Version 1.3

Chapter 1 – Introduction

Overview

NetWatch is a web based management product that provides a very detailed amount of network information through an intuitive, easy to understand graphical interface.

Key Product Features

- Monitors Network devices reporting on status, alerts and utilisation.
- Provides a graphical representation of the network where devices are represented as nodes connected by lines on a user definable background.
- Generates status change and response time alerts via email, SMS, network popup etc.
- Allows multiple backgrounds/ maps and easy positioning of devices.
- Includes user definable Bandwidth monitor
- Ships with internal Syslog server and SNMP trap receiver.
- Can be supplied as a hardware solution or installed direct from CD.

Minimum System Requirements

IBM Compatible PC Pentium III
256 MB RAM
10 GB Hard Disk Space
MS Windows NT 4.0 SP6, Win2K, Win XP
800X600 256 colour adaptor and monitor
IE 6.0 or greater.
LAN Adapter

Installing NetWatch

- Open the CDROM drive from windows explorer.
- If the CD does not auto-run then: Click on the icon named ‘setup.exe’ to start installing NetWatch.
- The install shield wizard allows you to choose which port the netwatch web server runs on. The standard and default web server port is port 80. However if another application is running on port 80 (E.g. IIS) you should install the netwatch web server on a different port.

- NetWatch uses the MySQL database to store configuration and historical information. This is the largest part of NetWatch, so you may wish to install it on a drive other then your system drive. To do this select "custom" from the set-up type screen. Then choose "MySQL" and change the destination drive/directory.
- When the installation completes NetWatch will be successfully installed **and can be used by accessing the User Interface.**

Accessing the User Interface

After NetWatch is installed and running you can access the user interface of NetWatch by pointing a web browser to the machine running NetWatch. If you chose a port other than port 80 during installation you must specify it in the URL, e.g. to access NetWatch running on port 8080 on the local machine, go to:

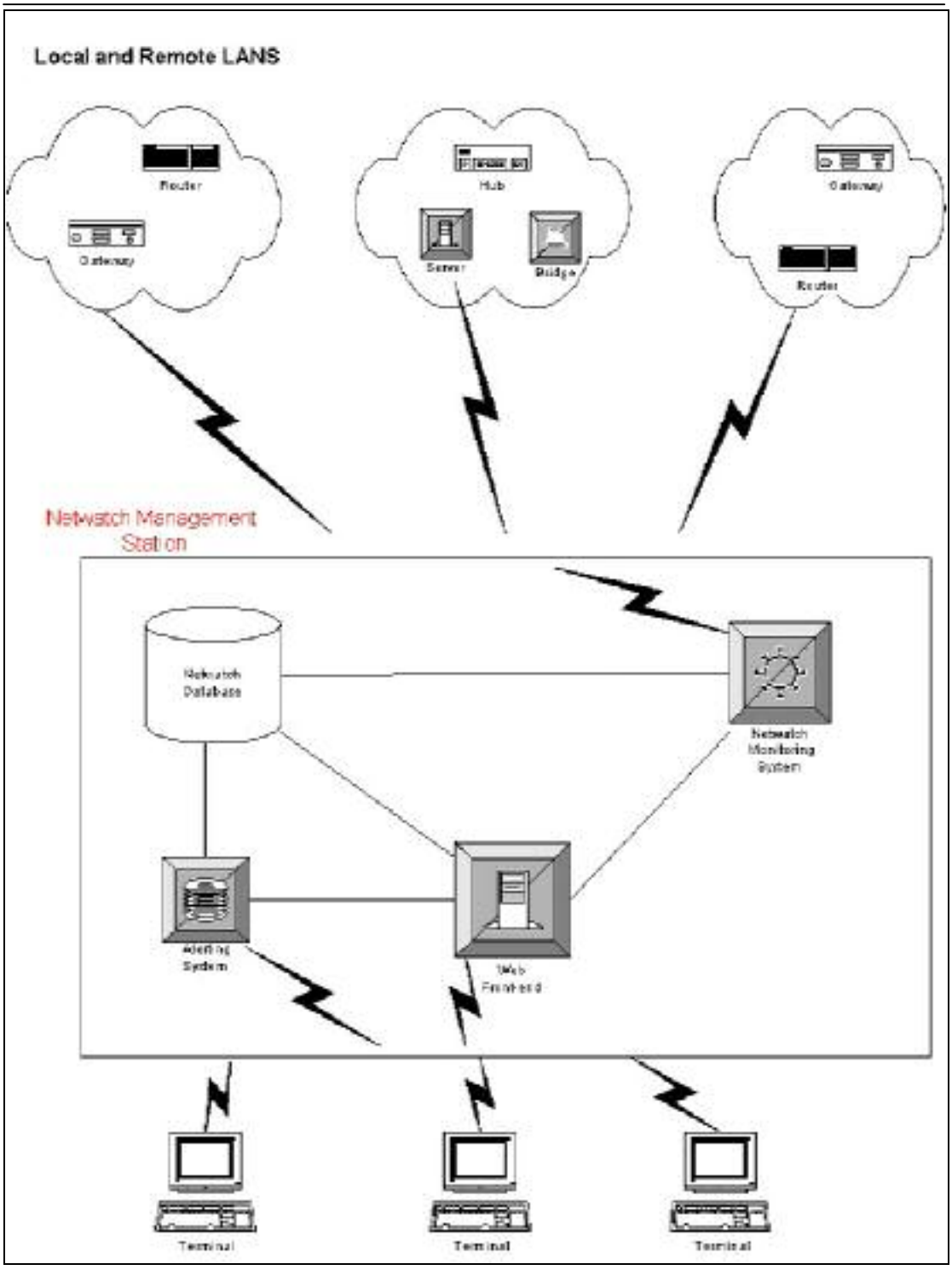
```
http://127.0.0.1:8080/
```

Once NetWatch is successfully installed, NetWatch and all its related components are installed as services. These services can be stopped and started accordingly using the NetWatch Service Manager. The details of the services are below:

Service	Details
NetWatch	System service can be Stopped / Started
MySQL	Database service can be Stopped / Started
Tomcat	Web Server service can be Stopped / Started

Architecture Overview.

NetWatch is a completely web based network management tool. Using its unique web front-end, services on network devices can be configured and monitored from anywhere on a local LAN or on the Internet.



NetWatch Monitoring System

The monitoring system is the core element within NetWatch. It performs the work of monitoring the status of the services provided by a device and keeps track of the amount of traffic going in and out of various channels on that device. It also acts as a receiver to SNMP traps and syslog messages, which are generated by various network devices.

NetWatch Database

MySQL was strategically chosen as the database for NetWatch because of the speed with which it performs SQL queries.
It also handles connections very efficiently, thus making it ideal for a web based product like NetWatch. The database stores all NetWatch configuration data and logs.

Alerting System

NetWatch contains a complex alerting system, which alerts the user to certain situations on a device. When an alert occurs this is immediately seen from the web front-end. Alerts can be also sent through E-mail, SMS, syslog and various or media. **For detailed information on the alerting system refer to Chapter 4**.

Web Front-end

The web front-end plays a very important role with in NetWatch in that it provides the user interface of NetWatch. NetWatch uses a technology called Java Server Page (JSP) in conjunction with our database for controlling the content and appearance of our web front-end. Using this technology NetWatch is able to provide complex reporting to the user.
The JSP pages are served to the user by using a specific web server (which runs on configurable port e.g. 8080) that is installed with NetWatch.

