

Remote Manager

Reference Manual and User Guide



Table of Contents

1.0	Introduction	5
1.1	Database	5
1.2	Front End.....	5
1.3	Active Mode / Multi Active Mode	5
1.4	Listening Mode	6
1.5	Poll Schedules	6
1.6	Audit Trail	6
2.0	Installing Remote Manager	7
2.1	System Requirements.....	7
2.2	Installing Remote Manager	7
2.3	Installing the Communications Device Driver	7
2.4	Configuring Remote Manager	8
2.5	Configuring Internet Explorer	9
2.6	Launching Remote Manager.....	10
3.0	Main Screen Overview	11
4.0	Site Editor	12
4.1	Tabbed Areas:	13
4.2	Creating, saving and deleting units	25
5.0	Built-in Terminal Program.....	27
6.0	Find	28
7.0	Operations	30
7.1	Choosing units for remote operations.	31

7.2	Operation Types	32
7.3	Launching update operations.....	38
7.4	Results	38
7.5	Active Mode	38
7.6	Multi Active Mode	39
7.7	Listening Mode	40
7.8	Scheduled Operations	41
8.0	Results & Re-Polls	43
8.1	Remote Operation Session Summary.....	43
8.2	Retry Operations.....	44
8.3	Session Results	44
8.4	Activity Log	46
9.0	Group & Site-Specific Parameter Management.....	48
9.1	Groups.....	48
9.2	Power Group Membership	49
9.3	Site Specific Parameters.....	50
9.4	Assignments	52
9.5	Power Delete	53
10.0	Importing and Exporting Units	54
10.1	Common procedures	54
10.2	Import by Site Number.....	55
10.3	Import or Export by Primary Key.....	55
11.0	Options	58
11.1	General Standard	58
11.2	General Advanced	59
11.3	General SSH	61
11.4	Listening Options	61
11.5	Active Options.....	62
11.6	Multi Active Settings.....	62

11.7	User Interface	63
11.8	Users	64
11.9	Permissions	64
11.10	Email	64
11.11	Report Options	65
12.0	Polling	66
12.1	Polling Principles	66
12.2	Creating a Polling Schedule	67
12.3	PPP Reports	68
12.4	TPAD Reports	77
12.5	Eventlog Outage Report	84
12.6	Configuration Differ	87
13.0	Reports	90
13.1	Date and time selection	90
13.2	Group Selection	90
13.3	Unit Selection	90
13.4	Report Selection	90
13.5	TPAD Reports	90
13.6	PPP Reports	91
14.0	Stat Setup	96
14.1	Adding a Statistics Class	96
14.2	Always use direct IP	96
14.3	Tidy Bins	96
15.0	Map – Real Time Performance Monitoring	97
15.1	Map View	97
15.2	Show / Hide Groups	98
15.3	Non-contactable sites	98
15.4	TPAD sites	98
15.5	GSM/3G Sites	98

15.6	GPS data.....	99
15.7	Map Options	99
16.0	Example I - Updating firware and Configuration	101
16.1	Starting Point	101
16.2	File Links	101
16.3	Update Commands.....	102
16.4	Merge the file links with the other units in the group.....	103
16.5	General Options.....	105
16.6	Remote File & Configuration Update Options	106
16.7	Performing the Upgrade.....	107
16.8	Viewing the results.....	107
17.0	Example II – Monitoring the performance of a GPRS/3G/UMTS/HSDPA network.....	110
17.1	Outline	110
17.2	Router Configuration.....	110
17.3	Remote Manager Configuration	112
17.4	Ensure that polling occurs at a specific time	118

1.0 INTRODUCTION

Remote Manager is a database driven management system that can be used to:

- manage firmware and configuration upgrades on remote Digi Transport routers
- collect hourly performance data and produce graphs and reports based upon this data
- highlight problem sites in real time on a map
- show the current location of sites on a map from GPS information
- check that the configuration files on the remote units match the base configuration files

Remote Manager is NOT an SNMP or event based management tool.

1.1 Database

The database is capable of storing:

- unique identifiers for each router (e.g. site name, site number, serial number, address)
- connection details for each router
- user configurable site-specific parameters for each router
- commands to issue in order to update the configuration
- files to load in order to update the configuration and/or firmware
- history of commands issued and files loaded for each router
- group membership (a router can be a member of more than one group)

1.2 Front End

Remote Manager allows any files, or update commands to be quickly assigned to “groups” of routers. Updates on individual routers or groups of routers can then be performed by the following methods:

- Active Mode – remote manager actively connects to one router at once
- Multi Active Mode – Remote Manager actively connects to up to 50 routers concurrently
- Listening Mode – single operation on each serial number
- Listening Mode – reoccurring operations on each IP address (operation runs again if serial number associated with the IP address changes)
- Listening Mode – reoccurring operations on each IMSI (operation runs again if serial number associated with the IMSI changes)

1.3 Active Mode / Multi Active Mode

In Active Mode Remote Manager actively connects to one router at once using a variety of connection methods, the most common being “Direct IP”. Once connected, Remote Manager will update the configuration and/or firmware as appropriate.

Multi Active Mode provides the same functionality as active mode in addition allowing connection to up to 50 routers concurrently.

1.4 Listening Mode

In listening mode Remote Manager will “listen” for UDP IP packets containing the IP address, serial number and other information from the remote router. Once such a packet is received, if an update is required, Remote Manager will connect to the router on the IP address and perform the operation.

Listening mode can be used to automatically upgrade the firmware and configuration including site specific settings as routers are installed and/or swapped out. This is sometimes referred to as “Zero Touch”

In order for this to be possible it is necessary to know in advanced **one** of the following:

- The serial number of the router that will be sent to each site
- The IP address of each site
- The IMSI number that is allocated to each site (IMSI is a unique identifier on every GSM/UMTS SIM card)

There are three types of listening mode operations:

- Single operation on each serial number
- Multiple operations on each IP address
- Multiple operations on each IMSI

1.5 Poll Schedules

Remote Manager can be scheduled to poll units automatically on a regular basis to:

- Collect network performance statistics and generate reports. The reports can be saved to disk and emailed automatically.
- Collect text files (such as event logs and configuration files). The files can be saved to disk or zipped up and emailed automatically.
- Check configurations – the complete configuration of the remote routers can be compared with golden configuration files. A report can be generated and emailed showing any sites that do not adhere to the golden configuration.

1.6 Audit Trail

Remote Manager stores details of all files and commands ever issued to remote routers in order to facilitate auditing. These reports can be exported to other programs. (e.g. for further data manipulation or just viewing on different PCs)

2.0 INSTALLING REMOTE MANAGER

2.1 System Requirements

The System Requirements for Remote Manager vary depending upon the number of remote units to be managed and also the number of units to be operated on simultaneously. For less than 1000 units the following specification should be adequate

- Pentium or AMD processor 2.0 GHz or faster
- 1GB Memory
- 3.0 GB Hard Disk Space
- Microsoft Windows XP Professional operating system
- Microsoft Windows 2003 server (at least 2GB RAM recommended)
- Or Microsoft Windows Vista (at least 2GB RAM recommended)
- 1 communications ports. (Up to ten may be required when operating in multi-active-mode using a non Direct IP connection method with multiple simultaneous connections.)

2.2 Installing Remote Manager

To install Remote Manager run the supplied msi program. Make a note of the chosen destination installation folder as it will be required later.

Reboot the PC if prompted to do so.

2.3 Installing the Communications Device Driver

If you intend to dial out over ISDN using a non-direct IP connection method, before launching Remote Manager it is necessary to install the driver for the local communications device (i.e. Terminal adaptor) that is to be used by Remote Manager. Any Sarian or Digi Transport router can be used that has both a serial port and an ISDN interface.

To install the driver in Windows XP, access the control panel and choose “Phone & Modem Options”, Located in the Printers & Other hardware sub section.

Click on the “Modems” tab and then click “Add”.



On the dialog box which then appears check the “Don’t detect my modem I will select it from a list” check box and click “Next.”



Click on “Have Disk” and browse to the Remote Manger installation folder. Located in this folder is a file called “RemManMulti.inf”. This driver is appropriate for any Sarian or Digi Transport router with a serial and ISDN interface. Click on “Open” then click “OK”. The inf file contains a driver with 12 different names to enable a different driver to be used for each communications port on your PC:

- Com01 Sarian Systems ISDN Device
- Com02 Sarian Systems ISDN Device
- Com03 Sarian Systems ISDN Device etc ..

Select the name matching the COMM port number that you wish to install the Sarian Device on.

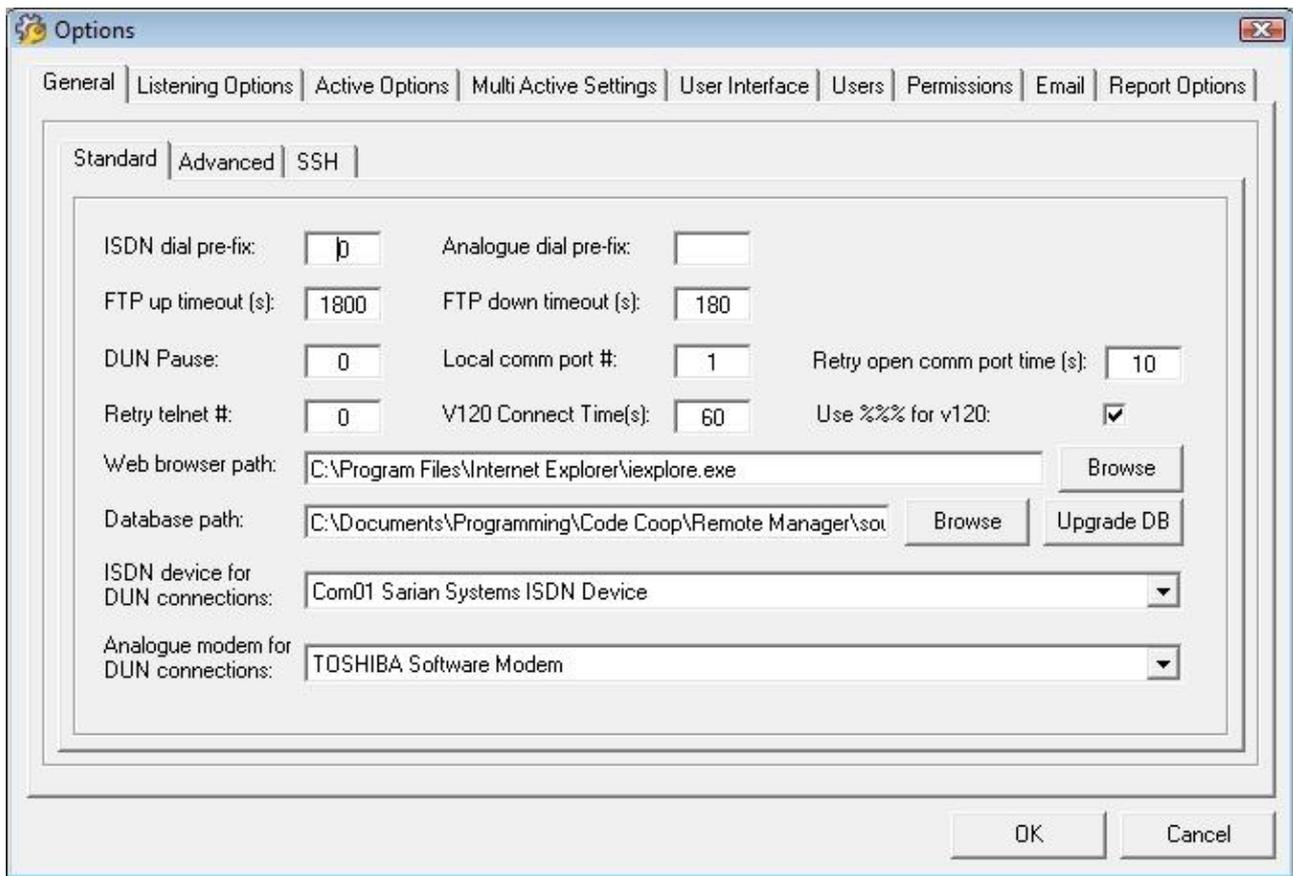
Click “Next”, choose the Windows communication port that your device is connected to and click “Next” again. If a driver signing warning dialog box appears, click “Continue Anyway.” Finally click “Finish”. Repeat this procedure for as many serial communication ports as you wish to use with Remote Manager. (Remote Manager currently supports 10 serial communications ports.)

2.4 Configuring Remote Manager

Launch Remote Manager (see section 2.6). If a registration code is required you will need to contact your vendor to receive this.

On the “Main Screen” toolbar click the “Options” button.

The following dialog box will be displayed:



In the “Local comm port #” field enter the PC communications port number that your ISDN device is connected to.

In the ISDN device for DUN connections drop down list, select the ISDN device installed following the instructions in the previous section.

Finally click the OK button.

- ✓ *If Remote Manager is to be used in Multi Active Mode for non “Direct IP” connection methods (where up to ten units can be operated on simultaneously), it is necessary to select the other COMM ports and ISDN devices on the screen accessed by the “Multi Active Settings” tab.*

2.5 Configuring Internet Explorer

As Remote Manager can make use of Internet Explorer it is necessary to ensure that the following settings are correct.

In Internet Explorer select “Internet Options” from the “Tools” menu.

Under “Browsing History” click on Settings. Ensure that Internet Explorer is configured to “Check for newer version of stored pages” “Automatically”. Click OK.

Next select the “Connections Tab”. Ensure that “Never dial a connection” is selected. Click OK.

Finally click on LAN Settings and ensure that Internet Explorer is NOT configured to use a proxy server or automatically detect settings or use an automatic configuration script. All check boxes on this screen should be un-checked. Click OK on this screen and again on the “Internet Options” screen.

