# SERVER VIEW

Server View is a software product which provides, within a local area network, an intelligent monitoring and signalling system that allows a visual check to be made on the network server from a Windows workstation.

In case a system failure requires a service call to be made, the field engineer is aided in troubleshooting since a series of information on the system which were collected before the failure occurred are provided.

Server View has the following components:

- **Agents**, which are installed on the server and allow the:
  - monitoring of hardware components
  - collection of operational failures
  - identification of performance data.
- The **Manager application** which, resident and running on a Windows workstation connected to a network, provides the system administrator or field engineer with the interface required to monitor the system.



Dialog between the Agents and the Manager application is provided by **SNMP** (Simple Network Management Protocol).

The database used to monitor the system components is called **MIB** (Management Information Base) and consists of a group of ".mib" files located on each server on the network to be monitored (refer to the last section in this Appendix).

The item used by the Agents to signal a failure is called **Trap** and is an asynchronous message.

## Documentation

The following Server View hard copy and online information is available:

- Hard copy "***Server View - Getting Started***". It contains all information concerning:
  - Performance and characteristics
  - Hardware/software prerequisites
  - Installation/deinstallation procedures
  - Activation
  - Trap management.
- **Readme file**, selectable by clicking on the Windows "Server View" icon. This file ***must be read before activating Server View*** since it provides information on the login to use in order to work as the system administrator. This file also contains information on how to backup the database and on some current Server View restrictions.

- **Online documentation** selectable by clicking on the Windows "Server View" icon. The online documentation consists of four documents that can be selected from the main menu:
  - **Overview**. Provides an introduction to Server View.
  - **User Guide**. After providing a detailed description of all interface components (Tool Bar, symbols, colors, mouse usage, function keys), this guide provides a **tutorial** that will help acquire a certain degree of familiarity with the Server View tool.
  - **Monitoring**. Describes the server's monitoring environment represented by icons and images.
  - **Traps Management**. Contains a list of all the asynchronous messages (traps) along with their meaning and actions to undertake.

To quickly access the online documentation it is suggested to keep this document open together with Server View so that you can switch from the Server View environment to the online documentation by simply pressing the ***ALT-TAB*** key sequence.
The online documentation Help files can also be directly displayed from the Server View work environment by selecting the ***Help*** option followed by ***Open*** and, in the Server View installation directory (for example c:\sview), by double clicking on the name of the desired Help file.

- **General Help** activated by means of the ***Help*** option or by pressing the ***F1*** key. It provides a general guide on the use of Server View.

  **Contextual Help** activated by means of the ***Help*** button within a Window. This Help can provide information on the contents of the current Window or, in a more precise way, of a field or item which is active in the window at that moment. In this case the initial portion of the Help description concerns the window in general while the end portion (which can be displayed by simply scrolling the text) concerns the currently selected item of that window.

## Operating Environment

As far as the hardware/software prerequisites are concerned, the Server View installation and activation procedures are explained in Chapter 7 of the "***Server View - Getting Started***" manual. However, a brief description on how to install the Manager application on a Windows workstation and on the different servers (Agents) is provided.

## Installation and Configuration

### Installing the Manager Application

The TCP/IP-32 protocol provided in the Starter Kit of each SNX system is the fundamental prerequisite for the Manager application.

**Note:** *Press the **F3** key or click on the **EXIT** button to interrupt installation at any time.*

| Action | Description |
|---|---|
| Insert Disk 1/4 into drive A:. | |
| Under Windows, select ***File*** from the Program Manager or File Manager. | |
| Select ***Run***. | |
| Type ***A:\setup*** and press **ENTER**. | |
| Select ***Install the Server View system*** and confirm with ***OK***. | After having made a copy of some files, a request is made to select the desired installation operation. In a successive Setup session, the Server View database clear operation can be activated from this window. |
| Answer ***Yes*** or ***No*** to the message ***Do you wish to install the bitmaps?*** | You are asked if you wish to install geographic maps to be used as background in the graphics representation of networks. If you answer *No* you can still install these maps in a later Setup session. |
| Specify the pathname where you wish to install Server View and confirm with ***OK*** (the default pathname is C:\SVIEW). | A check is made on the space required for installation; if this space is not enough another pathname can be specified or installation can be interrupted and started again once enough space is created. |
| Fill in the ***Subnet Address*** field with the complete address of the subnetwork that the server to be monitored is connected to (for example 131.1.165.254).<br>Fill in the ***Media Type*** field by selecting the type of subnetwork (the default is 10BASET). | **Warning:** If the complete subnetwork address is not provided and the default one is used, the search operation performed on the system connected to the subnetwork and performed by Server View during the autodiscovery phase (described further on) may become much slower.<br><br>Click on the ***RESET*** button to correct any typing error in this window. |
| Insert the different installation disks (2/4, 3/4, 4/4) as instructed to do so at the end of installation and click on ***OK***. | A new *Server View* group consisting of three icons is created in Windows. |