Chapter 2 – NetWatch Configuration

To configure NetWatch click the "Administration" button on the welcome screen.

Global System Settings

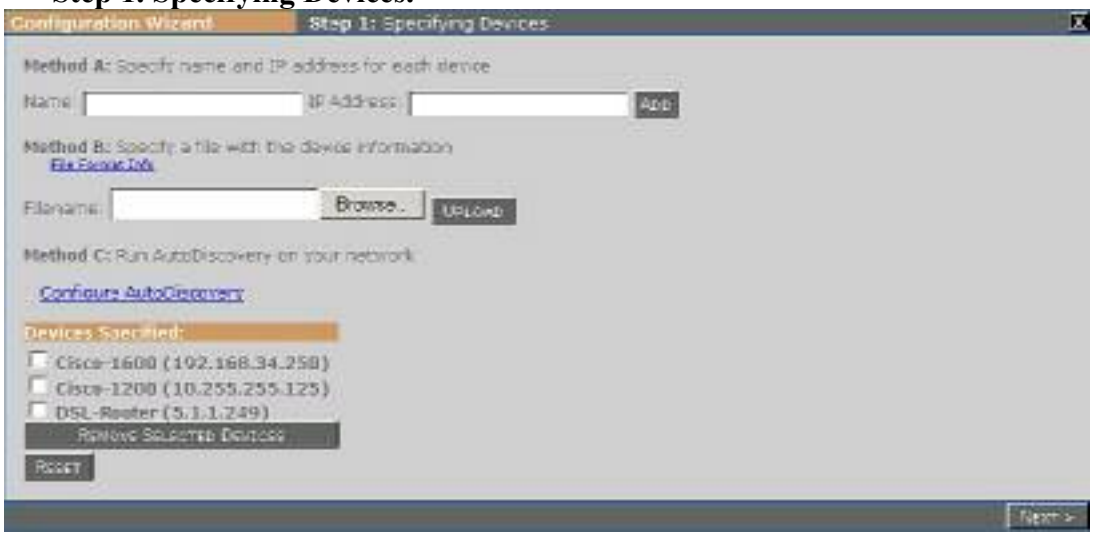
These are settings that affect the operation of the whole NetWatch system. If you installed NetWatch into a folder other than the default, please ensure these settings are correct.
To access the System Settings page click on the "System Settings" button. The various options are explained below:

Parameter	Description
Company name	The name of the company using NetWatch
System name	A general name given to your NetWatch system
Administrator	The name of the person who maintains the NetWatch system
Email "from" address	The source address on any email alarm sent by NetWatch, e.g. administrator@companyname.com
Email subject line	The subject on any email alarm sent by NetWatch
SMTP server	The address of the default SMTP server used for sending email alarms
NetWatch install directory	The directory where NetWatch is installed
Default backup directory	The default directory where NetWatch backups will be stored
Default visual background	The map that is loaded by default when you choose "View your Network" from the welcome screen
Keep records for…	The period after which records are deleted from the NetWatch database
Use a maximum of…	The maximum number of Sockets that will be used for TCP port scans. As sockets are a limited resource it is recommended that this does not exceed 500 sockets.
Maximum DB connections	The Maximum Number of database connections that can be opened at any one time. See MySQL Appendix.
MySQL install directory	The folder where MySQL is installed
RMI port	RMI is the system by which the web server and NetWatch server communicate. If another program that uses RMI is installed, such as Cisco Works, it may be necessary to change this value.
Use Syslog Server	Set to **Yes** if you want to receive Syslog messages. Note that you need to restart the NetWatch service to apply changes to this setting.

Setting up a Device

The process of setting of a network device for monitoring is done in a very intuitive and easy to use 'Configuration Wizard' with five simple steps. 'Next' and 'Previous' buttons are provided for navigation within the wizard.

Step 1. Specifying Devices.



This step involves specifying the devices you wish to monitor. Devices that are set up together will all contain the same configuration. If you want devices with different configurations they should be set up through the wizard separately.

You can add devices in one of three ways:

A. Enter the Name and IP Address of each device you want to monitor and click 'add'. To add a number of devices this can be done repeatedly.

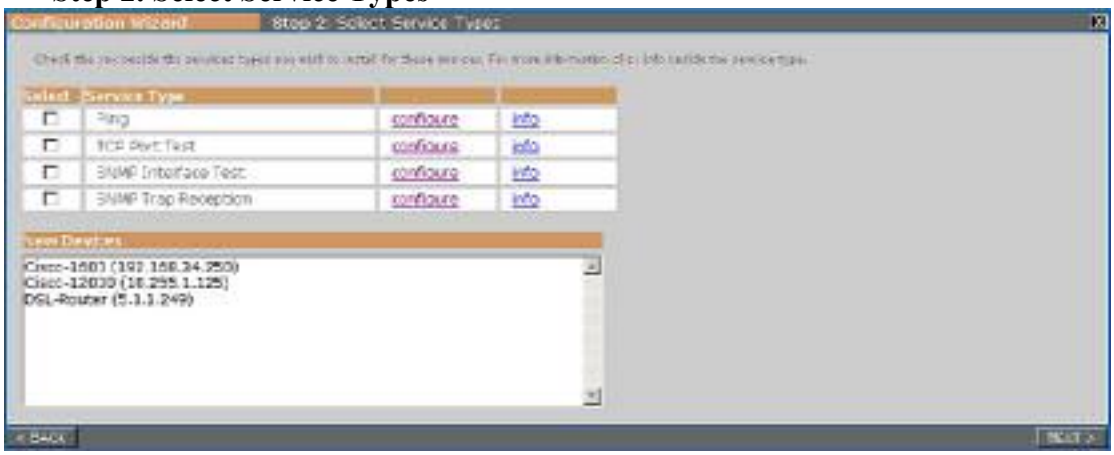
B. You can create a text file containing all the devices and their IP addresses. You can then 'browse' to this file in the wizard and click 'Upload' to load all the devices. Each line of the import file should have the device name followed by a space and an IP address, followed by a carriage return. Make especially sure that the last line ends with a carriage return.

Sample Import File Format
Router1600 192.168.34.9
Router3200 192.168.34.2
Router3202 192.168.34.5

C. Auto Discovery: Given a starting IP address and appropriate community strings NetWatch will automatically discover your network and allow you to add devices found as NetWatch devices. You can choose either CDP or route table discovery or use both together. The discovery can be filtered by using multiple IP range or Network filters.

If you are unhappy with the devices you have added, clicking on the 'Reset Device List' button will clear the list. Once you have loaded your device(s) you may proceed to step 2 by clicking the 'Next' button.

Step 2. Select Service Types



This step involves selecting the types of NetWatch service that you wish to use to monitor the device(s). There are four individual service types:

Ping

A simple ping operation to test whether or not the device is responding. Response time for the operation can also be recorded. An alert can be triggered when the ping status changes or if response time exceeds a threshold.

TCP Port Test

Selected TCP ports are tested for status. For example, you may wish to monitor the status of the SMTP port on your mail server. This test makes sure that connections can be made to that port and records when it changes status. Configuration allows you to set up multiple profiles for monitoring commonly used groups of ports. Alerts can be triggered when ports change status, or if response time exceeds the configured threshold.

