TME 10 NetView for Windows NT** Release Notes
Version 5.0a

TME 10 NetView for Windows NT Release Notes (November 1997)

Copyright Notice

Trademarks

Notice

TME 10 NetView for Windows NT

Release Notes

Release Notes

The following Release Notes provide important information about using and installing TME 10 NetView for Windows NT Version 5.0a. These notes are the most current information for the product and take precedence over all other documentation. Please read these notes thoroughly before installing or using this product.

TME 10 NetView for Windows NT provides a comprehensive set of network management tools and a robust framework for managing enterprise-wide networks from Intel and Alpha based Windows NT 4.0 platforms. It includes a broad range of user-oriented applications for fault, configuration, and performance management of heterogeneous multivendor devices and open networks using SNMP. It also includes the industry-standard OpenView APIs that software developers require for seamlessly integrating their management applications into the framework.

These release notes include the following topics:

- "Installation" on page 2
- "Maintenance" on page 11
- "New Features in Version 5.0a" on page 17
- "New Features in Version 5.0" on page 33
- "Defects Fixed in Release 5.0a" on page 46
- "Known Defects in Release 5.0a" on page 49
- "Documentation Errata" on page 57

- "IBM Redbooks" on page 58

Installation

This section contains information about installation requirements, such as hardware and software requirements, NetView account, SQL database, and Microsoft SQL Server requirements. This section also includes information about potential installation problems.

Migrating from a Previous Version of TME 10 NetView for Windows NT

From a Version Prior to Version 5.0

There is no migration available for versions prior to Version 5.0 of TME 10 NetView for Windows NT. You must select **Yes** in response to **Delete all existing NetView files, settings, and databases?** in the **Overwrite the Current Installation** dialog.

From Version 5.0 or Version 5.0a

If you have installed TME 10 NetView for Windows NT Version 5.0 or Version 5.0a and wish to preserve your databases and customizations, select **No** in response to **Delete all existing NetView files, settings, and databases?** in the **Overwrite the Current Installation** dialog. See "Migration" on page 17 for more information.

Hardware Requirements

These are the hardware requirements:

- Intel PC or Alpha PC. For Intel PCs, Pentium 90 minimum.

- 48 MB of RAM for Intel PCs, 64 MB of RAM for Alpha PCs. (Additional memory will improve performance and is necessary for large networks.)

- 128 MB paging space.

- NTFS partition or a FAT partition that supports long file names. See "FAT File Partitions" on page 7 for more information about using a FAT partition.

  - For Intel PCs using Microsoft Access for NetView databases, use an NTFS partition with at least 160 MB of available disk space.

  - For Intel PCs using Microsoft SQL Server for NetView databases, use an NTFS partition with at least 212 MB of available disk space.

  - For Alpha PCs, use an NTFS partition with at least 212 MB of available disk space.

- Network adapter card.

- SVGA graphics card and monitor (minimum 800x600 pixels x 16 colors), 1024x768 is recommended.

Software Requirements

These are the software requirements:

- Windows NT Version 4.0.

- TCP/IP protocol installed and configured.

- SNMP Service installed and configured.

  If you must install the kit without the SNMP Service running, use the **-ss** flag with the setup program. We highly recommend that you install with the SNMP Service running. If it is not running, you must have a seed file for autodiscovery to work.

- Optional: MS SQL Server V6.5 is supported on both Alpha and Intel. It is no longer required on Alpha for SQL support, as Alpha machines now install MS Jet engine (MS Access) if SQL Server is not installed. (See "SQL Databases" on page 5 for more information.)

Installation Account

Install the NetView program from an account that has Administrator privileges. After Setup, you must reboot your system for NetView changes to take effect.

Installation Process

Setup updates the registry with NetView environment variables: CAT_PATH, LANG, NV_TCL, TRALERTD_CONF, TRAPD_CONF, MIBDB, MIBFILES, NLSPATH, NV_DRIVE, APPMON_TIMER_SEC, AND OVwHelpDir. If any of these names are used by other applications, setup prompts you to overwrite the value. The PATH environment variable is modified to include **\usr\ov\bin**.

Setup creates the nvinstal.log file that tracks the progress and records the details of the installation. This information is stored in the system directory (for example, \winnt\system32). The Installation Log icon in the NetView program group displays the log.

Setup edits the **\<winnt>\system32\drivers\etc\services** file to add NetView port numbers. If the port number is used for other applications, a message box asks you to manually update the file. Examine nvinstal.log for details on why setup failed and how to edit the file manually.

Setup creates a NetView Program Menu (available from Windows NT Start) and the NetView Program Group with icons for the most common NetView programs.

NetView Accounts

The NetView program requires a NetView account on the server and on the client. NetView accounts are created during installation. During both the server installation and the client installation, the installation process asks for a password. The password must be the same on the server and on the client to allow access between the client and the server.

For performance reasons it is not advised to install NetView on a Domain or Backup Domain Controller. However, if you do so, you

need to be aware that the installation tries to create a NetView account on the local machine. This is all right on a primary Domain Controller, but NT does not allow you to create an account, local or domain, on a Domain Backup Controller. To install NetView on a Domain Backup Controller, first create a NetView domain account. Then install NetView from a Command Prompt window in the NetView kit directory by enter the following command:

```
setup.exe -nu
```

This command installs NetView using an existing NetView account.

Creating the NetView Account Manually

Two important points to note if you are creating or checking the NetView account:

- The NetView account must belong to the Administrators group.

- In the User Manager, you must select **Policies --> User Rights --> Advanced User Rights --> Log on as a Service**.

SQL Databases

- On Alpha and Intel machines, if SQL Server is not installed, NetView uses Access databases and installs the drivers, if necessary. If SQL Server is installed, but you want to use Access instead, set the environment variable DATABASE_TYPE to ACCESS using the System icon on the Control Panel before installing NetView.

- If the NetView server is running SQL Server, then clients connect remotely to the SQL Server. SQL Server does not need to be installed on the NetView client.

Microsoft SQL Server

This section contains information pertinent to Microsoft SQL Server.

SQL Server Licenses

Microsoft SQL Server V6.5 is supported on both Alpha and Intel platforms.

Although you only need to install SQL Server on the NetView server machine when you are using SQL Server as the SQL database for NetView, you need to count the number of clients as well as the server when determining the number of SQL Server licenses you need. You will need a license for each NetView client and a license for the server itself.

SQL Server Configuration

- IMPORTANT: You must configure the SQL Server to use Integrated or Mixed security before installing the NetView program. The SQL Server default is Standard security, which results in NetView failing. If you do not configure security to Integrated or Mixed, a login dialog box is displayed on the screen for Windows applications and the NetView daemons cannot connect to the database.

  To configure the SQL Server to use Integrated or Mixed security:

  1. Go to the Microsoft SQL Enterprise Manager.

  2. Select your server on the Server Manager window. Then select **Server --> SQL Server --> Configure.** A dialog box is displayed.

  3. On the Security Options tab page in the dialog box, click either the Windows NT Integrated or Mixed radio button for the Login Security Mode.

- If you anticipate many events, 20000 or more, then you should increase the size of the tempdb database. A reasonable size is 50 MB for this situation.

- The **\usr\ov\databases\odbc\create_sqldb.bat** file is used by the installation process to create the SQL Server devices, databases, and database schemas used by NetView.

FAT File Partitions

NetView can be installed on a FAT partition that supports long file names. Install NetView from a command prompt window in the NetView kit directory by entering the following command:

```
setup.exe -fat
```

This command enables NetView to use a FAT partition.

Potential Installation Problems

This section describes potential installation problems and what to do if these problems occur.

IP Name Resolution

Both the NetView client and the NetView server need to be able to resolve each others IP address and name, including deriving the NetBIOS name (computer name). Currently, NetView derives the NetBIOS name from the resolved IP address. If the address, for example 16.1.0.23 resolves using DNS to netview.tivoli.com, then the NetBIOS name is assumed to be NETVIEW.

To continue this example, if the NetBIOS name is MYNODE instead of NETVIEW, the following message would be displayed from the client installation:

```
Unable to connect to NetView Server sharename \\NETVIEW\NetView
```

To avoid this problem, if the NetBIOS name is different, add an alias in the HOSTS file, (**%SystemDrive%\system32\drivers\etc\HOSTS**) similar to the following:

```
16.1.0.23  MYNODE
```

You should add aliases on the server for each client whose computer name is not the same as the one derived from the IP name.

IP address and name resolution is important for communication between the NetView client and the server and can cause problems if unexpected resolutions occur.

To aid in diagnosing such problems, use the **\usr\ov\bin\host.exe** utility to see how NetView is resolving IP addresses and names. If

---

successful, **host.exe** displays the name resolution from the address and the reverse resolution from the name. Check to see that the IP addresses and names are what you expect. Using the /s switch the **host.exe** utility can use **net send** to send a pop-up box to the machine to verify that the NetBIOS name is for the correct machine.

```
host.exe [/s] [IP address | IP name | NetBIOS name]
```

With no parameters, the **host.exe** utility gets the local address and resolves it. You can use the **host.exe** utility from the server to verify IP addresses for all the clients.