## Installing/Deinstalling the Agents and Configuring the SNMP Environment

**Note:** *Each server to be monitored must have the TCP/IP or IPX protocol and the SNMP environment installed and active for each operating system. Furthermore, the "DPT Storage Manager" modules and, for resilience systems, the "SNX Resilience Support" module, must also be installed for each operating system.*

| **MICROSOFT WINDOWS NT** | |
|---|---|
| **Stage** | **Action** |
| Agent installation | Insert the ***Olivetti Server View Management Agents for Windows NT 1/1*** disk into drive A:. |
| | After logging in as system administrator, from Windows activate ***File Manager***, select drive ***A*** and double click on ***I\NT\SETUP.EXE***. |
| | During installation you are requested to specify the system model. |
| | Once installation is complete, the system must be shutdown and then booted again. |
| PowerNet installation | Insert the ***APC PowerNet Agent for Windows NT*** disk into drive A:. |
| | From Windows activate ***File Manager***, select drive ***A*** and double click on ***SETUP.EXE***. |
| | During installation you are also requested to provide the setup parameters for the UPS. |
| | At the end of installation a new group called ***PowerChute Plus*** is created***.*** |
| SNMP configuration | From the Control Panel window, select ***Network***, select the ***SNMP*** protocol, click on ***configure***, add, for example, ***public*** and associate this to the IP-address of the Windows workstation that will receive the trap indications. |
| Agent deinstallation | From the Control Panel, stop the ***SNMP***, ***SN_SRV***, ***SN_HOST***, ***SN_SRC***, ***SN_COND*** services and the ***SRVDR*** driver. |
| | Using regedt32: remove ***System\CurrentControlSet\Services\ SNMP\Parameters\ExtensionAgents\9*** , from the Software\Olivetti subdirectory remove ***SNMP***, ***SN_SRV***, ***SN_HOST***, ***SN_SRC***, ***SN_COND***, from the System\CurrentControlSet\Services subdirectory remove ***SN_SRV***, ***SRVDR***, ***SN_HOST***, ***SN_SRC***, ***SN_COND***. |
| | In MS-DOS remove, from the "SystemRoot"\System32 subdirectory, the ***OLIAGENT.DLL***, ***OLIMIB.DLL***, ***ZOLIMIB.DLL***, ***SN_SRV.EXE***, ***SN_HOST.EXE***, ***SN_SRC.EXE***, ***OLISRC.EXE***, ***SN_COND.EXE*** files and then remove from the "SystemRoot"\System32\drivers directory the file ***SRVDR.SYS***. |
| | When deinstallation ends the system must be shutdown and then booted again. |
| PowerNet deinstallation | Use the removal utility supplied by referring to the contents of the Readme file. |