SNMP Interface Test

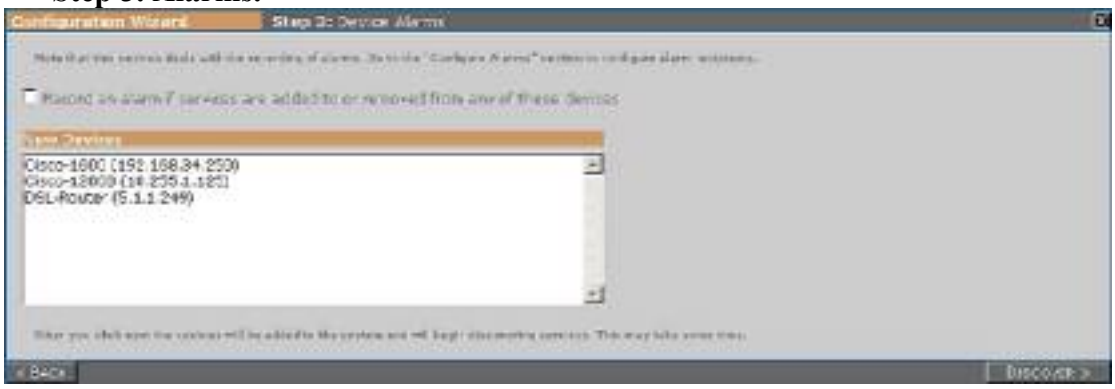
Interfaces on the device are polled for status, utilisation and response time. Status changes are recorded as well as, optionally, detailed utilisation statistics and SNMP request response time, both of which can be graphed. Alerting occurs on status change, response time and on utilisation levels. Note that an SNMP community string is required.

SNMP Trap Reception

Generic SNMP Traps are received and recorded. Note that only traps and notifications from devices configured with this service type will be recorded. An alert can be triggered when a trap is received. At the current version, only the six generic traps are received: Cold Start, Warm Start, Link Up, Link Down, Authentication Failure and EGP Neighbour Loss.

For more information on SNMP for the Interface Test or Trap Reception, see Appendix B: SNMP. Further details of each service type can be found be clicking its related ‘info’ link. To change the default values for timeouts and expected response times, click the ‘configure’ link beside the service type**.** For more detailed information on service types see Chapter 8: Services, Discovery and Polling.

Step 3. Alarms.



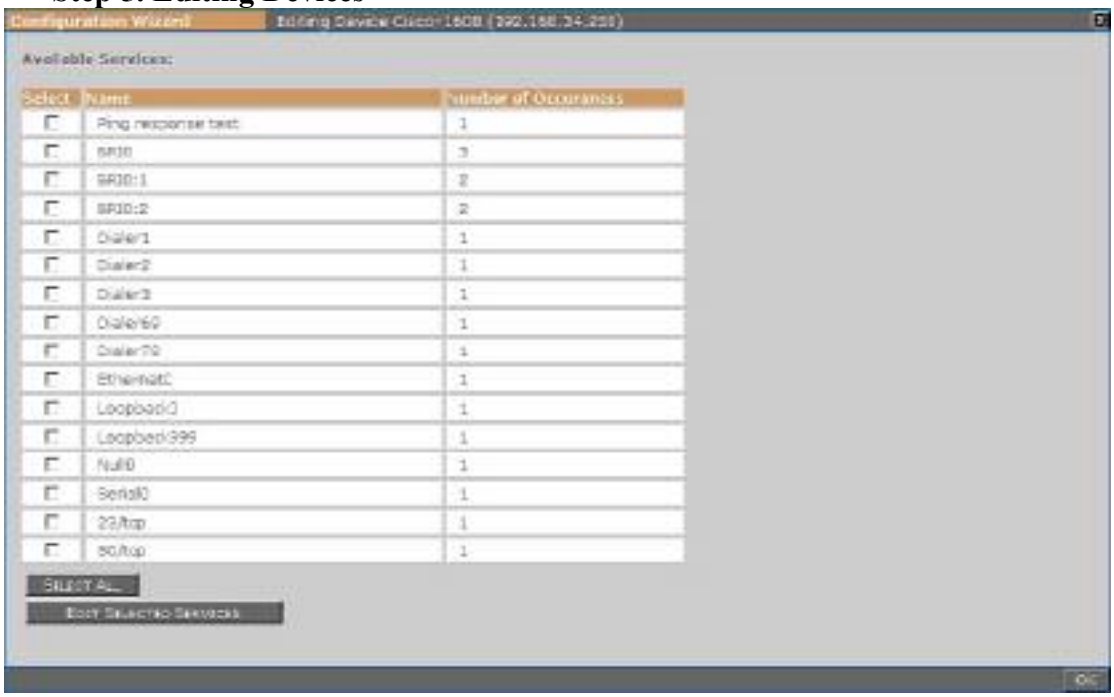
In this step you can choose to have an alarm raised when the list of individual services is detected for each device. This may occur, for example, if interfaces are added to or removed from a device that is being monitored using the SNMP Interface Test. To have this alarm raised, select the checkbox before clicking 'Next'. **For more information see Chapter 4**.

Step 4. Discovery

Once you reach this step the devices have been added to NetWatch and are in the process of discovering individual services of the types you selected. The 'Discovery Status' column shows whether this is complete for each device. The page will refresh every minute, or you can click the 'Refresh Status' to refresh manually. The time taken for discovery to finish depends on the the service types selected and the scale of the device. For example, the TCP port service can take a long time for discovery to complete, while the Ping and SNMP Trap services will take a negligible amount of time.

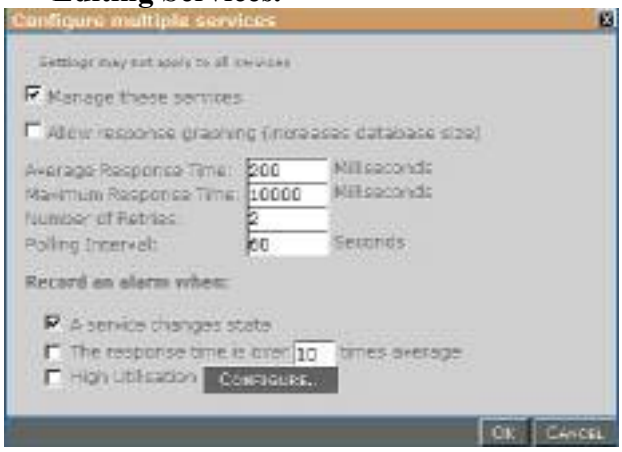
When the status of a device reads 'ready' the device can be edited. To edit a device select it and click 'Edit Selected Devices'. You can edit more than one device at a time, and you can come back and edit more devices as they complete their discovery. At any time before you finish the wizard, the **Configured?** Column on Step 4 keeps track of what devices have been edited in this session. The **Editing Device** window, described below, will pop up when you edit a device or devices; if you edit any devices you *must* click on 'Finish' on this screen when you are finally finished in order to save the changes you have made.

Step 5. Editing Devices



This step shows a listing of all the services discovered for a set of devices. Services can be configured individually or in groups. To edit a service select it and click 'Edit selected services'.

Editing Services.



There are a number of settings that can be configured for each service. Each of these settings has a default.

A service can be *managed* or *unmanaged* using the provided checkbox. If a service is unmanaged this means it will not be polled for status information.
The polling interval is the amount of time between polls. You can increase this to reduce the amount of network traffic created by NetWatch.

The Average and Maximum response times of services can also be set. These response times are set in milliseconds. (1000 milliseconds=1 Second).