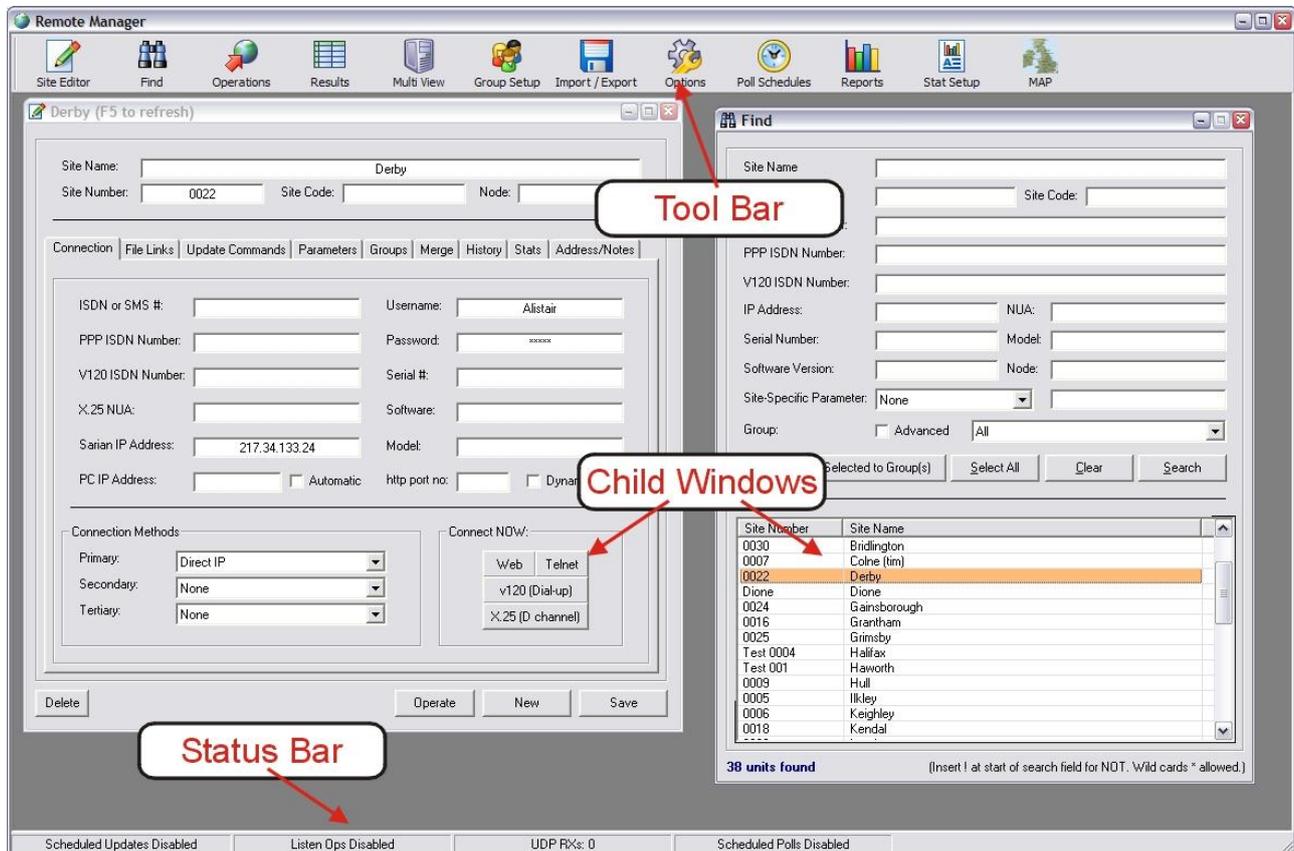
2.6 Launching Remote Manager

A shortcut to launch Remote Manager can be found in the Windows start menu. After launching Remote Manager you will need to log in with the default username of “username” and password of “password”.

- ✓ *Clicking on the “Options” button and selecting the “Users” tab will allow you to add, edit or remove username and password combinations.*

3.0 MAIN SCREEN OVERVIEW

The Remote Manager “main screen” consists of a multi-document window with a toolbar at the top and a status bar at the bottom.



Clicking on a tool-bar button will cause a “child window” to be displayed in the area below. The child windows can be moved (and sometimes re-sized) by the user. The next time the same child window is opened it will appear in its previous position i.e. its position when last closed.

Holding down the Ctrl and Shift keys, and repeatedly pressing the Tab key allows the user to switch between the child windows. This is useful if a child window you wish to use is hidden behind another child window.

To exit the program, click on the cross at the top right of the main screen. If Remote Manager is currently performing a remote operation, a system beep will sound and Remote Manager will not terminate. To exit the program as soon as possible, ensure that “Listening Mode” is disabled, any active mode operations are cancelled and scheduled polling is disabled.

4.0 SITE EDITOR

The site editor screen is primarily used to add or edit details for individual routers. The top of this screen contains fields in which to record the site name and site number. The middle section of this screen contains a number of tab-selected areas used for various purposes. The bottom section of this screen allows the site details to be saved, new units to be created and existing units to be deleted.

Unlike most other areas of Remote Manager, changes made in the “Site Editor” are not saved to the database until the “Save” button is clicked.

The screenshot shows the 'Haworth (F5 to refresh)' window. At the top, there are input fields for 'Site Name' (containing 'Haworth'), 'Site Number' (containing 'Test 001'), 'Site Code', and 'Node' (containing 'CODDAF5'). Below these is a tabbed interface with tabs for 'Connection', 'File Links', 'Update Commands', 'Parameters', 'Groups', 'Merge', 'History', 'Stats', and 'Address/Notes'. The 'Parameters' tab is active, showing fields for 'ISDN or SMS #', 'PPP ISDN Number' (123), 'V120 ISDN Number', 'X.25 NUA', 'Router IP Address' (192.168.50.254), 'http port no.', 'PC IP Address', 'Username' (alstair), 'Password' (masked with asterisks), 'Serial #' (65472), 'Firmware' (5074), 'Model' (DR6420-HIA), and 'IMSI'. There are also checkboxes for 'Dynamic IP', 'Automatic', and 'Use SSH & SFTP' (checked). At the bottom left, there are 'Connection Methods' dropdowns for 'Primary' (Direct IP), 'Secondary' (None), and 'Tertiary' (None). At the bottom right, there is a 'Connect NOW:' section with buttons for 'Web', 'Telnet', 'SSH', 'V120', and 'X.25 (D)'. At the very bottom of the window are buttons for 'Delete', 'Operate', 'New', and 'Save'.

Site Name

The “Site Name” field is a text field used to store the name of the site. Every site in the database must have a name.

It is recommended that each site has a unique name but this is not a requirement. Two or more sites may have the same site name.

Site Number

The “Site Number” field is also a text field and must be used to store the remote sites’ number.

Every site in the database must have a number. It is recommended that each site has a unique number but this is not a requirement. Two or more sites may have the same site number.

- ✓ *This field is not limited to numerical characters it is recommend that leading zeros are included in any number scheme that does not start with a letter. E.g. for site 1 use "000001" instead of "1". This will ensure that if you choose to "sort by number" in certain other sections of Remote Manager, the results will be as you are likely to expect.*

Site Code

The Site Code field is a text field that may be used for any purpose. Remote Manager does not use this field for any special purpose.

Node

The purpose of this field is to facilitate automatic "linking" of individual and unique files to different routers. See section 4.1.6 for more details.

4.1 Tabbed Areas:

4.1.1 Connection

The connection tabbed pane stores the connection details for the individual router selected. It also stores other miscellaneous information for example the firmware version, serial number and model type.

This area also provides instant access to remote routers via the "Connect NOW" functionality.

ISDN or SMS#

For ISDN sites with MSNs, this field can be used to store the main ISDN number of the remote unit. Usually this will not be a number that the remote unit will answer on, so Remote Manager will never dial this number. The number(s) that the remote unit will actually answer on should be stored in either the "PPP ISDN Number" field or the "V120 ISDN Number" field.

For cellular deployments, the phone number of the remote unit should be stored here. This number will be used if Remote Manager needs to send an SMS message to the remote unit.

PPP ISDN Number

This field should be used to store the PPP ISDN number of the remote unit. The remote unit should be configured to answer with PPP when "dialled" on this number. Remote Manager will create a dial-up-networking (DUN) connection to this number during a "Remote Operation" or "Connect NOW" session.

V120 ISDN Number

This field should be used to store the V120 ISDN number of the remote unit. The remote unit should be configured to answer with V120 when "dialled" on this number. Remote Manager will use this number for certain types of "Remote Operation" or a v120 "Connect Now" session.

X.25 NUA

This field should be used to store the X.25 NUA of the remote unit.

Remote Manager will use this NUA to connect to remote units during certain types of "Remote Operation" or an X.25 "Connect Now" session.

Currently Remote Manager is capable of connecting to remote units over X.25 via 2 methods.

- Via a serially connected TransPort or Sarian router which is connected to an X.25 network
 - Via a "Gateway TransPort/Sarian" which is connected to an X.25 network. The "Gateway TransPort/Sarian" must have an IP address accessible from the Remote Manager PC.
- ✓ *Remote Manager will append the remote command sub address of "99" onto the "X.25 NUA" when calling. (This will allow Remote Manager to connect to a command session on the remote router.)*

Router IP Address

This field should contain the IP address of the remote unit. The default IP address is 1.2.3.4 as this is the default IP address of a TransPort/Sarian unit answering with PPP instance 0.

If the router has an IP address directly accessible from the Remote Manager PC then this IP address should be entered here.

It is possible to configure a primary and backup IP address in this field. This is useful if the remote unit can be connected to the network via more than one interface (or APN or SIM in the case of cellular). To use this functionality, both IP addresses should be entered into the same field separated by an exclamation mark. Also ensure that on the "Options" screen "Retry connection #:" is set to a value greater than zero.

By default, over IP interfaces Remote Manager will attempt to connect to the remote unit via Telnet using TCP port 23 or SSH on port 22. However if the remote router's Telnet server is available on a different port number, this can be specified after a colon.

The following text represents the syntax for the "Router IP Address" field:

<Primary IP>[!<Secondary IP>][:<Telnet port number>]

The square brackets are used above to indicate that everything other than the primary IP is optional.

http port no

If the web server on the remote TransPort/Sarian is to be accessed via a non standard http port number (e.g. a number other than 80) this number can be configured here. Remote Manager will then use this port number for any "Connect NOW" Web sessions.

Dynamic IP address

When Remote Manager is used in "Listening Mode" it is capable of updating remote units after receiving the IP address of the remote unit in a UDP packet. If this IP address is dynamic rather than static, then Remote Manager needs to behave differently so this check box should be checked.

PC IP Address

By default, when dialling into a remote router using Windows™ dial-up-networking, the remote router will assign an address to the PC during the PPP negotiation. The remote router may be configured not to do this. In this case the IP address of the PC must be specified manually in this field.

- ✓ *Please note that in this case the "Automatic" check box must also be un-ticked.*

Automatic

Normally the "Automatic" check box should be ticked. This indicates that when connecting to a remote unit via Windows™ dial-up-networking, the remote unit will assign an IP address to the PC during the PPP negotiation. In the case where this does not happen this check box must be un-

ticked and the “PC IP Address” field must be populated with an appropriate value.

Username

The username field should contain the username that Remote Manager will use to authenticate with the remote unit. This username will be used for command line sessions (e.g. via Telnet, SSH, X.25 or V120) as well as for the dial-up-networking (DUN) connections.

Password

The password field should contain the password that Remote Manager will use to authenticate with the remote unit. This password will be used for command line sessions (e.g. via Telnet, SSH, X.25 or V120) as well as for the dial-up-networking (DUN) connections.

Serial #

This field can be used to store the serial number of the remote router.

- ✓ *Remote Manager can be configured to collect this information from the remote units.*

Firmware

This field can be used to store the version of software (firmware) loaded on the remote unit. Remote Manager can be configured to collect this information from the routers.

Model

This field can be used to store the model type of the remote router. Remote Manager can be configured to collect this information from the routers.

IMSI

This field can be used to store the IMSI from the SIM card in the remote router. Remote Manager can be configured to collect this information from the routers.

Use SSH & SFTP

When this check box is ticked, instead of using Telnet and FTP for remote operations, SSH and SFTP will be used.



Clicking this key will toggle the display of the MD5 Fingerprint text field which shows the SSH MD5 fingerprint Remote Manager has stored for this site. If the MD5 fingerprint for a site has changed it is necessary to enter the correct fingerprint into this field or to delete it. If the fingerprint is deleted from the site editor, Remote Manager will update the field next time it connects to the site via SSH or SFTP.

- ✓ *This applies to Operations only, the field will not be updated after a “Connect NOW” SSH session. The MD5 fingerprint will be checked during a “Connect NOW” SSH session however.*

Connection Methods

Connection methods are different “ways” of connecting to remote units.

Three list boxes allow a primary, secondary and tertiary connection method to be specified for each unit. These settings will be used for any remote operations that can be accomplished entirely by command line access to the remote unit.

- ✓ *In the case of uploading files to the remote unit, direct IP or a PPP connection will always be used. If the primary connection method is set to Direct IP then direct IP will be used, otherwise PPP will be used.*

The following connection methods are currently available:

X.25 D channel

Remote manager will connect to the remote unit by placing an X.25 call This can be achieved through a locally connected TransPort/Sarian unit which is connected to an X.25 network or via a "Gateway TransPort\Sarian" which is connected to an X.25 network. The "Gateway TransPort\Sarian" must have an IP address accessible from the Remote Manager PC. To enable "gateway mode" see the configuration settings in the "Options" screen.

Remote manager will connect to the remote command sub address (99) to access the remote command session and perform the operation.

PPP ISDN B channel

Remote manager will create a dial-up-networking (DUN) connection using the "modem" selected in "ISDN Device for DUN connections" on the options screen.

After launching the DUN connection Remote Manager will connect to the IP address specified in the "IP Address" field to perform the operation.

V120 ISDN B channel

Remote manager will connect to the remote unit using v120 rate adaptation via a locally connected Sarian or TransPort router or terminal adaptor. The v120 ISDN number will be called and then the remote command session accessed to perform the operation.

Direct IP

Remote Manager will connect directly to the IP address specified in the "IP Address" field. In this scenario the Remote Manager PC must have direct IP access to the remote unit. This is the most commonly used connection method.

Analogue Modem PPP

Remote manager will create a dial-up-networking (DUN) connection using the "modem" selected in "Analogue modem for DUN connections" on the options screen.

After launching the DUN connection Remote Manager will connect to the IP address specified in the "IP Address" field to perform the operation.

V120 then PPP

For sites that answer with V120 but when an IP connection is required for the operation.

Remote Manager will connect via V120, issue the command "bind ppp 0 asy 0", hang up, connect via PPP and issue the command "bind v120 0 asy 0". This is no longer needed as modern firmware can be configured to detect whether an incoming call is PPP or V120.

V120 variable ring count then PPP

For sites where multiple routers answer with V120 on the same ISDN number and an IP connection is required for the operation.

Remote Manager will connect via V120 and check if the serial number of the router it has connected to is the router it needs to update. If the serial number is wrong it will increment the ring

count of the remote router (ATS0) hang up and try again until the correct router answers.

If the serial number is correct it will enable PPP answering, hang up and reconnect via PPP.

Direct IP via router PPP

Remote Manager will first establish a Telnet/SSH connection with the gateway router, (as configured under Options → General → Advanced → X.25 Telnet Gateway/ PPP Sarian Gateway. It will program the specified PPP instance with the ISDN phone number, username and password from the site editor. It will issue a PPP deactivation command to ensure the gateway PPP link is down. Finally it will establish a Telnet/SSH connection to the remote router routing through the gateway router. This feature means that the gateway router does not need to be programmed with the phone number of each site. It also means that each site can be configured with the same IP address. This connection method can obviously not be use to connect to multiple units concurrently.

Connect Now

The “Connect Now” functionality allows the user instant access to remote unit by via any of the correctly configured connection methods. Command line access is allowed through all connection methods , web browser access through IP based connection methods only.

Web

Clicking on the “Web” button will cause Remote Manager to access the remote unit according to the following rules:

If “Direct IP” is selected as the primary connection method or the SHIFT key is held down when “Web” is clicked then Remote Manager will launch the web browser and instruct it to connect to the IP address specified in the “IP Address” field.

If any other selection is present in the primary connection method, then Remote Manager will launch a DUN connection before launching the web browser.

When DUN is used to connect to the remote site, a “Disconnect Now” button will appear. Clicking this button will hang-up the DUN connection.

