulatory Notices

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.

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.

License Rights

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.

Open Source Content

This product may contain Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

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

The European Union's WEEE directive and the UK's WEEE regulation require that products sold into EU countries and the UK must have the crossed-out wheelie bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheelie bin label means that customers and end-users in EU and UK countries should not dispose of electronic and electrical equipment or accessories in household waste.

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

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 mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

© 2022 Motorola Solutions, Inc. All Rights Reserved

Contact Us

The Centralized Managed Support Operations (CMSO) 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 Centralized Managed Support Operations (CMSO) 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
MN005959A01-A	Original release of the *InfoVista User Guide*. Applies to system releases A2019.1 and A2019.2.	September 2019
MN005959A01-B	Updated sections: • Configuring Trap Receiver Address on page 31 • Connecting and Powering On Virtual Machine on page 26	October 2019
MN005959A01-C01	Updated sections: • Restoring InfoVista Databases on page 43 Revised for system release A2020.1.	June 2020
MN005959A01-D	Revised for system release A2020.HS.	August 2020
MN005959A01-E	Updated sections: • Importing InfoVista Virtual Machine on page 20 • Configuring InfoVista on page 27 • Configuring the InfoVista License Key on page 31 • Configuring Trap Receiver Address on page 31 • Adding and Removing SNMPv3 Users on page 35 • Changing Security Settings on an InfoVista Instance on page 36 • Recovering InfoVista on page 100 • Database Disaster Recovery on page 101	October 2020
MN005959A01-F	Updated sections: • Setting up InfoVista Virtual Machine on page 20 • Recovering InfoVista on page 100	February 2021
MN005959A01-G	Updated sections: • Importing InfoVista Virtual Machine on page 20 • Zone Core Virtual Machine Boot Order on page 25	August 2022

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.

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.
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.
InfoVista Documentation	*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** or open the **Help** section of the InfoVista client.

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), Juniper SRX Routers, 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.

NOTE: 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
Ethernet LAN Switch	• HP/Aruba LAN Switch Port Performance • HP/Aruba LAN Switch Group Top 10 Port Performance • HP/Aruba LAN Switch Port Name/MIB Index No.
Juniper SRX Router	Individual reports (daily, weekly, monthly or yearly): • Juniper GW Performance • Juniper GW Port Performance • Juniper GW TWAMP Packet Loss • Juniper GW TWAMP Round Trip Delay • Juniper GW TWAMP RttJitter Group reports (daily, weekly, monthly or yearly): • Juniper GW Group Top 10 Performance • Juniper GW Group Top 10 Port Performance • Juniper GW Group Top 10 TWAMP Round Trip Delay • Juniper GW Group Top 10 TWAMP RttJitter and Packets Loss
Motorola Network Resource	• MNR Performance • MNR CWR LMI Performance • MNR Interface Performance

Device	Reports
	• 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 • 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.

NOTE: Motorola Solutions provides the confidential passwords to approved users. Contact your Centralized Managed Support Operations (CMSO) 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 **NOTE:** 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

User Input Required	Notes
<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
NOTE: DNS Server IP Addresses are required only if your organization uses Centralized Authentication.	
<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. **NOTE:** 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).

Related Links

Configuring InfoVista Virtual Machine on page 28
Connecting and Powering On Virtual Machine on page 26

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 Gettling Started* book
- InfoVista license key

NOTE: If you do not have the necessary license keys, contact the Centralized Managed Support Operations (CMSO).

Chapter 2

InfoVista Installation

This chapter details the installation procedures relating to InfoVista.

2.1 Software Installation

Motorola pre-installs all the required software before system installation. However, in the event of equipment failure or expansion, InfoVista can be installed manually according to several scenarios.

Full Software Installation

Full software installation is typically conducted before product shipment. It usually consists of a full installation of operating system software and application software.

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

Software Re-Installation

Software re-installation is performed after system installation, to load new equipment with software or to perform system configuration changes.

Table 3: Frequent 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 want to re-install all software under advice from the Centralized Managed Support Operations (CMSO). Where to begin: Software Pre-Installation Requirements and Considerations on page 19.
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 19.

2.2 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.

2.3 Setting up InfoVista Virtual Machine

Use this procedure to set up an InfoVista as a virtual machine on a virtual server.

NOTE: For ESXi 7.0, the certified web browser for VMware ESXi Embedded Host Client and VMware vSphere Client is Microsoft Edge 88.0.705.50 or later.
For ESXi 6.5, the certified web browser for VMware ESXi Embedded Host Client and VMware vSphere Web Client is Microsoft Internet Explorer 11 or later.

Process:

1. Import the InfoVista Virtual Machine. See Importing InfoVista Virtual Machine on page 20.
2. Configure vCenter for newly deployed virtual machines. See Configuring the vCenter for the Newly Deployed VM on page 22.
3. Startup and shutdown the virtual machine. See Setting the Virtual Machine Startup and Shutdown Order on page 23.
4. Connect and Power On the Virtual Machine. See Connecting and Powering On Virtual Machine on page 26.

2.3.1 Importing InfoVista Virtual Machine

Use this procedure to set up an InfoVista Virtual Machine (VM).

Prerequisites:
From your system administrator, obtain:

- *Motorola Virtual Appliance* media (Disc 1 and 2, which contain the Windows 2012 InfoVista virtual machine files)
- Virtual Server Host (ESXi-based server) IP address
- ESXi-based server administrator account name and password

Ensure that 7-Zip and VMWare PowerCLI module are installed on the Windows-based device that you use to deploy InfoVista OVF.

Procedure:

1. Insert the *Virtual Appliance – InfoVista DVD 1* into the Windows-based workstation.
2. From the *Virtual Appliance – InfoVista DVD 1*, copy all the files to the hard drive of your Windows device.
3. Eject the *Virtual Appliance – InfoVista DVD 1*.

4 Insert the *Virtual Appliance – InfoVista DVD 2*.

5 From the *Virtual Appliance – InfoVista DVD 2*, copy all the files to the hard drive location used in step 2.

6 Start the File Explorer and navigate to the directory where you pasted the virtual machine files.

7 Right-click the `IV-Astro-`***`<RR.RR.RR>.<XX-XX>`***`.zip.001` file,

where:

`<RR.RR.RR>` is the release number information

`<XX-XX>` is the OVF image version

8 From the menu select **7-Zip→Extract Here**.

The extraction process is complete.

9 Open the **PowerShell** console with administrative privileges by performing the following actions:

a Right-click **Start** and select **Search**.

b Type in: `powershell`

c Right-click **Windows PowerShell** and select **Run as administrator**.

d If the **User Account Control** window appears, click **Yes**.

e If you are not logged on with an administrative account, enter the admin credentials.

10 At the **PowerShell** prompt, enter:

```
Set-PowerCLIConfiguration -InvalidCertificateAction ignore
-confirm:$false
```

11 At the **PowerShell** prompt, check for server connections by entering:

```
Get-VMHost
```

12 If the console displays a list of connected servers, disconnect from them by entering:

```
Disconnect-VIServer -Server * -Confirm:$false -Force
```

13 Define the following variables:

- `$OvfPath = '`***`<OvfPath>`***`'`
- `$Password = '`***`<Password>`***`'`
- `$Server = '`***`<ServerIP>`***`'`
- `$VMName = '`***`<VMName>`***`'`

where:

`<OvfPath>` is the path to the `.ovf` file with the VM located on your computer

`<Password>` is the root account password for the server

`<ServerIP>` is the IP address of the ESXi host server

`<VMName>` is `infovi1` or `infovi2` for the InfoVista in the backup core/

14 Define the variable for the IP address of the VMware ESXi server's Network Management interface by entering:

```
$vmhost = Get-VMHost -Name $Server
```

15 Connect to the ESXi server by entering:

```
Connect-VIServer -Server $Server -User 'root' -Password $Password
```

16 Check available datastores by entering:

```
Get-Datastore
```

17 Define the variable for the datastore on which the VM is to be deployed by entering:

```
$Datastore = (Get-Datastore)[<ListItem>]
```

where ***<ListItem>*** is the number of the datastore starting from zero. If you have only one attached datastore, for ***<ListItem>*** provide `0` (`$Datastore = (Get-Datastore)[0]`).

18 Deploy the VM by entering:

```
Import-VApp -Name $VMName -VMHost $vmhost -Datastore $Datastore -
DiskStorageFormat Thick -Source $OvfPath
```

IMPORTANT: Importing the VM in `Thick` format may take longer than a regular import. Do not cancel the import even if the PowerCLI reports no progress. Canceling the import may leave the VM in an invalid state.

19 Log on to the VMware ESXi Embedded Host Client by performing the following actions:

a Launch the web browser.

b In the address bar, enter the IP address of the VMS host.

c If a certificate warning appears, continue to the page.

The form of the warning and steps to ignore it depend on the web browser.

d In the **User name** field, enter: `root`

e In the **Password** field, enter the password.

f Click **Log in**.

20 In the **Navigator** pane on the left, click **Virtual Machines**.

21 From the list of VMs, select the newly imported VM and click **Actions**.

22 From the **Actions** drop-down menu, select **Edit settings**.

23 On the **Virtual Hardware** tab, click **Network Adapter**.

24 From the drop-down list, select network mapping for your VM. Click **OK**.

25 Once the InfoVista Server VM is imported, verify that the **Navigator** pane displays the InfoVista server VM name.

26 If you cannot locate the VM name, expand the list in the left pane.

27 Remove the media from the drive.

Return to Process

Setting up InfoVista Virtual Machine on page 20
Recovering InfoVista on page 100

2.3.2 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.

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

Prerequisites: Ensure that an Open Virtualization Format (OVF) virtual machine was deployed after the vCenter was originally configured.

Procedure:

1. Open the VMware vSphere Web Client by launching a web browser and connecting to `https://`***`<vCenter IP>`***`/ui`

   NOTE: Ignore/Accept any warnings about the connection security or self-signed certificates.

2. Log on to the VMware vSphere Web Client as an administrator, using the name `administrator@z00`***`<Z>`***`vcs`***`<H>`***`.zone`***`<Z>`***

   where:

   <Z> is the zone number

   <H> is the vCenter instance number

3. In the navigation pane on the left, click **Hosts and Clusters**.
4. Expand the node and right-click the **Zone*<X>*** HA cluster.

   where:

   <X> is the zone number.

5. Select **Settings**.
6. On the **Configure** tab, in the **Configuration** node, select **VM Overrides**.
7. Click **Add**.
8. In the window that opens, select the check box for the virtual machine you are configuring. Click **Next**.
9. In the **VM Restart Priority** row, select the **Override** check box, and set startup priority for the VM. See Zone Core Virtual Machine Boot Order on page 25.
10. In the **Start next priority VMs when** row, select the **Override** check box, and from the drop-down list select **Powered On**.
11. Click **Finish**.
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. On the **Configure** tab, in the **Configuration** node, select **VM/Host Groups**.

    b. Select the group for the VMS host where the virtual machine resides and click **Add**.

    c. Select the check box next to the virtual machine and click **OK**.

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

    d. Click **OK**.

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

Return to Process

Setting up InfoVista Virtual Machine on page 20
Recovering InfoVista on page 100

2.3.3

Setting the Virtual Machine Startup and Shutdown Order

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

For detailed information about the boot order, see Zone Core Virtual Machine Boot Order on page 25.

NOTE: For virtual machines that are present in K core, the boot order is the same as in the zone core.