| NOVELL NETWARE | |
|---|---|
| **Stage** | **Action** |
| Agent installation | Insert the ***Olivetti Server View Management Agents for Novell NetWare 1/1*** Disk into drive A:. |
| | From the system console type:<br>***LOAD A:NETWARE\INSTALL*** |
| | Answer ***Y*** or ***N*** to the self-explanatory requests displayed during installation. In particular you are requested to specify the system model. |
| | At the end of installation you can select whether or not to immediately activate the modules installed. |
| PowerNet installation | Insert the ***APC PowerNet Agent*** disk into drive A:. |
| | After logging in as system administrator, from Windows activate ***File Manager***, select drive ***A*** and double click on ***SETUP.EXE***. |
| | At the end of installation a new user group called ***powerchute*** and with initial password "***apc"*** is created. |
| SNMP configuration | In the SYS:\ETC\TRAPTARG.CFG configuration file, specify the IP address or the IPX address of the Windows workstation which will receive the trap indications, as follows:<br><br>#IP Address<br>***Protocol UDP***<br>***131.1.1.5***<br><br>#IPX Network Number: MAC Address<br>***Protocol IPX***<br>***00001289:00001B31651F*** |
| Agent deinstallation | Unload ***SN_SRVx***, ***SN_HOSTx***, ***SN_SRCx***, ***SN_CONDx***. |
| | From the SYS:SYSTEM directory remove ***SN_SRVx***, ***SN_HOSTx***, ***SN_SRCx***, ***SN_CONDx***. |
| | Remove the automatic loading of the SNMP subagent from the AUTOEXEC.NCF file. |
| PowerNet deinstallation | Cancel the installation directory (default SYS:PWRCHUTE) with all of its files. |
| | Remove the following lines from the AUTOEXEC.NCF file:<br>***SEARCH ADD SYS:PWRCHUTE***<br>***LOAD AIO***<br>***LOAD AIOCOMX***<br>***LOAD PWRCHUTE SYS:PWRCHUTE***<br>***LOAD POWERNET SYS:PWRCHUTE*** |
| | Cancel the ***powerchute*** user name. |

| SCO OPEN SERVER | |
|---|---|
| **Stage** | **Action** |
| Agent installation | Insert the ***Olivetti Server View Management Agents for SCO*** disk into drive A:. |
| | After opening a session by loggining in as ***root***, run the ***Custom*** utility and select the following in this order: ***Software***, ***Install new***, ***Full product***. |
| | Answer the requests displayed and, in particular, answer ***Y*** when requested to rebuild the kernel. |
| | At the end of installation the system must be shutdown and rebooted again. |
| SNMP configuration | In the following files, enter the IP address of the workstation that will receive the trap indications:<br>***/etc/snmpd.trap***<br>***/etc/snmpd.comm*** |
| Agent deinstallation | After opening a session by logging in as ***root***, run the ***Custom*** utility, select the package to remove, select the ***Remove Software*** command and answer ***y*** when asked whether to reconstruct the kernel. |
| | At the end of the deinstallation phase the system must be shutdown and booted again. |

| NOVELL UNIXWARE | |
|---|---|
| **Fase** | **Azione da compiere** |
| Agent installation | Insert the ***Olivetti Server View Management Agents for Novell UnixWare*** disk into drive A:.. |
| | After opening a session by logging in as ***root***, type the following command: ***pkgadd -d diskette1*** |
| | Select the Server View for UnixWare package and follow the instructions displayed to complete the installation. |
| | Rebuild the kernel by typing: ***/etc/conf/bin/idbuild*** |
| | At the end of installation the system must be shutdown and then booted again. |
| SNMP configuration | In the following files, indicate the IP address of the workstation that will receive the trap indications:<br>***/etc/netmgt/snmpd.trap***<br>***/etc/netmgt/snmpd.comm*** |
| Agent deinstallation | After opening a session by logging in as ***root***, type the following command: ***pkgrm srvview*** |
| | Rebuild the kernel, shutdown the system and the boot it again. |

## Login

During the activation of Server View, specify a login name immediately after having selected the Server View icon in the same name group under Windows. The Readme file indicates the login to use in order to operate as system administrator, which is "***sview***" (small letters). Using a different login will still grant access to Server View but with less rights since the system will consider the person logged in as a Normal User.

The login defined for the system administrator is specified in the "\sview\bin\onyx.ini" file and can be changed; in any case there is always one system administrator.

## Graphical Representation of the Network and Autodiscovery

Immediately after a login is provided, Server View activated (by selecting "Open" in the "File" menu) and the transmission protocol selected (for example IP), you are proposed to perform and Autodiscovery operation on the network in order to automatically search all the systems connected.



If Autodiscovery does not need to be executed, manually create a graphical representation (view) of the subject network. For simplicity, this representation may be split into different parts (for example dividing the network into the number of floors that the building in which it is installed consists of).