When the “Dynamic IP address” check box is ticked, instead of using the IP Address in the “IP Address” field Remote Manager will look up the current IP address for the serial number in the “Serial #” field in the listening table. Additionally, when Remote Manager has connected to the remote unit it will log in via Telnet/SSH and check that the serial number of the remote unit is as expected. If the serial number is incorrect the user will be warned.

If the Ctrl key is held whist the “Web” button is clicked, Remote Manager will attempt to connect to the secondary IP address rather than the primary IP address.

If the “Use SSH & SFTP” check box is ticked. Remote Manager will connect using HTTPS rather than HTTP.

In all cases Remote Manager will attempt to authenticate with the remote user using the username and password in the site editor before launching the web browser. The web browser will be connected to <ip of site>default.asp. The user will therefore not be required to enter a username and password manually.

Telnet

Clicking on the “Telnet” button will cause Remote Manager to access the remote unit according to the following rules:

If “Direct IP” is selected as the primary connection method or the SHIFT key is held down when “Telnet” is clicked then Remote Manager will launch the in-built terminal program and connect and authenticate to the IP address specified in the “IP Address” field.

If any other selection is present in the primary connection method, then Remote Manager will launch a DUN connection before launching the in-built terminal program.

When DUN is used to connect to the remote site, a “Disconnect Now” button will appear, clicking this button will hang-up the DUN connection.

See section 5.0 for details on using the in-built terminal program.

When the “Dynamic IP address” check box is checked, instead of using the IP Address in the “IP Address” field Remote Manager will look up the current IP address for the serial number in the “Serial #” field in the listening table. Additionally, when Remote Manager has connected to the remote unit it checks that the serial number of the remote unit is as expected. If the serial number is incorrect the user will be warned.

SSH

Clicking on the “SSH” button will cause Remote Manager to access the remote unit according to the following rules:

If “Direct IP” is selected as the primary connection method or the SHIFT key is held down when “SSH” is clicked, Remote Manager will launch the in-built terminal program and connect and authenticate to the IP address specified in the “IP Address” field.

If any other selection is present in the primary connection method, then Remote Manager will launch a dial-up-networking (DUN) connection before launching the in-built terminal program.

When dial-up-networking (DUN) is used to connect to the remote site, a “Disconnect Now” button will appear. Clicking this button will hang-up the dial-up-networking (DUN) connection.

See section 5.0 for details on using the in-built terminal program.

When the “Dynamic IP address” check box is checked, instead of using the IP Address in the “IP Address” field Remote Manager will look up the current IP address for the serial number in the “Serial #” field in the listening table. Additionally, when Remote Manager has connected to the remote unit it checks that the serial number of the remote unit is as expected. If the serial number is incorrect the user will be warned.

If the Ctrl key is held whilst the “Web” button is clicked, Remote Manager will attempt to connect to the secondary IP address rather than the primary IP address.

V120 Dial-up

Clicking on the “V120 (Dial-up)” button will cause Remote Manager to connect via V120 to the remote unit using the ISDN number specified in the “V120 ISDN Number” field. Once connected, Remote Manager will access the remote command session, authenticate with the remote unit and then launch the in-built terminal program.

See section 5.0 for details on using the in-built terminal program.

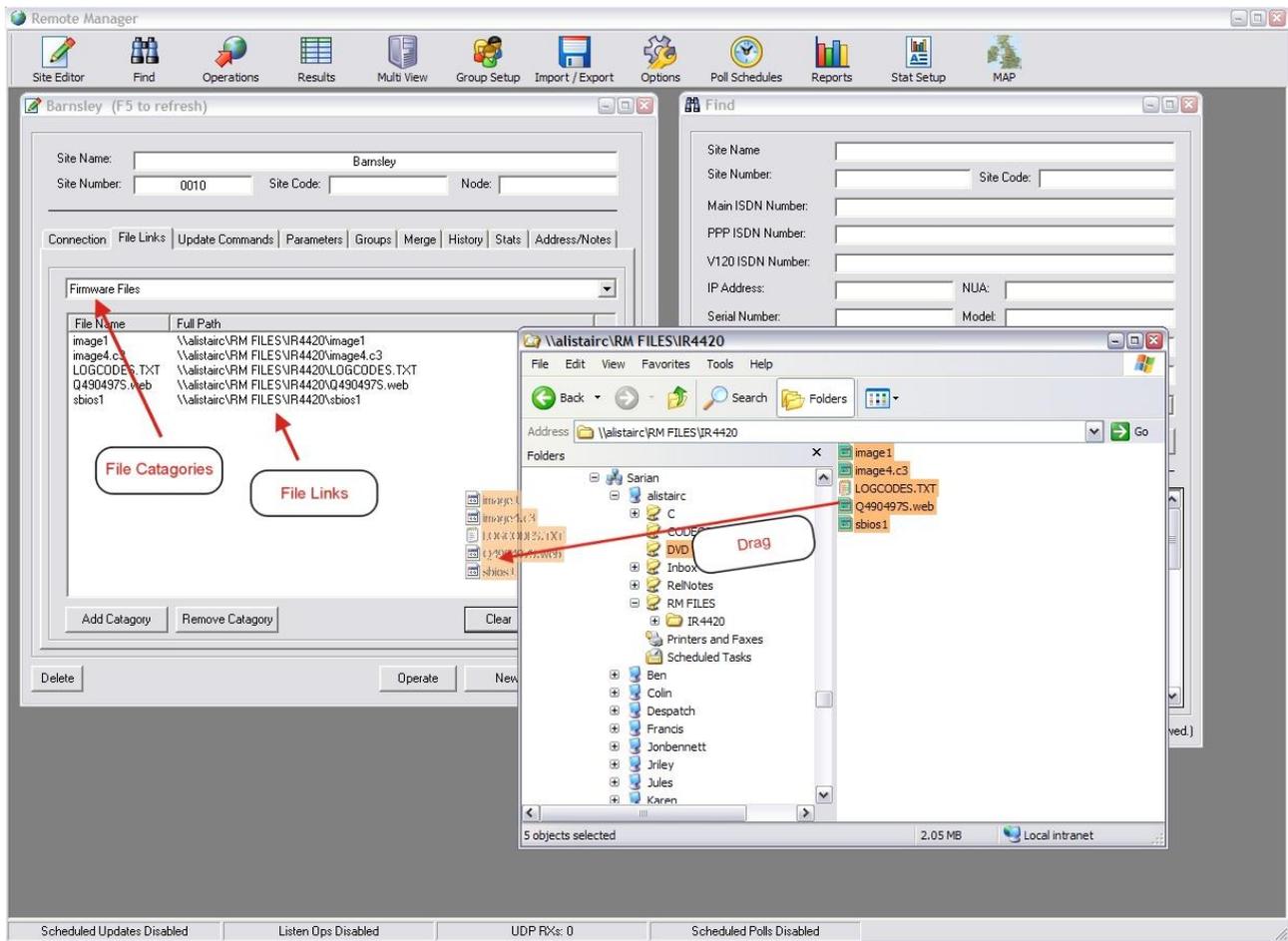
X.25 (D channel)

Clicking on the “X.25 (D-channel)” button will cause Remote Manager to connect via X.25 to the remote unit using the NUA specified in the “X.25 NUA” field. Once connected Remote Manager will access the remote command session, authenticate with the remote unit and launch the in-built terminal program.

See section 5.0 for details on using the in-built terminal program.

4.1.2 File Links

The “File Links” area allows file links to be assigned to the remote unit for the purpose of uploading from the PC to the remote unit during a remote operation.



The drop down list (top) contains a number of file “Categories”. These “Categories” are primarily to help organise the file links. For example it might be desirable to split the files into 2 categories e.g. firmware files and configuration files.

The main list view (centre) displays a list of the files links assigned to the current unit that are also members of the category selected in the drop down list.

To add file links to the list, simply open Microsoft Windows Explorer, select the files you desire to “link”, click and drag these files into the list view area.

The files themselves will not be stored in the database. It is the responsibility of the user to create a folder structure in which to store the files.

Even if Remote Manager is currently to be run on only one PC and all the files to be uploaded are stored on that same PC, it is recommend that files are mapped via a network UNC (universal naming convention). This will allow other PCs running Remote Manager on the network to access the same files in the future.

An example of a UNC is as follows:

\\RemMan1\RemManFiles\2002.07.09 Cust\image

- \\RemMan1** → This is the network name (host name) of the PC running Remote Manager.
- \RemManFiles** → This is the share name (or the name of the shared folder) on the PC running Remote Manager.
- \2002.07.09 Cust** → This is the sub-folder name of the folder containing the files to be linked.
- \image** → This is the name of the actual file that is linked to the current unit

The “Clear” button can be used to quickly delete ALL file mappings from ALL categories for the currently selected unit.

Individual units or groups of units can be selected in the list view with the mouse or keyboard and then deleted by pressing the “Delete” button on the PC keyboard or clicking the “Delete” button on the “File Links” screen.

New file categories can be added or removed by clicking the “Add Category” and “Remove Category” buttons respectively.

- ✓ *If a file category is currently in use (i.e. at least one file link is a member of the category) it cannot be removed.*

It is important to understand that file links are assigned to units on an individual basis. i.e. if 10 files are linked to 10 units, the underlying database will contain $10 \times 10 = 100$ file links. This means that it is possible to link individual files to individual units. (e.g. a config file). However it is not recommended that individual configurations are managed in this manner as Remote Manager provides separate support for site-specific parameters.

If a file is linked with any of the following names, special behaviour will occur when the file is actually loaded onto the remote unit:

sbios1

A move “sbios1 sbios” will command will be issued to upgrade the boot loader. This technique **must** always be used if the boot loader (sbios file) is to be upgraded.

image1

“del image” and then “ren image1 image” commands will be issued. This is so that the image file will only be updated if and when the FTP upload of the new image file has been successful. This reduces the risk associated with upgrading the image on file on a remote unit. This technique can only be used on remote units with enough free flash space for simultaneous storage of two copies of the image file.

***.web**

If uploading a file with the three character .web extension or wb2 extension, Remote Manager will first check to see if there is already a file on the remote unit with a .web or .wb2 extension. If there is Remote Manager will delete it before starting the upload. In order to use the minimum amount of flash space necessary on the remote unit, Remote Manager will not upload the web file until any image1 and sbios1 files have been fully upgraded *i.e.* the commands mentioned in the previous two paragraphs have been issued. To FTP a .web or .wb2 file to the router, it is therefore necessary to ensure that “rename and reboot” operation option is selected for a “File Update” or a “File and Configuration Update” operation. If this is not appropriate, rename the web file to some other extension and issue an update command to rename it back to .web or .wb2.

4.1.3 Update Commands

The “Update Commands” area is where commands that are to be issued to a remote unit (in order to update the configuration) are entered.

The update commands area contains a large text area where multiple lines of text can be entered. Each line of text is treated as a separate configuration command and will be issued to the remote unit when a relevant remote operation is executed.

To enter a command simply “type” (or “paste” from the clipboard) the appropriate command into the text field on the “Update Commands” tabbed pane.

To remove a field, simply delete the command from the large text field on the “Update Commands” area.

It is important to understand that each command is assigned to each unit on an individual basis. *i.e.* If 10 commands are assigned to 10 units, the underlying database will contain $10 \times 10 = 100$

command assignments. This means that it is possible to assign individual commands to individual units and thus update the values of site-specific parameters. However it is not recommend that site-specific parameters are managed in this manner as Remote Manager provides separate support for site-specific parameters.

For a “File & Configuration Update” remote operation only, prefixing any command with the “~” character will cause the command to be entered BEFORE the files are uploaded. (Rather than after the file is loaded and (optionally) the unit has been rebooted as is the case with any command not prefixed with “~”.) A save command is not issued after any prefixed commands so if the operation option “Reboot and reconnect after upload” is selected the effect of these prefixed commands will not be saved to flash.

- Any command prefixed with “~” will be ignored by the “Configuration Update” operation.
- Commands that are entered here will look similar to the contents of the config.da0 file.
- To set a TransPort/Sarian router parameter value back to its default, set it to an exclamation mark.

e.g. to remove a username from the “ppp 0 username” parameter, issue the following command:

“ppp 0 username !”

For more information on the use of the “~” character see section 7.2.4

4.1.4 Parameters

The parameter area lists the names and values of site-specific parameters. The values of site-specific values can be edited manually by selecting the appropriate cell and typing in the value from the PC keyboard.

The following special keys/key-combinations are available:

Ctrl+C → Copy

Ctrl+V → Paste

Ctrl+X → Cut

Delete → Deletes the entire entry

Backspace → Deletes the last character in the entry.

Double clicking a site-specific parameter value will display the selected value in a special editor if more powerful editing is required (The editor supports the use of cursor keys *etc.*).

Each group of units can have site-specific parameters assigned to it. Therefore the site-specific parameters that are displayed on this screen are dependant upon the group(s) that this unit is currently a member of; See section 9.0 (Group & Site-Specific Parameter Management) for details.

Remote Manager can be configured to connect to the remote sites and obtain the values of the site-specific parameters and store them in the database automatically. See section 7.2.5 for details.

Site-specific parameters values can be imported or edited in bulk by making use of the Import/Export facility. See section 10.0 for details.

4.1.5 Group Membership

The “Group Membership” area can be used to view or change the groups that the current unit is a member of.

The list box on the left hand side (LHS) shows the group(s) that the unit is currently a member of. The list box on the RHS shows the group(s) that the unit is not currently a member of.

To assign the current unit to a new group or groups, simply select the group(s) that you wish the unit to be a member of on the right hand side (RHS) and click the “Assign selected groups to unit” button.

To withdraw membership from a group or groups, simply select the group(s) that you do not wish the unit to be a member of on the LHS and click the “Remove unit from selected groups” button.

4.1.6 Configuration Merge

The Configuration Merge facility allows many of the values in the editor to be assigned to whole groups of units rather than just the unit currently loaded in the editor. This is necessary if new firmware or configurations are to be rolled-out to groups of units.

Additionally it is possible to clear site-specific parameters for groups of units and to assign individual file links to individual units based upon the “Node” field on the “Connection Details” screen.

Merging the current details to groups of units

Currently the following values can be merged:

- Update Commands
- File links
- Connection Methods
- IP Address
- Dynamic IP
- PC IP address
- SSH/SFTP mode
- Automatic IP
- Username
- Password
- Stat Collection settings
- SSH MD5 fingerprint

To use the configuration merge facility simply select the group or groups to which the current configuration is to be transferred. Make the appropriate selection in the drop down list to either:

- Update units that are in ALL of the selected groups

or

- Update units that are in ANY of the selected groups.

Next click the “Transfer current configuration to all units in selected groups.” button.

A dialog box will then be displayed with options relating to the list above.

Make the appropriate selections and click the “Merge Now” button. A progress bar will display the progress of the configuration merge. This procedure can take several minutes for large groups of units. This procedure cannot be cancelled once the “Merge Now” button has been clicked.

Clearing site-specific parameters from groups of units

The values of all the site-specific parameters for all the units in the selected groups can be deleted. This is achieved by selecting the appropriate groups and then clicking the “Clear all site-specific parameters from all units in selected groups.” button.

Bulk linking of individual files to individual units.