When and where to use:

Procedure:

1. Log on to the VMware ESXi Embedded Host Client by performing the following actions:
   1. Launch the web browser.
   2. In the address bar, enter the IP address of the VMS host.
   3. If a certificate warning appears, continue to the page.

      The form of the warning and steps to ignore it depend on the web browser.
   4. In the **User name** field, enter: `root`
   5. In the **Password** field, enter the password.
   6. Click **Log in**.
2. In the **Navigator** pane, under **Host**, click **Manage**.
3. In the **Manage** pane on the right, navigate to the **System** tab.
4. In the menu, click **Autostart**.
5. Above the list of settings, click **Edit settings**.
6. In the dialog box that opens, perform the following actions:
   1. Set **Enabled** to **Yes**.
   2. Set **Start delay** to `120` seconds.
   3. Set **Stop delay** to `120` seconds.
   4. From the **Stop action** drop-down list, select **Shut down**.
   5. Set **Wait for heartbeat** to **No**.
   6. Click **Save**.
7. In the list of VMs, select each VM and click **Enable**.
8. Set the startup order by using the **Start earlier** button.

Return to Process

Setting up InfoVista Virtual Machine on page 20
Recovering InfoVista on page 100

2.3.3.1 Zone Core Virtual Machine Boot Order

NOTE:
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	Automatic Startup
1	ZC	Enabled
2	Transcoder	Enabled
3	ISGW	Enabled
4	PDG-Conv	Enabled
5	PDG-HPD	Enabled
6	PDG-IV&D	Enabled
7	License Manager	Enabled
8	ATR	Enabled
9	DC-System	Enabled
10	Intermediate CA	Enabled
11	CWES	Enabled
12	DC-Zone	Enabled
13	IPCAP	Enabled
Any Order	AuC	Enabled
	BAR	Enabled
	PAM	Enabled
	CSMS	Enabled
	GDG	Enabled
	LMP	Enabled
	SSS	Enabled
	Syslog	Enabled
	UCS	Enabled
	UEM	Enabled
	UNC	Enabled
	UNC DS	Enabled
	vCenter App	Enabled
	ZDS	Enabled
	ZSS	Enabled
Manual Startup	DESU Waypoint	Disabled

Related Links

Configuring the vCenter for the Newly Deployed VM on page 22

Setting the Virtual Machine Startup and Shutdown Order on page 23

2.3.4 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 20 procedure.

NOTE: 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 20.

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.

   NOTE: 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 **Save**.

4. 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.

Return to Process

Setting up InfoVista Virtual Machine on page 20
Recovering InfoVista on page 100

Related Links

User Input and Variable Requirements on page 17

Chapter 3

InfoVista Configuration

This chapter details the configuration procedures relating to InfoVista.

3.1

Configuring InfoVista

Use this procedure to configure the InfoVista server.

Process:

1. Configure the InfoVista virtual machine. See Configuring InfoVista Virtual Machine on page 28.
2. Upgrade the VMware Tools. See “Upgrading VMware Tools on Windows-Based Virtual Machine" in the *Virtual Management Server Software User Guide*.

   NOTE: If the upgrade process reports a newer version of VMware Tools installed, you can skip this step.
3. Configure the Primary InfoVista Server. See Configuring the InfoVista Server on page 29.
4. Configure the Backup InfoVista Server. See Configuring the InfoVista Server on page 29.

   NOTE: Perform this Procedure only if the system implements the Dynamic System Resilience feature.
5. Configure the InfoVista License Key. See Configuring the InfoVista License Key on page 31.
6. In IVReports, **Reports** tab, ensure that all the expected network devices have been discovered. See Accessing the InfoVista Client on page 33.
7. Configure the Trap Receiver Address on InfoVista. See Configuring Trap Receiver Address on page 31.
8. Set the Boot Order for the Workstation/Server. For all Windows-based devices in the ASTRO® 25 system, do one of the following:
   - Remove the USB devices from the boot order.
   - Ensure that USB devices do not appear before the hard drives in the PC boot order.

   NOTE: 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.
9. 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*.
10. 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.
11. Install the threat-prevention software. See “CSMS – Deploying McAfee Client Software to Host-Based Threat Prevention Clients” in the *Core Security Management Server Feature Guide*.

3.1.1

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 26.
- The Windows Server 2012 Product Key must be obtained from the system administrator.
- The administrator password must be obtained from the system administrator.

NOTE: For details, see User Input and Variable Requirements on page 17.

Procedure:

1. Click the **Console** tab on the right side of the screen.

   The Console tab for the InfoVista displays the Settings Wizard.

2. 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.

3. Enter the `Windows Server 2012 Product Key`. Click **Next**.

   The **License Agreement** window appears.

4. Click **I accept**.

   A message appears stating that a password for the built-in administrator account must be typed.

5. Type the new `administrator password` twice and press FINISH.

   The login screen appears.

6. 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.

Return to Process

Configuring InfoVista on page 27
Recovering InfoVista on page 100

Related Links

User Input and Variable Requirements on page 17

3.1.2 Configuring the 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.

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

2. Log on to the VMware ESXi Embedded Host Client by performing the following actions:
   a. Launch the web browser.
   b. In the address bar, enter the IP address of the VMS host.
   c. If a certificate warning appears, continue to the page.

      The form of the warning and steps to ignore it depend on the web browser.
   d. In the **User name** field, enter: `root`
   e. In the **Password** field, enter the password.
   f. Click **Log in**.
3. In the **Navigator** pane on the left, click **Virtual Machines**.
4. In the list of virtual machines that appears on the right, right-click the virtual machine that you want to upgrade and select **Console→Launch Remote Console**.

   The Virtual Machine Remote Console opens.
5. From the main menu, select **VMRC→Removable Devices→CD/DVD drive 1→*<drive_letter>***
6. Insert the *InfoVista Plug-In* media to the CD/DVD drive.
7. Navigate to `E:\` and double-click `infoVista_scripts.msi`

   Installation scripts are copied to `C:\Program Files\Motorola\AstroIV\scripts`
8. Remove the *InfoVista Plug-In* from the CD/DVD drive.
9. From the console's main menu, select **VMRC→Removable Devices→CD/DVD drive 1→*<drive_letter>***
10. Insert the *Windows Supplemental* media to the CD/DVD drive.
11. From the **Start** menu, select **All Programs→Accessories →Windows PowerShell**.
12. Right-click **Windows PowerShell** and select **Run as Administrator**.

13 Change directory to `C:\Program Files\Motorola\AstroIV\scripts` and run the command `.\InstallIV.ps1`

14 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.

15 After the message `Enter the local administrator password:` appears, type the local administrator password twice and press ENTER.

16 After the message `Enter the Co-located Zone ID [1-7]:` appears, type the appropriate Co-located Zone ID and press ENTER.

17 In the prompt asking for the time zone, select the appropriate and click **OK**.

18 When prompted, select your WAN Link type.

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

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

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

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

23 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.

Return to Process

Configuring InfoVista on page 27
Recovering InfoVista on page 100

3.1.3 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).

   NOTE: 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.

   NOTE:
   Keys from previous versions of Infovista Server do not work with Infovista Server 5.0 or later. 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.

Return to Process

Configuring InfoVista on page 27
Recovering InfoVista on page 100

3.1.4 Configuring Trap Receiver Address

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

NOTE: 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 Double-click **IVreport** icon on the desktop. If not available, press **Windows** button and type `ivreport`, then click on the icon that appears.

  The **InfoVista** login window opens.

2 In the **Login** window, perform the following actions:

  a In the **User name** field, enter: `Administrator`

  b In the **Password** field, enter the appropriate password.

  c Leave the **Server name** field blank.

  d Click **OK**.

  The **InfoVista** window appears.

3 In the **InfoVista** 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** window.

  The window disappears.

Return to Process

Configuring InfoVista on page 27
Recovering InfoVista on page 100

Chapter 4

InfoVista Operation

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

4.1 InfoVista Access

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. See Accessing the InfoVista Client on page 33.

Accessing InfoVista from 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.

Accessing InfoVista with the TNPS

You can log on to the TNPS, which is a Windows 2012 server, to perform administrative tasks. From the server, you can access the customized InfoVista menu and perform tasks from that menu. The same user accounts are used to gain access to the application.

Accessing the InfoVista Client from a Client Workstation

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

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.

4.1.1 Accessing the InfoVista Client

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

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

Procedure:

1. Perform one of the following actions:
   - For NM and TNM clients, log on with a user account belonging to both “secadm” and “confgaud” groups in Active Directory.
   - For TNPS, log on as the administrator or viewer to the TNPS server.
2. From the **Start** screen, go to **Apps list** and start **IVreport**.
3. Right-click **IVreport** icon and select **Run as Administrator**.

4 In the **InfoVista server connection** window, log on as the administrator or viewer. Click **OK**.

The InfoVista window appears.

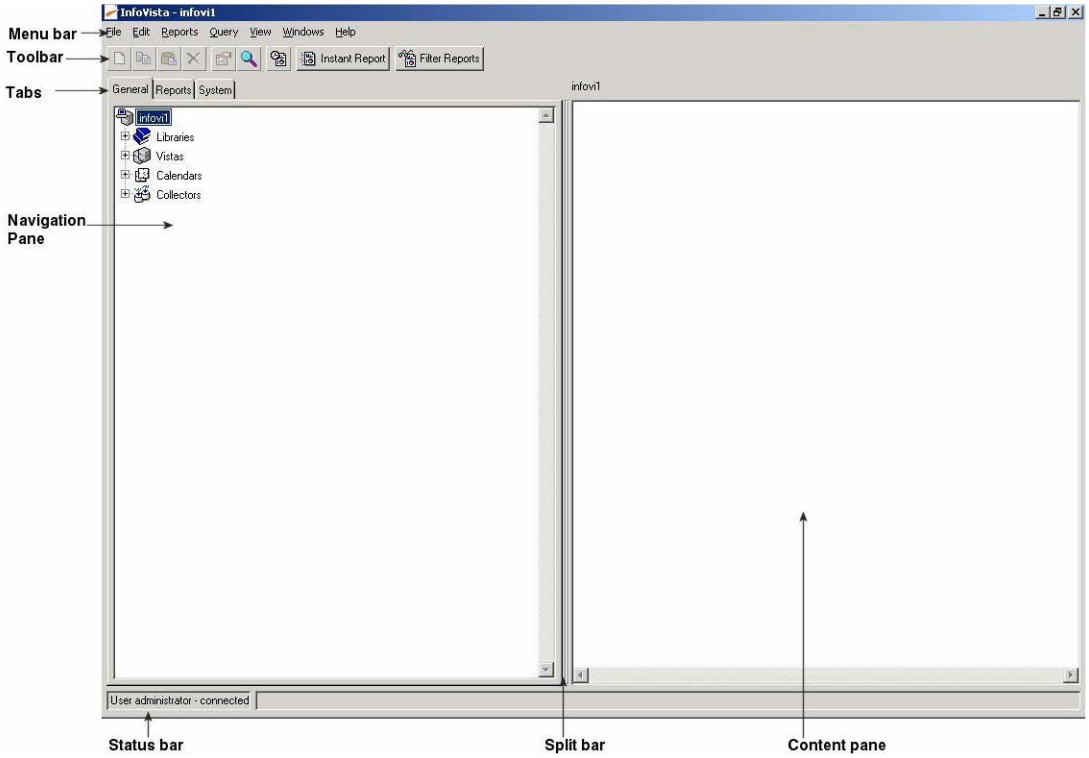
Return to Process

Configuring InfoVista on page 27

4.1.2 InfoVista Client Window Overview

The appearance of the InfoVista interface depends on the privilages of your account.