You can choose to raise an alarm when the service changes status or when it is slow to respond.
For more information on configuring services refer to Chapter 4.

Data Archiving.

Data archiving is used to store historical bandwidth usage figures for Daily, Weekly, Monthly and Yearly graphs. Data Archiving is turned off by default. When data archiving is turned on the amount of Hard disk space required is considerably increased. For example, an average Access Router for 10 days requires approximately 17 megabytes of space.

Enabling Data Archiving.

Archiving is enabled through the 'Administration' section of Netwatch. The 'Archiving' configuration page allows you to specify how long you wish to store Daily, Weekly, Monthly and Yearly usage figures. This page also gives you on idea of how much space archiving will require on your hard disk based on your current configuration. Note that these are just estimates and you will need to monitor your disk usage to prevent the disk from filling up. A full disk in NetWatch will prevent monitoring from taking place.

Disabling Data Archiving.

To disable archiving simply set the Daily, Weekly, Monthly and Yearly archive periods to '0' and save the changes.

Chapter 3 – NetWatch Visualisation

NetWatch provides a unique way to visualise your network, by creating a network visual over a background image. The background can be any image in the form of a gif, jpg or jpeg file.

Managing Visual Backgrounds

A visual can use any graphic image as a background. These background images can be uploaded into the visualisation section and used for a new visual set-up. The background image for a visual can be changed at any time without otherwise affecting the visual in any way – i.e. the nodes and links on the visual are not affected.

Visual Backgrounds Supplied with NetWatch

NetWatch supplies you with a number of built in images for building your visuals. When you install NetWatch, they are automatically available in the **Edit Visuals** page. Additional graphics are also available on your NetWatch CD, in the **MapImages** directory, or from the NetWatch page on the Crannog Software website. For more information, contact support@crannog-software.com. Visual backgrounds can be geographical maps, blank images or even conceptual drawings of your network or system.

To Create a New NetWatch Visual

- In the **Admin** section, navigate to the **Background Admin** page.
- Select the graphic file you wish to use for the background using the **Browse** button.
- In the **Description** field give the Visual a recognisable name.
- Click 'Upload' to create the visual.

To Rename a Visual

- Navigate to the **Background Admin** section.
- Changes the **Name** field next the file.
- Click 'Update'.

To Delete a Visual

- Navigate to the **Background Admin** section.
- Click the 'delete' button next the graphic you wish to delete.

To Create a Visual with an Existing Background

- Navigate to the **Background Admin** section.
- Click the 'clone' button next the graphic you wish to delete.
- Enter a unique name for the new visual.
- Click 'Update'.

To Change the Background image of a Visual

- Navigate to the **Background Admin** section
- Click the **Change Map** button next the visual whose background you wish to change.
- Select the desired background image and click OK**.**

Drawing the Visual

A NetWatch visual allows your Network to be viewed in a unique way where each configured device is considered a network node. Nodes are placed on the map to represent devices on your network, with links drawn between them to represent the network paths.

Enter Administration Section.

- Click on the **Edit Visuals** button.

Add and Position Network Nodes

- Right-click on the network visual
- Click **Add Node**
- Select the node from the list provided
- If required, left-click on the node and drag the node to the desired position.

Add links between two nodes.

The link represents the network interface the 2 nodes use for communication.

- *Right* click on a node this is called the 'Connected from' node. All link information (i.e. status and utilisation) will come from this device.
- Select **Add Link**.
- Select the interface corresponding to the link.
- Drag the provided line from the 'connected from' node to the 'Connected to, node and left click.
- Select to interface on the 'Connected to' node then the link is complete.

Define actions for Node and Links

In the **User** view, the nodes and links provide possible actions on the right-click *context menu*. By default, a link provides the option to show utilisation on that interface and a node lets you view a list of services or a list of alarms for that device. You can also add other actions that correspond to URLs that are opened in a browser window. These actions, where configured, will appear on the context menu.

To add an action to a Node\Link: -

- In **Edit Visuals** right-click the Node\Link and select **Define Actions**.
- In the popup Dialog, enter an Action Label and URL in the spaces provided.
- Click **Add** and, when all actions are added, **OK**.

Set the default action taken on clicking a Node\Link.

The default action taken when left-clicking a node\link in viewer mode can be defined here in edit mode. This can be a built-in or user defined action.

- Right-click the node and select **Set Default Action**.
- Select the action to be executed when a user right clicks that node.
- If you select **Display Map** then select a map from the list that appears.

Align Node Descriptions.

The node description can be above, below or to the right or left of the node. This feature is useful when nodes become cluttered on the network Visual or if the text colour clashes with a background item.

- Right-click on the desired node.
- Select **Description Alignment**.
- Choose the required alignment.

Set Node Description Colour

The node descriptions are white by default. This colour can be changed to either green or black using the 'Description colour' menu item.

Saving Configuration Set-up

Once you are finished creating your visual set-up, save your configuration by clicking save in the **Admin** panel on the map.

Using a NetWatch Visual

When you click on 'View your Network' on the welcome screen you enter a visualisation mode where nodes or links cannot be modified and the status of each node is updated automatically. You can select the visual you wish to monitor from the list in the top left. The legend shows you what the various colours mean. If you wish to find out more about a node or link, you can try one of the following:

View Node Alarms

- Right click on the desired node
- Select 'Show alarms' from the menu.

View Node Reports

- Right click on the desired node
- Select 'Show Services' from the menu.

Using Node Tools Submenu

The tools submenu allows you to:

1. View the Node Configuration
2. Ping the Device
3. Perform a simple SNMP Get.

View Traffic between 2 Nodes

- Right click on the desired link
- Select 'Show Utilisation' from the menu.

Node Colour Code System

Green: No alarms Present and all *managed* services are currently up.
Yellow: Alarms are Present. (View Node Alarms.)
Red: One or more of the managed services of this device are down.

Link Colour Code System

Grey: The Link is not being managed.
Dark Green: Utilisation is less than 10%.
Light Green: Utilisation is less than 30% and greater than 10%.
Yellow: Utilisation is less than 50% and greater than 30
Light Orange: Utilisation is less than 80% and greater than 50%.
Dark Orange: Utilisation is less than 80% and greater than 50%.
Red: The link is down.

For quick reference on these colour codes, see the panel at the bottom of the map.

Chapter 4- The Alerting System

How NetWatch Alerting Works

NetWatch can throw alerts when certain events occur or if thresholds are exceeded on the network. When an alert is thrown, it is logged to the database and displayed on the http reports and indicated on the NetWatch visuals. It can also be forwarded to various recipients.

What Can Trigger an Alert?

There are various different types of alert, all caused by different events or conditions:

Device Alerts

These are alerts that occur on a device as a whole. Currently there is one type of device alert:

- **Service List Alert**
  This alert is triggered whenever services are added to or removed from a device. This can happen, either during manual discovery of a device in the Edit Devices or Add Devices sections, or automatically, if NetWatch detects that SNMP interfaces have been added or removed from a router.

To add or edit the Service List Alert, go to **Add Devices** or **Edit Devices** in the **Admin** section and proceed through the wizard to **Step 3**. Select the option to "**Record an alarm if services are added to or removed from any of these devices**".