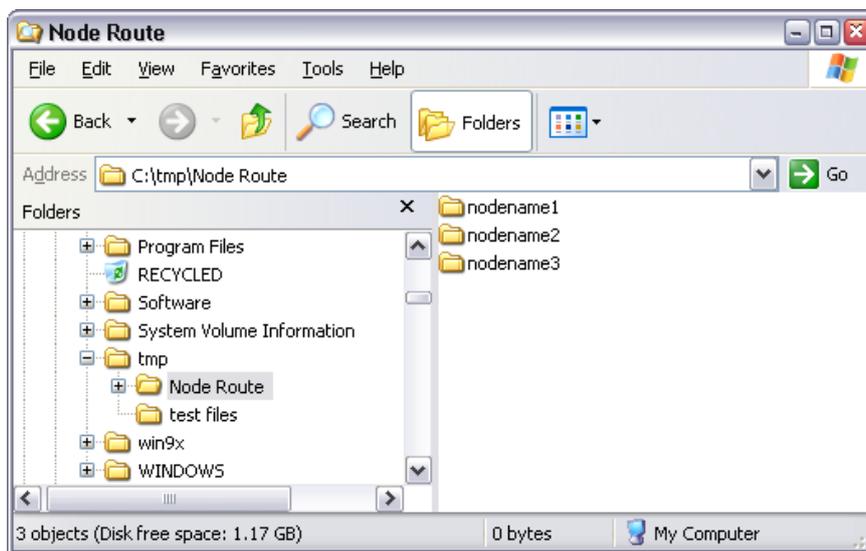
It is possible to add file links for individual files to individual units in an automated manner.

This is made possible by the inclusion of the “Node” field on the “Connection Details” screen. This node field will usually (but not necessarily) be set to a unique value for each individual unit. A file/folder structure should be set up such that sub-folders with the name of the “Node” field values exist in some folder.

For example, consider 3 units each with separate node names:

- nodename1
- nodename2
- nodename3

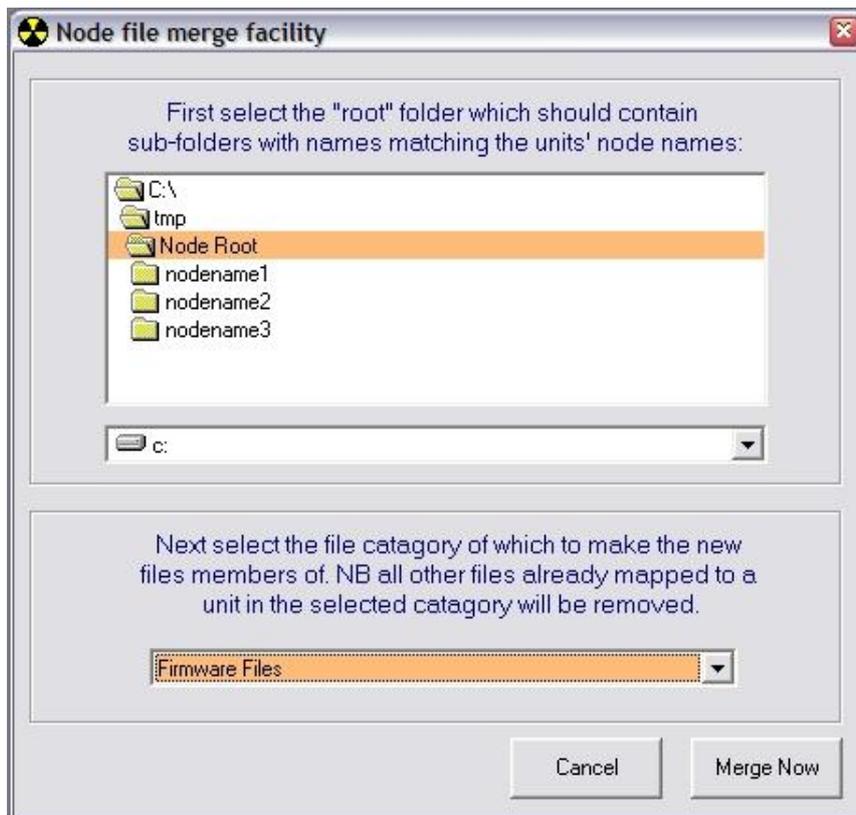
A folder should be created which has the “Node” field values as sub folders as shown in the example figure below.



When the merge operation is run, the files in each of the sub folders will be added as file links to the unit(s) where the sub-folder name matches the “Node” field value.

To perform this operation, first select the group(s) of units that the file links are to be added to. Then click the “Link files to units in selected groups based upon node name.” button.

The following dialog box will be displayed.



Select the root folder in the top section of the dialog box. (The root folder is the folder that contains the sub-folders with the same names as the value of the “Node” fields.) Next select the file category that the new files links are to be members of in the bottom section of the dialog box. Finally click the “Merge Now” button and the file links will be added to the units as appropriate. A progress bar will display the progress of this procedure.

Copy Site Number to Node

This button when clicked will copy the contents of the site number field to the site node field. This is useful if your folder structure of site specific files is based on site number.

4.1.7 History

The history area displays historical information pertaining to the unit currently loaded in the Site Editor

Listening mode IP address history

If Remote Manager has been used to perform an operation on the remote unit in “Listening Mode”, then the IP addresses used (which may be dynamic) will be visible in the “Listening mode IP address history” box.

Additionally, Remote Manager will display at the top of this list, the last IP address it received via a UDP packet for this unit regardless of whether a remote operation has been performed on the unit via “Listening Mode” or not.

Remote operation session history

All the remote operations ever performed on the current unit are listed in the remote operation session history list. Clicking on a list entry will display a summary of files loaded and commands issued during the selected operation.

The “Display ALL history” button will list the files loaded and commands issued in all remote

operations for the current unit.

4.1.8 Stats

If stats are to be collected from a unit by means of a scheduled poll, after the “Statistic Class Type” has been created on the “Stat Setup” screen, it must be mapped to the unit on this tabbed pane of the site editor. Highlight the required stat class on the right and assign it to the unit by clicking the “Assign selected stats to unit” button underneath.

- ✓ *Remember that the “Merge” facility can be used to apply the current selection to entire groups of units.*

4.1.9 Address/Notes

The address section can be used to store the address of the remote unit. If the post code or the Latitude and Longitude fields are populated then these will be used by Remote Manager to plot the site on the Map. The Map is visible by clicking on the “MAP” button provided that Microsoft MapPoint™ is installed.

The notes field is intended to be used for historical purposes e.g. on 1st December this site rang up with problem “X” and the solution was to do “Y”.

The “Go to Lat/Long or Post Code on map” button can be used to load the Map and zoom into the site currently loaded in the site editor.

4.2 Creating, saving and deleting units

4.2.1 The “New” button.

To create a new unit click on the “New” button. The user will be prompted to save the current site if changes have been made.

- ✓ *A new unit is not actually created in the database until the “Save” button is clicked.*

The user will be prompted to specify whether or not the new unit should be based upon the settings currently present in the editor.

Choosing “Yes” will cause the new unit to:

- Be a member of all the groups that the current unit is a member of
- Have the same site-specific data that the current unit has
- Have the same connection methods that the current unit has
- Have the same update commands that the current unit has
- Have the same file links that the current unit has

The following fields will be wiped blank:

- Site Name
- Site Number
- Main ISDN number
- PPP ISDN number
- V120 ISDN number
- X.25 NUA
- Serial Number
- Software Version

- Model
- Site Code
- Node
- Address Fields
- Note Field
- http port number

4.2.2 The “Save” Button

To update the database with the settings currently in the site editor click the “Save” button. No changes made in the site editor are saved to the database until the “Save” button is clicked.

4.2.3 The “Delete” Button

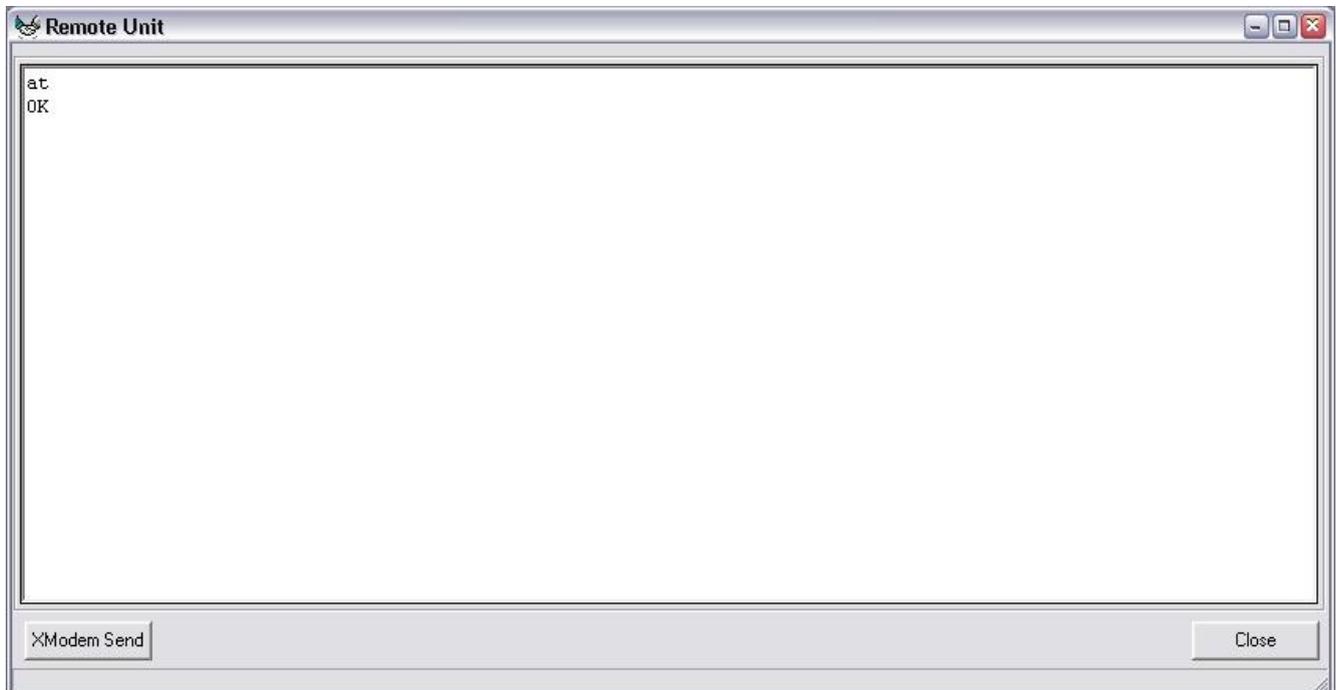
To delete a unit in the database click on the “Delete” button when the unit is loaded in the site editor. It is not possible to delete units that:

- Are member of groups
- Have site-specific parameter values
- Have file links
- Have update commands
- Have history (i.e. Have been involved in a Remote Operation.)
- Have stats

To delete units that cannot be deleted by this method, see “Power Delete” section 9.5.

5.0 BUILT-IN TERMINAL PROGRAM

The built-in terminal program allows command line access to the Remote TransPort/Sarian unit. The built-in terminal program is usually launched by the use of the "CONNECT NOW" feature on the "Site Editor".



Whenever the terminal program is launched by Remote Manager, Remote Manager will automatically authenticate with the remote unit so it is not necessary for the user to do so.

It is possible to open more than one terminal program simultaneously when the remote units can be connected to using a direct IP connection.

The "XModem Send" button can be used to transfer a file from the PC to the remote TransPort or Sarian router via the X-modem file transfer protocol. The remote unit must be prepared for this file transfer e.g. by issuing the "xmodem <filename> <CR>" Sar/OS command.

The terminal program has copy and paste features built in. These can be accessed either by right clicking in the text area and making the appropriate selection on the pop-up menu or using the control keys:

Ctrl+C → Copy

Ctrl+V → Paste

- ✓ *The paste command includes a special feature to paste clipboard contents line by line leaving a short pause between lines. This means that remote units can have their configurations updated by the user simply pasting into the terminal program a few updated lines from the config.da0 file.*

Clicking the "Close" button will close the terminal program and in some cases the connection to the remote unit as well. (V120 & X.25 over ISDN D-Channel)

6.0 FIND

The “Find” screen can be used to search for units in the database in order to:

- Load the units into the site editor
- Assign the units to a group (*i.e.* prior to performing a remote operation on the group)
- Remove the units from a group

The search criteria can be entered in one or more of the following fields:

- Site Name
- Site Number
- Site Code
- Main ISDN Number
- PPP ISDN Number
- V120 ISDN Number
- IP Address
- NUA
- Serial Number
- Model
- Software Version
- Node
- Site-Specific Parameter Value
- Notes

The search can also be restricted to units that are members of any one group by making a selection in the “Group” drop down list.

Clicking the “Advanced” check box allows the search to be restricted to units that are members of several selectable groups. Making a selection in the drop down list (only visible when the “Advanced” check box is checked) allows results to be restricted to units that are members of **all** selected groups (“ALL Selected”) or units that are members of **any** of the selected groups (“ANY Selected”).

If entries are made in more than one of the search criteria fields, the search results will only contain units that satisfy all of the search criteria *i.e.* match all search fields.

By default, the site name field automatically “wild-cards” the search. For example entering “Leeds” in the site name will result in a match if “Leeds” is found anywhere in the site name.

Also by default all other fields must match exactly the entry in the database to result in a “hit”.

All fields (apart from “Site Name”) allow the user to specify wild cards by the use of an asterisk character (*). A few examples follow:

Searching for “01274*” in the PPP ISDN Number field will result in a match for all units where the PPP ISDN number begins with the area code “01274”.

Searching for “*99” in the “Serial Number” field will result in a match for all units where the serial number ends with the numbers “99”.

Searching for “*393A*” in the Site Number field will result in a match for all units where the site number contains the characters “393A” in order but anywhere in the site number.

Prefixing the search field with an exclamation mark (!), will result in a hit if the unit does NOT contain the value entered into the search field.

Once the search criteria has been entered, clicking the “Search” button will perform the search. The number of matches will be displayed on the LHS and the individual search results are displayed in a list at the bottom of this screen.

Double clicking a search result will select a unit to be loaded into the site editor.

Clicking the “Add/Remove Selected to Group(s)” button will allow the units you have selected from the search results to be added or removed from one or more groups.

Clicking the “Select All” button will select all the units found.

7.0 OPERATIONS

A “Remote Operation” is some function that is performed on a remote unit. This might be:

- collecting data from the remote unit
- updating the configuration of the remote unit
- uploading new firmware to the remote unit

Remote Manager supports 3 main methods of executing a remote operation:

- Active Mode
- Multi Active Mode
- Listening Mode (of which there are 3 sub types)

Active Mode

In Active Mode Remote Manager actively connects to one router at a time once using a variety of connection methods, the most common being “Direct IP”. Once connected, Remote Manager will update the configuration and/or firmware as appropriate. Remote Manager can be configured to update 1000’s of routers via active mode, but it will only connect sequentially so this could take a long time.

Multi Active Mode

In Multi Active Mode actively connects to up to 50 routers concurrently, using a variety of connection methods, the most common being “Direct IP”. Once connected, Remote Manager will update the configuration and/or firmware as appropriate. Remote Manager can be configured to update 1000’s of routers via Multi Active mode, and if sufficient bandwidth is available, the average time per operation can be up to 50 times as fast as Active mode.