Figure 1: InfoVista Window (General Tab)



The InfoVista Client window contains the following elements:

- Menu bar and Toolbar.
- 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.

4.1.3 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.

NOTE: 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 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

4.2.1 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. Expand the library of the device for which you want to modify security configuration settings.

   Step example: Expand **Libraries**, and then select **Motorola→ Motorola Network Resources→ Vistas→Motorola Network Resource→Instances**
   The list of all instances appears.

5 Double-click the selected instance.

A new window shows the properties of the instance.

6 In the **General** tab, click the icon located on the right from **Property values**.

A new window with Property values appears.

7 In the **Property Values** window, in the **General** tab, scroll down to **snmpv3 - Security Name** property. In the **Value** section, enter the **Username**. To apply the change, click **OK**.

8 In the Instance window, click OK again to apply change.

The window dissapears and the change is applied.

4.2.2
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.

NOTE: 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 for which you want to modify security configuration settings.

Step example: Expand **Libraries**, and then select **Motorola→ Motorola Network Resources→ Vistas→Motorola Network Resource→Instances**
The list of all instances appears.

5 Double-click the selected instance.

A new window shows the properties of the instance.

6 In the **General** tab, click the icon located on the right from **Property values**.

A new window with Property values appears.

7 In the **Property Values** window, in the **General** tab, scroll down to the appropriate SNMPv3 parameter you want to modify, such as **snmpv3 - Authentication Password**.

8 Type new data in the **Value** field and click **OK**.

The window dissapears.

9 In the Instance window, click OK again to apply change.

The window dissapears and the change is applied.

4.2.3

Discovering Devices and Verifying the Auto-Discovery

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

NOTE: 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 36.

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.

4.2.3.1

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 45.
To set up the Auto-Discovery task on the primary Infovista server, see Scheduling the Auto-Discovery Task on page 40.

4.2.3.2

Verifying the Auto-Discovery

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

NOTE: 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 38.

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.

NOTE: If the reports do not appear as expected, contact the Centralized Managed Support Operations (CMSO).

4.2.3.3

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.

NOTE: 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`

NOTE: 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.

NOTE: 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.

4.2.4

Deleting Motorola Network Resources Manually

In a replacement scenario, when a Motorola Network Resource (MNR) was replaced by another device that uses the same IP address, the original device entry must be removed manually from the InfoVista database.

After the IP address of the original MNR device is no longer in the InfoVista Server database, the discovery script can configure the new device and assign the proper set of reports automatically.

Prerequisites: Obtain the IP address of the replaced device.

Procedure:

1 Log on to **IVreport** as `ivadmin`

2 On the **General** tab, expand **Vistas→Motorola Network Resources→Instances**.

3 On the device list, double-click the name of the device that was replaced.

4 In the **Properties** window, click on the icon next to the **Property values** field.

5 In the **Property values** window, confirm that the IP address of the selected device matches the IP address of the device that you replaced. Close the window.

6 In the **Instances** node, right-click the device you want to remove. From the context menu, select **Delete**.

7 When prompted for confirmation, click **Yes** or **Yes to All**.

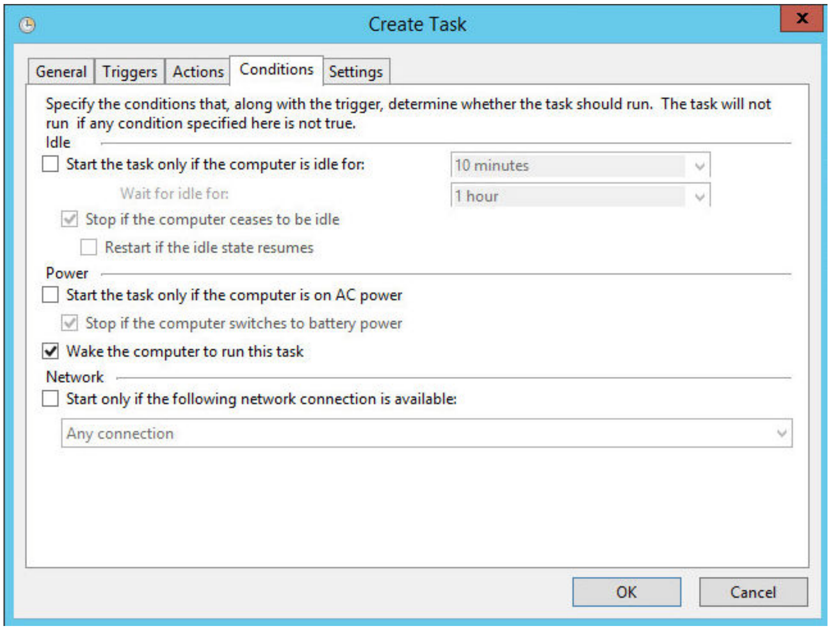
Postrequisites: Launch the discovery script manually. See Running the Discovery Script Manually on page 45.

4.2.5
Scheduling the Backup Tasks

When and where to use: Database Backup stores the flat files of the InfoVista databases to the hard drive.

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.



Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition specified here is not true.

Idle

□ Start the task only if the computer is idle for: 10 minutes

Wait for idle for: 1 hour

☑ Stop if the computer ceases to be idle

□ Restart if the idle state resumes

Power

□ Start the task only if the computer is on AC power

☑ Stop if the computer switches to battery power

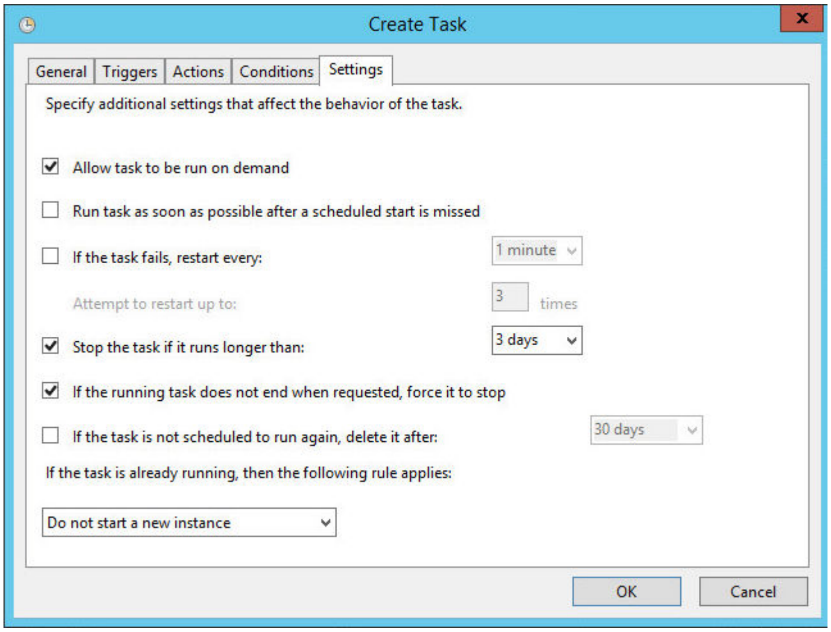
☑ Wake the computer to run this task

Network

□ Start only if the following network connection is available:

Any connection

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



Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

☐ Run task as soon as possible after a scheduled start is missed

☐ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

☑ Stop the task if it runs longer than: 3 days

☑ If the running task does not end when requested, force it to stop

☐ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

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.

4.2.6

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.

4.2.7

Scheduling the Auto-Discovery Task

Auto-Discovery looks for new devices and adds them to InfoVista and creates the appropriate reports.

NOTE: 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**.

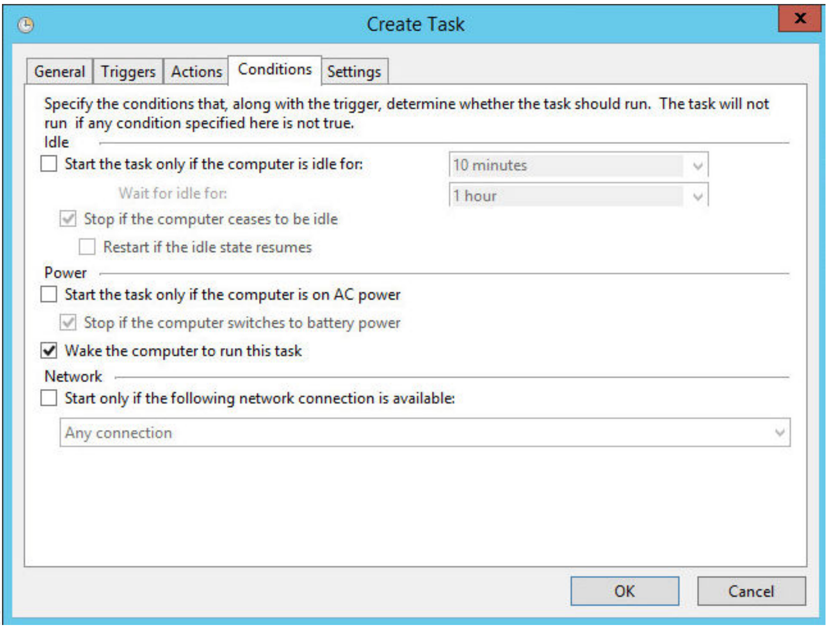
3 In the **General** tab, enter **Name** "Auto Discovery" and **Description** "Automatic task to discover network devices monitored by Infovista Server".

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:



Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition specified here is not true.

Idle

☐ Start the task only if the computer is idle for: 10 minutes

Wait for idle for: 1 hour

☑ Stop if the computer ceases to be idle

☐ Restart if the idle state resumes

Power

☐ Start the task only if the computer is on AC power

☑ Stop if the computer switches to battery power

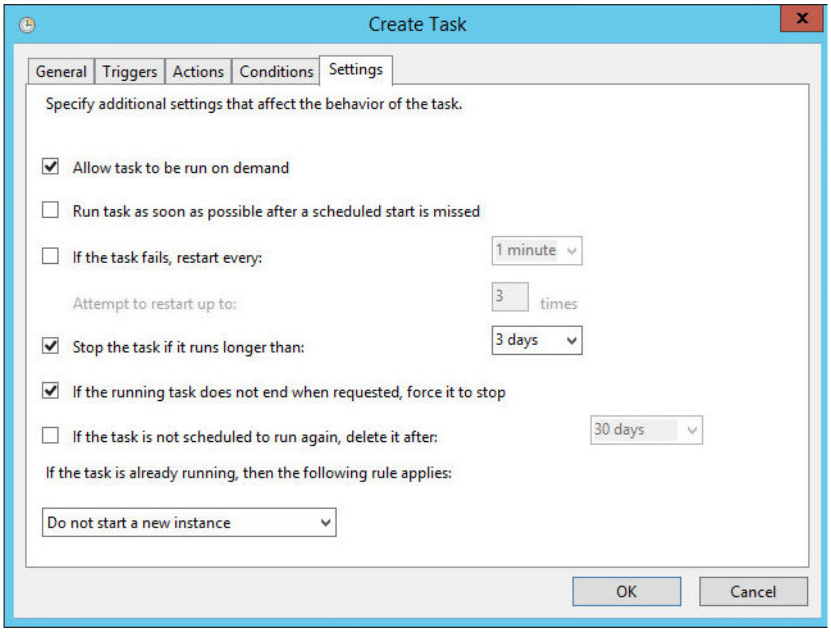
☑ Wake the computer to run this task

Network

☐ Start only if the following network connection is available:

Any connection

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



Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

☐ Run task as soon as possible after a scheduled start is missed

☐ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

☑ Stop the task if it runs longer than: 3 days

☑ If the running task does not end when requested, force it to stop

☐ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

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.