By activating Autodiscovery, instead, a search is automatically made on all systems (with the Server View Agent) connected to the network whose subnet address has been defined during the installation of the Agents. Also displayed are any other connections to other networks.

For a system to be viewed during the Autodiscovery phase, at least one SNMP protocol must be available in order to dialog with the Manager application of the Windows workstation.

## Notes and Warnings

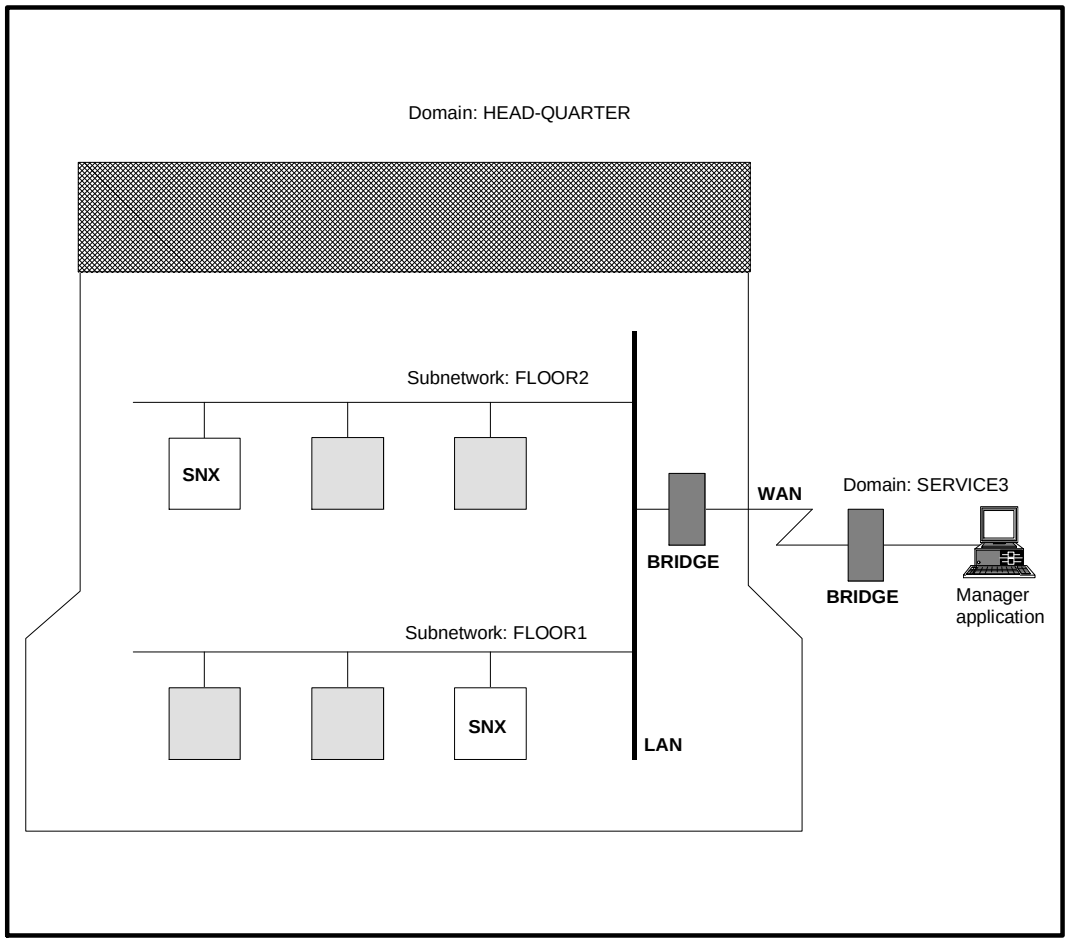
- If several windows have been opened, the lowest level window must always be closed in order to be able to access the higher level one.
- After making any change in a configuration environment, the **EXECUTE** button must be selected for the change to actually take effect.
- In order to be able to access the configuration options relating to the servers connected to the network, it is possible to work in the following two ways:
  - Selecting "Configuration/Configuration Options" from the Management Menu
  - Selecting "Configuration/MIB Browser", always from the Management Menu. In this case the configuration options are graphically represented in a tree structure of MIB information.