Listening Mode

Listening mode operations are created by ticking the check box “Listening Mode (IP Only)” on the “Remote Operations” screen. When “Execute Operation” is ticked the user must choose from a choice of three operation sub types.

The “Enable Listen Ops” button on the Multi View screen must be used to enable listening mode operations.

Listening Mode – single operation on each serial number

This mode is designed primarily for rolling out updates to routers with dynamic IP addresses. It can also be used during commissioning to automatically apply a configuration to a router when it first connects to the WAN network and sends a UDP heartbeat packet.

To use this mode the correct serial number must be present for each site in the site editor. Also the remote routers must be configured to send a UDP heartbeat to the Remote Manager PC IP address. (The parameters for this are called "Heartbeat IP/destination" and "Heartbeat interval (s)" on the TransPort or Sarian router’s Ethernet or PPP interface configuration web pages.) If the IP address is dynamic, then the “Dynamic IP” check box must also be ticked on the site editor page.

Remote Manager will wait until it receives a UDP heartbeat containing the serial number of a unit that it is due to perform an operation on. Once such a UDP heartbeat packet arrives, RM will perform the operation on that unit. If successful the operation will be marked as complete and no further changes will be made to the remote router.

Listening Mode – reoccurring operations on each IP address

This mode is designed for use in a system where each site has a fixed IP address that is somehow

locked to the site and not the router.

To use this mode the correct IP address must be present in the site editor for each site.

Once an operation has been set up for a group of units, any UDP packet that arrives from an IP address matching that in the site editor for one of the units in the operation will trigger an update. Once this update has occurred the serial number of the site will be updated in the site editor. No further operations will be performed on this IP address provided the serial number does not change. If the unit on site is swapped out and replaced with a new unit, then the serial number in the UDP packet from the fixed IP address will change and another operation will be performed. It is thus possible to have routers automatically updated with the latest firmware and site specific settings when they are swapped out.

Care must be taken not to have more than one “Listening Mode – reoccurring” operation valid for one site at once. Sites can be added or removed from the operation by going to the “Results” screen, right clicking on the operation session in question and selecting “Add/Remove Units from Session”

Listening Mode – reoccurring operations on each IMSI

This mode is designed for use in a system where each site has a SIM card allocated to it. To use this mode the correct IMSI (SIM card) number must be assigned to each site in the site editor.

Once an operation has been set up for a group of units, any UDP packet that arrives with an IMSI number matching that in the site editor for one of the units in the operation will trigger an update. Once this update has occurred the serial number of the site will be updated in the site editor. No further operations will be performed on the router with this IMSI number provided the serial number does not change. If the unit on site is swapped out and replaced with a new unit, provided the SIM card is taken out of the old unit and inserted into the new unit, the serial number in the UDP packet from this IMSI will change and another operation will be performed. It is thus possible to have routers automatically updated with the latest firmware and site specific settings when they are swapped out.

Care must be taken not to have more than one “Listening Mode – reoccurring” operation valid for one site at once. Sites can be added or removed from the operation by going to the “Results” screen, right clicking on the operation session in question and selecting “Add/Remove Units from Session”

7.1 Choosing units for remote operations.

Remote operations can be performed on individual units or one or more groups of units.

To perform a remote operation on one or more groups of units, ensure that the “By Group” tab is displayed and make an appropriate selection in the “Groups to update” list box. In the drop down list select either “Units in ANY selected group” or “Units in ALL selected groups”. If “Units in ANY selected group” is selected then a remote operation will be performed on all units that are a member of any of the selected groups. If “Units in ALL selected groups” is selected then a remote operation will only be performed on units that are members of ALL the selected groups.

To perform a remote operation on an individual unit, ensure that the “By Site” tab is selected and then type the site name or number into the text field. When a match is found the unit details will be displayed in the area below.

- ✓ *To switch between entering a single unit by site number or site name, click the label entitled “Click here to search by number” or “Click here to search by name”.*

It is usually easiest to perform an operation on just a single group of units. Use of the “Add/Remove Selected units from Group(s)” button on the “Find” screen is usually the best way to ensure that the group contains only the units you want to perform the operation on.

7.2 Operation Types

The operation to perform is chosen by making a selection in the “Select Operation” drop down list. Clicking on the “Configure Operations” button will display a dialog box that allows various options to be set for the chosen operation.

It is important to realise that these options are global in nature. For example, consider that a remote operation is created and executed with the operation options configured with certain settings. Consider also that some of the updates were unsuccessful and the user has decided to re-run the same operation at a later time. If before the operation is re-run, the operation options are changed, the new operation options will apply when the operation is re-run.

To re-run an operation see section 8.2.

The following section details the remote operations and their various options.

7.2.1 Directory Wiping Update

This operation was included for a specific project and is unlikely to be useful for the majority of users.

7.2.2 Configuration Update

When run in active or multi active mode, the "Configuration Update" operation will attempt to connect to the remote unit via the primary connection method. If this fails an attempt to connect on the secondary and then tertiary connection methods will be made.

Assuming one of the connection methods is successful, once connected, any configuration update commands assigned to the remote unit will be executed and normally saved.

If the “Check remote for correct serial number” check box is ticked then after connecting to each remote unit Remote Manager will check that the serial number of the remote unit matches that currently stored in the database for the unit. If the serial number does not match then the operation will be aborted.

In the operation options, if the "Include site specific parameters" check box is checked then any site-specific parameter values currently stored in the database will also be programmed into the remote unit.

If the “Save Changes” check box is ticked, then after issuing the configuration update commands Remote Manager will save the changes to flash on the remote TransPort/Sarian by issuing a “config 0 save” command.

If the "Check for read only config.da0" check box is selected, Remote Manager will check the status of the config.da0 file. If this file is found to be read-only then it will be marked as read-write, the save command issued and then marked as read-only once again.

If the “Mark all configuration & firmware files as read only” check box is selected, all files on the Remote TransPort/Sarian that belong to the following list will have the permission changed to read-only. (If the permission is currently set to read write.)

- image
- filter.bin
- sregs.dat
- x3prof
- nobios.bin
- image4.c2
- image5.c2

- contains “.web”
- contains “.wb2”
- logcodes.txt
- config.da0
- config.da1
- fw.txt

If “Collect serial # and firmware version when done” is selected, then Remote Manager will read the serial number and firmware version of the remote unit and overwrite the values in the database for this unit to match.

If “Set time before disconnecting” is ticked then Remote Manager will issue a command to set the time on the remote unit to the current system time on the Remote Manager PC.

7.2.3 File Update

The “File Update” operation uploads the files assigned to the remote unit via FTP or SFTP. In an “Active Mode” operation Remote Manager will connect to the remote unit either via PPP or direct IP. This depends upon the setting of the primary connection method for the individual units.

In the operation options, it is possible to configure this operation to only upload files of the selected categories by making the appropriate selection in the list box. Checking the "All file categories" check box will ensure that files in all categories will be uploaded to the remote unit regardless of the selection in the list box.

If a file named sbios1 is uploaded, a "move sbios1 sbios" command will be issued in order to upgrade the boot-loader. (But only if the "Reboot and reconnect after upload" check box is ticked.)

If a file named image1 is uploaded, “del image” and then “ren image1 image” commands will be issued. (But only if the "Reboot and reconnect after upload" check box is ticked.) This is so that the image file will only be updated if and when the S/FTP upload of the new image file has been successful. This reduces the risk of upgrading the image file on a remote unit. This technique can only be used on remote units with enough free flash space for two copies of the image file.

If uploading a file with the three character .web or .wb2 extension, Remote Manager will first check to see if there is already a file on the remote unit with a .web or .wb2 extension. If there is Remote Manager will delete it before starting the upload. In order to use the minimum amount of flash space necessary on the remote unit, Remote Manager will not upload the web file until any image1 and sbios1 files have been fully upgraded. (This only occurs if the "Reboot and reconnect after upload" check box is ticked.)

If the “Check remote for correct serial number” check box is ticked then after connecting to each remote unit Remote Manager will check that the serial number of the remote unit matches that currently stored in the database for that unit. If the serial number does not match then the operation will be aborted.

If the "Reboot and reconnect after upload" check box is ticked (default), the unit will then be rebooted after the S/FTP upload is complete and any sbios and image files have been fully updated. Remote Manager will then re-connect to the remote unit in order to check that the unit is still functional. Before attempting to re-connect Remote Manager will wait for the amount of time specified in the section “Wait XXX seconds for remote unit to reboot”

If the "Check for read only files" check box is checked then Remote Manager will check if any of the files on the remote TransPort/Sarian are read-only before attempting the upload. If any read-only files are found they will be marked as read-write, overwritten and then marked as read-only again.

If the “Mark all Configuration & Firmware files as read only” check box is ticked, all files on the Remote TransPort/Sarian that belong to the following list will have the permission changed to read-only. (If the permission is currently set to read write.)

- image
- filter.bin
- sregs.dat
- x3prof
- nobios.bin
- image4.c2
- image5.c2
- contains “.web”
- contains “.wb2”
- logcodes.txt
- config.da0
- config.da1
- fw.txt

If “Collect serial # and firmware version when done” is ticked, then Remote Manager will read the serial number and firmware version of the remote unit and overwrite the values in the database for this unit with the values just read.

If “Collect IMSI” is ticked, Remote Manager will read the IMSI out of the remote unit and overwrite the values in the database for this unit with the current value.

If “Use Remote Directories” is ticked, Remote Manager will try to upload the files to the remote directory specified for the file category. Note that most TransPort/Sarian firmware does not support remote directories and that this behaviour is reserved for special projects.

7.2.4 File & Configuration Update

When run in active mode or multi active mode, the "File & Configuration Update" operation will first connect to the remote unit via PPP or direct IP. This depends upon the setting of the primary connection method for the individual units.

Remote Manager will then upload the files assigned to the remote unit via S/FTP. In the operation options it is possible to configure this operation to only upload files of the selected categories by making the appropriate selection in the list box. Ticking the "All file categories" check box will ensure that files in all categories will be uploaded to the remote unit regardless of the selection in the list box.

If a file named sbios1 is uploaded, a "move sbios1 sbios" command will be issued in order to upgrade the boot-loader. (But only if the "Reboot and reconnect after upload" check box is ticked.)

If a file named image1 is uploaded, “del image” and then “ren image1 image” commands will be issued. (Again only if the "Reboot and reconnect after upload" check box is ticked.) This is so that the image file will only be updated if and when the FTP upload of the new image file has been successful. This reduces the risk of upgrading the image file on a remote unit. This technique can only be used on remote units with enough free flash space for two copies of the image file.

If uploading a file with the three character .web or .wb2 extension, Remote Manager will first check to see if there is already a file on the remote unit with a .web or .wb2 extension. If there is Remote Manager will delete it before starting the upload. In order to use the minimum amount of flash space necessary on the remote unit, Remote Manager will not upload the web or wb2 file until any

image1 and sbios1 files have been fully upgraded. (This will only occur if the "Reboot and reconnect after upload" check box is ticked.)

If the "Check remote for correct serial number" check box is ticked then after connecting to each remote unit Remote Manager will check that the serial number of the remote unit matches that currently stored in the database for that unit. If the serial number does not match then the operation will be aborted.

If the "Program site specific parameters" check box is ticked, then any site-specific parameter values currently stored in the database will be programmed into the remote unit normally after the reboot.

If the "Reboot and reconnect after upload" check box is ticked (default), the unit will then be rebooted after the FTP upload is complete and all sbios and image files have been fully updated. Remote Manager will then re-connect to the remote unit and issue the update commands and optionally program in any site specific parameter values. Before attempting to re-connect Remote Manager will wait for the amount of time specified in the section "Wait XXX seconds for remote unit to reboot"

If the "Reboot and reconnect after upload" check box is not ticked then the upload commands and site specific parameter commands will be issued immediately and saved.

- ✓ *Any "update commands" prefixed with "~" will be issued before the FTP upload. This can be a handy way to disable potentially dangerous parts of the configuration whilst the FTP upload completes e.g. "~ppp 1 rebootfails !" could be used to disable automatic reboot of the remote unit during the FTP upload. When the TransPort/Sarian is rebooted by Remote Manager at the end of the FTP transfer any such configuration changes will be lost (e.g. in the above example the reboot behaviour will be restored to normal).*

If the "Check for read only files" check box is ticked, then Remote Manager will check if any of the files on the remote TransPort/Sarian are read only before attempting the upload. If any read-only files are found they will be marked as read-write, overwritten and then marked as read-only again. Additionally, before attempting a configuration change save, Remote Manager will check the status of the config.da0 file. If this file is found to be read-only then it will be marked as read-write, the save command issued and then marked as read-only once again.

If the "Always mark firmware & config files read only" check box is ticked, all files on the Remote router that belong to the following list will have the permission changed to read-only. (If the permission is currently set to read write.)

- image
- filter.bin
- sregs.dat
- x3prof
- nobios.bin
- image4.c2
- image5.c2
- contains ".web"
- contains ".wb2"
- logcodes.txt
- x3prof
- config.da0
- config.da1

- fw.txt

If the “Collect serial # and firmware version” check box is ticked, Remote Manager will overwrite the serial number and firmware version in the database with those on the remote site at the end of the operation.

If the “Collect IMSI” check box is ticked, Remote Manager will overwrite the IMSI in the database with the current IMSI read back from the site.

If “Use Remote Directories” is ticked then Remote Manager will try to upload the files to the remote directory specified for the file category. Note that most TransPort/Sarian firmware does not support remote directories and that this behaviour is reserved for special projects.

If “Add GPRS PIN no to config.da0 file” is ticked, Remote Manager will extract the current PIN number, PPP 1 username and PPP 1 password from the site and replace the PIN number, username and password in the config.da0 file with these details before uploading. Note that the config.da0 file you are loading must contain the exact text:

```
modemcc 0 epin *
```

```
ppp 1 username *
```

```
ppp 1 epassword *
```

For this replacement to work.

If the “Append SSPs to config.dax file” check box is ticked, RM will append the site specific parameters to the bottom of the config.da0 file before uploading the file to the site. This is essential if you are going to reboot the remote site and the site specific parameters are required in order for it to reconnect to the network. Note that any [CFG] and [END CFG] statements must be manually stripped out of the config.dax file that Remote Manager is configured to load. This is because the SSPs will be appended literally to the end of the config file and if [END CFG] is present they will be after this line and thus ignored by the router.

If the “Switch to SSH after reboot” check box is ticked, when Remote Manager reboots the remote unit it will enable the site editor database entry “SSH\SFTP” for this site and attempt to connect to the site using SSH rather than Telnet after the reboot. This is useful if the new configuration files that have just been loaded have disabled Telnet and enabled SSH.

7.2.5 Retrieve Site Specific Parameter Values

When run in active mode or multi active mode, the “Retrieve site-specific parameter values” operation will attempt to connect to the remote unit via the primary connection method. If this fails the secondary and then tertiary connection methods will be used if required.

Assuming that one of the specified connection methods is successful, the current value of any site-specific parameters will be read from the remote unit and saved into the database. The serial number, software version, model number and IMSI will also be recorded if the appropriate check boxes are ticked.