4.2.8

InfoVista Database Backup

All backups are scheduled to be performed automatically. The backup schedules are created during installation and configuration of the software. In addition, a manual backup mechanism is provided. For restores, see Restoring InfoVista Databases on page 43 in this manual or contact the Centralized Managed Support Operations (CMSO).

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 5: 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

4.2.8.1

Automatic Backup Process During Installation and Configuration of TNPS

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

NOTE: 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.

4.2.8.2 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 96. 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.

4.3 Restoring InfoVista Databases

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

NOTE: See InfoVista Database Backup on page 42 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.

   NOTE: For more information, see InfoVista Database Backup on page 42.
2. Peform one of the following actions:

If…	Then…
If the backup file has `.7z` extension	unpack the file by performing the following actions: **a** Launch command console by pressing **Windows** button and entering: `cmd` **b** Right-click the appearing **Command Prompt** icon and select **Run as Administrator**. **c** In the Command Prompt window, enter the following commands: • `d:` • `cd "d:\IV-Customizations\DB-Backup\Backup"` **d** Select the applicable backup file.

If…	Then…
	e Uncompress the selected file by entering: "c:\program files (x86)\7-Zip\7z.exe" e db-backup_***<x>***.7z where ***<x>*** is a number between 1 and 7. **f** Wait for the extracting process to complete and go to step step 3.
If the backup file has no extention,	perform the actions described in step step 3.

3. Open the Start screen, type `ivconfiggui.exe` and press **Enter**.

   The **InfoVista Server Configuration** window opens.

4. Go to **Database** tab.
5. In Database Schemas section, click on **Restore...** button.
6. 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.

7. Start IVreport and verify if the data is restored.

Return to Process

Recovering InfoVista on page 100

4.4 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 40.

NOTE: 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.

NOTE: 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**.

NOTE: 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.

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.

4.5
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`

NOTE: 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.

Return to Process

Recovering InfoVista on page 100

Chapter 5

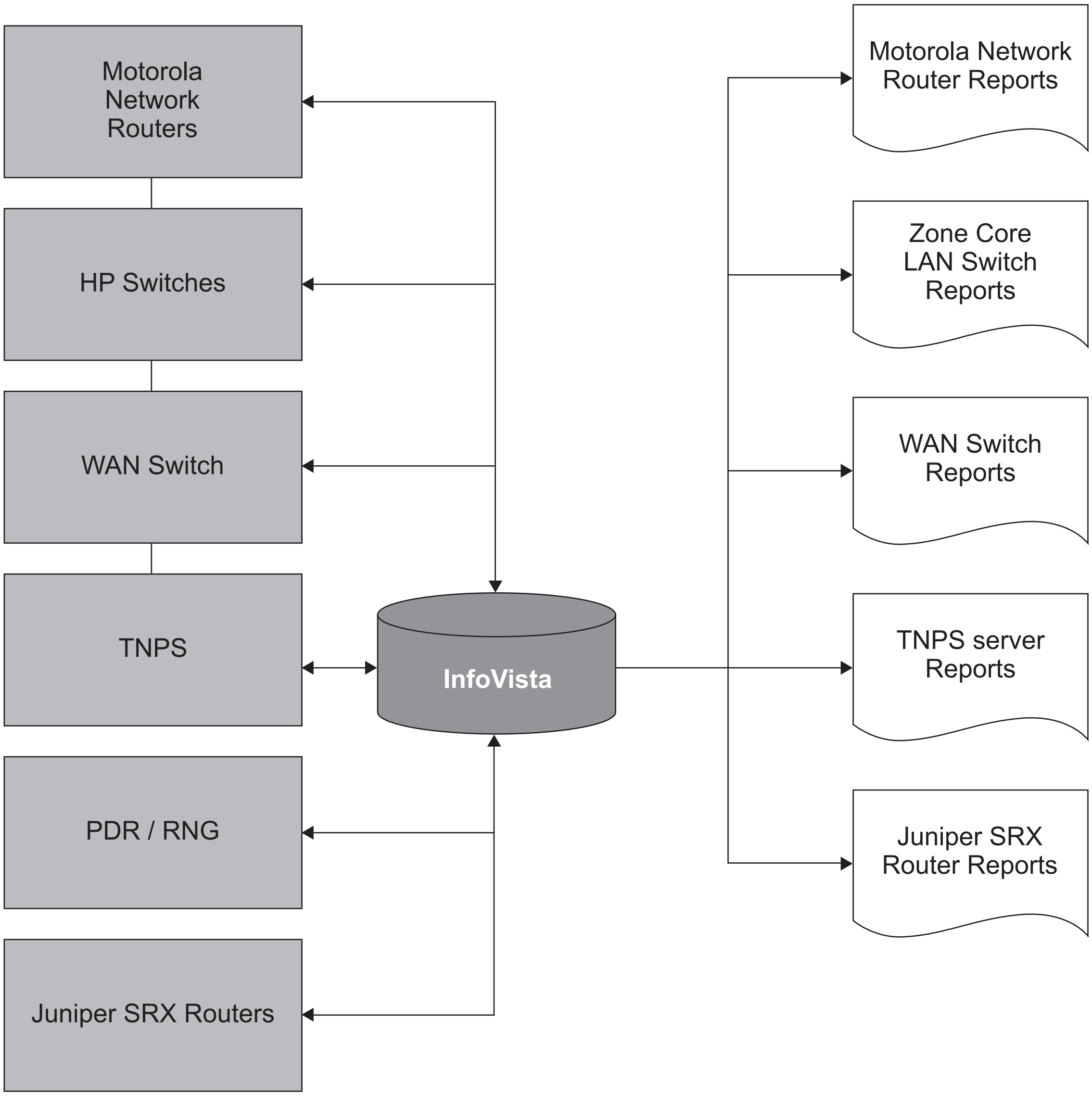
InfoVista Reports

This chapter provides report information relating to InfoVista.

5.1 Report Overview

InfoVista performance management software allows you to monitor the performance of critical devices in the IP network. InfoVista reports can be used for capacity planning and troubleshooting.

Figure 2: Types of Reports Compiled by InfoVista



5.1.1 Libraries, Vistas, and Instances

Motorola Solutions stores resource data in customized libraries (VistaViews).

Libraries

Each InfoVista library addresses the reporting for a specific vendor device type. A Vista is an object that is used to model a type of resource. You cannot modify these libraries.

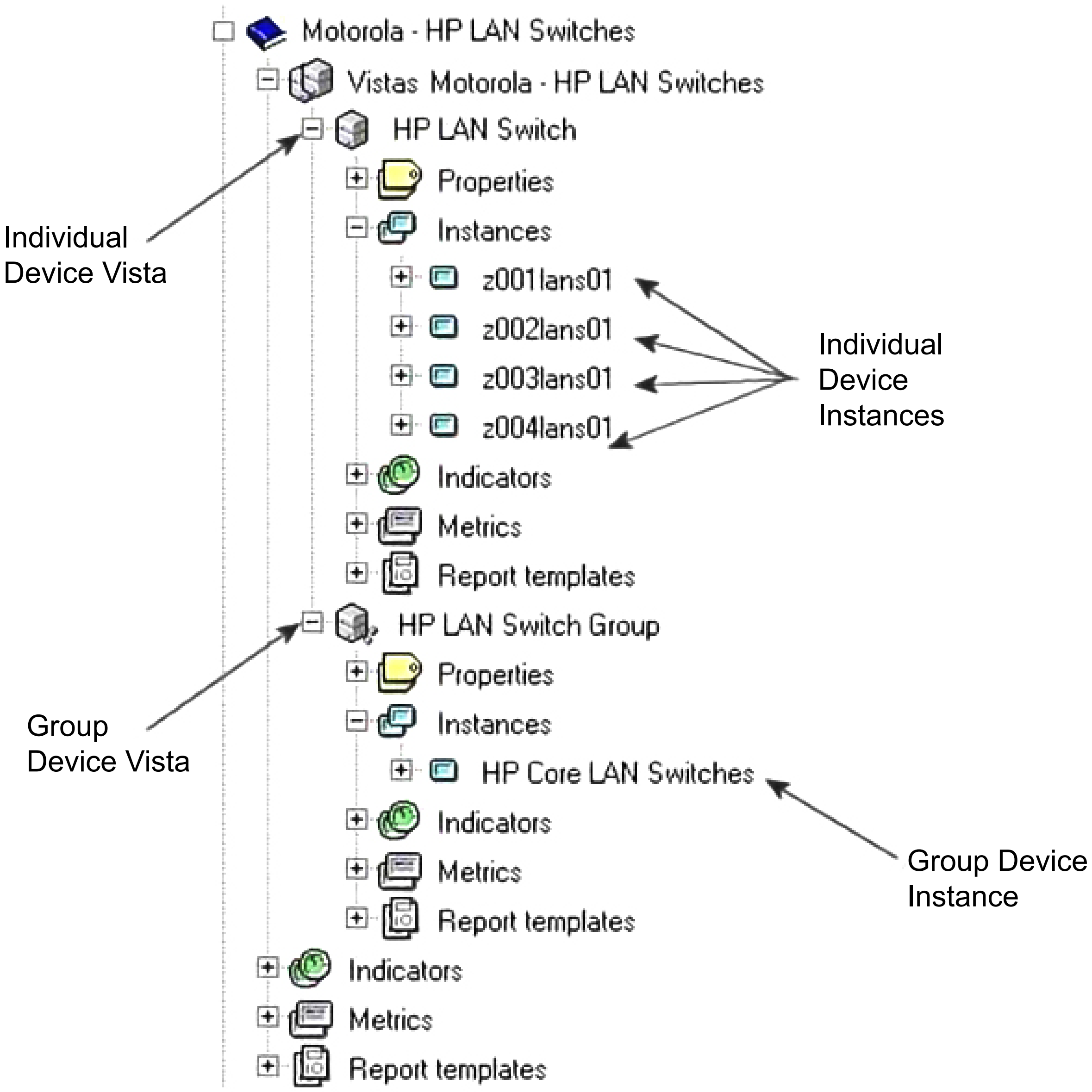
Other required libraries, which come pre-installed with InfoVista, must be present in the system in order for the Motorola-customized libraries to work. Motorola does not support the creation of reports using the report templates in these libraries.

Vistas

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 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 3: Vistas and Instances



The Vista contains the following data 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 Traps 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 49.

5.1.2

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
- Yearly

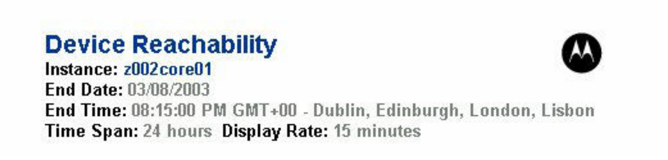
The name of the reports generated from an instance-report template pair is the instance name with the report template name in parentheses.

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

5.1.3

Report Template Title Information

Figure 4: Report Template Title Information



Device Reachability
Instance: z002core01
End Date: 03/08/2003
End Time: 08:15:00 PM GMT+00 - Dublin, Edinburgh, London, Lisbon
Time Span: 24 hours **Display Rate:** 15 minutes

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. **NOTE:** 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.