NetView Cannot Connect to Share

Sometimes the NetView client cannot connect to the NetView share on the server. This may be due to an existing connection on the client machine to a drive on the server using another account on the server. If this is the case, disconnect that share on the client and reinstall NetView. Windows NT does not allow a machine to access two different shares using two different accounts on the same remote machine.

ODBC Problems

If you find that the ODBC installation on your machine has problems, either during or after the NetView installation, you can install ODBC directly from the ODBC directory on the NetView installation kit.

Typical indications pointing to a bad ODBC installation include frequent auto-restarts of the Event Browser or the Event Browser suspends with the 'spinning disk' popup. Ensure that the versions of the ODBC drivers and SQL Server or Access driver are valid. You can check the version from the NT Explorer. Select the file name and press **Alt-Enter**, or select the file name and press the right mouse button and select **Properties**.

File Name	Intel	Alpha
%SystemDrive%\system32\odbccr32.dll	V2.50.3006	V2.50.3321
%SystemDrive%\system32\sqlsvr32.dll	V2.65.0201	V2.65.0201 (or later)
%SystemDrive%\system32\odbcjt32.dll	V3.40.27.28 (or later)	N/A

You can find a later version of ODBC in the **odbc** subdirectory on the installation CD-ROM.

On Intel, run the file:

`intel\odbc\dataacc.exe`

On Alpha, run the file:

`alpha\odbc\setup.exe`

In some cases it is necessary to deinstall ODBC before attempting to reinstall.

When installing ODBC, you can ignore the section on creating data sources because the NetView installation creates the data sources. Then install NetView again.

If you continue to experience problems with ODBC, it is possible that there is still a mismatch with the ODBC DLLs. As a last resort, you can do the following:

1. Rename the following ODBC DLL files. Before renaming these files, exit all applications that might use these files including the Control Panel.

```
%SystemDrive%\system32\dbnmpntw.dll
%SystemDrive%\system32\msjt3032.dll
%SystemDrive%\system32\msjter32.dll
%SystemDrive%\system32\msjtint32.dll
%SystemDrive%\system32\odbc32.dll
%SystemDrive%\system32\odbccp32.dll
%SystemDrive%\system32\odbccr32.dll
%SystemDrive%\system32\odbcgt32.dll
%SystemDrive%\system32\odbcint.dll
%SystemDrive%\system32\odbcji32.dll
%SystemDrive%\system32\odbcjt32.dll
%SystemDrive%\system32\odbctl32.dll
%SystemDrive%\system32\sqlsvr32.dll
```

2. Invoke the registry editor, **regedt32.exe** and save the two subtrees listed below. (Select the ODBC subtree and select **Registry --> Save Key** to save the subtree.) Then delete each of the following subtrees:

   - **HKEY_LOCAL_MACHINE\SOFTWARE\ODBC**
   - **HKEY_CURRENT_USER\Software\ODBC**

3. Reinstall NetView.

Insufficient Disk Space

If you have problems installing, first verify that there is sufficient disk space. Next verify that there is a minimum of 120 MB of paging space. To do this, select the Windows NT System Icon from the Control Panel and then press the **Virtual Memory** button.

The ovtopmd Daemon Will Not Start

If you cannot start the ovtopmd daemon after installation, the **ovw_fields** command might not have completed its execution. See "Options --> Server Setup --> Databases --> Clear Databases" on page 52 for more information.

TCP/IP Settings

Check that your TCP/IP settings are correctly configured for IP
address, Subnet Mask, and Domain Name.

Installation Manager

If you run the Installation Manager from the Start menu, you may
receive the following message:

```
Can't find the file installm.exe
```

If you receive this message, put the NetView CD back into the CD
drive and run it again.

Maintenance

As a NetView administrator, you should plan on performing a few
maintenance tasks occasionally. The tasks you will need to perform
will depend on the needs of your site. This section outlines the tasks.

Changing the Management Station's IP Address or Name

Server

If you have installed NetView in the Single User mode or Server
mode there is nothing you need to do on the Management Station.

If you have NetView clients connected to this NetView server, you
need to check the following on each client:

- Ensure that the client can resolve the new IP address and name.
  You can check this using the host.exe utility. Add an entry to
  the \%SYSTEMDIR%\system32\drivers\etc\hosts file for the
  new address and name of the server.

- Use the Registry Editor to modify the ServerName and
  ServerAddress entries in
  HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\TME 10
  NetView\CurrentVersion.

- Ensure that the NetView share is still mounted correctly.

Client

If the NetView client changes its IP address or name, ensure that the NetView server can resolve the new name and address and derive the correct NetBIOS name. Use the host.exe utility to check this and make a new entry (or modify the existing one) in the file \%SYSTEMDIR%\system32\drivers\etc\hosts on the NetView server machine.

/usr/ov/log/nv.log (NetView Server and Client)

The **/usr/ov/log/nv.log** is the NetView product-specific log file. Information as well as error conditions are logged in this file. If you are experiencing a problem, the NetView support team will want to view this file.

Because this file grows over time, you should rename it periodically, perhaps keeping only one renamed version.

/usr/ov/log/oldevents.log (NetView Server Only)

Events are stored in the SQL database by default. To prevent the SQL database from growing too large, the trapd daemon periodically removes the oldest events from the database. You can control how many events are preserved and schedule when, or if, purging should occur. To do this, select **Options --> Server Setup** and use the trapd daemon page. You can also optionally specify that events should be written to a log file before being purged from the database. Because this file grows over time, you need to have a policy on how to archive this file.

/usr/ov/bin/playitagain.sam (NetView Server Only)

If you are running NetView clients, this file will grow over time.

The map events corresponding to manage, unmanage, acknowledge, or unacknowledge are used to update the icon status colors on each map in a NetView client/server environment and are stored in this file.

When the NetView console starts, it reads this file and processes any events it may have missed since the last time it was running.

There is no reason to archive this file. However, before you delete it, you must ensure that all the client maps are up to date.

MS Access Database for Events

The NetView installation uses a Microsoft Access database to store events if an SQL Server is not present. This is true only for Intel machines. This Microsoft Access database can become fragmented causing a decrease in performance and an increase in the use of disk space. You might want to periodically stop the NetView Service and compact the database. To compact the database, select **Start --> Settings --> Control Panel --> ODBC --> System DSN --> Compact**.

SNMP Data Collection

By default, SNMP data that is collected is stored in the SQL database, which grows over time. To prevent this database from growing too large, a process runs each night that removes the oldest data from the database. To control how many records are preserved and schedule when, or if, purging should occur, Select **Options --> Server Setup** and then select the **Schedule SnmpCollect Data to Delete** pull-down on the Files page.

You can also use your own SQL database tools to monitor, archive, and purge the database. See "SQL Database Schemas for Event System, snmpCollect, and Topology" for more information.

Note: The installation creates an 'at' Scheduler entry for the **snmpodump -x5000** command. NetView will normally maintain the Scheduler queue by deleting or replacing entries. You can check this by entering the **at** command at the command prompt to view Scheduler entries.

SQL Database Schemas for Event System, snmpCollect, and Topology

If you want to access the SQL database directly for current reports and queries, you might find the information in this section useful.

NetView can use either Microsoft Access or Microsoft SQL Server databases. This is decided at NetView installation time.

If SQL Server is installed, note that a device named NetViewDev is created to hold the database NetViewDb which holds the NetView schema.

The schemas are the same for Access and SQL Server databases.

Schema for Event System

The following table describes the schema for the event system:

Table	Field	Type
enterpriseName	enterpriseOID	char(64)
	enterpriseName	char(50)
eventOwners	ownerID	int
	ownerName	char(80)
events	enterpriseOID	char(64)
	generic	int
	specific	int
	node	char(60)
	description	char(60)
	source	int
	severity	int
	category	int
	time	timestamp
	hasNote	boolean
	eventID	int
	ownerID	int

moreDescription	eventID	int, dups ok
	moreDescription	char(255)
	id	int
Notes	eventID	int
	theNote	char(255)
trapNames	enterpriseOID	char(64)
	specific	int
	generic	int
	enterpriseName	char(50)
	specificName	char(20)

Schema for snmpCollect

The following table describes the schema for snmpCollect, including Availability:

Table	Field	Type
mibLookup	mibID	int
	mibName	char(80)
SnmpcollectData	mibObject	int
	instance	int
	ipAddress	int
	startTime	int
	endTime	int
	value	double
	stationID	int
	theKey	int

SnmpcollectStation	stationID	int
	station	char(60)
uptimeSummaryTable	dbKey	int
	nodeName	char(60)
	ipaddress	int
	stateStartTime	datetime
uptimeTransitionTable	ipAddress	int
	upOrDown	int
	timeStart	datetime
	timeStop	datetime
	id	int

Schema for Topology

The following table describes the schema for topology (**topo2sql.exe** dump utility):

Table	Field	Type
Networks	objectID	int
	IPAddress	char(30)
	status	char(16)
Nodes	objectID	int
	objectID2	int
	Name	char(50)
	status	char(16)
	IPAddress	char(30)
	MACAddress	char(20)

Segments	objectID	int
	IPAddress	char(30)
	status	char(16)

New Features in Version 5.0a

This section describes the new features in this release.