If the “Check remote for correct serial number” check box is ticked then after connecting to each remote unit Remote Manager will check that the serial number of the remote unit matches that currently stored in the database for the unit. If the serial number does not match then the operation will be aborted.

If the “Instead of saving site specific data from unit to database, check that the data on the remote unit matches that stored in the database” check box is ticked. Then instead of reading the values of the site specific parameter in the remote unit and storing them in the database, RM will check that the current values in the remote units match those in the database. If they do not match then the operation will fail and the reason for the mismatch will be recorded in the log. (Click “View Log” on the “Operations” screen.)

Normally when connecting to a remote unit RM will delete all the values it has stored for the site specific parameters and then read back the new values. If an error occurs whilst reading back

some of the new values then this can leave blank entries. If the “Do not delete values of existing SSP” values check box is ticked then the current values will not be deleted, any values still present will be overwritten with the current value.

7.2.6 Connectivity Test

When run in active mode or multi active mode, the "Connectivity Test" operation will attempt to connect to the remote unit via the primary connection method. If this fails the secondary and then tertiary connection methods will be used if required.

Assuming one of these connection methods is successful Remote Manager will optionally "log-in" to the remote unit depending upon the status of the log-in check box on the operation options screen.

Checking the "Override individual unit connection methods" check box will cause Remote Manager to use the connection methods specified here rather than those specified on the individual units when performing the connectivity test.

The “Try all selected connection methods” check box will cause Remote Manager to try all connection methods regardless of whether an attempt on the previous connection method was successful or not. If special site specific parameters are available (CT Primary, CT Secondary & CR Tertiary), then the result of the connectivity test on each connection method will be stored in the site specific parameter. See section 9.3.5 for more details.

7.2.7 BERT Test

Remote Manager can run a Bit Error Rate Test (BERT) on remote TransPort/Sarian units provided that the remote units respond to the “loop a” command and that the locally connected unit is a 2000 series TransPort/Sarian or later.

Remote Manager will collect:

- The number of bit errors (up to a maximum of 922337203555477 errors).
- The number of seconds in the test containing at least 1 bit error.
- The number of Severely Errored Seconds (SES). This is where more than 6000 bit errors occurred in one second.

When a BERT is run Remote Manager will first connect to the remote unit using the available connection methods. Next Remote Manager will instruct the remote router to answer the next call with the ISDN interface set to loop-back mode. Remote Manager will then instruct the locally connected router to perform a BERT test on the remote unit and collect the results. If the router connected successfully on the unit's v120 number then the BERT test will be performed on the v120 number, otherwise the BERT test will be performed on the PPP number.

The length of time in seconds for the BERT test can be specified as a global option in the “Remote Operation Options”.

On a healthy ISDN line 1 or 2 errors in a 60-minute test (3600 seconds) is acceptable.

7.2.8 Set time after connecting to remote units

If the “Set time after connecting to remote units” check box is selected, then for a:

- Configuration Update
- File Update
- File & Configuration Update

operation, Remote Manager will set the time of the remote unit immediately after connecting. If this fails for any reason Remote Manager will not terminate the operation with an error (as it would for every other problem)

7.3 Launching update operations.

A number of check boxes on the “Operations” screen determine which type of operation will be performed.

The “Listening Mode” check box is used to determine whether the remote operation will be accomplished by listening mode or active mode.

The “Scheduled Operation for later” check box will cause the active mode operation to be run at a later time.

The “Multi Active Mode” check box will cause the operation to be run in multi active mode (see section 7.6).

The “Retry Failures” check box, will cause Remote Manager to re-run any operations that fail first time. The number of retries that will occur is determined by the settings in the “Active Options” tabbed pane of the “Options” screen.

The “Halt On Failure” check box if ticked will cause Remote Manager to terminate the remote operation session if an operation on a single unit fails. This can be used if you are not confident about the changes you are making and wish to avoid repeating any serious mistakes you might have made on all the units in the session.

Once the appropriate settings have been made, the “Execute Operation” button should be used to initiate the remote operation.

7.4 Results

The result of each operation attempt will be displayed in the “Remote Operation Log” accessed by clicking the “View Log” button. Any failures will be highlighted in red. A reason for the failure will also be visible in the log. This log is lost when Remote Manager is shut down but it is possible to save a copy of this log by clicking on the “Save Log” button. The same information can be viewed later in the results screen. See section 8.3.

7.5 Active Mode

For an active mode operation, as soon as the “Execute Operation” button is clicked Remote Manager will attempt to connect to the first unit to be updated. A progress bar positioned at the bottom of the “Remote Operations” screen will display the progress as a ratio of the sites attempted / total sites to connect to. If appropriate a further progress bar will appear when “S/FTPing” files to the remote unit to display the S/FTP progress for the site currently being updated.

Clicking “Stop Operation” at any time will cause Remote Manager to stop running the operation as soon as the action on the unit currently being updated is complete. It is possible to re-run (or resume) an operation at a later stage by clicking on the “Retry Operations” button in the “Results Screen” after selecting the operation session in the list. Units that have not been attempted will be attempted first followed by units that failed on previous attempts. Units on which the operation was successful last time will not be updated again. It is also possible to instruct Remote Manager to re-run the operation on individual units regardless of whether the operation was successful in any previous attempt. See the results section (8.1) for guidance on this.

It is possible to use more than one instance of Remote Manager (on more than one PC or on the same PC) to speed up the active mode operations. To do this, ensure that all instances of Remote Manager (on the different PCs) are reading from the same database. On the primary RM PC, set an active mode operation running. On the other Remote Manager PCs, find the currently running operation in the “Remote Operation Session Summary” screen. (See section 8.1.) Click on the “Retry Operations” button and this will cause the other instances of Remote Manager to work on the same “Operation Session” simultaneously. Remote Manager uses a record locking technique to ensure that more than one instance of Remote Manager will not attempt to update the same site

at the same time. Once a site has been successfully updated it will not be updated by further instances of Remote Manager. Any sites that are skipped because they have already been operated on successfully or are currently in the process of being operated on will be shown by black entries in the log.

7.6 Multi Active Mode

When “Multi Active Mode” is selected, Remote Manager will connect to up to 50 units simultaneously to perform the remote operations. The maximum of 50 simultaneous units can only be achieved when using the “Direct IP” connection method. Using the following methods a maximum number of 10 units can be updated simultaneously;

- dial up networking connections
- v120 connections
- X.25 connections

With “Multi Active Mode”, if not using “Direct IP” connection methods it is necessary to configure Remote Manager to use as many COMM ports and ISDN devices as are required. This is accomplished by making changes on the “Multi Connect Settings” tabbed pane of the “Options” screen (See section 11.6.).

For any connection method other than “PPP ISDN B channel” the transition from normal “Active Mode” to “Multi Active Mode” should be fairly trivial. For non “Direct IP” connection methods simply ensure that the TransPort/Sarian devices attached to the PC communications ports are capable of making simultaneous calls on the protocols that are to be used (*i.e.* v120, X.25 etc).

For the connection method “PPP ISDN B channel” it is first necessary to re-configure the Remote routers so that they all have different IP addresses. It is also necessary to ensure that no two remote routers that will be connected to simultaneously have IP addresses in the same “network”. Otherwise the PC would not be able to determine which dial-up-networking (DUN) connection to route the IP packets through.

The easiest way to achieve this is to ensure that each Remote TransPort/Sarian has an IP address on a different network.

It is normally necessary to re-configure 2 parameters on the remote TransPort/Sarian unit to achieve this. These are the PPP parameters “ipaddr” and “ipmin” for the PPP instance that will be answering the ISDN call.

“ipaddr” is the actual IP address of the PPP instance answering the call and “ipmin” is the IP address that will be assigned to the dial-up-networking (DUN) adaptor of the PC. Unlike with normal polling mode, these 2 IP addresses must be in the same network.

- ✓ *With normal “Active Mode”, the dial-up-networking (DUN) connection that Remote Manager creates will have the TCP option “Use default gateway on remote network” set. This means that all packets to an IP address on a different network will go through this connection. This is why when a TransPort/Sarian with the default configuration assigns the PC an IP address of 10.10.10.0, the PC is able to route packets to the TransPort/Sarian on IP address of 1.2.3.4 (on a different network) through this connection. With “Multi Active Mode”, the “Use default gateway on remote network” option is not set in the dial up networking connection. So the IP address of the dial-up-networking (DUN) adaptor on the PC must be on the same network as the remote TransPort/Sarian’s IP address.*

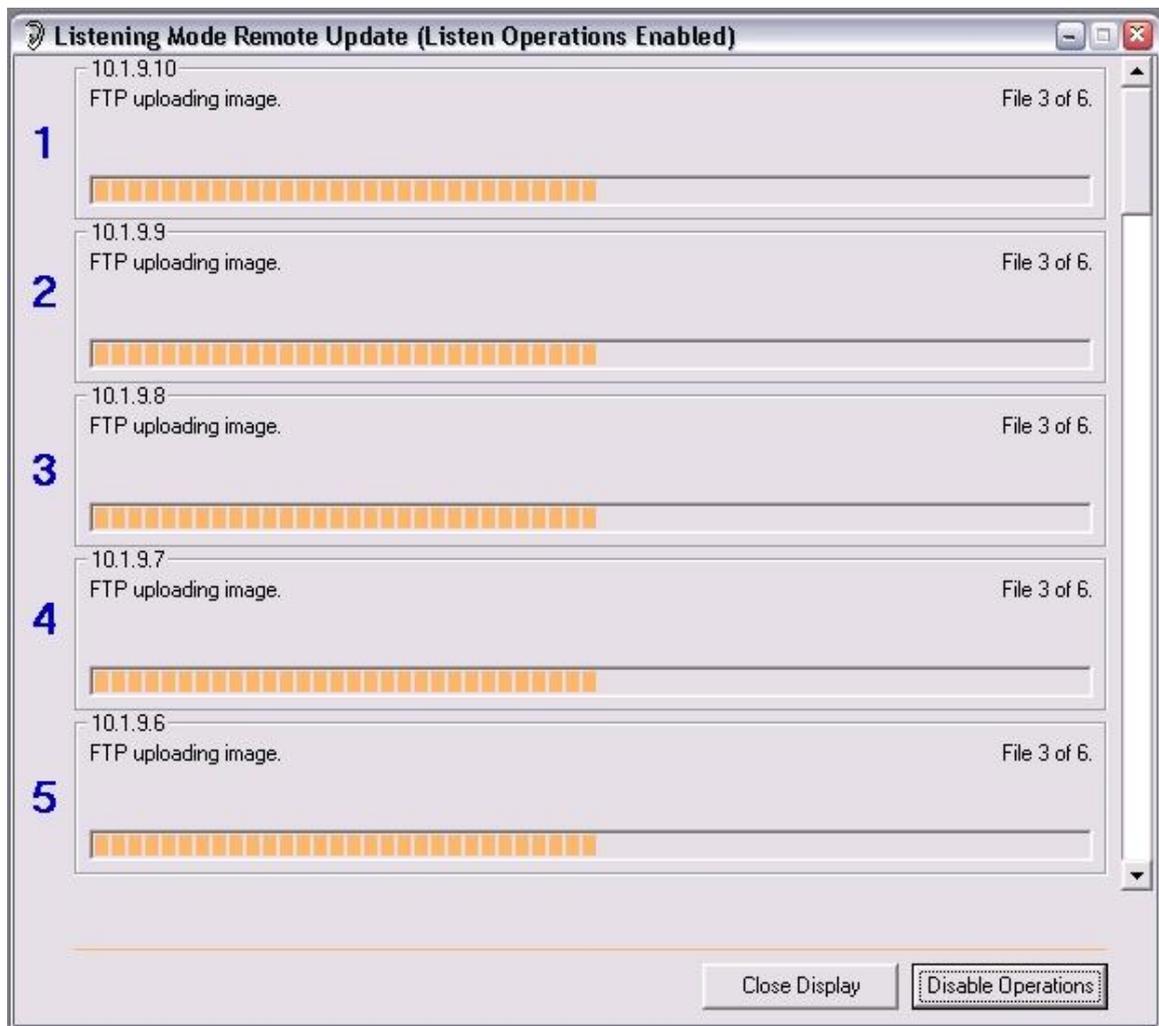
An example of a suitable class C addressing scheme follows. For every site set the last digit of the IP address to 1 and the “ipmin” value to 2. Change the second and/or third octets of the IP address to alter the network for each site.

Entry	ppp 0 ipaddr	ppp 0 ipmin
Site 1	192.0.1.1	192.0.1.2
Site 2	192.0.2.1	192.0.2.2
Site 3	192.0.3.1	192.0.3.2
Site x	192.78.32.1	192.78.32.2

When “Execute Operation” is clicked, Remote Manager will display the progress of each simultaneous update on the “Multi View” screen. This screen comprises a scrollable list of 50 status areas that show the individual progress of all units undergoing a remote operation.

7.7 Listening Mode

Clicking on the “Execute Operation” button in “Listening Mode” will cause the “Multi View” screen to be displayed. This screen comprises a scrollable list of 50 status areas which show the individual progress of all units undergoing a remote operation via “Listening Mode”. (This is the same screen that is used in multi active mode.)



If listening mode operations have not been enabled already in the current Remote Manager session then Remote Manager will not yet attempt any operations. To enable listening mode operations click on the “Enable Operations” button. The listening mode message in the status bar will change to “Listen Ops Enabled”.

- ✓ Whenever Remote Manager is running it “listens” for UDP packets from remote units containing the IP address, unit identity and serial number of the remote unit. Whenever such a packet is received, it is stored in the “Listening Table” in Remote Manager similar to the one shown below:

Unit Identity	Serial Number	IP Address	Time Stamp
Test 4%>	6527	10.1.9.4	04/08/2002 16:00:00
Test 5%>	5559	10.1.9.5	04/08/2002 16:00:00
Test 6%>	2840	10.1.9.6	04/08/2002 16:00:00
Test 7%>	4997	10.1.9.7	04/08/2002 16:00:00
Test 8%>	5477	10.1.9.8	04/08/2002 16:00:00
Test 9%>	5482	10.1.9.9	04/08/2002 16:00:00
Test 10%>	2235	10.1.9.10	04/08/2002 16:00:00
Test 10%>	5879	10.1.2.88	04/08/2002 16:00:00
Wash Angel GPRS Test	7403	62.136.14.216	26/11/2002 09:51:50
ss7404>	7404	10.246.248.35	26/11/2002 12:27:40

- ✓ The listening table can be accessed by clicking on the UDP packet count (“UDP RXs:”) in the status bar at the bottom of Remote Manager. The listening table will be updated every time a UDP packet is received.

Whenever Listening Operations are enabled, Remote Manager will continuously check the database for any units that require updating. If the serial number of a unit that requires updating is found in the “Listening Table” and various other criteria are met, an attempt will be made to perform a remote operation on the unit.

- ✓ If a unit is marked as having a dynamic IP address on the “Connection Details” screen of the “Site Editor” and if the remote operation requires a reboot, Remote Manager will wait for a new UDP packet containing the new IP address after the reboot before completing the operation.

7.7.1 Listen Operation Options

A number of Listening Mode Operation Options govern the exact behaviour of Remote Manager with regard to updating remote units in listening mode. These options can be found by clicking on the “Options” button of the main toolbar and then clicking on the “Listening Options” tab.