5.1.4

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.

5.1.5

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.

5.1.6

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

5.1.7

Traps

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

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.

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.

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.

5.1.8

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.

5.1.9

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.

5.2 Report Navigation

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

The reports generated by InfoVista are stored in the following folders:

- System-level folders, which contain 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.
- LAN-shared folders, in which 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.

5.2.1 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.

NOTE: 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 96.

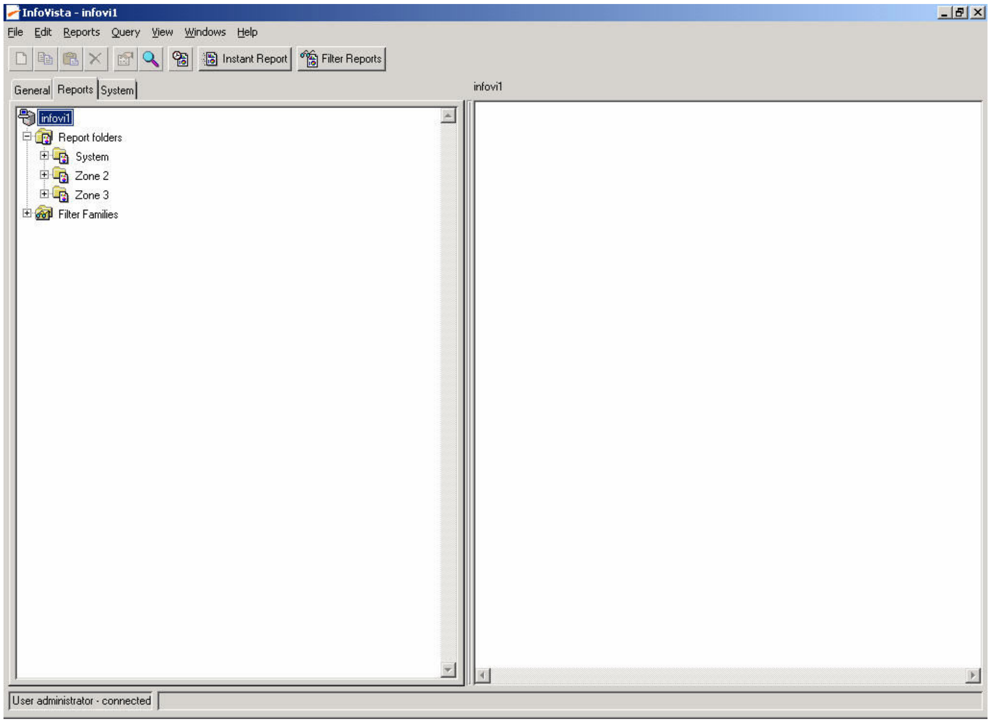
Procedure:

1 Access the InfoVista client using the method described in InfoVista Client Window Overview on page 34. (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 5: InfoVista Window (Reports Tab)

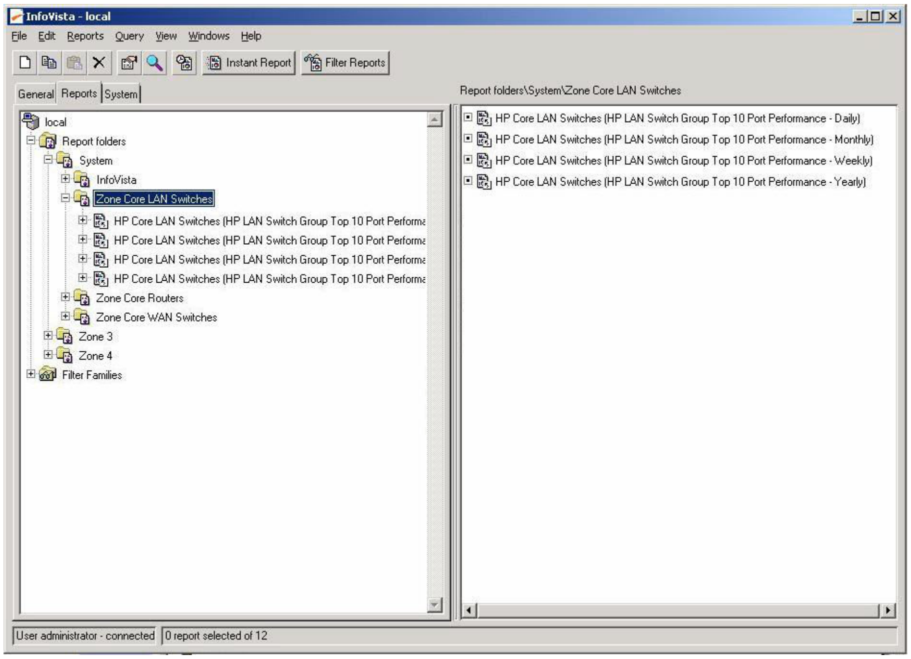


The folders appear.

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

NOTE: 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.

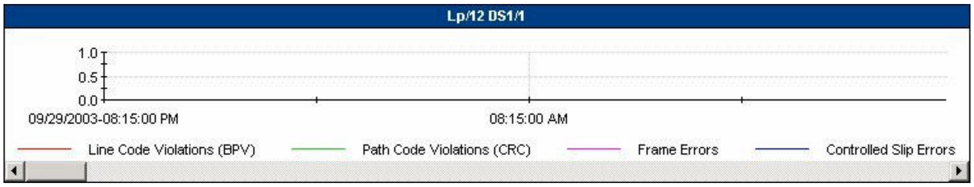
Figure 6: System Level Folders


InfoVista - local
File Edit Reports Query View Windows Help
Instant Report
Filter Reports
General
Reports
System
local
Report folders
System
InfoVista
Zone Core LAN Switches
HP Core LAN Switches (HP LAN Switch Group Top 10 Port Performa
HP Core LAN Switches (HP LAN Switch Group Top 10 Port Performa
HP Core LAN Switches (HP LAN Switch Group Top 10 Port Performa
HP Core LAN Switches (HP LAN Switch Group Top 10 Port Performa
Zone Core Routers
Zone Core WAN Switches
Zone 3
Zone 4
Filter Families
Report folders\System\Zone Core LAN Switches
HP Core LAN Switches (HP LAN Switch Group Top 10 Port Performance - Daily)
HP Core LAN Switches (HP LAN Switch Group Top 10 Port Performance - Monthly)
HP Core LAN Switches (HP LAN Switch Group Top 10 Port Performance - Weekly)
HP Core LAN Switches (HP LAN Switch Group Top 10 Port Performance - Yearly)
User administrator - connected
0 report selected of 12

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 7: Report Viewer Window

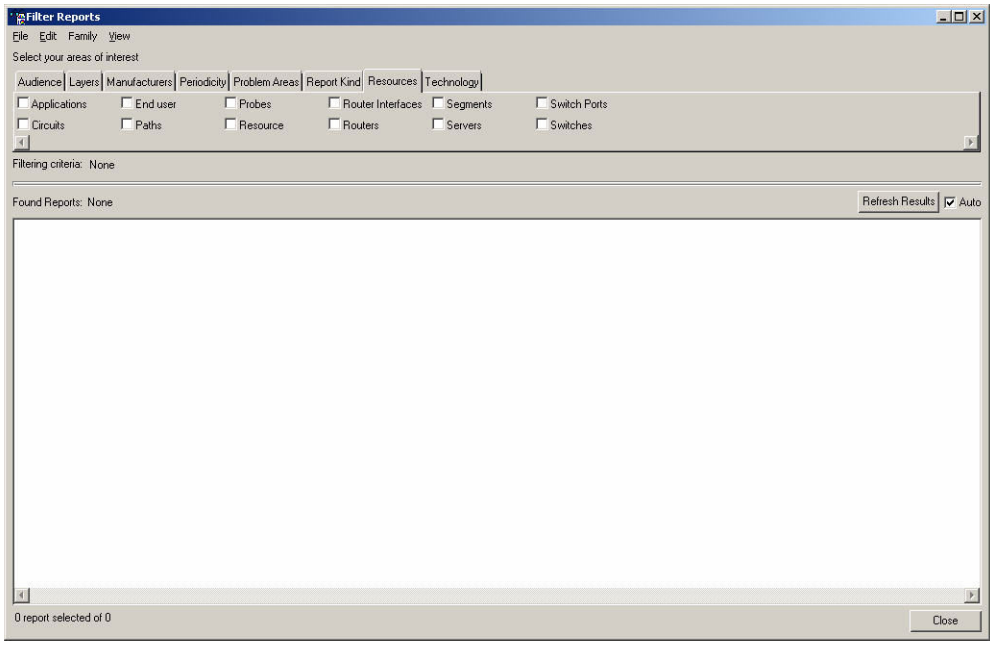


The report appears in the Report Viewer window. The title bar contains the instance name with the report template name in parentheses. The menu bar contains menu options specific to the report viewer window, and the drill downs list drills down to related reports.

5.2.2
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 8: Filter Reports Dialog Box



Filtering criteria: None

Found Reports: None

0 report selected of 0

5.2.3 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).

5.2.4
Filtering Reports

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

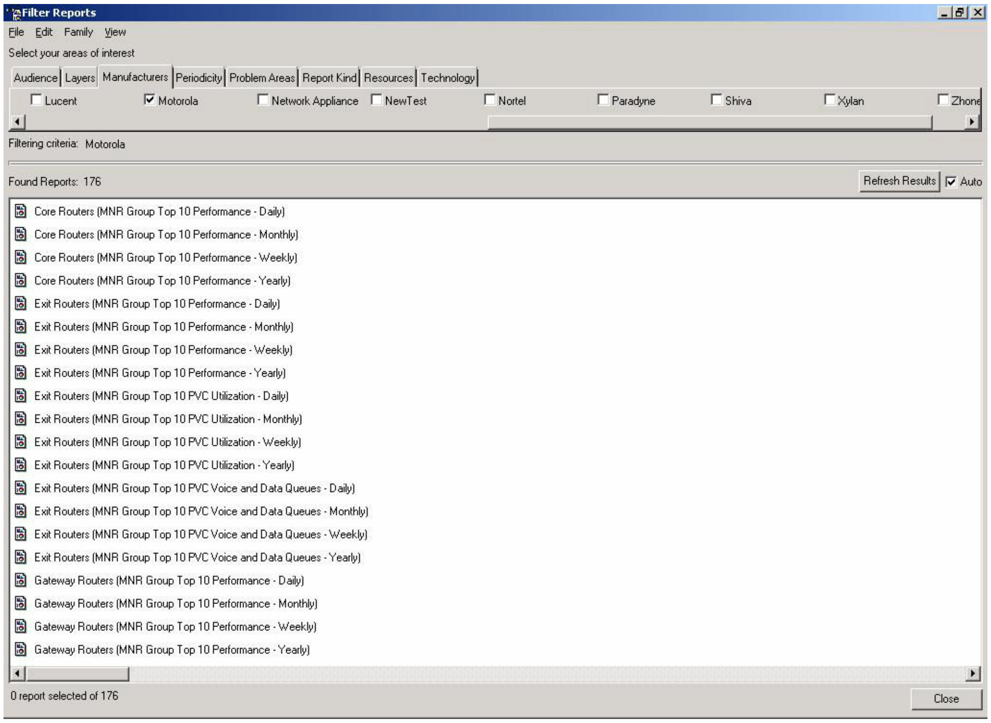
Procedure:

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

   The **Filter Reports** window appears.