Installation

Installation has the following new features:

- Alpha machines no longer require MS SQL Server. If SQL Server is not installed, the installation will install the MS Jet engine (MS Access) as it does on Intel machines.

- Setup removes previous snmpodump scheduled jobs. Previously, entering the **at** command at the command prompt would show obsolete scheduled job entries after new installations.

- The **ovw_verify** command runs to check registration files during installation.

- Migrating from a NetView for Windows NT Version 5.0 system is now supported. To migrate the ovw object database, the SQL database, and customizations, select **Upgrade**.

Migration

The format of the object database and the schema of the snmpCollect_db was changed for V5.0a requiring a migration to preserve the existing V5.0 databases.

When you select **No** to the prompt to **Delete all existing NetView files, settings, and databases?** in the **Overwrite the Current Installation** dialog, note the following:

- The installation migrates the existing object (ovw) databases, if necessary

■ The installation preserves your configuration changes to files in the following directories:

- \usr\ov\conf\

- \usr\ov\lrf\

    Note: The new shipped versions can be found under \usr\ov\newconfig.

- trapd.conf

    A set of Cisco trap definitions have been added to trapd.conf. However, if you do an Upgrade install, your existing trapd.conf will be preserved instead. To prevent this, copy the file located in \usr\ov\newconfig\ovsnmp-run\trapd.conf to \usr\ov\conf\trapd.conf and restart the daemons.

- snmpcol.lrf

    If you are migrating there is one manual task you should do. The snmpCollect daemon depends on nvcold, and this dependence was added to snmpcol.lrf. If you migrated, you should go to the snmpCollect daemon page in Server Setup, make an innocuous change to trigger a save, and exit. This will update the file and ensure that snmpCollect has the dependency.

Discovery and Status Polling

Discovery and status polling have the following new features:

■ The netmon daemon supports a new discovery option for seed file entries only. This limits discovery to entries in the **netmon.seed** file.

■ The netmon daemon can handle more interfaces per machine. The previous limit of 16 was increased to a default of 64. You can change this limit in the registry variable MaxIfaces at HKEY_LOCAL_MACHINE\SOFTWARE\Tivoli\TME 10 NetView\CurrentVersion.

- The netmon daemon now allows seed file entries not to communicate with SNMP. Previously, netmon would issue messages if it could not get SNMP responses from IP addresses in the seed file.

- Support is included for IP names as negative netmon seed entries.

- The netmon daemon can detect ifTypes that are out of range and set to them to "other".

- You can change netmon's ping timeout values on the netmon setup page.

- You can schedule off periods for polling. See "Scheduling Off Periods For Polling" on page 20 for information on how to do this.

- You can now dump netmon's network (region) list in netmon's trace file (\usr\ov\log\netmon.trace) using the **event -b openview -e NMAC_EV -a 14** command. You can also now dump MLM Node List and MLM NetList and MLM-related nodes and interfaces using the above syntax for the **event** command, but specify 29, 30, 31, or 32 with the **-a** flag.

Forcing Discovery of a Node When Ping Spray Is Enabled

To force a new node poll of a specific node, select the node and select the **Test --> Ping** menu option to ping the selected node. Select the node that NetView is running on (for example, your node), and then select the **Test --> Demand Poll** menu option. This forces the netmon daemon to query its own (updated) ARP cache looking for hints about other nodes in the subnet where the selected node was pinged.

However, if netmon is configured to use Ping Spray, the ARP cache will not be queried on non-routing nodes during a demand poll. To use this method you must disable netmon's use of Ping Spray. To do this, select **Options --> Server Setup --> Daemons --> Netmon Daemon**, and change the setting for "Discovery Using Ping Spray" from "Yes" to either "Only Initially" or to "No". When asked to Stop

or Restart netmon, click the **Yes** button, and repeat the steps outlined in the previous paragraph.

Scheduling Off Periods For Polling

You can now enable weekly off periods for status, configuration, and discovery polling. For example, you might not care about polling over the weekend for certain subnets or ranges of nodes. To schedule off periods for polling, select **Options --> Polling...**. On the Polling Options dialog, enable Polling Off Periods and click on the **Edit** button to edit the default file, **\usr\ov\conf\offperiods.conf**. The format of this file is as follows:

```
<IPaddress> <StartDay> <StartTime> <EndDay> <EndTime> <PollTypes>
```

Where:

IPaddress Specifies the IP address, expressed in numerical dot notation, of the node or nodes that you do not want to poll. You can use IP address ranges and a wildcard character (*) to specify multiple nodes.

StartDay Specifies the day of the week that you want to start the polling off period. Specify the day by the first three letters, such as Sun, Mon, Tue, and so on. This field is not case sensitive.

StartTime Specifies the time of day that you want to start the polling off period. Specify the time in 24 hour time (colon separated).

EndDay Specifies the day of the week that you want to end the off period. Specify the day as described for StartDay.

EndTime Specifies the time of day that you want to end the polling off period. Specify the time as described for StartTime.

PollTypes Specifies the poll types that you want to turn off. Enter one or more of the following: p, c, d to specify ping, configuration, and discovery, respectively.

For example, you would add entries in the
\usr\ov\conf\offperiods.conf file similar to the following:

```
16.21.144.140 Fri 23:00 Mon 6:00 pcd
16.21.[140-150].* Fri 23:00 Mon 6:00 pcd
```

After editing the **\usr\ov\conf\offperiods.conf** file, click on **Apply** or
OK on the Polling Options dialog. The changes take effect
immediately without stopping the daemons.

SNMP Data Collection

SNMP data collection has the following new features:

- Improved Data dialog

  The Data dialog in the MIB Data Collector has been replaced
  with an easier-to-use, faster dialog. The new dialog matches the
  Collected Data page of the Object Properties dialog. Filtering by
  Time, MIB, and Instance is now available. Automatic updating
  of the data is no longer available but current data can be
  obtained at any time by clicking **Apply**.

- SmartSets

  In the MIB Data Collector it is now easier to specify that data is
  to be collected from a SmartSet. After selecting **New** from the
  main window you still choose the MIB Object ID or the MIB
  Expression in Collection Wizard: Step 1, but in Collection
  Wizard: Step 2 you now have a new pair of radio buttons that
  let you choose whether to collect on a SmartSet or a set of
  nodes. If you choose to collect on a SmartSet, the set of
  SmartSets is presented for you to choose from.

- Additional conditions for threshold and rearm values

  Prior to this release, the default condition was restricted to
  greater than (>) for threshold and less than or equal to <= for
  rearm. That is, if the MIB value is greater than the threshold
  value, the threshold is triggered and a trap is generated. No
  more traps are generated until the MIB value is less than or
  equal to the rearm value. Then a rearm trap is generated.

You can now specify any of the following conditions for the threshold and rearm events using the **Tools --> MIB --> Collect Data** option or the **setthresh** command:

`=, !=, >, >=, <, <=, changed, notchanged`

Each of the first six conditions (=, !=, >, >=, <, <=) operate in a similar way to the default condition with respect to the threshold and rearm values. The last two conditions (changed and notchanged) simply check the previous MIB value that was obtained and check whether the new value is the same or has changed. The threshold and rearm values are ignored in this case.

The following table lists each threshold condition and the corresponding condition for rearm.

Threshold	Rearm
=	!=
!=	=
>	<=
<	>=
changed	notchanged
notchanged	changed

The following two flags have been added to the **setthresh** command to specify the threshold and rearm conditions:

Flag   **Purpose**

-a threshold_condition

        Specifies the threshold condition.

        Where *thresholdCondition* can be one of the following values:

        `=, !=, >, >=, <, <=, CHANGED, NOTCHANGED`

The new syntax for the **setthresh** command is as follows:

```
setthresh T [-o objectIdName]
            [-i instanceNum]
            [-s SuspendRes]
            [-n sourceName]
            [-c collectType]
            [-m collectionMode]
            [-p pollingInterval]
            [-v thresholdVal]
            [-r rearm Val]
            [-t thresholdType]
            [-a thresholdCondition]
```

SmartSets

SmartSets have the following new features:

- By default, SmartSet submaps are populated upon creation. Previously, the SmartSet symbols would be blue until you activated them by double-clicking, at which point they would be populated. This behavior can be turned off in the registry.