Service Alerts

These alerts can be triggered on one or more services within the devices:

- **Status Change Alert**
  Triggered when a service changes state. This is relevant to all services that have the concept of state, i.e. Ping Test, TCP Port Test and SNMP Interface test
- **Response Time Alert**
  Each of the services mentioned above involves a poll of some sort, whether it be a Ping operation, TCP port connection or an SNMP poll. These services are configured with an expected response time for the operation. NetWatch can trigger an alert when the response time exceeds a set multiple of that expected response time.
- **Utilisation Alert**
  You can set network traffic thresholds for the purpose of alerting. The utilisation alert will trigger when traffic rises above a set percentage utilisation, either immediately or after the traffic level is sustained over a specified time period.

To add or edit a service alert for a new device, when you get to the **Discovery** stage with discovery complete, edit the required devices and select the services on which you want to configure the alerts. Click **Edit Services** to show the **Configure Services** window. The bottom section of this window deals with alerts. The type of alert shown depends on the type of services that you are editing. Note that not all alerts apply to all services so if, for example, you have selected a ping service and an interface

service, the utilisation alert will only apply to the interface service. Click **OK** when finished and make sure you click **Finish** on the device wizard to apply the changes.

To add or edit a service alert for an existing device, go to **Edit Devices** in the **Admin** section. Select the required device and proceed to the final stage where the **Available Services** are listed. Select the required services and click **Edit Selected Services** and proceed as described above. Once again, when you are finished, make sure to click **Finish** on the device wizard to apply the changes.

Receiving Alerts

Once an alert has been triggered, it is recorded in the database. This makes it immediately available to the alert reports and the NetWatch visuals that include the device. Alert controllers can then forward the alert to recipients using either Email or Syslog.

Web Based Reports

Every alert raised is displayed in a report, from where you can acknowledge the alert. **This report is described in further detail in chapter 5**. This report is also available from a visual. If a node is yellow on a visual it has unacknowledged alerts.

Email

These are alerts that are sent to specific users or groups, which are set up for the specific device or service. Email alerts are sent when an alert is thrown, however you can set up delays for most alerts and you can also set up alerts only to be thrown if a number of alerts are generated in a certain time period (throttling).

SMS

These are an extension of email alerts in that you can use an SMTP to SMS gateway to forward an alert by text message to a GSM mobile phone. Crannog software provides a product called **SMS Manager** for this purpose. Contact Crannog Software for more details.

Syslog

The alert message, just as in the email, is forwarded to a specified address as a syslog message. This is useful for integrating with other enterprise management software.

Setting up Alert Controllers

To set up Alert Controllers go to the Configure Alarms page in the Admin section. This will give you the following options

- SNMP Notification Alerts
- Service List Alerts
- Response Time Alerts
- Status Change Alerts
- Utilisation Alerts

The options within each alert controller are always the same. An alert will be handled by one alert controller, depending on the type of alert indicated by its name. Within the alert controller configuration, you can set one or both of the two options:

Email Recipient

This allows you to set up a number of email recipients, specifying the SMTP server to use. If you only have one SMTP server, it makes sense to set the default server in the **System Settings** page in the **Admin** section. If you don't specify an SMTP server in the alert controller configuration, this default server will be used. Enter as many email addresses as required.

Syslog Recipient

This sends the alert to a specified address using the Syslog protocol. You can specify one or more IP addresses to which the messages will be sent.

Chapter 5: The Reporting System

NetWatch prides itself on its ability to report on network status anywhere at anytime. All NetWatch reports can be viewed through an Internet browser and are 100% web based. This enables the user to view reports on the move instead of being tied down to a centralized monitoring machine based in head office or the computer department.

Alerts

NetWatch alert reports show the current alerts triggered by the system. These are shown when you first open up the reports section. In this section a user can acknowledge alerts to tell the system they have been viewed and to not send out an email or SMS alert if not already sent. In this section the user can view unacknowledged alerts, view acknowledged alerts and view all alerts. You can also pick a device in the list of devices and choose to view alerts just for this device.

Devices

NetWatch device reports show the status of the devices since last poll by the NetWatch backend. Here you can see if the device is online or if it is unresponsive. You can also click on the quick links to try to telnet to the device or to ping it. If you click on the device name link you will be shown the services for this device.

Services

NetWatch service reports show the status of the services on the device. These can be interface tests, bandwidth graphs and ping response test results. By default only managed interfaces or services are shown here, click the show unmanaged to view all services. For interfaces that are managed and support bandwidth collection you can click on the link in the tools section to see the bandwidth graph for that interface.

Utilisation

There are two specific utilisation report types:

1. This utilisation report shows in a tabular format the Current, Average and Max percentage utilisation values for each device within the last 24 hours.
2. This utilisation report shows the amount of bandwidth each interface of a certain device used for a certain, month along with the device total for that month.

Configuration Reports

NetWatch configuration reports show the current, up to the minute configuration details for a particular device. Simply click on a device name in the list and press the show configuration button. This will show all the managed – unmanaged interfaces and services on the device in a report format along with its configured elements, such as alerting options.

Syslog Messages

NetWatch syslog reports show a list of syslog messages received by the system. The **All Syslogs** button shows a report on all syslogs received by the system. You can also click on a device in the list of devices to view a report on Syslogs received from that device only.

Chapter 6: Syslogs

The Syslog protocol is an event notification protocol that allows a machine be it a Server, Hub, Switch or Router to send event notification messages to 'event message collectors' -also known as 'Syslog servers'.

Syslogs and NetWatch
NetWatch has its own built in fully featured Syslog server. Any Syslog messages sent to the NetWatch Server will be stored in a Syslog message event database.

Enabling Syslog Reception
To allow NetWatch to receive syslog messages, turn on the "Use Syslog Receiver" option on the Admin | System Settings page. The NetWatch service requires a restart after changing this setting.

Syslog Severity/Priorities and Reporting
Each syslog sent from a device has an encoded severity. These are described in the following table.

Emergency:	System is unusable.
Alert:	Action must be taken immediately.
Critical:	Critical Conditions.
Error:	Error Conditions.
Warning:	Warning Conditions.
Notice:	Normal but significant condition.
Informational:	Informational messages.
Debug:	Debug-level messages.

Each one of these severity levels is assigned to a NetWatch priority level as decided by the administrator in the 'Syslog Configuration Section'.

Only messages of a certain priority will be viewed and processed by the reporting system. The 'Syslog Configuration Section' can also configure this.

For details of viewing and processing syslog messages refer to Chapter 5 'The Reporting System'.

Configuring Devices to Send Syslogs to NetWatch
For Syslogs to be viewed and processed by NetWatch devices must be configured to send its Syslog messages to the NetWatch Server.
Using the CISCO IOS for example syslogs are sent to the NetWatch Server with the following command:

Logging *Hostname or A.B.C.D* (IP address of the NetWatch Server)

Chapter 7: Utilities

Backing up the database from the web interface
To back up your database from the web front end you need to open the backup control from the utilities section. This brings up **Netwatch Backup** screen. Enter in a folder on the server to backup to, or you can leave this blank and the default folder will be used. The default folder is set-up in the system settings section and defaults to "c:\NetWatchbackup". Once you have either entered a folder or you are happy to use the default, then you can press the backup button, which will copy the current database and visuals folder to the backup directory.

This may take some time, as the database can be quite large depending on the amount of devices in the system. Also make sure you have enough space on the NetWatch machine to copy the volume of information – ideally, the free space should be much greater than the side of the **MySQL** directory and its contents, as the bulk of this will be backed up in this operation.

Manual backup of maps and database
Optionally you can do a manual backup of the maps and the database. This can be done by copying the maps folder from the **NetWatch\tomcat\webapps** folder to a backup folder. Next, open the **MySql\data** folder and copy the penknife directory in the data section to a backup folder.