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

Figure 9: Filter Reports Results



Filter Reports
File Edit Family View
Audience Layers Manufacturers Periodicity Problem Areas Report Kind Resources Technology
Refresh Results
Close

Select your areas of interest

□ Lucent ☑ Motorola □ Network Appliance □ NewTest □ Nortel □ Paradyne □ Shiva □ Xylan □ Zhone

Filtering criteria: Motorola

Found Reports: 176 ☑ Auto

- Core Routers (MNR Group Top 10 Performance - Daily)
- Core Routers (MNR Group Top 10 Performance - Monthly)
- Core Routers (MNR Group Top 10 Performance - Weekly)
- Core Routers (MNR Group Top 10 Performance - Yearly)
- Exit Routers (MNR Group Top 10 Performance - Daily)
- Exit Routers (MNR Group Top 10 Performance - Monthly)
- Exit Routers (MNR Group Top 10 Performance - Weekly)
- Exit Routers (MNR Group Top 10 Performance - Yearly)
- Exit Routers (MNR Group Top 10 PVC Utilization - Daily)
- Exit Routers (MNR Group Top 10 PVC Utilization - Monthly)
- Exit Routers (MNR Group Top 10 PVC Utilization - Weekly)
- Exit Routers (MNR Group Top 10 PVC Utilization - Yearly)
- Exit Routers (MNR Group Top 10 PVC Voice and Data Queues - Daily)
- Exit Routers (MNR Group Top 10 PVC Voice and Data Queues - Monthly)
- Exit Routers (MNR Group Top 10 PVC Voice and Data Queues - Weekly)
- Exit Routers (MNR Group Top 10 PVC Voice and Data Queues - Yearly)
- Gateway Routers (MNR Group Top 10 Performance - Daily)
- Gateway Routers (MNR Group Top 10 Performance - Monthly)
- Gateway Routers (MNR Group Top 10 Performance - Weekly)
- Gateway Routers (MNR Group Top 10 Performance - Yearly)

0 report selected of 176

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.

5.2.5
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.

5.2.6
Drilling Down on Reports

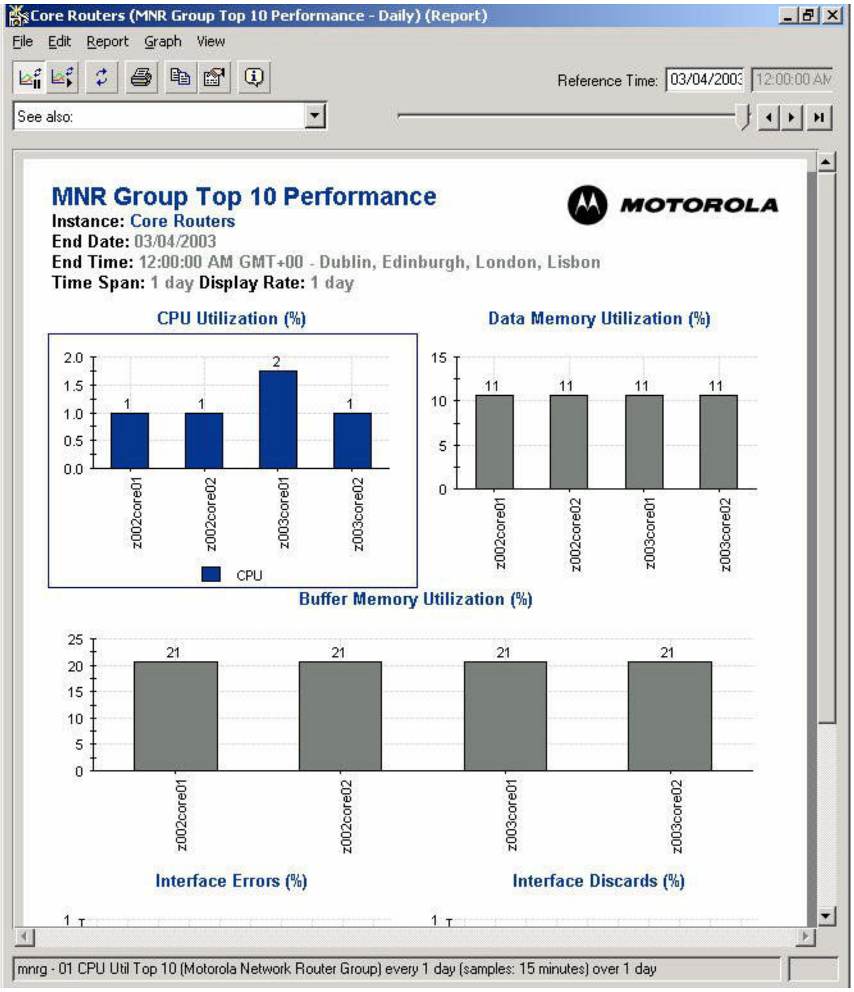
When and where to use: Use this procedure to drill down from a group report to an individual report on an instance in a graph.

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



Core Routers (MNR Group Top 10 Performance - Daily) (Report)

Reference Time: 03/04/2003 12:00:00 AM

See also:

MNR Group Top 10 Performance

Instance: Core Routers
End Date: 03/04/2003
End Time: 12:00:00 AM GMT+00 - Dublin, Edinburgh, London, Lisbon
Time Span: 1 day **Display Rate:** 1 day

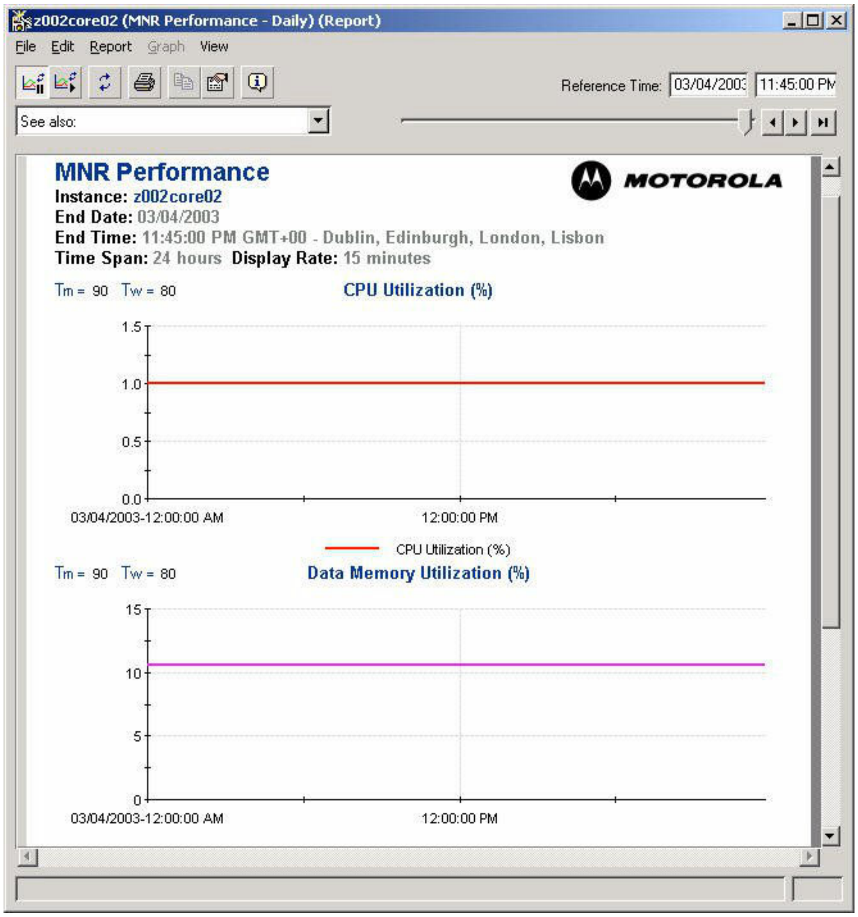
mnrg - 01 CPU Util Top 10 (Motorola Network Router Group) every 1 day (samples: 15 minutes) over 1 day

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 11: MNR Performance – Daily Report



z002core02 (MNR Performance - Daily) (Report)

Reference Time: 03/04/2003 11:45:00 PM

MNR Performance

Instance: z002core02
End Date: 03/04/2003
End Time: 11:45:00 PM GMT+00 - Dublin, Edinburgh, London, Lisbon
Time Span: 24 hours Display Rate: 15 minutes

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

5.2.7

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.

   NOTE: 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.

5.3

Uses of InfoVista Reports

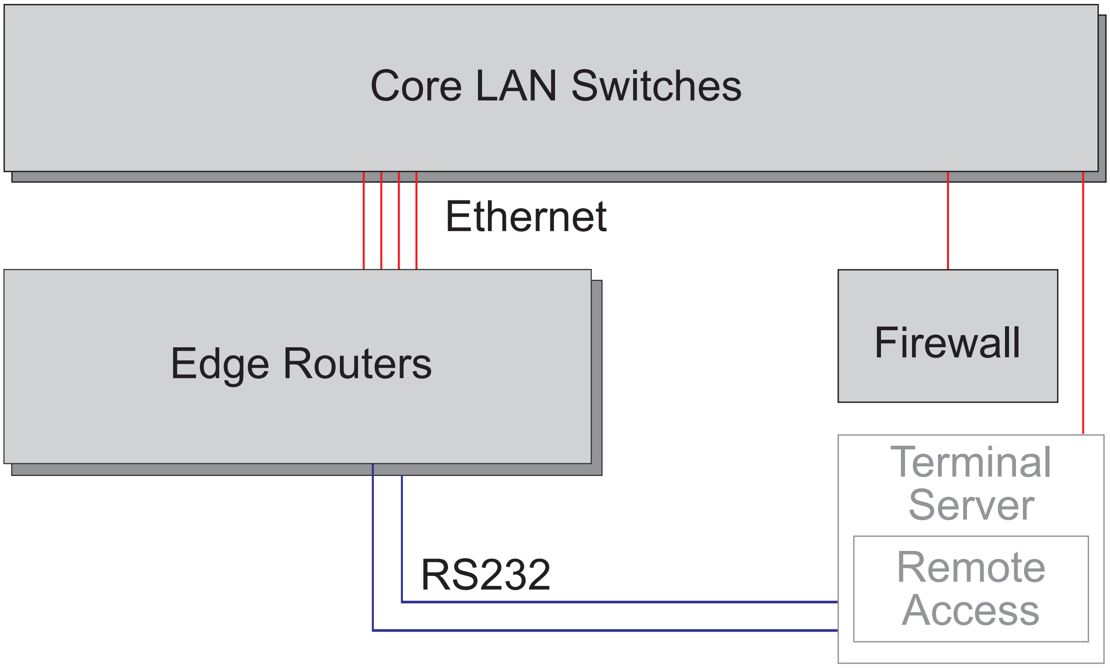
You can use InfoVista reports for proactive network performance, troubleshooting, and network capacity planning.

5.3.1
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, Juniper SRX Routers, 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 12: Devices Monitored by InfoVista in a New Build System (Example)

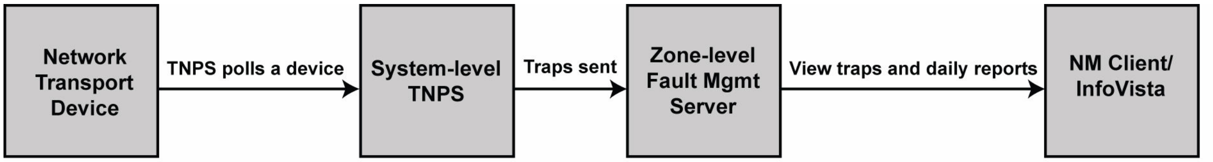


5.3.2
Performance Management Troubleshooting

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 13: Performance Data and Trap Flows



T_ADF_perform_data_trap2

5.3.3 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.