- Previously, some of the symbols within SmartSet submaps were missing their inner shapes, but this has been corrected.

- Three new SmartSets have been added:

    BadMasks Contain all symbols that netmon flags as having an inconsistent subnet mask

    BadOIDs Contains all symbols that have a sysObjectID that is unrecognized

    MLMs Contain all discovered Mid-Level Managers

- A new category for existing SmartSets has been added on the Find Simple tab page. Select **Find By Other Properties** and click **Other**. To modify the selection available in the combo boxes for Type and Other, edit the **\usr\ov\conf\finddialog.conf** file.

    Both of these comboboxes are used to find objects with particular Boolean attributes set (for example, "isComputer", "isWorkstation", "isMailServer"). The finddialog.conf file allows the user to say that, for example, an item named "Workstation"

---

should appear in one of these two comboboxes and the ovwdb Boolean field "isWorkstation" should be used for matching purposes when this item is selected.

There is no fundamental difference between the contents of the two comboboxes. By default, the product ships with the "Type" combobox filled with attributes that are associated with objects of a particular type and the "Other" combobox filled with attributes that are associated with the default SmartSets. This is under the user's control, however, as the user can change the entries that appear in either combobox by editing \usr\ov\conf\finddialog.conf and restarting the NetView Console.

How to Create New SmartSets

You can group objects together into SmartSets. Start by using the **Find** command to search for a common property. Then press the **Create SmartSet** button. This creates a SmartSet based on the results of the **Find** command. For more information, select **Help --> Help Topics**. In the Contents tab, click on **Working with Objects** and **MIBS --> Working with SmartSets** for a list of topics about SmartSets. You can also click on the Index tab. Then search for SmartSets.

Event Browser

If you create a new filter setting and Save that setting, the name you give to that file appears in the filter drop-down list on the Event Browser toolbar.

NetView Console

The NetView Console has the following new features:

- Client applications can now check if the NetView share is mounted.

- You can now print zoomed submaps.

- When you invoke the Summary Report application (**Tools --> Summary Report**) and choose Statistics and Nodes to Monitor, the settings are saved and restored for you each time you invoke

the Summary Report application. Settings in the Options dialog are also saved and restored.

- The SNMP community name is now displayed on the Object Properties General tab page.

- A new Availability tab page has been added to the Object Properties dialog.

Client/Server

You can now restrict client access to be read-only for specific users and machines. From the Server Setup Client/Server page, click **Edit Permissions** and add entries for each combination of user and machine name for which you want to limit to read-only access.

Availability Tracking

NetView now keeps track of when nodes go up and down and records these transactions in the ODBC database. You can view this data, along with statistics, such as MeanTimeBetweenFailures, in the following three ways:

- The new page in the Object Properties dialog.

- The **uptimer.exe** command line utility. This can be used to dump the availability tracking data.

- The Visual Basic program sample, Availability, located in \usr\ov\prg_samples\availability. This program sample contains both the source code for the application and a separate setup program to install all files needed to run the compiled Visual Basic application.

    Note: This program sample works only on Intel platforms and Microsoft Access databases. The program sample has not been tested with Alpha or with Microsoft SQL Server.

Paging Support

NetView's paging support consists of two parts: a program to submit a pager request and a daemon that processes pager requests by dialing a paging carrier and transmitting the page.

The **nvpage** command can be used to submit a page to the system-wide pager request queue. The system-wide pager request queue is maintained by the nvpagerd daemon. nvpagerd is run on the system that has telephony hardware installed and the Windows NT telephony settings have been established to use the telephony hardware.

You can now configure an event to issue a call to a pager when the event is received. To do this, select **Options --> Trap Settings** and enter the **nvpage** command as an executable command in the Trap Settings dialog. See the **\usr\ov\doc\pager.readme** file for complete details.

Regional Manager Support

NetView for Windows NT can now act as a Regional Manager to offload discovery and status polling (ping) to specific subnets, or segments within subnets by working with Mid-Level Managers (MLMs) installed on the network. The following sections describe how NetView for Windows NT works with MLMs.

It is recommended that you not run the MLM on the same node as NetView to avoid conflicts with their respective event subsystems.

Polling

The netmon daemon will not discover nodes using SNMP or ping sprays nor status poll nodes in a region that is specified to be managed by an MLM. Instead, the MLM performs discovery and status polling and conveys the information to NetView using the following TME 10 MLM enterprise traps: MLM_NewNodes, MLM_StatusDown, and MLM_StatusUp.

The netmon daemon periodically polls the MLM nodes for their Discovery table as defined in the Mid-Level Manager for Windows NT MIB Definition, which is located in the **\usr\ov\snmp_mibs\mlm.mib** file. No SNMP requests for ARP Table

information or Routing Table information are made to the MLM node unless the MLM node has interfaces to other networks. The netmon daemon stills polls nodes in regions that are managed by MLM nodes for configuration data using SNMP to accurately represent the MLM-managed nodes on the map.

Subnet Masks

The subnet mask of the MLM node is needed to accurately define the region being managed by the MLM node. An assumption made by the netmon daemon is that all nodes within a subnet being managed by an MLM node will have the same subnet mask as the MLM node itself. Hints about nodes in a subnet managed by an MLM node that do not have a matching subnet mask will be ignored. Note that nodes with inconsistent subnet masks are logged in the **\usr\ov\log\badmasks.log** file (if enabled), and that Inconsistent Subnet Mask events are logged in the Event Browser. If the node is successfully added to the topology (for example, its subnet mask is at least well formed), then the BadMasks SmartSet should contain such nodes as well.

Map Operations

It is recommended that regions being managed by MLM nodes *not* be unmanaged then managed, as the map status of such nodes may remain UNKNOWN for extended periods of time, leading to confusion. This is because netmon does not status poll the MLM-managed nodes and the MLM only sends status events when status changes. To force netmon to update nodes, select the **Test --> Demand Poll** or **Test --> Ping** operations. The netmon daemon ignores the manage and unmanage actions on nodes in MLM-managed regions.

The **Object --> Discover** option has no affect on subnets being managed by an MLM node.

SmartSets

When netmon is instructed to recognize nodes running MLMs, it will set the "isMLM" field for those nodes in the ovw object database. Such nodes will then appear in the new MLMs SmartSet.

How to Enable NetView as Regional Manager

See the Mid-Level Manager for UNIX or Windows NT documentation on how to setup the MLM to forward traps to the Regional Manager running NetView for Windows NT.

To activate netmon as a Regional Manager:

1. Select **Tools --> MIB --> Load** and load the **mlm.mib** file.

2. Select **Options --> Server Setup --> Daemons --> netmon page** to enable MLM support.

    The netmon daemon can learn about the nodes running MLM from an MLM nodes seed file or by recognizing traps received from MLMs or both.

    If you select the MLM nodes seed file method, edit the MLM seed file and enter the IP addresses of the nodes running the MLM you are interested in.

After netmon is instructed to recognize MLM nodes, netmon assumes the role of Regional Manager. If netmon is not instructed to recognize MLM nodes, then netmon discontinues its role as a Regional Manager, even if MLM nodes exist in the topology. When netmon is not acting as a Regional Manager, nodes that had been managed by an MLM node will now be actively managed by netmon, and netmon resumes discovery and status polling.

addtrap Utility

The following additions have been added to the addtrap utility.

■   A switch (-d) has been added to indicate the display type of the application specified (if any) for the **action** command.

■   Error reporting is now more helpful when incorrect syntax is used. The correct syntax is:

```
addtrap.exe -n enterprise-name
-l trap-label
-i ent-object-id
-g gen-trap
-s spec-trap
-o source-ID
-S severity-flag
-t status-type
-c category
-f cmd-flag
-F format-specification
[if cmd-flag is '!'
                [-C command]
                [-A argument] ]
                [-d hidden|console|windows]
```

If arguments contain space, use double quotation marks.

SNMP Options Dialog

The SNMP Properties dialog box for specific Nodes now accepts a list of nodes from the following three sources:

- A comma-separated list in the Name or IP Address box

- By clicking the **Get Selected From Map** button

- By checking the **Use SmartSets** checkbox and selecting a SmartSet from the drop-down list

Web Interface

TME 10 NetView Web Interface For Windows NT can be installed after intalling NetView on an NT server. This product provides a dynamic Web interface to the maps, objects, and events as well as diagnostic network tools.

The Web Interface is a separate product contained in the self-extracting executable, **nvwebkit.exe**, which is located in the same directory as the NetView For NT kit. Refer to the separate readme file for information about this product.

NVDBTools

Three tools have been added to modify and query NetView's object database from the command line in order to vastly reduce the effort to customize the database and produce reports. It also allows integration with TME 10 Inventory to collect and retain hardware and software information across the enterprise.

Each utility is in \usr\ov\bin. For more details on each of these tools, see the respective Readme files in \usr\ov\doc.