# Examples of Monitor Sessions

**Note:** *In the examples that follow, the actions to be performed are indicated by specifying the options that can be selected from menu. The same operations can also be performed by selecting the corresponding icons from the tool bars.*

## Manually Creating a Graphical Representation of the Network

Provided below is an example of the manual creation of a graphical representation, or *view* of a network ("Head Quarter"), consisting of two subnetworks ("Floor1", "Floor2"), one for each floor of the building, and monitored from remote as shown in the following figure.




Press the ***F1*** key for information on how to create a grapical representation of the network.

| Action | Description |
|---|---|
| Select: ***New View***. | |
| Enter the name of the graphical representation: for example ***Oliservice***. | |
| Select: ***OK***. | A symbol representing the newly created view with its own name associated (*Oliservice*) is displayed. |
| Select the "*Oliservice*" symbol by clicking on it twice. | An empty window relating to the "*Oliservice*" view" is displayed. |
| Select: ***Create Domain***. | |
| Type the name of the domain: for example: ***Head-Quarter***. | |
| Select: ***OK***. | The symbol of the newly created domain to which the name "*Head-Quarter*" is associated is displayed within the "*Oliservice*" window. |
| Select the following again: ***Create Domain***. | |
| Enter the name of the domain where the Manager application workstation is located: for example ***Service3***. | |
| Select: ***OK***. | The symbol of the second domain to which the "*Service3*" name is associated is also displayed. |
| To draw a straight line connecting the two domains: position the cursor on the "*Head-Quarter*" symbol, press **CTRL** and the right mouse button (which must be held down), move the cursor to the "*Service3*" symbol and release the mouse button. | The newly traced straight line indicates that the two domains are connected in a WAN. |
| Double click on the "*Head-Quarter*" symbol to select it. | The "*Oliservice: Head-Quarter*" window containing a small domain symbol (in our case "*Service3*") is displayed to remind that "*Head-Quarter*" is connected to "*Service3*". |
| Click the right mouse button any where in the "*Oliservice: Head-Quarter*" screen. | |
| Select: ***Create Subnetwork***. | |
| Select: ***Bus***. | |
| Define the type of network and its address. | |
| Enter the name of the subnetwork: for example ***Floor1***. | |
| Select: ***OK***. | |
| If necessary, move the subnetwork to a specific position within the window. | The newly created subnetwork is represented by a segment. |
| Select the subnetwork symbol by double clicking on it. | |
| To create a subsystem of the "*Floor1*" subnetwork, select: ***Create Subsystem***. | The "*Create New Subsystem*" window is displayed. |
| Select the subsystem type and product. | |
| Select: ***OK***. | |
| Enter a subsystem name and address other than "community" (for example ***100.1.10.10***, ***public)***. | |

| Action | Description |
|---|---|
| Select ***Transport Parameters*** if the following parameters are to be changed: Flow Control Window, Transport Time, Retry Count. | A window is displayed in which the parameters for dialoging with Server View are specified. |
| Select ***OK*** twice. | |
| With the left mouse button move the icon of the newly created subsystem to the desired position. | |
| In the exact same way, create the "*Floor2*" subnetwork with its own server and with bridge systems. | |

## System Monitoring and Trap Interpretation

### Polling

For the Manager application to know when a system is connected, powered on and active it must be able to poll this system. Polling is set by default but can be modified by selecting the network and the following items in this order: ***Management***, ***Performance***, ***Polling Summary***.

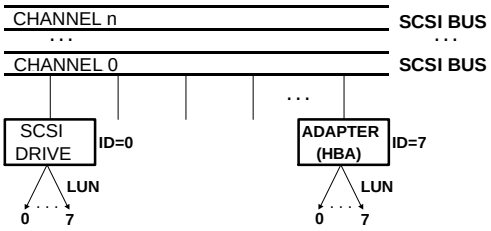
There are three types of polling:

- **Alarm Polling:** The system is interrogated to find out whether it is active or if an alarm has occurred. If the time interval set between one Alarm Polling and the next is too short, there is a considerable increase in line traffic over the network. If this interval is too long, there is a risk of not being promptly informed on the occurance of a failure.
- **Threshold Polling:** For more details on system operation, alarm thresholds can be set which, once exceeded, determine that the system is not working at its best. This type of polling therefore checks when the defined thresholds are exceeded.
- **Statistics Polling:** This type of polling is performed at predefined time intervals and allows to generate statistics concerning system operation. The collected data can be displays in a graphical format.