5.3.4 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.

5.3.5 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.

5.4 Motorola Network Resource Reports

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

5.4.1

Types of Motorola Network Resources

Table 10: Types of Resources

Router Model	Function
GGM 8000	All, except Peripheral
S6000	All, except Distributed Conventional Subsystem
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*.

5.4.2

Reports and 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

NOTE: 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.

5.4.3
MNR Performance Report

Report Overview

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 Motorola Network Resources on page 62.

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.

Report Graphs

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.

5.4.4
MNR CWR LMI Performance Report

Report Overview

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.

Report Graphs

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.
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.

5.4.5
MNR Interface Performance Report

Report Overview

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 Motorola Network Resources on page 62.

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.

Report Graphs

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.

5.4.6

MNR Group Top 10 Performance Report

Report Overview

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 Motorola Network Resources on page 62.

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.

Report Graphs

NOTE: 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.
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).

5.4.7

MNR WAN Link Performance Report

Report Overview

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.

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

Report Graphs

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
mnrEthWanIfPerfIPLRPktNotRcvd	Lost Packets	Number of packets that were not received by the receiving endpoint for last interval.
mnrEthWanIfPerfIPLRTxPktNum	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
mnrEthWanIfPerfIPDV99PercentNum	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.

MIB Object Name	Report Object Name	Description
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.

5.4.8
DS1/E1 Interface Performance Report

Report Thresholds

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

Graph/Table	Description
	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).
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.

5.4.9
MNR PVC Utilization Report

Report Overview

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 Motorola Network Resources on page 62.

NOTE: 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.

Report Graphs

NOTE: 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.

5.4.10
MNR PVC Queue Performance Report

Report Overview

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 Motorola Network Resources on page 62.

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.

Report Graphs

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).

Graph/Table	Description
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.

5.4.11 MNR Group Top 10 PVC Utilization Report

Report Overview

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 Motorola Network Resources on page 62.

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.

Report Graphs

NOTE: 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 outbound 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.

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

Report Overview

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 Motorola Network Resources on page 62.

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.

Report Graphs

NOTE: 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.

5.5

Juniper SRX Router Reports

This section covers reports generated by SRX Routers.

SRX Routers generate individual and group reports on a daily, weekly, monthly or yearly basis.

Table 27: Juniper SRX Router Reports

Report		Collects Performance Information for the Following Devices:
Juniper GW Performance	Individual	Edge, Prime-Access, Hub, Site
Juniper GW Port Performance	Individual	Edge, Prime-Access, Hub, Site
Juniper GW TWAMP Packet Loss	Individual	Edge, Prime-Access, Hub, Site
Juniper GW TWAMP Round Trip Delay	Individual	Edge, Prime-Access, Hub, Site
Juniper GW TWAMP RttJitter	Individual	Edge, Prime-Access, Hub, Site
Juniper GW Group Top 10 Performance	Group	Edge, Prime-Access, Hub, Site
Juniper GW Group Top 10 Port Performance	Group	Edge, Prime-Access, Hub, Site
Juniper GW Group Top 10 TWAMP Round Trip Delay	Group	Edge, Prime-Access, Hub, Site
Juniper GW Group Top 10 TWAMP RttJitter and Packets Loss	Group	Edge, Prime-Access, Hub, Site

5.5.1 Juniper SRX Routers in the ASTRO System

Routers from the Juniper SRX series are used extensively in ASTRO® 25 systems.

Table 28: Functions of Juniper SRX Routers in the ASTRO® Infrastructure

Router Model	Function
Juniper SRX345	Hub, Firewall, Site, Stateful Site Firewall
Juniper SRX1500	Edge, Site, Firewall, Prime-Access Router, Stateful Site Firewall

5.5.2 Juniper GW Performance Report

Report Overview

Juniper GW Performance is an individual report that is created for each Juniper SRX Router in the system. It collects CPU and memory utilization on the Router.

For the types of routers in your system, see Juniper SRX Routers in the ASTRO System on page 73.

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.

Report Graphs

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 29: Juniper GW Performance Report Description

Graph/Table	Tm	Tw	Description
Instantaneous CPU Utilization (%)	90	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.

5.5.3 Juniper GW Port Performance Report

Report Overview

Juniper GW Port Performance is an individual report that is created for each port on a single Juniper SRX router.

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.

Report Graphs

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 30: Juniper GW 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%.

5.5.4 Juniper GW TWAMP Packet Loss

Report Overview

Juniper GW Two-Way Active Measurement Protocol (TWAMP) Packet Loss report indicates the percentage of packets lost between two network devices. TWAMP reports for each device show all direct connections between the device and other routers supporting TWAMP.

For the types of routers in your system, see Juniper SRX Routers in the ASTRO System on page 73.

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.

Report Graphs

Table 31: Juniper GW TWAMP Packet Loss Description

Graph/Table	Description
Packet Loss (%)	The graph indicates the percentage of packets lost between network devices.

5.5.5 Juniper GW TWAMP Round Trip Delay Report

Report Overview

Juniper GW Two-Way Active Measurement Protocol (TWAMP) Round Trip Delay report indicates time required for a packet to be sent to another network device and for the acknowledgment to be received back (in microseconds). TWAMP reports for each device show all direct connections between the device and other routers supporting TWAMP.

For the types of routers in your system, see Juniper SRX Routers in the ASTRO System on page 73.

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.

Report Graphs

Table 32: Juniper GW TWAMP Round Trip Delay Description

Graph/Table	Description
Round Trip Time Jitter (microseconds)	The graph indicates variation in delay time for successive packets.

5.5.6

Juniper GW TWAMP RttJitter Report

Report Overview

Juniper GW Two-Way Active Measurement Protocol (TWAMP) Round Trip Time (RTT) Jitter report indicates variation in delay time for successive packets (in microseconds). TWAMP reports for each device show all direct connections between the device and other routers supporting TWAMP.

For the types of routers in your system, see Juniper SRX Routers in the ASTRO System on page 73.

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.

Report Graphs

Table 33: Juniper GW TWAMP RttJitter Description

Graph/Table	Description
Round Trip Time Jitter (microseconds)	The graph indicates time required for a packet to be sent to another network device and for the acknowledgment to be received back.

5.5.7

Juniper GW Group Top 10 Performance Report

Report Overview

Juniper GW Group Top 10 Performance is a group report that is created for the groups of Juniper Routers in the system. For the types of routers in your system, see Juniper SRX Routers in the ASTRO System on page 73.

It shows the Top **N** (up to 10) routers with the highest values for all statistics in the Juniper GW 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.

Report Graphs

NOTE: Group reports do not generate threshold traps.

Table 34: Juniper GW Group Top 10 Performance Report Description

Graph/Table	Description
CPU Utilization (%)	The top 10 routers that have the highest CPU Utilization.
Total Memory Utilization (%)	The top 10 routers that have the highest Total Memory Utilization.

5.5.8

Juniper GW Group Top 10 Port Performance Report

Report Overview

Juniper GW Group Top 10 Port Performance is a group report that is created for each port on a group of Juniper routers. It is a system-level report.

It shows the Top **N** (up to 10) ports with the highest values for all statistics in the Juniper GW 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.

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

Report Graphs

Table 35: Juniper GW 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.)

5.5.9

Juniper GW Group Top 10 TWAMP Round Trip Delay Report

Report Overview

Juniper GW Group Top 10 TWAMP Round Trip Delay is a group report that is created for each port on a group of Juniper routers. It is a system-level report.

It shows the Top **N** (up to 10) ports with the highest values for all statistics in the Juniper GW TWAMP Round Trip Delay 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.

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

Report Graphs

Table 36: Juniper GW Group Top 10 TWAMP Round Trip Delay

Graph/Table	Tm	Tw	Description
Round Trip Delay – Average (microseconds)	N/A	N/A	The top 10 routers that have the largest average Round Trip Delay.

Graph/Table	Tm	Tw	Description
Round Trip Delay – Maximum (microseconds)	N/A	N/A	The top 10 routers that have the highest Round Trip Delay.

5.5.10
Juniper GW Group Top 10 TWAMP RTT Jitter and Packets Loss

Report Overview

Juniper GW Group Top 10 TWAMP Round Trip Delay is a group report that is created for each port on a group of Juniper routers. It is a system-level report.

It shows the Top **N** (up to 10) ports with the highest values for all statistics in the Juniper GW TWAMP RttJitter and Juniper GW TWAMP Packet Loss reports. 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.

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

Report Graphs

Table 37: Juniper GW Group Top 10 TWAMP RTT Jitter and Packet Loss

Graph/Table	Tm	Tw	Description
RTT Jitter – Average (microseconds)	N/A	N/A	The top 10 routers that have the largest average RTT Jitter.
Round Trip Delay – Maximum (microseconds)	N/A	N/A	The top 10 routers that have the highest RTT Jitter.
Packets Loss (%)	N/A	N/A	The top 10 routers that have the highest Packet Loss percentage.

5.6
Ethernet LAN Switch Reports

This section provides information on HP and Aruba LAN Switch reports:

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

5.6.1
HP/Aruba LAN Switch Port Performance Report

Report Overview

HP/Aruba LAN Switch Port Performance is an individual report that is created for each port on a single Ethernet LAN switch. The title of the report depends on the Ethernet LAN switch in the system.

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.

Report Graphs

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 38: HP/Aruba 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).

Graph/Table	Tm	Tw	Description
			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. **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.

Graph/Table	Tm	Tw	Description
			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.

5.6.2 HP/Aruba LAN Switch Group Top 10 Port Performance Report

Report Overview

HP/Aruba LAN Switch Group Top 10 Port Performance is a group report that is created for each port on a group of Ethernet LAN switches. It is a system-level report. The title of the report depends on the Ethernet LAN switch in the system.

It shows the Top **N** (up to 10) ports on the HP LAN switch with the highest values for all statistics in the HP/Aruba 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.

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

Report Graphs

Table 39: HP/Aruba 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.)

5.6.3 HP/Aruba LAN Switch Port Name/MIB Index No. Report

Report Overview

The HP/Aruba 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/Aruba LAN Switch

Port Performance report. This report is only generated for the two Ethernet LAN switches in the core and not the LAN Switches at the sites. The title of the report depends on the Ethernet LAN switch in the system.

Report Graphs

Table 40: HP/Aruba 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. • 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.

5.7 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

NOTE: 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.

5.7.1 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)

5.7.2 RNG Context Activation Report

Report Overview

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.

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

Report Graphs

Table 41: 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.

5.7.3 Packet Data Channel Access Report

Report Overview

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.

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

Report Graphs

Table 42: 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.
pdgPDRRNGProxyStatsPDEndOfData RecvTCHCount	PD End Of Data Indications received from Sites	Number of Packet Data End Of Data Indications received from all Sites.

5.7.4 SDU Transmissions Report

Report Overview

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

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

Report Graphs

Table 43: 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.

5.7.5 Mobility Report

Report Overview

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.

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

This table presents RNG Packet Data Channel Access information.