NVDBImport.exe

This utility can be used to import object field values into the NetView object database from a file. For example, if you want to set a new field called **isSite2** to **TRUE** for the list of nodes at Site 2 and create a SmartSet for them, perform the following steps:

1.   Create a file with the list of nodes.

2.   Create the field **isSite2** with the value **TRUE**.

3.   Run the NVDBImport.exe utility to update the database.

If you need to recreate the database, you can quickly restore your customization. If you already have a customized database, use NVDBFormat to generate this file for you.

Several sample template files are included.

NVDBExport.exe

This utility exports the NetView object database into an SQL database for either Microsoft Access or Microsoft SQL Server. You can either export the entire database into a set of tables, or use the configuration file to customize the table formats and populate them with entries based on rules. For example, you can create a table containing just the critical nodes and relevant fields, such as IP Hostname and sysContact. Then use an SQL report writer to generate reports.

NVDBFormat.exe

This utility can be used to generate custom text or HTML reports on NetView's object database complete with header and footers including some aggregate information. It can also generate a file of your customizations that subsequently can be used by NVDBImport to update a new database.

Several sample template files are included.

NVDBToMIF.exe

The purpose of this tool is to integrate the power of NetView's network awareness with the scope of TME 10 Inventory's ability to collect and retain hardware and software information across an enterprise.

This tool exports the object database fields for a specific object in the NetView database or for all objects. It then creates three files in the user's indicated output directory.

- netview_export.mif

- netview_<DBTYPE>_createtables.sql

- netview_<DBTYPE>_createviews.sql

The SQL files can be used by a TME 10 Inventory user to prepare tables and views within Inventory's RDBMS. These tables will be used to store the data that is presented in the netview_export.mif file. See the Desktop Management Interface specification for more information on the syntax and content of MIF files.

Wake on LAN

This tool can be used to wake up machines that are compliant with the "Magic Packet" specification for wake-up nodes. This includes special software and hardware on the target platform. This feature is not available on the Alpha platform in this release.

You can run this tool either by selecting **Tools --> Wired for Mgt -->Wake-Up** from the NetView Console or from the command line.

Desktop Management Interface

Desktop Management Interface (DMI) is a technology by which PCs can be more manageable by providing extensive information on their hardware and software resources. This feature is not available on the Alpha platform in this release.

From the NetView Console, select **Tools --> DMI...** to:

- Dynamically query DMI nodes for DMI information relative to specific groups with the Baseline Wired for Management specification.

- Dynamically query DMI nodes for specific group information and then store that information within the native NetView object database. This information can be used to diagnose a machine that is in a down state.

Application for Finding Network Services

A new application has been supplied with this NetView release that detects which TCP-related services exist on IP nodes. This application, nvsniffer.exe, is set up by the installation process as a Scheduler 'at' job to be run nightly.

nvsniffer uses a configuration file to determine which TCP service to query and as a result will automatically define new fields for objects and include them in existing or new SmartSets. For more details, see **\usr\ov\doc\nvsniffer.readme**.

Miscellaneous New Features

The following miscellaneous new features have been added:

- Servers now have isNode capability.

- The number of extraneous messages written in the **nv.log** file is reduced.

- A set of Cisco trap definitions have been added to trapd.conf. However, if you do an Upgrade install, your existing trapd.conf will be preserved instead. To prevent this, copy the file located in **\usr\ov\newconfig\ovsnmp-run\trapd.conf** to **\usr\ov\conf\trapd.conf** and restart the daemons.

- Three new fields have been added to the object database:

  - isMLM

  - hasBadOid

  - hasInconsistentSubnetMask

New Features in Version 5.0

This section describes the new features in Version 5.0.

NetView Console

Several new features have been added to make the Console more useful. These include:

- Submap Sorting

  Select **Submap --> Sort by..** to see a list of object properties that can be used to sort the symbols. For example, Label, IP Address, Status and many others. This can be useful to quickly find a particular node or see holes in the IP address ranges.

- Dynamic Property Tips for each symbol

  See "Dynamic Property Tips and the tips.conf File" on page 43.

- Hide symbols matching a particular status color.

  Click on the palette of status colors on the Tool Bar to hide all the symbols of that status color. Click again to redisplay them.

- The submap zoom factor has been increased to 15X.

- The Navigation Tree Layout is preserved between sessions if you select **Console Settings --> Open the last set of Submaps**.

New Object Property Pages

Two new tab pages have been added to the Object Properties dialog:

Events   Displays events for that node in the same format as the Event Browser

Data Collection Displays SNMP collected data for that node

NetView Map Enhancements

Ring Submaps

Ring submaps now display as buses. To display these submaps as rings rather than buses, change the DisplayRingSubmapAsBus key in the registry file to 0. This key is in **HKEY_CURRENT_USER --> Software --> Tivoli --> TME 10 NetView --> CurrentVersion**.

Changing the Status Color of an Object

The **nvstatustrap.bat** batch file is included in the **\usr\ov\bin** directory to help you set up events to change the status (and color) of an object in a submap. You can use the batch file on the command line to change an object's status and as a template for other uses. The **nvstatustrap.bat** batch file uses the following three parameters:

- Status (Up, Down, Normal, Unknown, Marginal, Critical, User1, User2)

- Object name of the target

- IP name of your node (management station)

If you are unsure about the Object name, display Object Properties for the object, select the General tab page, and look at the Object Name field.

Some objects, such as Locations and Segments, have their status set by default to be **Propagated from Children**. Display the Object Properties on the Symbol tab page to check the values. Such objects cannot have their status changed using the above procedure. However, if you change the status to **Set for this Symbol Only**, this procedure works.

Status Propagation for Nodes With Multiple Interfaces

If a node, such as a router, has multiple interfaces and one interface is down (critical), then the node appears red inside the subnet and segment where the critical interface resides. The node appears green in all other subnets and segments where the node's interfaces are up (normal). The node appears yellow (marginal) at the IP Internet level, where the compound status of the node is displayed. Red, green, and yellow are the NetView default colors for status.

Time Synchronization Between NetView Server and Clients

NetView attempts to keep the system time of the clients and server in synchronization. This is important for maintaining the propagated map actions, such as manage, unmanage, acknowledge, and unacknowledge on each client's map.

Be default, the time is checked when the NetView Console starts up and every hour after that. You can change when NetView checks the time by setting the following system variable in the System dialog on the Control Panel:

```
TIMESYNC_INTERVAL=3600          (seconds)
```

By default, the tolerance is 1 second. You can change this by setting the following system variable:

```
TIMESYNC_VARIANCE=1             (seconds)
```

Client/Server Map Propagation

The client/server model for the maps consists of a centralized object and topology database, but a localized map database. This means that you can expect all maps to share object and topology properties including object status and configuration attributes. Because the map database is localized, you can customize each client map differently. A set of key map operations are propagated to all maps:

- Manage
- Unmanage
- Acknowledge
- Unacknowledge
- Adding nodes
- Deleting nodes

Only the propagation of adding and deleting nodes is supported. Use the **getservermap.bat** utility to manually distribute customized maps.

If you enter Dynamic Host Configuration Program (DHCP) IP address ranges in the **netmon.seed** file and select the default to show non-responding DHCP clients as the User1 color, instead of Critical, please note the following restriction for this release. When a DHCP client does not respond to status polling, the symbol status changes to User1. However, when you exit the NetView console and restart it, the status of these symbols is displayed with the Critical color.

Software Development Kit

All NetView APIs except XOM/XMP are included in this release.

You should be aware of the following restrictions:

- If you run a third party application and it returns an OVwInit error, there might be old DLLs in the system32 area and the third party application is not being run from the **\usr\ov\bin** directory, where newer copies of these DLLs are located. One way to determine if this is the problem is to move the third party executable to the **\usr\ov\bin** directory and run the application from there. The DLLs in question are:

  - **dtbl32.dll**
  - **icmp.dll**
  - **mfc30.dll**
  - **msvcrt20.dll**
  - **muscrl32.dll**
  - **ntserv.dll**
  - **nutc.dll**
  - **socket.dll**
  - **tcldll.dll**
  - **wct32d.dll**
  - **wrt32d.dll**

- The routine OVSelect() is provided in the SNMP API library to use while waiting for socket data from sockets opened using the OVsnmpOpen() routine. This routine must be used instead of the WinSocket select() call. The interface arguments for

OVSelect() are the same as those in the WinSocket select() routine. The function prototype can be found in the **\usr\ov\include\ov\ovsnmpapi.h** header file.

- Asynchronous creation of Open Topology objects is not functional for this release. To create objects using the NetView Open Topology (nvot) API, you must first enable synchronous creation using the nvotSetSynchronousCreation() call. Refer to the *NetView for Windows NT Programmer's Reference* for more information.