### Trap

If a failure is detected during an Alarm Polling, a Trap is immediately indicated on the screen. Some of these indications request the intervention of the field engineering service. The table that follows lists the Traps for which field engineering intervention is required.

As far as the messages concerning the SCSI drives are concerned, refer to the figure on the side for interpreting the identifiers.



| Trap | Action |
|---|---|
| Thermal Fan on Main Box is *Degraded* | One of the fans that does not have to be used at the moment has failed. The system continues to operate correctly but the faulty fan needs to be replaced as soon as possible in order to restore the system's redundant configuration. |
| Thermal Fan on Main Box is *Failed* | One of the fans that needs to be used has failed and therefore the system has shutdown. The faulty fan needs to be replaced immediately. |
| Power Supply *Degraded* | The redundant power supply has failed. The system works correctly but the power supply needs to be replaced as soon as possible in order to restore the system's redundant configuration. |
| Disk Area *xx* status is *Degraded* | The redundant power supply on the PEM is faulty or one of the secondary fans does not work. The system works correctly but the power supply or fan needs to be replaced as soon as possible in order to restore the system's redundant configuration. |
| Disk Area *xx* status is *Failed* | The redundant power supply in the PEM has failed or one of the secondry fans does not work. The system works correctly but the power supply or the fan needs to be replaced as soon as possible in order to restore the system redundant configuration. |
| SCSI Controller *xx* status is *Failed* | The SCSI controller is faulty and must be replaced. If the error is caused by the SIMMs, simply add others or replace the faulty ones. |
| Logical drive unit LUN *xx*, with ID *yy*, on channel *zz*, connected to adapter *ww Degraded* | An error has occurred in a redundant Array Group. The system continues to work correctly but the faulty unit must be replaced as soon as possible. |
| Logical drive unit LUN *xx*, with ID *yy*, on channel *zz*, connected to adapter *ww Failed* | An error has occurred in a non-redundant Array Group or simultaneous errors have occurred on several drives of a redundant Array Group. Replace the faulty logic drive. |
| Physical drive unit LUN *xx*, with ID *yy*, on channel *zz*, connected to adapter *ww Missing* | The drive is not physically present in the system or does not respond on the SCSI bus. Check the hardware configuration and the physical SCSI connections. |
| Physical drive unit LUN *xx*, with ID *yy*, on channel *zz*, connected to adapter *ww Failed* | A serious drive error has occurred. If this drive belongs to a redundant Array Group, the system will continue to work correctly. It is, however, suggested to replace the faulty drive as soon as possible. |
| Physical drive unit LUN *xx*, with ID *yy*, on channel *zz*, connected to adapter *ww* has exceeded the software errors Factory Defined threshold of *tt* with a value of *kk* | The drive works correctly but has exceeded the threshold of recoverable software errors. It is suggested to replace the drive since it could fail in a short time. |
| Physical drive unit LUN *xx*, with ID *yy*, on channel *zz*, connected to adapter *ww* has exceeded the unrecovered hard errors. Threshold of *tt* with a value of *kk* | The drive has exceeded the threshold of unrecoverable hardware errors. It is suggested to replace the drive since it could fail in a short time. |
| Physical drive unit LUN *xx*, with ID *yy*, on channel *zz*, connected to adapter *ww* has exceeded the data inconsistencies threshold of *tt* with a value of *kk* | The drive has exceeded the threshold of data inconsistencies. It is suggested to replace the drive since it could fail in a short time. |
| Physical drive unit LUN *xx*, with ID *yy*, on channel *zz*, connected to adapter *ww* has exceeded the block reassignment threshold of *tt* with a value of *kk* | The drive has exceeded the threshold of operations for the reallocation of faulty sectors. Since there is no more space for new reallocations, the drive needs to be replaced since it could fail in a short time. |

## Displaying System Information

To be able to display the hardware and software information concerning an SNX server simply double click on the icon representing the server connected to the network. The **Subsystem Window** is displayed containing icons representing the macro-subjects of which information can be obtained. Server View will then display example information on each of these subjects.