Report Graphs

Table 44: 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.
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.

5.7.6

RNG Channel Resources Report

Report Overview

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.

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

Report Graphs

The following table presents RNG PDCH Channel usage.

Table 45: 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.

MIB Object Name	Report Object Name	Object Description
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.

5.7.7

RNG Inbound and Outbound Data Profile Report

Report Overview

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.

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

Report Graphs

Table 46: 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 47: 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.
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.
pdgPDRRNGProxyStatsUnCnfIBCount	Unconfirmed Messages received from MSUs	Number of unconfirmed messages received from all Mobile Subscriber Units.

5.7.8 RNG HPD Packet Data Service – UP Connect Information Report

Report Overview

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.

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

Report Graphs

Table 48: 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. **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 .

5.8
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.

NOTE:

- 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

5.8.1
PDR Roaming and Registration Statistics Report

Report Overview

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.

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

Report Graphs

Table 49: 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.

5.8.2
PDR ICMP Traffic Report

Report Overview

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.

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

Report Graphs

The following table presents PDR ICMP data traffic.

Table 50: ICMP Traffic

MIB Object Name	Report Object Name	Object Description
pdgPDRStatsICMPMsgRecvRFCount	Inbound ICMP messages	Number of ICMP messages from subscribers forwarded by the PDR.
pdgPDRStatsICMPMsgRecvLANCount	Outbound ICMP messages	Number of ICMP messages forwarded to subscribers by the PDR.
pdgPDRStatsICMPMsgDiscCount	ICMP messages discarded	Number of ICMP messages discarded.
pdgPDRStatsICMPPckGenCount	ICMP messages generated	Number of ICMP messages generated by the PDR.

5.8.3
PDR IP Bearer Service Statistics

Report Overview

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

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

Report Graphs

Table 51: IP Bearer Service Statistics

MIB Object Name	Report Object Name	Object Description
pdgPDRStatsIPPckObCount	Outbound IP Packets	Subscriber destined IP Packets forwarded by the PDR.
pdgPDRStatsIPPckIbCount	Inbound IP Packets	Subscriber sourced IP Packets forwarded by the PDR.
pdgPDRStatsIPPckDiscCount	IP Packets discarded	Subscriber sourced and destined IP packets discarded due to ingress filtering, or bad IP header.
pdgPDRStatsRFC2507ErrNonTCPHdrCmpCount	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.
pdgPDRStatsRFC2507IBNonTCPHdrCmpCount	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 decompressed.
pdgPDRStatsRFC2507OBNonTCPHdrCmpCount	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.
pdgPDRStatsBcstIPPckCount	Broadcast IP Packets	The number of broadcast messages received by the PDR.
pdgPDRStatsBcstIPPckDiscCount	Broadcast Packets Discarded	The number of broadcast messages received by the PDR that were not deliverable (and were generated ICMP error messages).
pdgPDRStatsBcstDroppedCount	Broadcast Packets Dropped	The number of broadcast messages received by the PDR that were not deliverable, due to buffer overload (and were not generated ICMP error messages).

5.8.4 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.

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

5.9 System Wide Devices Reports

This section provides information on:

- Device Reachability
- InfoVista SNMP Traffic Analysis

5.9.1
Device Reachability Report

Report Overview

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.

Report Graphs

Table 52: 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).

5.9.2
InfoVista SNMP Traffic Analysis Report

Report Overview

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.

Report Graphs

Table 53: 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.
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:	

Graph/Table	Description
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.

5.10

GCP 8000 Report

Report Overview

GCP 8000 reports cover each port in a single GCP 8000 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.

Report Graphs

Table 54: GCP 8000 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).

Graph/Table	Tm	Tw	Description
			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 repre-

Graph/Table	Tm	Tw	Description
			sented 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.

Chapter 6

InfoVista Troubleshooting

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

6.1 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.

6.2 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*.

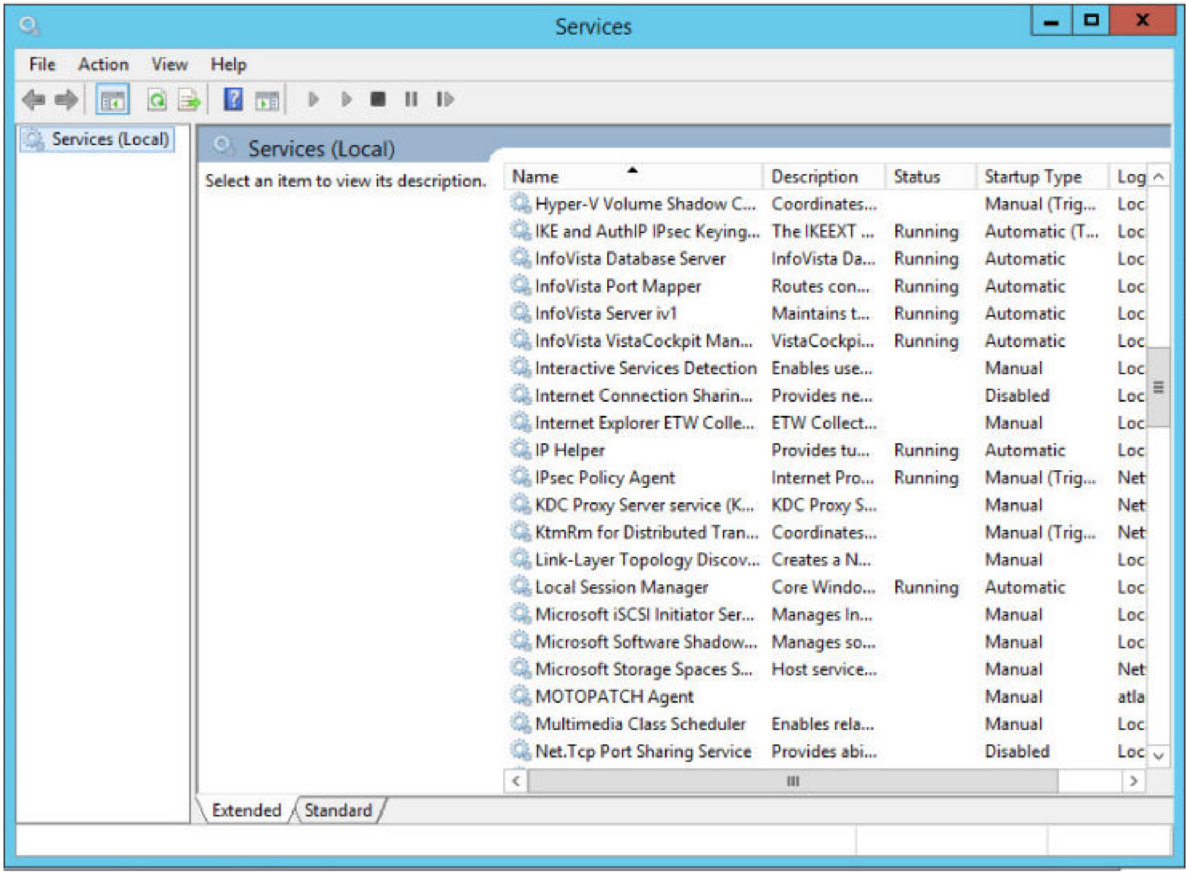
6.3 Troubleshooting InfoVista Services

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 14: Services Window



Services (Local)

Select an item to view its description.

Name	Description	Status	Startup Type	Log
Hyper-V Volume Shadow C...	Coordinates...		Manual (Trig...	Loc
IKE and AuthIP IPsec Keying...	The IKEEXT ...	Running	Automatic (T...	Loc
InfoVista Database Server	InfoVista Da...	Running	Automatic	Loc
InfoVista Port Mapper	Routes con...	Running	Automatic	Loc
InfoVista Server iv1	Maintains t...	Running	Automatic	Loc
InfoVista VistaCockpit Man...	VistaCockpi...	Running	Automatic	Loc
Interactive Services Detection	Enables use...		Manual	Loc
Internet Connection Sharin...	Provides ne...		Disabled	Loc
Internet Explorer ETW Colle...	ETW Collect...		Manual	Loc
IP Helper	Provides tu...	Running	Automatic	Loc
IPsec Policy Agent	Internet Pro...	Running	Manual (Trig...	Net
KDC Proxy Server service (K...	KDC Proxy S...		Manual	Net
KtmRm for Distributed Tran...	Coordinates...		Manual (Trig...	Net
Link-Layer Topology Discov...	Creates a N...		Manual	Loc
Local Session Manager	Core Windo...	Running	Automatic	Loc
Microsoft iSCSI Initiator Ser...	Manages In...		Manual	Loc
Microsoft Software Shadow...	Manages so...		Manual	Loc
Microsoft Storage Spaces S...	Host service...		Manual	Net
MOTOPATCH Agent			Manual	atla
Multimedia Class Scheduler	Enables rela...		Manual	Loc
Net.Tcp Port Sharing Service	Provides abi...		Disabled	Loc

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.

> **NOTE:** 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 7

InfoVista Reference

This chapter contains supplemental reference information relating to InfoVista.

7.1 InfoVista Client User Accounts

InfoVista uses a variety of account types, each with defined privileges and tasks.

NOTE: Motorola Solutions provides the confidential passwords to approved users. Contact the Centralized Managed Support Operations (CMSO) for additional information.

Table 55: 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 **NOTE:** The InfoVista Runtime license prevents you from modifying or adding to any library. You can only import a new library.

7.2 Installing InfoVista Client Application Software

Use this procedure to install InfoVista on the TNM client or NM client.

Procedure:

1. Insert *InfoVista Version 6.1* 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 8

InfoVista Disaster Recovery

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

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

8.1 Recovering InfoVista

NOTE: For ESXi 7.0, the certified web browser for VMware ESXi Embedded Host Client and VMware vSphere Client is Microsoft Edge 88.0.705.50 or later.
For ESXi 6.5, the certified web browser for VMware ESXi Embedded Host Client and VMware vSphere Web Client is Microsoft Internet Explorer 11 or later.

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

Process:

1. 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 20.
3. Configure vCenter for newly deployed virtual machines. See Configuring the vCenter for the Newly Deployed VM on page 22.
4. Startup and shutdown the virtual machine. See Setting the Virtual Machine Startup and Shutdown Order on page 23.
5. Connect and Power On the Virtual Machine. See Connecting and Powering On Virtual Machine on page 26.
6. Configure the InfoVista virtual machine. See Configuring InfoVista Virtual Machine on page 28.
7. Configure the InfoVista License Key. See Configuring the InfoVista License Key on page 31.
8. Configure the Primary InfoVista Server. See Configuring the InfoVista Server on page 29.
9. Configure the Backup InfoVista Server. See Configuring the InfoVista Server on page 29.

   NOTE: Perform this Procedure only if the system implements the Dynamic System Resilience feature.
10. Configure the Trap Receiver Address on InfoVista. See Configuring Trap Receiver Address on page 31.
11. 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*.
12. Restore the database backup file as described in Restoring InfoVista Databases on page 43.
13. Run the Discovery Script manually. See Running the Discovery Script Manually on page 45.
14. Set the Boot Order for the Workstation/Server.

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

NOTE: 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.

15 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*.

16 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.

17 Installing the Antivirus Software. See "CSMS – Deploying McAfee Client Software to Host-Based Threat Prevention Clients" in the *Core Security Management Server Feature Guide*.

8.2

Database Disaster Recovery

Restore the database backup file as described in Restoring InfoVista Databases on page 43.