- If you have a third party application that dynamically loads one or more of the NetView DLLs from within a third party DLL, you might experience run-time memory management problems with the SmartHeap DLL (**sh32w32.dll**) that is shipped with the NetView kit. The **sh32w32.dll** file provides memory management capabilities (for example, maloc, new, free, delete) to the NetView components. To avoid memory management problems, make sure that your application and/or DLLs are set up to be multi-threaded for DLLs. Using Microsoft Visual C++, select Project Settings, and set the C/C++ Code Generation settings for the **Use Run-Time Library** item to be **Multithreaded using DLL**.

- If your application uses SmartHeap dynamic link libraries, we recommend that you use the same version of SmartHeap (V3.2) used by the NetView components. If you do not use SmartHeap V3.2, results may be unpredictable.

TME 10 Enterprise Console Integration

This section describes the steps to install and configure the TME 10 Enterprise Console Event Adapter (TEC Adapter) for TME 10 NetView.

1. Decide which version of the TEC Adapter you will use: the TME or non-TME version. If your Windows NT machine has the TME 10 Framework installed, then follow the steps labeled for TME. If the TME 10 Framework is not installed, follow the steps labeled for non-TME. If you are not sure if the TME 10 Framework is installed, check for the subdirectory

              \Tivoli\bin\w32–ix86\TME. If this subdirectory exists, the TME 10 Framework is installed.

2. Copy the appropriate executable from the **\usr\ov\bin** directory:

For...	Enter...
TME	copy tecad_nv6k_tme.exe tecad_nv6k.exe
non-TME	copy tecad_nv6k_non_tme.exe tecad_nv6k.exe

3. Register with NetView by entering the following command in a command window:

    `ovaddobj \usr\ov\lrf\tecad_nv6k.lrf`

4. Identify the event server to be used by editing the **\usr\ov\conf\tecad_nv6k.conf** file.

For...	The ServerLocation entry format is...
TME	ServerLocation@Event Server
non-TME	ServerLocation=\<hostname\>, where \<hostname\> is the name of the host running the TEC. Also, specify the SeverPort entry for non-TME in the following format:

                          `ServerPort=<number>`

                          Where \<number\> is the port number used by the TEC event server to listen for events. Specify 0 (zero) if the TEC event server is using portmapper. (This is typically the case.)

5. The TEC Adapter uses the following files on a NetView server:

File	Description
tecad_nv6k.exe	Is the executable.
tecad_nv6k.conf	Is the global configuration file.
tecad_nv6k.err	Contains the tracing options.
tecad_nv6k.cds	Contains event class mapping specifications.

tecad_nv6k.lrf	Is the NetView registration file.
tecad_nv6k.oid	Contains the mapping of SNMP object identifiers to names.

You can modify these files to add or remove events sent to the event server.

6. Customize the TEC to understand NetView events. Perform these steps on your TEC server. Refer to the TEC documentation for more information.

   a. Copy the following files in the **\usr\ov\conf** directory to the system running the TEC:

   - **tecad_snmp.baroc**
   - **tecad_nv6k.baroc**
   - **tecad_ov.baroc**
   - **ov_default.rls**

   b. If you do not have a default rule base for your environment, create one with the following command:

   ```
   wcrtrb -d <directory> My_rb
   ```

   c. Copy the TEC-supplied default rule base (named Default) into your rule base. Enter the following command:

   ```
   wcprb -cr -f Default My_rb
   ```

   d. Import the event classes into the rule base you will be using. Enter the following sequence of commands:

   ```
   wimprbclass tecad_snmp.baroc My_rb
   wimprbclass tecad_ov.baroc My_rb
   wimprbclass tecad_nv6k.baroc My_rb
   ```

   e. Import the rules into the rule base. Enter the following command:

   ```
   wimprbrules ov_default.rls My_rb
   ```

   f. Compile the rule base. Enter the following command:

   ```
   wcomprules My_rb
   ```

g. Restart the event server to load the new rule base. Enter the following sequence of commands:

```
wstopesvr
wloadrb My_rb
wstartesvr
```

7. For TME users only, complete these steps:

a. Add the relative $BINDIR\bin path to the NT system environment, run:

```
winnt\system32\drivers\etc\Tivoli\setup_env
```

Then enter the following commands:

```
bash
echo $BINDIR
```

Set the path in the System dialog from the Control Panel.

b. Reboot the machine.

c. On the TMR Server, create an Administrator with the Label, User Login Name, and Group Name of NetView (assuming NetView is the name of the account the user logs in under). Edit logins to include:

```
NetView@hostname_of_machine_running_Netview_Server
```

Set the Resource Roles for Event Server to have User privileges.

8. Start the event adapter and test. If TME 10 NetView has been restarted, the event adapter is started automatically. Otherwise, start the event adapter by entering the following command:

```
ovstart tecad_nv6k
```

Send a sample node down event for a host of your choice:

```
event -e NDWN_EV -h <hostname>
```

A node down event is displayed in the TEC Events Display. If an event does not display, check the following:

- ■ That the event server is identified properly in the
  \usr\ov\conf\tecad_nv6k.conf file

- ■ That the TEC Event Server processed the event classes and
  rules successfully

Table Printing Support

You can print tables in dialog boxes by pressing the **Ctrl-P** key
combination. For example, you can print the Locate Route table from
a **Test --> Locate Route** command or the IP Services table from a
Monitor --> Network --> IP Services command. The output may be
out of alignment.

Trap Forwarder

You can forward traps from one management station to another. For
example, you might have a centralized management station that
manages networks for the entire division and management stations at
each site for specific locations. The management stations at the
individual sites can forward traps to the centralized management
station.

The **trapfrwd** daemon forwards traps from one management station
to another. The **trapfrwd** daemon uses the **trapfrwd.conf** file to
determine where to send traps and what traps to send. The NetView
program supplies a **trapfrwd.conf** file for you to edit. In this file,
type the host names of the management stations to send traps
between the [Hosts] and [End Hosts] tags. For example:

```
[Hosts]
mgtsys1
mgtsys2
[End Hosts]
```

Then, type the trap numbers (the trap numbers are from the
trapd.conf file) between the [Traps] and [End Traps] tags. For
example:

```
[Traps]
591790
589824
[End Traps]
```

To add a comment in the **trapdfrwd.conf** file, precede the line with a pound sign (#). For example:

```
[Hosts]
#Central Management station is
bigmgt
[End Hosts]
```

After you configure hosts and traps in the **trapfrwd.conf** file, you can run the **trapfrwd** daemon from a command window. To run the **trapfrwd** daemon, enter the following command sequence from a command window:

```
ovaddobj \usr\ov\lrf\trapfrwd.lrf
ovstart trapfrwd
```

SmartSets for Business Functions

The NetView program supplies three predefined SmartSets that you can use to group objects together by any business function that is important to you. These three predefined SmartSets are BusinessSet1, BusinessSet2, and BusinessSet3. For example, you might want to group all order entry systems together in BusinessSet1, all billing systems in BusinessSet2, and all payroll systems in BusinessSet3.

To group systems into one of these SmartSets:

1. Select the object on the submap.
2. Select **Object --> Properties**.
3. Click on the Other tab. Then select **LANMAN** from the drop-down list.
4. Click on the Business Set you are creating (isBusinessSet1, isBusinessSet2, or isBusinessSet3.)
5. Click the **Verify** button to check your selection.
6. Click **OK**.

Dynamic Property Tips and the tips.conf File

The NetView program provides static and dynamic property tips. A property tip is a snippet of information that is displayed when you pass the cursor over a symbol in the submap. Dynamic properties are identified with an asterisk (*) in the property tips drop-down list. Dynamic property tips are specified in the **\usr\ov\conf\tips.conf** file and are potentially very slow, because they use SNMP requests to gather the information to display and they block waiting for the response.

Dynamic property tips are specified with an entry in the **\usr\ov\conf\tips.conf** file. Each entry consists of the following two fields, separated by an equal sign (=):

- The name of the property tip
- The MIB object ID whose value is to be displayed as the property tip.

  The MIB object ID must be prefaced with the word MIB. You type a MIB object ID using its numeric value or English name. For example:

  ```
  SNMP In Packets = MIB
  .iso.org.dod.internet.mgmt.mi-2.snmp.snmpInPkts
  ```

Other formatting considerations are:

- Use the pound sign (#) at the beginning of each line for comment entries.

- Use a backslash (\) to extend a property tip entry beyond one physical line.

- Blank lines are permitted.

- All text in this file is case sensitive.

The nvservice Command

The **nvservice** command enables you to manage the NetView
Service. The NetView Service runs the NetView daemons at system
startup and across login sessions. The recommended method to
manage the NetView Service (check the status, start, and stop the
NetView Service) is to use Server Setup. However, you can also use
the **nvservice** command in the following format:

```
nvservice [options]
```

Where *options* are:

Option   Meaning

-install   Installs the service.

-remove   Removes the service.