### Configuration

Provides ample information on the configuration of the system and of its components. For example, clicking on the **System Information** icon displays information relating to the CPU board, memory or security. Clicking on **Server Information** displays information relating to the system (type, model, BIOS).

### Utilization

Provides information on the use of the system resources. For example, selecting the **CPU** icon displays a table containing the percentages of CPU utilization.

### Mass Storage

Provides information on the system mass storage devices. For example, selecting the Physical Drives option displays a map which includes the Host Bus Adapter (HBA) and all the peripherals connected to it. Therefore, selecting the icon of a determined SCSI peripheral displays the following information:

- **HBA:** Index of the SCSI adapter to which the peripheral is connected.
- **Channel:** Index of the SCSI channel (SCSI bus adapter instance) to which the peripheral is connected.
- **Id:** Univocal identifier of the peripheral on the SCSI bus.
- **Lun:** Represents the Logical Unit Number which univocally identifies the peripheral on the SCSI bus.
- **Firmware Revision:** Revision level of the peripheral's firmware.
- **Vendor:** Name of the supplier of the peripheral.
- **Model:** Peripheral model.
- **Device Type:** Type of peripheral.

### Serious Problem

Provides information on components whose malfunction could cause serious system failures. For example, selecting **Thermal Status** followed by **Main Box** displays information on the current temperature in the system main box.

**Network**

Provides information on the network boards installed in the system. For example, selecting **MIL II** followed by **IP Address** displays of table listing the IP addresses.

**UPS**

Provides information on the Uninterruptable Power Supply (UPS).

## Setting Thresholds

To monitor the system in the best possible way, thresholds can be set to improve the evaluation of system performance.

Thresholds can be set for any system attribute.

Provided below is an example in which a threshold is set for the amount of line traffic received by the system.

| Action | Description |
|---|---|
| Select: ***Management***, ***Performance***, ***Set Threshold***. | The "*Threshold Polling Settings*" window is displayed. |
| Select: ***Subsystem Polling***. | All the fields of this window can be accessed. |
| Fill in the ***Polling Period*** field by entering, for example, the value ***3***. | This value indicates that Polling will take place every three minutes to check the threshold. |
| Select the attribute for which a threshold needs to be set: ***IP Rx total***. | |
| Select: ***Attribute Polling***. | An asterisk is displayed next to the selected attribute. |
| Assign value ***80*** to the ***Threshold Value Upper*** field. | The value set indicates that an error condition will be signalled if more than 80 packets are received within a period of time. |
| Assign ***Rate (Per Minute)*** in the ***Threshold Mode*** field: | Indicates the mode and format in which the data are collected (in our case every minute). This setting depends on the data collection device that can work through a counter, using percentages, or as in our case at preset time intervals. |
| Assign the value ***2*** to the ***Fault Severity Level (1-5)*** field. | Defines the level of importance if the threshold is exceeded. |
| Select: ***OK***. | |

**Note:** *To prevent exceeding a threshold which would result in the signalling of an error condition, the system can be kept under control by means of statistics and the display of graphs indicating the trend of the more important attributes.*

## MIB Files and the Monitoring of Non-SNX Systems

Each resource to be monitored using the Server View Manager application must have its own MIB file installed in the system in which the resource is present. All the MIB files of the system resources that could be monitored form a database of information that the Agents can access to send information to the Manager application through the SNMP protocol.

To monitor a system connected to a local area network, it is therefore necessary that the SNMP (which allows the data exchange between systems) be present and active on this system along with the MIB files relating to the system resources.

Server View has been developed for the systems of the SNX SYSTEMA product line, but information on different systems, such as LSX 5000 or simple client PCs, can also be obtained.

If the non-SNX system connected to the network is configured with an active SNMP environment but does not have the MIB files:

- You can find out whether the system is operational or not.
- You can find out its configuration (limited) by clicking on the "Configuration/Information/Information Server" icons.

■