Restoring from a backup
To restore backed up files, shut down all three services from the **NetWatch Service Manager** and copy back over the files. If the backup was a manual one, simply reverse the process described above. If it was a backup from the **NetWatch Backup** page, copy the contents of the **database** directory to the **mysql\data\penknife** directory and copy the entire **netwatch** backup directory into the live **netwatch** directory. Restart the three services and check the NetWatch output log and NetWatch error log to make sure that the system started up successfully.

NetWatch Security
NetWatch provides the option to apply password protection on the user, operator and administrator sections of NetWatch**. For information on enabling NetWatch Security see Chapter 9.**

Search visuals for specific IP addresses
NetWatch allows you to search for a device by IP address on the system. Go to the **Search** page in the **Utilities** section and specify the IP address and press **Enter**. A list of maps containing a device with this address will be displayed. The device name corresponding to that IP address will also be shown.

Setting up a licence
A NetWatch licence is required to run NetWatch continuously. You will receive the licence, either in a binary file or in ASCII hex code format. To load the licence, go to the **Licensing** page in the **Utilities** section. Depending on the format of the licence:

- Paste in the hex format if that is how you received the licence and click **Decode,** or
- Browse to the binary licence file (extension .lic) and click **Load.**

The licence details will be displayed on the screen along with an expiry date, if any. To save this license to the system, click **Update** to complete the operation.

Logs
The NetWatch logs provide system administration information and are mainly used for system maintenance and debugging. These logs can also be found in file form on the NetWatch server: the NetWatch service logs will be in the **\Netwatch** directory, while the Tomcat logs can be found in the **\Netwatch\tomcat** directory.

Manual
This is an online PDF version of the NetWatch manual.

Status
The NetWatch Server Status page provides details, which are important to keep track of for the smooth running of NetWatch. The information supplied includes:

- The time the system was started
- Free Disk Space
- Free Memory
- Total System Memory
- The number of device managed by NetWatch
- The total number of managed services.

Note that, if memory or disk usage runs low, these items will be highlighted in red.

Chapter 8: Services, Discovery and Polling

If you are new to configuring NetWatch, please refer to Chapter 2, “Configuration” for a step-by-step guide to setting up devices before reading this chapter. This chapter describes in detail the operation and advanced configuration of the various types of monitoring NetWatch can carry out on a device.

How NetWatch services work

Most of the information gathered by NetWatch about a network is gathered on a device-by-device basis. Each device on a network, be it a router, switch or application server offers a number of different services to its users, including network management stations like NetWatch. These services are things like basic network connectivity, connections to other networks and applications like web or telnet servers. Since the services offered by a device are of several different types, NetWatch handles them differently.

Discovery

Whenever you change the types of service you wish to monitor on a device, you must discover services on the device. What this does is contact the device to determine what individual services of each type the device supports. For example, when a device with an SNMP Interface Test service type is discovered, a service is created for each interface the device contains.

Each service type can be configured with default properties that are applied to each of the services it creates. These properties set things like the average and maximum response times NetWatch should experience when it checks the status of a service on the device. You can change these properties for some or all of the services after they have been discovered if you find the defaults are producing too many alerts.

The SNMP Interface Test service

The SNMP Interface Test service type can be added to any device that supports SNMP. See Appendix B for more information about SNMP. On discovery, a service is created for each interface the device supports. You may find that many more services are created than the device has physical interfaces. This can happen for many reasons; some WAN interfaces are divided into many lower-capacity sub interfaces; ISDN interfaces are usually reported by a router as separate bearer channels; virtual dialler interfaces are often detected; and sometimes an interface is listed by a device more than once on order to provide special management features.

This service type is one of the most powerful supported by NetWatch. Along with testing the status of an interface, a service can be configured to read usage information for the interface. This allows you to create graphs of bandwidth utilisation for an interface, and allows the map applet to colour links according to their percentage utilisation.

When you add the SNMP Interface Test service type there are several options you can configure to control how the discovered services will work.

- **Average Response Time:** This is the average time in milliseconds you would expect a successful check of the status and utilisation of a single interface to take. This is used to decide when to raise an alert that a device is responding slowly. If you are unsure of this, leave the default value of 200 milliseconds. If you are monitoring a device across a slow WAN link, or if you experience a lot of slow response time alerts on the device it may be a good idea to raise this value.

- **Maximum Response Time:** This is the maximum number of milliseconds NetWatch will wait for a response from the device before retrying a check or giving up. After the third timeout NetWatch will stop trying to check the status of an interface and report a timeout as the status of that interface. You may find that some interfaces are reporting timeouts and some report a proper status; this can happen when a device is very busy and is ignoring a lot of the SNMP requests it receives. You may wish to change this value if you find this is the case; a shorter maximum response time with a higher number of retries would be more likely to get a status for each interface (at the expense of slightly more network traffic).

- **SNMP Community String:** This is the read-only community set up on your device. Usually a device supporting SNMP will have two communities, which are rather like passwords, one of which only allows the reading of values and the other that allows reading and writing of some values. In a great many cases the community that supports reading only is the default value, "public". If you find that the SNMP Interface Test is not working you may need to check this value. Note that this value belongs to the service *type* on the device; you can't change it for an individual service.

- **Use Netwatch Server Clock** By Default, Netwatch uses the time on the device being managed to record various time related statistics. This is the ideal solution in most situations. However on some highly utilised devices the time reported can be incorrect. In this situation it is advised that you use the time on the Netwatch server.

- **Test Community:** This performs a simple 'SNMP Get' to ensure the correct SNMP community string has been configured for this particular device**.**

- **Management Policy:** This allows you to decide what tasks will be carried out by each service created by the agent. You can choose which services are managed and whether utilisation statistics are gathered. You can easily change these settings for each service at a later date. The options are:

- **Use default management settings for new services:** The default, this allows NetWatch to decide how to deal with each newly created service. If this is selected most services will be managed when created, but some (for example,

ISDN, virtual and dialler interfaces) will be unmanaged. If NetWatch does not have specific support for the type of device you are setting up then all services will be managed when created. If this option is selected no newly created service will collect utilisation information until you choose to collect it.

- **Manage all new services, but no bandwidth collection:** All newly created services will be managed, but none will collect utilisation statistics. You can choose which interfaces to collect utilisation statistics for later.
- **Manage all new services, with bandwidth collection:** All newly created services are managed and those that offer utilisation information will collect it. Note that choosing this option could cause your database to become enormous as utilisation information takes up a lot of space.
- **Don't manage new services:** No new service is managed.

The TCP Port Status service

The TCP Port Status service type can be added to any device. On discovery it scans the device for listening TCP ports within the default "Common Ports" set and creates a service for each one found. A web server, for example, will have port 80 open for HTTP. Once services are created they are polled regularly to ensure they are still active. The options for the TCP Port Status Service type are quite straightforward. The 'Port Set' and the contents of a particular 'Port Set' that is scanned are configurable. You can also configure a 'Range Port Scan', which scans all ports within a predefined range.

- **Average Response Time:** As with the SNMP Interface Test, this is the number of milliseconds a successful check of a port should take. The default is 60 milliseconds since TCP connections can be made or refused very quickly. If you find that you receive a lot of slow response time alerts you may consider raising this value.
- **Maximum Response Time:** As with the SNMP Interface Test, this is the longest NetWatch will wait before giving up on a check and either retrying or reporting the port as timed out. Note that timed out is different to unavailable; if a device is working but the server listening to a port has crashed the device should refuse any request to open a connection to the port rather than ignore it.