-debug <parameters>

Runs the NetView Service as a console application for
debugging. For now use -debug with no parameters to
display a "gotit" message informing you of the progress.

-abort   Exits the NetView Service without first stopping daemons.

-stop   Stops the daemons and exits the NetView Service.

-cmd <command>

Creates the specified process. Avoid using this command.
This command creates a process but cannot create
Windows if your process uses Windows. For example, if
you specify Notepad, Notepad runs but no Notepad
window appears.

-help   Lists all of the valid command line flags and their
meanings.

-status   Finds the status of the NetView Service.

-installed   Determines if the NetView Service is installed or not.

Submap Bookmarks

The **View --> Bookmark** option allows you to place a marker on a submap. To place a bookmark on a submap:

1. Go to the submap you want to mark.
2. Select **View --> Bookmark**.
3. In the Submap Bookmarks dialog, click on **Add** to create a bookmark.
4. Click on **Close**.

In the Submap Bookmarks dialog, you can also remove a marker and go to the submap. To go to a submap, double-click on the submap name or click on the name and then select **Open**.

IntelliMouse Horizontal Scrolling

In addition to the IntelliMouse features documented in the NetView help, you can scroll a zoomed submap horizontally. To do this, hold down the **Ctrl** and **Shift** keys while simultaneously scrolling the mousewheel. If you move the mousewheel up, the submap is moved to the left. If you move the mousewheel down, the submap is moved to the right. For more information on IntelliMouse, select **Help --> Help Topics --> Index tab**. In the Index tab, search for IntelliMouse.

Predefined Filters in the Event Browser

The Event Browser now supplies predefined filters. You can select a predefined filter from a drop-down list in the Event Browser toolbar. The predefined filters are:

All Events Displays all events except for those with the Log Only category.

Error Events Displays events with the Error category.

Threshold Events Displays events with the Threshold category.

Status Events Displays events with the Status category.

Configuration Events
Displays events with the Node Configuration category.

Application Alert Events
> Displays events with the Application Alert category.

Events with Owners
> Displays events with owners.

Events with Notes   Displays events with notes.

Custom Filter   Does not use a predefined filter.

When you select a filter, the Event Browser loads the predefined filter and refreshes the Event Browser to display the events that match the filter.

Network and Subnetwork Aliases

You can assign names and aliases to specific networks and subnetworks using the **%systemroot%\system32\drivers\etc\networks** file. Place an entry in the file for each network or subnetwork you want to assign an alias. Each entry in the file represents one network. When the NetView program discovers the network, the NetView program displays the network on the map using the name from this file as the label.

The format of the file is:

```
<network name> <network number> [aliases...][#<comment>]
```

For example:

```
HeadQtrs     284.122.107
campus       284.122.108
```

Defects Fixed in Release 5.0a

The following defects have been fixed since the 5.0 release of TME 10 NetView for Windows NT:

- Using Property tips on the Console no longer consumes 100% of the CPU.

- Event Browser:

- The In-progress box no longer steals the window focus.
- The Event Browser deletes ctt* ODBC files that appear in the TEMP directory.
- The Event Browser can filter events on the log-only category.
- When a new filter is loaded, existing sorts no longer remain active.
- A database query timeout was causing the Event Browser to restart. The timeout has been increased to 60 seconds and no longer causes a restart if it does occur.
- The Event Browser starts up significantly faster for really large databases.
- If the trapd daemon terminates, the Event Browser can continue displaying new events once trapd has been restarted. It no longer consumes all the CPU.

■ Server setup:

- The pmd page has been removed, the defaults have been fixed so that they are consistent, and the correct settings are displayed on the netmon page.

- Obsolete dependencies on the gtmd daemon have been removed.

- All the appropriate daemons are now restarted after settings are changed.

■ The netmon daemon:

- The exception when netmon encounters ifTypes out of the enumerated range (list) specified in the **\usr\ov\fields\c\snmp_fields** file no longer occurs.

- DHCP client node name not being updated when the IP address is reused by a new DHCP client has been fixed.

- For some bridges and hubs, netmon would generate many status events for each interface unnecessarily. This is now fixed.

■ Utilities:

- The **snmpodump** utility can now delete all odbc SNMP collected data.

- The **snmpodump** startup time has been improved considerably.

- The **getservermap.exe** utility can copy new maps from other machines.

- Sometimes the **Test --> Demand Poll** and **Test --> Ping** operations did not update the status of the node correctly. This has been fixed.

■ Other daemons:

- The Access Violation error in ovspmd logging code when PATH is very long has been fixed.

- The ovwdb daemon automatically expands the cache size when necessary.

■ Graphing

When you select **Tools --> MIB --> Graph Data All**, all instances for all MIBs that are in the Collected Data ODBC database are now graphed.

■ Trap Settings

- There is some confusion with the use of back slashes (\ ) in the box for the action command labeled, "Run this command when the trap is received".

  This line can contain an executable followed by zero, one, or more arguments. The treatment of back slashes is different for the executable filepath and the arguments.

  The executable must contain single backslashes only in the filepath, for example:

  \usr\ov\bin\nvecho

  The arguments themselves may contain escape sequences such as '\n' (new line) or '\xnn' (hexadecimal representation of an ASCII character). Therefore, if back slashes are used

in a filepath in an argument, they must be doubled. For example

\usr\ov\bin\nvecho "$3 was received for $2\nSee \\users\\readme"

Note: The character after a variable ($2) is not deleted.

■   SmartSets

•   Previously, SmartSets used case-sensitive matches for text. This is now changed to case-insensitive to act similarly to the mechanism used by the Simple Find.

Known Defects in Release 5.0a

This section describes known defects in this release of TME 10 NetView for Windows NT. Where applicable and known, suggested work-arounds are identified. The defects are listed by category. Note that this might not be a complete list of defects.

Internationalization

Certain locale-specific differences may cause some NetView applications or daemons to fail, logging the failures in the **nv.log** file similar to:

```
<date> <time> [netmon] OVsInitComplete Failed: exiting
```

If the **nv.log** file contains entries similar to this, we recommend using the English (United States) locale setting. To determine your machine's locale setting, select **Start --> Settings --> Control Panel --> Regional Settings --> Input Locales**.

To add the English (United States) input locale, select the **Add** button and select English (Unites States) from the combo box. To remove your existing input locale setting, select the **Remove** button.

Server File Share Error on Client

If you are running the NetView console on a NetView client and you receive the following message:

```
The server file share is not mounted. Mount it on drive X:
    using the NetView account password.
```

The file share for the NetView server is not mounted on the NetView client. To correct this situation, run Windows NT Explorer. Then select **Tools..Map Network Drive**. Complete the dialog box as follows:

1.   For the Drive, choose the drive letter specified in the message. (X is used here as an example.)

2.   For the Path, enter `\\myserver\NetView`, where `myserver` is the name of the machine running the NetView Server.

3.   Click **OK**.

4.   When prompted for the password, enter the password for the NetView account on the Server machine.

MIBs

The NetView program MIB types are supported by SMIv1, but not SMIv2.

NetView Service and Windows NT 4.0 Service Pack 2

The NetView program fails if you upgrade a Windows NT 4.0 system to Service Pack 2 while the NetView Service is running.

To work around this problem, stop the NetView Service before installing Windows NT Service Pack 2. The installation of the Service Pack asks you to reboot the system. After the reboot, the NetView Service starts as part of the system initialization, and the NetView program works as expected.

Enable/Disable Open Topology Daemon Batch Files

The **otenable.bat** file adds the gtmd and xxmd open topology daemons to the list of daemons to start in the **ovsuf** file. After these daemons are added to the **ovsuf** file, you can take advantage of the open topology features and NVOT APIs. The **otdisable.bat** file removes the gtmd and xxmd open topology daemons from the list of daemons to start in the **ovsuf** file.

System

■ If you run the NetView program from a Domain Account, NetView runs slower than if you run it from a local account. Domain Controller accounts have more traffic due to retrieving file and user information.

■ If you have errors on startup, check the **\usr\ov\log\nv.log** file for error information.

■ If you have a large database and netmon is slowing down, select **Options --> Server Setup --> Daemons --> Netmon** to turn off ping spray because the cached information may be exceeding its storage limits.

Pull-down Menus

In the Monitor dialog box, do not set the **Options --> Restart Every interval** to less than the amount of time it takes for the operation to complete.

Monitor --> System

For data to be returned from any of these nine menu options, the SNMP agent on the node being queried must have been extended to support the host resource MIB.

Test Menu

In the Test dialog box, do not set the **Options --> Restart Every interval** to less than the amount of time it takes for the operation to complete.

Test --> Demand Poll

Getting secondary addresses for Demand Poll may take several
minutes.

Tools --> MIB --> Tool Builder

- Tools based on Form format do not successfully retrieve SNMP
  table values.