7.8 Scheduled Operations

It is possible to create an “Active Mode” or “Multi Active Mode” operation to be run at a later point in time. This is a scheduled operation. To create a scheduled operation:

- On the Remote Operations screen, tick the box labelled “Schedule Operation for later”.
- Click on the date and time controls underneath this check box and enter the date and time you wish the operation to run.
- Select the individual site or groups to update as normal.
- Select the operation type as normal.
- Tick the “Multi active mode” check box if the operation is to be carried out by multi active mode”.
- Click on “Execute Operation”
- Enter a name for the operation

The scheduled operation has now been created. Provided that scheduled operations are enabled the operation will be run on or after the scheduled date and time.

To enable scheduled operations, click on the “Scheduled Operations” tab on the “Operations” screen. Then click the button “Enable Scheduled Updates”. The scheduled updates message in the status bar will change to “Scheduled Updates Enabled”.

Also visible on this screen are any scheduled updates that have not yet been run. By clicking on “Edit Schedule” it is possible to change the time at which the scheduled update will run. Clicking on “Delete Schedule” will remove the entry from the list and de-schedule it.

- ✓ *It is still possible to view the deleted schedule as an operation in the Results screen and even manually run the operation by clicking on the “Retry Operations” button.*

8.0 RESULTS & RE-POLLS

The Operation Results can be accessed by clicking the “Results” button on the main toolbar.

This will display the “Remote Operation Session Summary” screen which lists all the Remote Operation Sessions ever attempted.

- ✓ *The results section is where re-polls of individual units and failed operations are initiated.*

8.1 Remote Operation Session Summary

The operation sessions are sorted by date with the most recent at the top. Clicking on a session name will display the statistics for the session in the area below.

Session Name	Creation Date	User Name
Get SSP	05/11/2009 13:54:34	ACRAVEN
Screen Shot Test	13/09/2002 21:21:09	Sarian
New site	30/07/2002 10:33:35	Sarian
New Site	25/07/2002 12:40:01	Sarian
New site	24/07/2002 14:29:59	Sarian
New site	24/07/2002 13:33:34	Sarian
Collect up-to-date sites specific values	17/07/2002 16:33:31	Sarian
Update Operation 10, Customer A Firmware Upgrade	12/07/2002 21:17:14	Sarian
Update Operation 9, Customer B Configuraiton Update	12/07/2002 16:23:18	Sarian
Update Operation 8, Customer A Collecting Parameters	12/07/2002 16:19:11	Sarian
Update Operation 6, Customer C Configuraiton Update	12/07/2002 16:16:58	Sarian
Update Operation 5, Customer D Configuraiton Update	12/07/2002 16:15:59	Sarian
Update Operation 4, Customer E Configuraiton Update	12/07/2002 16:12:11	Sarian
Update Operation 3, Customer F Firmware Upgrade	12/07/2002 16:04:29	Sarian
Update Operation 2, Customer G Firmware Upgrade	12/07/2002 15:53:29	Sarian

Update Operation 9, Customer B Configuraiton Update

Date of poll: 12/07/2002 16:23:18

Total units in session: 49

Operations not yet attempted: 0

Successful operations: **49**

Unsuccessful operations: 0

Time of first operation: 12/07/2002 16:23:19

Time of last operation: 12/07/2002 16:23:58

Valid From:

Valid to:

Reset Locks

Active Mode

VIEW FILTER (Use Wild-Card *)

Hide Selected Entries

Show Hidden Entries

Refresh View Activity Log Retry Operations Close

The statistics include:

- Date of poll
- Total units in session
- Total operations not yet attempted

- Successful operations
- Unsuccessful operations
- Time of first operation
- Time of last operation
- Valid From:
- Valid to:

Wherever there are unsuccessful operations, the “Unsuccessful operations” statistic will be highlighted in bold red text.

View Filter

The view filter allows unwanted operations to be filtered out. For example, entering “*Customer A*” into this field will cause Remote Manager to only show “Remote Operations” with “Customer A” in the title.

It is also possible to permanently filter out (or hide) certain entries. To do this select the entries you wish to hide and click the “Hide Selected” button. Whenever the “Show Hidden Entries” check box is NOT checked, the hidden entries will not be displayed.

To unhide all entries, hold down shift and click the “Hide Selected Entries” button.

To unhide individual entries, click the check box “Show Hidden Entries”, select the entries you wish to un-hide and then click the “Un-hide selected” button.

Operation Type

By making selections in the drop down list, it is possible to change the operation type e.g. from Listening mode to Multi Active Mode.

Refresh

Clicking the refresh button will cause the display to be updated (*i.e.* with any recently created remote operations).

8.2 Retry Operations

Clicking the “Retry Operations” button will cause Remote Manager to attempt to perform operations on all units in the selected session that have either failed or not been attempted previously. The remote operations will be attempted by “Active mode” regardless of the “Enabled for Listening Mode” setting. When this button is clicked the Remote Operations screen will automatically be launched to display the progress of the operations. If the original operation was created in multi active mode then the retry will also take place in multi active mode.

8.3 Session Results

Double clicking a session entry will cause the individual results for the selected session to be displayed in a new window. By making the appropriate entry in the drop down list at the top of the screen this window can be configured to display all results, successes only or failures only.

Screen Shot Test Results: Hit F5 for refresh

Show: All

Site Number	Site Name	Time Stamp	Result	Reason	Extra Info
20-1	20-1	13/09/2002 21:23:41	Success	No further information	
20-2	20-2	13/09/2002 21:26:32	Success	No further information	
20-3	20-3	13/09/2002 21:29:14	Success	No further information	
20-4	20-4	13/09/2002 21:31:56	Success	No further information	
20-5	20-5	13/09/2002 21:34:37	Success	No further information	
20-6	20-6	13/09/2002 21:37:19	Success	No further information	
21-1	21-1	13/09/2002 21:40:01	Success	No further information	
21-2	21-2	13/09/2002 21:42:43	Success	No further information	
21-3	21-3	13/09/2002 21:45:24	Success	No further information	
21-4	21-4	13/09/2002 21:48:06	Success	No further information	
21-5	21-5	13/09/2002 21:50:48	Success	No further information	
21-6	21-6	13/09/2002 21:53:29	Success	No further information	
22-1	22-1	13/09/2002 21:56:11	Success	No further information	
22-2	22-2	13/09/2002 21:58:54	Success	No further information	
22-3	22-3	13/09/2002 22:01:37	Success	No further information	
22-4	22-4	13/09/2002 22:04:19	Success	No further information	
22-5	22-5	13/09/2002 22:07:01	Success	No further information	
22-6	22-6	13/09/2002 22:09:43	Success	No further information	
23-1	23-1	13/09/2002 22:12:24	Success	No further information	
23-2	23-2	13/09/2002 22:15:06	Success	No further information	
23-3	23-3	13/09/2002 22:17:47	Success	No further information	
23-4	23-4	13/09/2002 22:20:29	Success	No further information	
23-5	23-5	13/09/2002 22:23:10	Success	No further information	
23-6	23-6	13/09/2002 22:25:51	Success	No further information	
24-1	24-1	13/09/2002 22:28:33	Success	No further information	
24-2	24-2	13/09/2002 22:31:15	Success	No further information	
24-3	24-3	13/09/2002 22:33:56	Success	No further information	
24-4	24-4	13/09/2002 22:36:37	Success	No further information	
24-5	24-5	13/09/2002 22:39:18	Success	No further information	
24-6	24-6	13/09/2002 22:42:00	Success	No further information	

Retry Selected Unit(s) Print Save Close

Each column can be re-sized and the new column and window size will be remembered for next time this screen is loaded.

Clicking on the column titles will allow the columns to be ordered alphanumerically by the column clicked (The default is to order the entries by the Time Stamp).

The “Save” button can be used to save the current display to a CSV file.

The “Print” button can be used to send the current display to a printer.

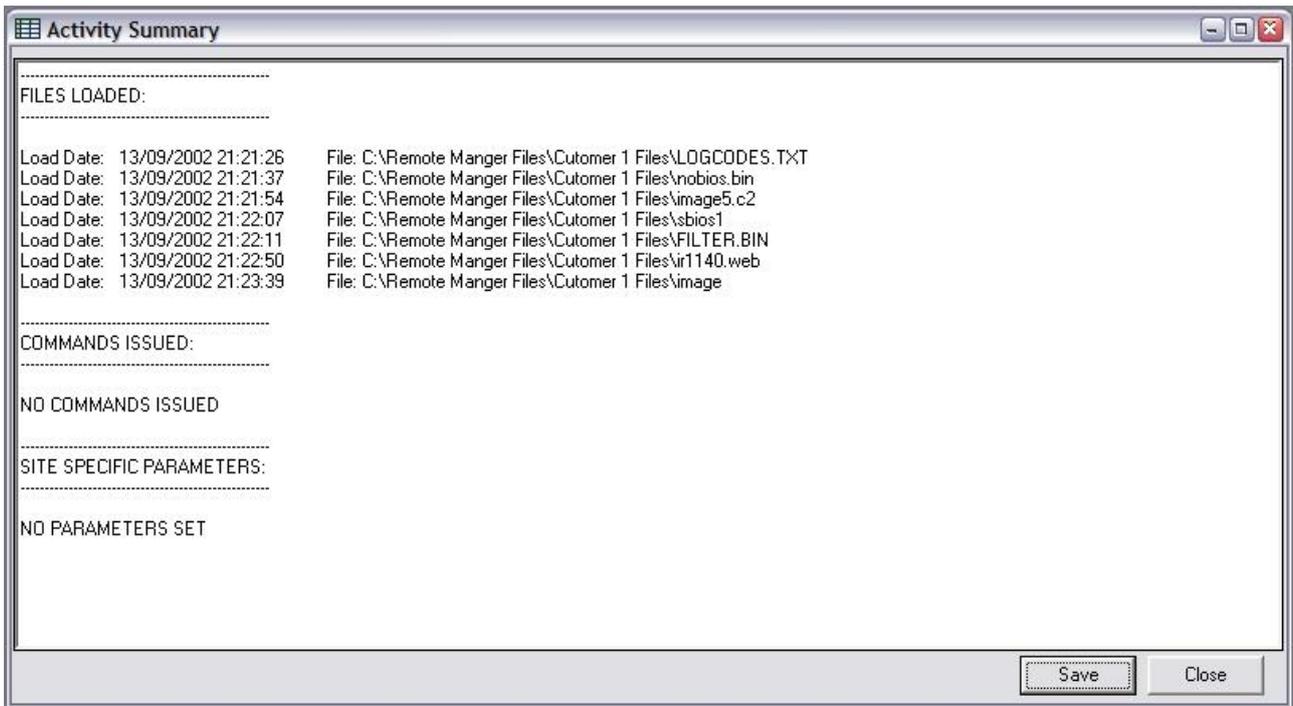
8.3.1 Retry Selected Unit(s)

Clicking the “Retry Selected Unit(s)” button will cause Remote Manager to re-run the remote operation on the selected unit(s) whether or not the previous attempt was successful. When this button is clicked the “Remote Operations” screen will automatically be launched to display the progress of the operations.

Retries initiated in this manner will always be carried out by normal “Active Mode” even if the original operation was run in “Multi Active Mode”.

8.3.2 Activity Summary

Double clicking any entry in the Session Results screen will cause a history window to be displayed listing any files uploaded, commands issued or site-specific parameters set during the remote operation.



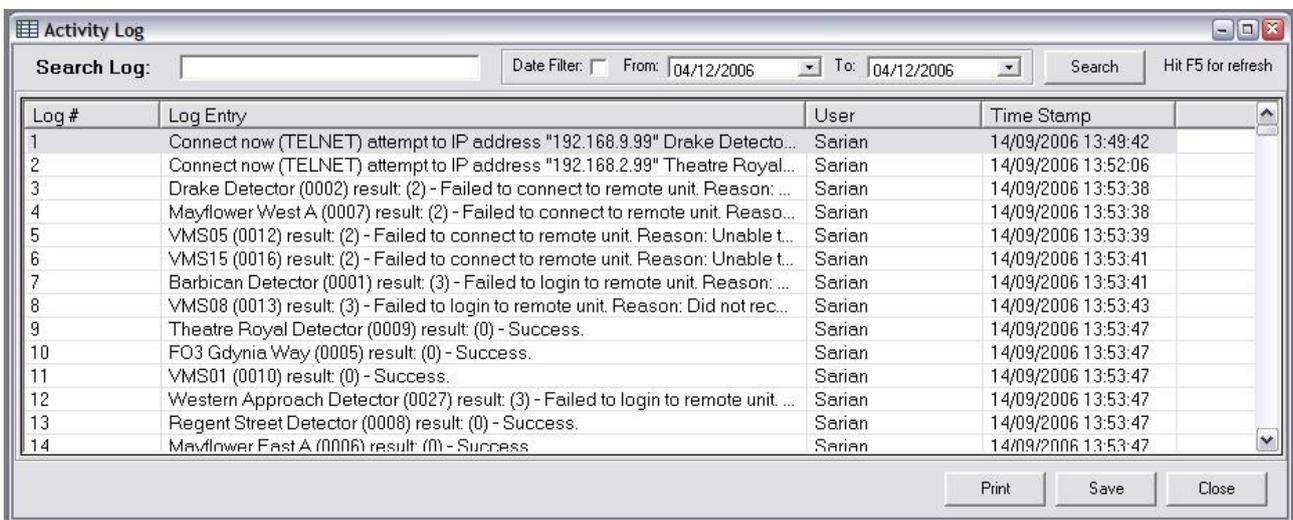
✓ *It is also possible to access this data on a per-unit basis via the history tab of the site editor*

8.4 Activity Log

One potential draw back of the “Session Results” and “Activity Summary” screens is that it only shows the result of the most recent attempt of an operation. For example if an operation fails twice and on the third attempt it is successful, the “Session Results” screen will show the “Result” as “Success”. By bringing up the detailed “Activity Summary” for the site it is sometimes possible to work out that there was more than one attempt at the operation (e.g. if it shows a file was loaded twice or a command was issued twice) but sometimes it will not be (e.g. if the serial number check failed, or the attempt to connect was not successful).

Clicking “View Activity Log” will show a log of every attempt and also the reason for the failure. So in this log if an operation is attempted three times and fails on the first two attempts, the reason for failure on the first two attempts can be found.

In addition to recording any remote operations it will also record the details of any “Connect NOW” attempts.



The “Date Filter” can be used to limit the amount of data displayed on the screen. By default only operations run on the current date will be displayed.

The “Search Log” field can be used to only display entries where the “Log Entry” contains the text in the “Search Log” field. To use the “Search Log” field, enter the text you wish to search for and then click the “Search” button. To remove the date restriction also un-tick the “Date Filter” check box.

9.0 GROUP & SITE-SPECIFIC PARAMETER MANAGEMENT

To access the group and site-specific parameter management click on the “Group Setup” button on the main toolbar.

Most Sar/OS parameters can be configured as site-specific parameters that Remote Manager can both set and read.