The Ping Response Test service

This is one of the simplest service types NetWatch supports. On discovery a single service is created that checks the device is responding to an ICMP echo request. This is the same test carried out when you use the "ping" command line tool present in virtually every operating system. The service type allows you to set the average and maximum response time that will be set in the service when it is created; if you change these default values at a later date they will have no effect. To change the average or default response time for the Ping Response Test you must configure the Ping Response Test service, not the service type.

Response Time Graphing

This can be enabled for both the *Ping Response Test* and *the SNMP Interface test*. It is configured using the configuration screen for the *Ping Response Test* and *the SNMP Interface test*. Once Response time graphing is selected the Response time

graph for each service can be viewed in the Reports section. It is important to note that response time graphing does use up a lot of extra database space.

The Receive SNMP Notifications service
If a device is configured to send SNMP Notifications, or "Traps" to NetWatch, you can choose to handle them by adding this service type to the device's configuration. See Appendix B for more information about SNMP notifications.

When you add the Receive SNMP Notifications service type to a device you must specify which of the traps the device sends you wish to record. NetWatch at the moment supports only the six standard SNMP traps. Every time a trap is received from a device with the Receive SNMP Notifications service type selected it is checked against the list of traps selected in the service type. If the trap is selected, it is recorded.

When services are discovered on a device with the SNMP Notification service type selected a service is created for each selected trap type. This allows you to alert on some of the recorded traps. For example you may wish to record link up and link down traps but alert on a cold start trap.

Configuring services
When you have discovered services on a device it is easy to change their settings from the defaults provided by the service type. When you select a service or a group of services to configure you can set most of the values you can set defaults for in the service type. In addition you can set how often NetWatch polls each service to check its status, and you can manage or unmanage a service.

Chapter 9: Security

Three levels of security are available in NetWatch. Each level allows access to different NetWatch functions.

Levels of Security

The levels of security are Administrator, Operator and Viewer. The Administrator has access to all NetWatch functions, including security administration. The Operator can view network visuals and has full access to all reports. The Viewer can view network visuals and reports.

Enabling Security

From the Admin menu, select Utilities and then Security. NetWatch comes with default passwords for each security level, which can be changed as required. Select the Enable Security button. You will then need to close the browser session and restart the Web Server (Tomcat) using the NetWatch Service Manager in the System Tray.

Appendix A: Crannog Software And Support

Crannog Software was founded in 1998 to meet the growing demand for niche data communications software. Since it's inception Crannog has concentrated mainly on management solutions for the burgeoning Cisco market, a direction we intend to continue in all future developments. The five-man management team has over 10 years experience designing and selling data communications solutions and include two of Irelands first Cisco Qualified CCIE engineers so our technical understanding of the market is second to none.

Our first product ISDNwatch is a tool for monitoring and managing ISDN data networks with particular emphasis on cost control and call visibility. Since its release in 1999 ISDNwatch has been a huge success, a trend we expect to continue with the current release of ISDNwatch Version 3.0 and higher, our billing module, ISDNreporter+ and our email to SMS gateway, SMS Manager.

The evolution of the NetWatch system marks a new path for Crannog Software and shows how Crannog are keeping up with the current trends of web based systems and applications. We believe that the end has come for centralized systems and distributed web based architectures will become the Standard for all types of software including corporate business and home user.

We have recently released our **NetFlow Monitor**, which provides full NetFlow traffic capture and analysis. Web based graphical information is presented to the user showing statistics on elements such as source/destination, 'top talkers', protocol types and protocol load on the network. Individual NetFlow monitors would be installed at each network site where these statistics are required.

Crannog have developed a reseller channel across most of Northern Europe and are currently targeting the US and Australasian markets with a number of strategic partnerships with local and global companies. We have grown rapidly over the past 18 months and expect to double our size again within the next year. Our upcoming new releases and a number of new projects in the pipeline will help develop our reputation as a supplier of leading edge management solutions for today's networked world.

Getting Technical Support
We like to hear as much feedback as possible from the users of our software, with this in mind should you have any ideas or questions about the software then feel free to contact us. However for technical support, when using NetWatch from Crannog Software, the users first point of contact should always be there reseller or whomsoever they purchased or acquired evaluation from. This means that you should receive a quicker and timelier response to your support query. Any support query, which is received, will be logged and given the utmost attention from one of our dedicated support team.

Contact information

To contact Crannog Software just follow the links below. We are always keen to receive feedback about our products and our website.

- General Information about Crannog Software
  info@crannog-software.com

- Email our Support Team with your queries
  support@crannog-software.com

- Enquire from our sales team about our products & services
  sales@crannog-software.com

- Enquire from our UK sales team about our products & services
  uksales@crannog-software.com

- Telephone: +353 1 454 9196
- Fax: +353 1 454 9312
- UK Office Telephone: +44 (1242) 520917

Irish Office
34 Greenmount Office Park,
Harold's Cross,
Dublin 6W
Ireland

UK Office
Unit 2 Court Mews,
268 London Road,
Cheltenham,
GL52 6JQ.

Appendix B: SNMP

SNMP, or Simple Network Management Protocol, is a widely used standard that allows network management software to query network devices for status and information regardless of the type of device and the software it runs. The original SNMP developed in 1988 is defined in RFC 1157, and the current version 3 is fully backwards compatible. NetWatch uses SNMP version 2c when available; otherwise it reverts to version 1.

MIBs
The SNMP standard defines a large number of properties organised into a hierarchy that describes virtually everything about a device that a network manager might want to know. This hierarchy is called a MIB or Management Information Base. The SNMP standard defines a large MIB called MIB2; this describes system properties, routing information, interface status and statistics and a lot more. A large number of standard extension MIBs exist; the Interface MIB is used by NetWatch when supported, since it offers better support for high capacity interfaces than the standard MIB.

SNMP offers a way for hardware and software vendors to supply their own device-specific information in the form of *Enterprise MIBs*; most vendors have their own MIBs in addition to supporting some of the standard MIB.

OIDs
Each value defined in a MIB is referenced by its OID or Object Identifier. This is a long sequence of numbers separated by dots. Each number in an OID describes a sub level of the MIB hierarchy, thus the OID for the sysDescr object is 1.3.6.1.2.1.1.1, which means
iso.org.dod.internet.mgmt.mib-2.system.sysDescr. Most of the standard MIBs you will come across will be in the mib-2 group, and all of the enterprise MIBs are underneath iso.org.dod.internet.private.enterprises.

Communities
The original version of SNMP used a very simple secret word scheme to protect the information available from a device. Most SNMP-compliant devices support two "communities", one of which can read the value of any variable in the MIB and one that also allows setting the values that can be configured. The community is passed to the device with each SNMP request. If you are not sure of the communities on a particular device a good guess for the read-only community is "public".

Notifications
A notification or trap is a small message sent by an SNMP agent to a management station to inform the management station of an event that has just happened. Traps can be used to reduce the network traffic and load on the device caused by rapidly polling values. SNMP defines six standard traps that tell when the device is powered on or soft booted, when a link goes up or down, when an SNMP request has been received with an invalid community and when a router loses connectivity with a neighbour. In addition, there are thousands of enterprise-specific traps defined by equipment and software vendors.