- Tools based on Table format provide inconsistent results if the
  first variable is non-table (that is, single instance), such as
  ifNumber followed by any of the ifTable variables.

- Only variables from one MIB table can be displayed in any
  single Table format tool.

Tools --> MIB --> Browser

The Windows NT 3.51 SNMP agent allows only read access for the
sysContact, sysName, and Location objects. According to the Internet
MIB-II definition in RFC 1158, these SNMP objects should allow
read/write access. For more information, refer to the Microsoft
Support Knowledge Base article, "Windows NT SNMP Agent Allows
Only Read Access", article ID Q129129, revision date 10–APR-1996.

Tools --> MIB --> Load

For your convenience, we include many MIBs from other vendors;
however, we do not support them or guarantee their correctness.

Options --> Server Setup --> Databases --> Clear Databases

If you clear NetView databases and the ovtopmd daemon does not
start when the daemons are restarted, check the **\usr\ov\log\nv.log** for
error messages similar to the following:

```
08/27/97 11:46:54 [ovtopmd] FATAL ERROR: Could not
 map field IP Address into OVwFieldId

08/27/97 11:46:54 [ovtopmd] Error opening openview
 topology database: Could not get OVW field ID, try running
 ovw_fields.
```

If these messages are in your log file, open a Command Prompt window and enter the **ovw_fields** command. Upon completion, you should be able to start all daemons.

IP Name/IP Address Problems

If the management station's IP name and IP address as configured for TCP/IP and stored in the registry are different from the values stored in the local hosts file (**<SystemRoot>\system32\drivers\etc\hosts**), then the NetView program does not function properly. To avoid this situation, the NetView installation procedure updates the **<SystemRoot>\system32\drivers\etc\hosts** file with the management station's IP name and IP address from the TCP parameters stored in the registry if there is no entry present. In addition, the NetView ovwdb daemon checks that the host name and address stored in the registry are consistent with those stored in the hosts file. If the two views do not match, then the following warning message is displayed:

```
An IP Address mismatch between the hosts file and the
  registry has been detected.
```

This should be corrected as soon as possible; however, ovwdb continues so that the installation procedure can complete.

On startup, the netmon daemon also checks that the two views match. If they do not match, the following error message is displayed and netmon exits:

```
An IP Address mismatch between the hosts file and the registry
has been detected:
    hosts file:
    registry:
```

Discovery does not occur until this problem is fixed. This can cause serious problems. You must correct the hosts file and restart the netmon daemon before discovery can occur.

If you want to disable the display of these error boxes and prevent netmon from exiting, set the environment variable NV_NOIPCHECK =1. However, error messages are still written to the **nv.log** file and the problem persists. We strongly recommend fixing the problem.

Daemons

The ovwdb Daemon

On management stations that have very large databases (more than 7500 nodes), daemons may take a long time to start causing **ovstart** to report that ovwdb is not running. To fix this, open a command window and issue the follow sequence of commands:

```
ovstop
ovstart trapd
ovstart ovtopmd
ovstart
```

The trapd Daemon

The trapd daemon no longer logs events before purging them. Logging events before purging is now optional. To change this setting, select **Options --> Server Setup --> trapd**.

SMS

SMS running with the NetView program can result in a `File not found` error when you try to display the System Properties using the **Object Properties --> System Tab** option and then click on the **System Properties** button. If you receive the `File not found` error, the NetView program could not find the **machine.exe** file. The NetView program uses the Configuration Registry variable **HKEY_LOCAL_Machine\SOFTWARE\Microsoft\SMS\Setup\Installation** directory to find the SMS installation directory, for example `c:\sms`. If the variable is blank, you will receive the error. To specify the directory, run **regedt32.exe**, double-click on that value and enter the name of the installation directory manually.

Submap Printing Problems with non-True Type Fonts

Submap printing does not display label text if a non-True Type font is selected as the object label font. To change to a True Type font:

1. Select **Options --> Console Settings**.
2. Click on the **Object Label Font...** button.

3. Select a font from the list that has the True Type markings to
    the left.
4. Click **OK**.
5. Click **OK**

Network Monitor Activity Status Bars

The Network Monitor Activity status bars on the bottom of the
NetView GUI disappear on Alpha systems periodically, giving the
appearance that there is no Network Monitor activity. The nmpolling
dialog, accessed through the **Options --> Polling** option, does show
the Network Monitor activity consistently and correctly.

Open Topology on Clients

Non-IP topologies do not get displayed on client maps.

Autodiscovery Problems

No Objects Displayed

If no nodes are displayed on the map after starting the NetView
program, make sure the following daemons are running: ovspmd,
ovwdb, trapd, ovtopmd, and netmon. If any of these daemons are not
running, exit the NetView program, stop the daemons, restart the
NetView program, and answer Yes to the dialog asking if you want
to restart the NetView daemons.

If you have installed the NetView program on an Alpha system with
less than 64 MB memory, which is less than the minimum
configuration, this may lead to nothing being displayed on the map.
Upgrade to at least the minimum configuration of 64 MB.

Performance Sluggish During Autodiscovery

Initial autodiscovery is resource intensive. The NetView status bar
contains Network Monitor Activity bars that allow you to monitor the
progress of autodiscovery. Look for the three bars in the status to the
right of the node count. The top bar displays new node polling
activity, the middle bar displays node configuration polling activity,
and the bottom bar displays status polling activity.

The NetView program has defined a number of ICMP and SNMP queue slots to be used during autodiscovery. The default numbers of queues for both Intel and Alpha are as follows:

PC	ICMP Queues	SNMP Queues
Alpha with Ping Spray	80	32
Alpha without Ping Spray	50	32
Intel with Ping Spray	70	32
Intel without Ping Spray	40	32

If the performance with the default values is too sluggish, you can adjust the number of active work queues doing autodiscovery by changing the Discovery Speed on the netmon tab page in the NetView Server Setup.

In general, more CPU cycles are consumed for an SNMP slot than for an ICMP slot. Therefore, we recommend keeping the number of ICMP slots fairly high and varying the number of SNMP slots.

If all nodes in your network are connected by interfaces that have explicit IP addresses, you can uncheck the field **Discover IP Nodes beyond Unnumbered Interfaces** in the NetView Server Daemons tab page for the netmon daemon. This decreases your network traffic.

You can configure the speed of discovery and the use of Ping Spray for your site by using **Options --> Server Setup --> Daemons --> Netmon Daemon**. See the "Configure autodiscovery for your site" topic in the help file.

Object Placed in Incorrect Segment

When a node is discovered and responds to pings, but does not have an SNMP agent that responds to queries, the NetView program is unable to gather information about the node's interfaces. In this situation, the NetView program assumes that the node belongs in a bus segment. If the subnet in which the node is contained does not

yet have a bus segment but does contain some other type of segment, then the NetView program puts the node in the existing segment.

This default behavior can be overridden by setting the environment variable NVDEFAULTSEGMENT. If NVDEFAULTSEGMENT is set, the above types of nodes are placed in the segment specified by this variable, creating a new segment if necessary. This environment variable can be set to one of the following values: BUS, STAR, TOKENRING, FDDIRING, SERIAL. You can also change the default behavior using **Options --> Server Setup --> Daemons --> Netmon Daemon**.

If a node does not support SNMP, no inner shape will be present. If a non-connector node does support SNMP, but the sysObjectID is not known by NetView, then the inner shape of the node is hollow. A hollow connector symbol is assigned if the node is configured to be an IP forwarding node. All nodes that report an unknown sysObjectID can be logged in the **\usr\ov\log\badoids.log** file or a file of your choice. Use the **Options --> Server Setup --> Daemons --> Netmon Daemon** tab page to specify logging.

Performance Monitor Support

NetView Performance Monitor support is not available in this release on the Alpha platform.

Program Incompatibilities

Lotus Notes Version 4.5 has been know to crash with a Quincy32 error causing other applications, including NetView, to fail.

Documentation Errata

The *TME 10 NetView for Windows NT User's Guide* and the online help state that the NetView program starts the Event Browser by default. The default has been changed, and the NetView program no longer starts the Event Browser. If you want the NetView program to start the Event Browser upon startup, select **Options --> Console Settings**.

IBM Redbooks

IBM's International Technical Support Organization (ITSO) produces a set of Redbooks, which are technical publications written by and for technical professionals. The Redbooks provide installation and implementation experiences, sample code, typical scenarios, and step-by-step "how to" procedures. For more information regarding Redbooks, point your Web browser at: http://www.redbooks.ibm.com.

The ITSO-Raleigh group has written a number of Redbooks for management including *Examples of Using TME 10 NetView for AIX V5 and TME 10 NetView for Windows NT*, form number SG24–4898–01. This Redbook includes code that provides an EUI API and a scripting interface to the NetView GUI (wteuiap6 and its driver program wtdriver6). You can obtain sample EUI APIs from http://www.redbooks.ibm.com and go to DOWNLOADS.