Traps are not reliable; a trap may be lost somewhere between an SNMP agent and a management station. There is a much less used message called an inform that aims to solve this problem.

The Windows snmptrap.exe service

Windows NT and 2000 have the ability to receive SNMP traps by using a service called “SNMP Trap Service”. Older versions of NetWatch made use of this service, but due to compatibility problems version 1.1.3 and above use a different means of receiving traps.
If you find that NetWatch does not receive SNMP traps, you may need to disable this service.

Windows 2000
Ensure you are logged in as an administrator of the machine running NetWatch. Open My Computer and then Control Panel. In the Control Panel, open “Administrative Tools” and then “Services”. Find “SNMP Trap Service” in the list, right click it and choose “Properties”. Choose “Manual” from the list beside “Startup type:”. If the “Stop” button is not greyed out, click it then click “Ok”.

Windows NT
Ensure you are logged in as an administrator of the machine running NetWatch. Open My Computer and then Control Panel. In the Control Panel open “Services”. Find “SNMP Trap Service” in the list and select it. Click the “Startup…” button and select “Manual” from the set of radio buttons at the top. Click “Ok”. If the “Stop” button is not greyed out, click it then click “Yes”. Finally, click “Close”.

Caveats
Other network management software may require the SNMP Trap Service to be running. If you have another NMS installed it may re-enable the trap service and prevent NetWatch from receiving traps. If you find this to be the case, please contact support@crannog-software.com and we will try to help you work around this problem.

Configuring SNMP on a Cisco Router
The following instructions describe how to configure SNMP on a Cisco router running IOS.

Care must always be taken when editing router configuration. If in doubt, consult your network engineer.

1. Telnet to the router:

```
C:\> telnet <router address>
User Access Verification

Password:<password>
```

2. Enter enable mode (note that the password may be different to the login password):

```
Router>enable
Password:<password>
```

3. Start configuring from the keyboard:

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

4. Add a read only community "public":

```
Router(config)#snmp-server community public RO
```

5. Enable standard SNMP traps:

```
Router(config)#snmp-server enable traps snmp
```

6. Add NetWatch as a trap receiver (to send traps with the community "public"):

```
Router(config)#snmp-server host <address of NetWatch> public
```

7. Quit config mode:

```
Router(config)#<CTRL-Z>
```

8. Store the configuration to flash:

```
Router(config)#wr mem
```

Further Information
For further information on SNMP, you can refer to any of the following:

Cisco Information on SNMP - www.cisco.com/warp/public/535/3.html
An SNMP tutorial by Yoram Cohen - www.rad.com/networks/1995/snmp/snmp.htm

Appendix C: NetWatch And IIS

NetWatch can be configured to use IIS as its default web server. To achieve this the following instructions must be completed. **We strongly recommend that, if the IIS server is to be accessible from the internet, that all service packs and security patches are applied before making the server available. For more information see http://support.microsoft.com**

1. Install IIS.

2. Stop Tomcat Service

3. Change the tomcat port to 8080 if it's running on port 80.
Open /tomcat/conf/server.xml and look for the 'Normal HTTP' section a change the port parameter from 80 to 8080.

4. Double-click isapi_redirect_nt.reg(if you are running NT) or isapi_redirect_200.reg (if you are running W2K) to import the extra configuration information into your registry. These files can be found in the following folder: - c:\NetWatch\tomcat.

5. Open IIS management console and create a new virtual directory called "jakarta" and make the physical path "C:\Tomcat\bin". Make sure that this virtual directory has "Execute" permissions.

6. In the IIS Management Console right-click on your machine name (not the root web) and select properties. Click the Edit button next to the "Master Properties" for the WWW Service. Select the "ISAPI Filters" tab and click "Add" Name the filter "jakarta" and for the executable, browse to C:\NetWatch\Tomcat\bin\isapi_redirect.dll file.

7. Now go to the control panel, select Services and restart the IIS Admin service (make sure Word Wide Web Publishing Service restarts as well). After you have restarted, go back to the ISAPI filters screen and make sure that the jakarta filter has a green arrow next to it. If it does, then everything is working.

8. In the IIS Management Console right-click on your web root and select properties. Now go to the Home Directory tab. Set the local path to c:\NetWatch\tomcat\webapps.

9. In the IIS Management Console right-click on your web root and select properties. Now go to the Directory Security tab. Click the edit button. Now uncheck the 'Integrated windows authentication' checkbox.

10. Restart the tomcat service.

11. Due to the security considerations with IIS, we strongly recommend that you install all of the available IIS security patches available from Microsoft. More information on this can be found from http://support.microsoft.com

Appendix D: Integrating Netwatch and Netflow

Firstly it is important to note that Netwatch and Netflow must be installed on two separate server machines. The integration of the two products is done thru the use of Netwatch Visuals. Once both Netflow and Netwatch are fully configured and your Netwatch visual is complete integration can begin.

The following example will guide you thru the process:

1. Two Cisco Router are being monitored be Netwatch and Netflow.

2. In the Netwatch 'Edit Visuals' section each router is plotted on a Visual and the Serial0 interface is drawn between each node.

3. You now have to find the URL that is used to view the Netflow Graph for the Serial0 interface in Netflow.

4. Now that you know the URL for the required Netflow graph you can use the 'Define Actions' feature in Netwatch to associate the Netflow Graph with the Correct Netwatch Link. (Define Actions is explained in further detail in Chapter 3).

Appendix E: Auto Discovery

Given a starting IP address and appropriate community strings NetWatch will automatically discover your network and allow you to add devices found as NetWatch devices.
Netwatch uses 2 different methods to discover your network. One can use one of the methods individually or you can use both together. These two methods are described below:

Discovery Methods

CDP Discovery
CDP is a Cisco **proprietary** protocol. It is used by Cisco routers and switches to ascertain information about neighbouring routers and switches. CDP is enabled in the configuration by default.

Route Table Discovery
This method of discovery scans a devices route table to ascertain information about your network. This method should be used if you have a non-Cisco network.

Discovery Filters
Netwatch Auto discovery can uses filters to limit the scope of the discovery.
These filters let you define the network(s) or address ranges(s) that you are interested in. Only devices that match the filter(s) will be discovered.
There are two types filters that can be applied:

Network Filters
With this type of filter you specify a Network Address and Network Mask. With this type of filter only device with this network subnet will be discovered.
E.g.
Network Address: 192.168.34.2
Subnet Mask: 255.255.255.0

With this type of filter only device with the IP address with 192.168.34.X will be discovered.

IP Address Range Filters
With this type of filter only devices within a specified IP address range will be discovered.

Appendix F: Third Party Software

NetWatch makes use of some third party libraries, distributed under various licenses.

jspSmartUpload

This product includes software developed by Advantys (http://www.advantys.com), distributed under the Advantys Freeware license contract, a copy of which is available at http://www.jspsmart.com/liblocal/docs/legal.htm#free.

MySQL

NetWatch uses **MM.MySQL v2.0.13** for database access, available at http://sourceforge.net/projects/mmmysql/ . This is distribute under the lesser GNU public license, a copy of which is available at http://www.gnu.org/licenses/lgpl.html.

Jakarta Tomcat

NetWatch includes software developed by the Apache Software Foundation: http://www.apache.org.
Jakarta Tomcat v3.2.3 is available at http://jakarta.apache.org/tomcat and is distributed under the Apache Software License, a copy of which can be found at http://www.apache.org/LICENSE.