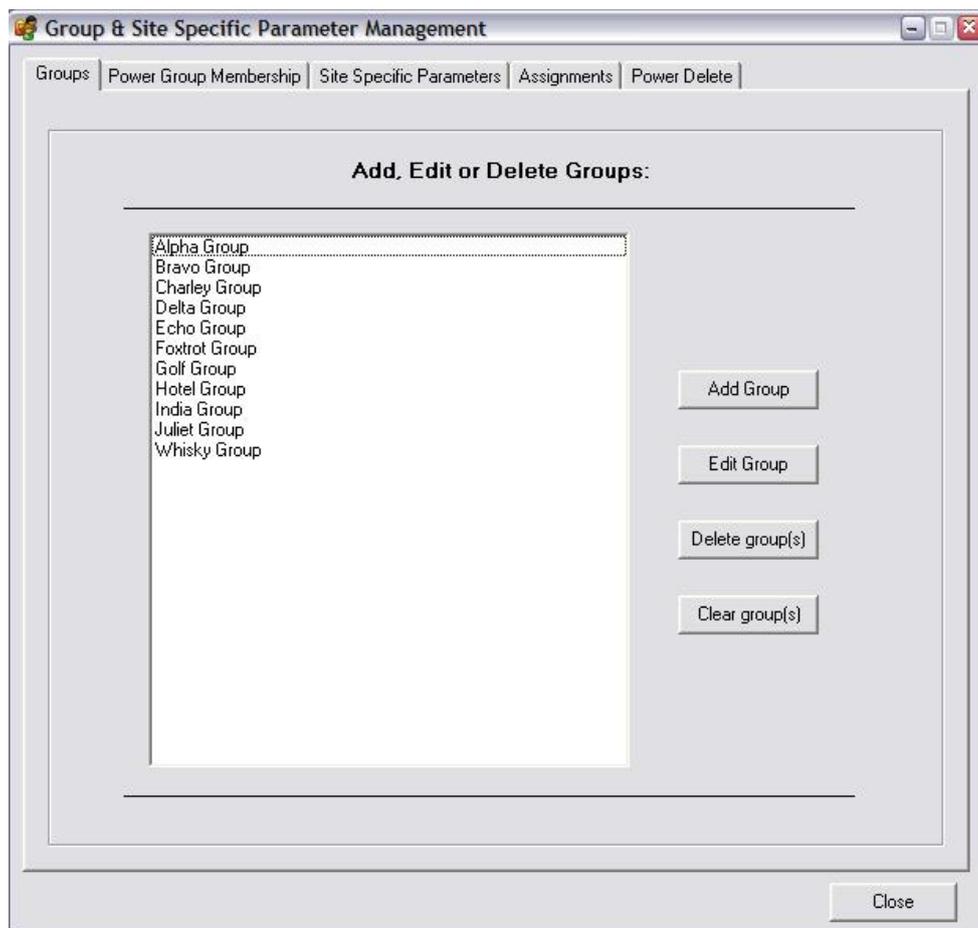
Remote Manager assigns site-specific parameters to groups. This means that the site-specific parameters available in the site editor for any one unit are dependent upon the groups that the unit is a member of.

The “Group & Site-Specific Parameter Management” section consists of a number of tabbed panes. These allow:

- Groups to be created, edited or deleted
- Units to be assigned / removed from groups on a bulk selection basis
- Site-specific parameters to be created, edited or deleted
- Site-specific parameters to be assigned or removed from groups
- All units in selected groups to be deleted (including the deletion of the unit history)

9.1 Groups

The “Groups” screen allows groups to be created, edited and deleted.



9.1.1 Creating a new group

To create a new group click on the “Add Group” button. Enter the name of the new group and then click OK.

9.1.2 Editing a group

To edit an existing group name, select the group to be edited and then click “Edit Group”. Edit the group name as appropriate.

9.1.3 Deleting a group

To delete a group select the group or groups to delete and then click the “Delete Group(s)” button. If the group to be deleted has members then the user will be warned about this but still allowed to delete the group. NB The sites that are members of this group will not be deleted; they will simply cease to be a member of the deleted group.

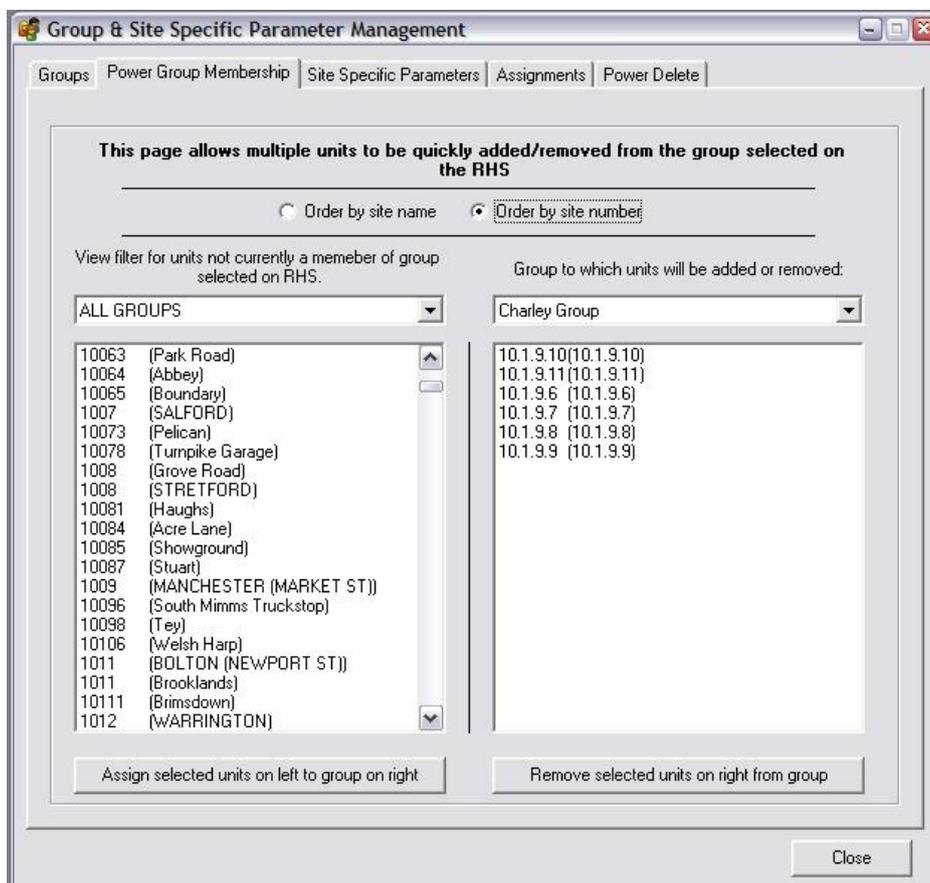
9.1.4 Clearing a group

To remove all units from a group or groups, select the appropriate groups and click the “Clear Group(s)” button.

9.2 Power Group Membership

The “Power Group Membership” screen allows units to be assigned or removed from a selected group in bulk.

The group that the units are to be added/removed from should be selected in the drop-down list on the RHS. The site names of all units that are currently a member of that group will be displayed in the list below.



The main list on the LHS shows all units that are not a member of the group selected on the RHS. The drop-down list on the LHS is a filter for this view. This makes it possible to view on the LHS all members of "Group A" that are not currently also a member of "Group B". To achieve this simply select "Group B" in the drop-down list on the RHS and select "Group A" in the drop-down list on the LHS.

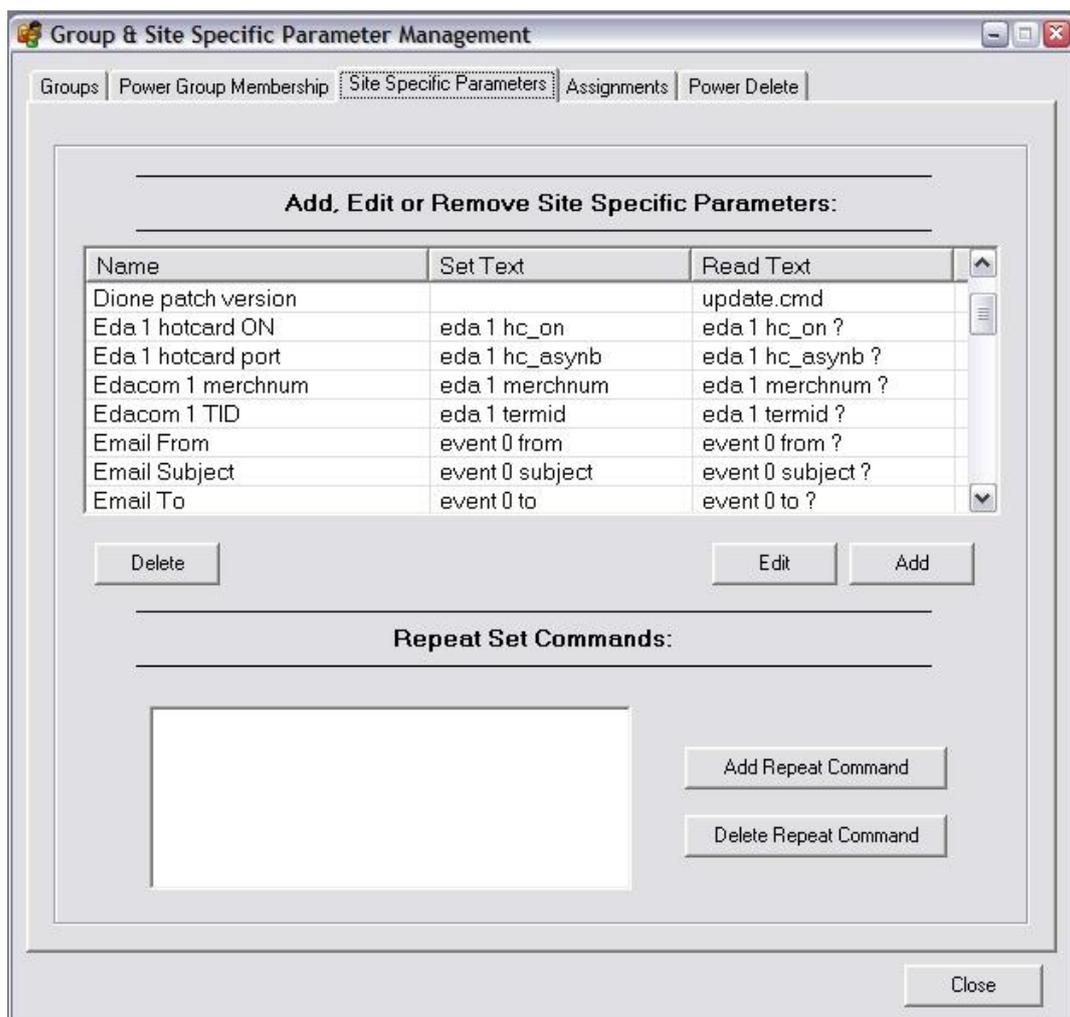
To assign or remove units from the group selected on the RHS, select the appropriate groups in the list boxes and then click "Assign selected units on left to group on right" or "Remove selected units on right from group" as appropriate.

9.3 Site Specific Parameters

The "Site Specific Parameters" screen allows site-specific values to be created, edited and deleted. A site specific parameter can be nearly any configuration parameter on a remote Transport\Sarian router. These parameters are completely user configurable *i.e.* the user enters the command to both read and set these parameters on the router into Remote Manager.

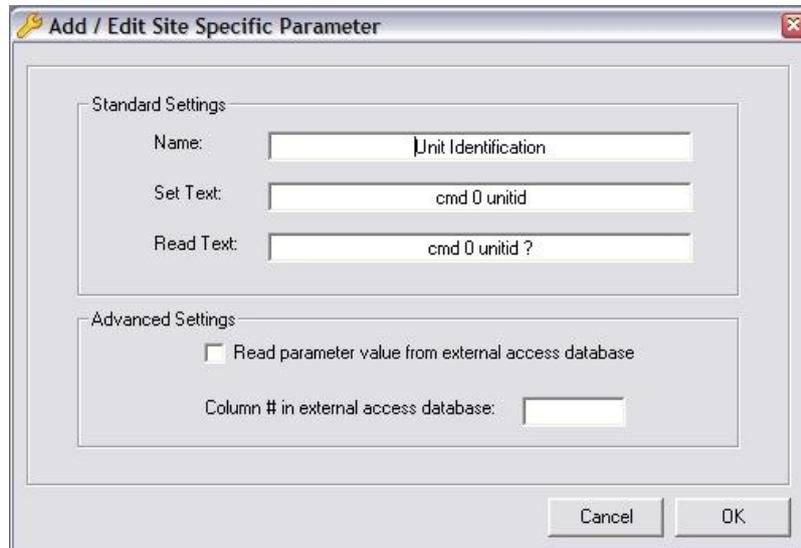
Sometimes special customer specific values (*i.e.* non router parameter values) are incorporated into Remote Manager. In this case the set-text and read-text entries act only to tell remote manager that the parameter in question is the customer specific value. In this case Remote Manager will function as it has been programmed to rather than executing the command on the remote unit. An example of this follows:

One Remote Manager user stores their own customer specific configuration files on the Sarian's\Transport's flash. Remote Manager has been programmed to read a version number out of one of the customer specific files and store this in the database as a site specific parameter.



9.3.1 Creating a new parameter

To create a new site-specific-parameter, click on the “Add” button. The following dialog box will be displayed:



In the “Name” field enter the name of the new site-specific parameter.

In the “Set Text” field, enter the Sar/OS command to program in the site-specific value. For example, the “Unit Identification” parameter is set (from the router’s command line) as follows:

```
“cmd 0 unitid the_name<CR>”
```

(Where <CR> is Carriage Return and “the_name” is the value of the parameter)

In the above example the following text would need to be entered into the “Set Text” field:

```
“cmd 0 unitid”
```

In the “Read Text” field enter the Sar/OS command to read the site-specific parameter (from the router’s command line). In the above example, the following text would be entered into the “Read Text” field:

```
“cmd 0 unitid ?”
```

Click “OK” to create the new site specific parameter.

9.3.2 Editing a parameter

To edit an existing parameter, select the parameter you wish to edit and click the “Edit” button.

9.3.3 Deleting a parameter

To delete a parameter, select the parameter you wish to delete and click the “Delete” button.

Currently it is not possible to delete site-specific parameters that are assigned to groups. If it is necessary to delete a site-specific parameter that is assigned to a group or groups, first remove the group assignment. See section 9.4.

9.3.4 Repeat set commands

When Remote Manager is programming the value of site specific parameter into a remote unit, sometimes it is necessary to program in this value more than once *i.e.* into many parameters.

An example of this is where Remote Manager is being used to manage routers with an authorisation table in (e.g. This is the case when a router is used with an Edacom device.). A

merchant number or floor limit may need to be set for several different card ranges yet only one site-specific value is required in Remote Manager. The Repeat set command facilitates this.

To add a repeat set command click on the “Add Repeat Command” button. When prompted enter the “set text” for the repeat command. There is no limit to the number of repeat commands that can be assigned to any one site specific parameter.

9.3.5 Special Read Only parameters.

Remote Manager is programmed with special behaviour for a number of read only site specific parameters. To use these features, create a new parameter, leave the “set text” blank and set the “read text” to a value from the table below.

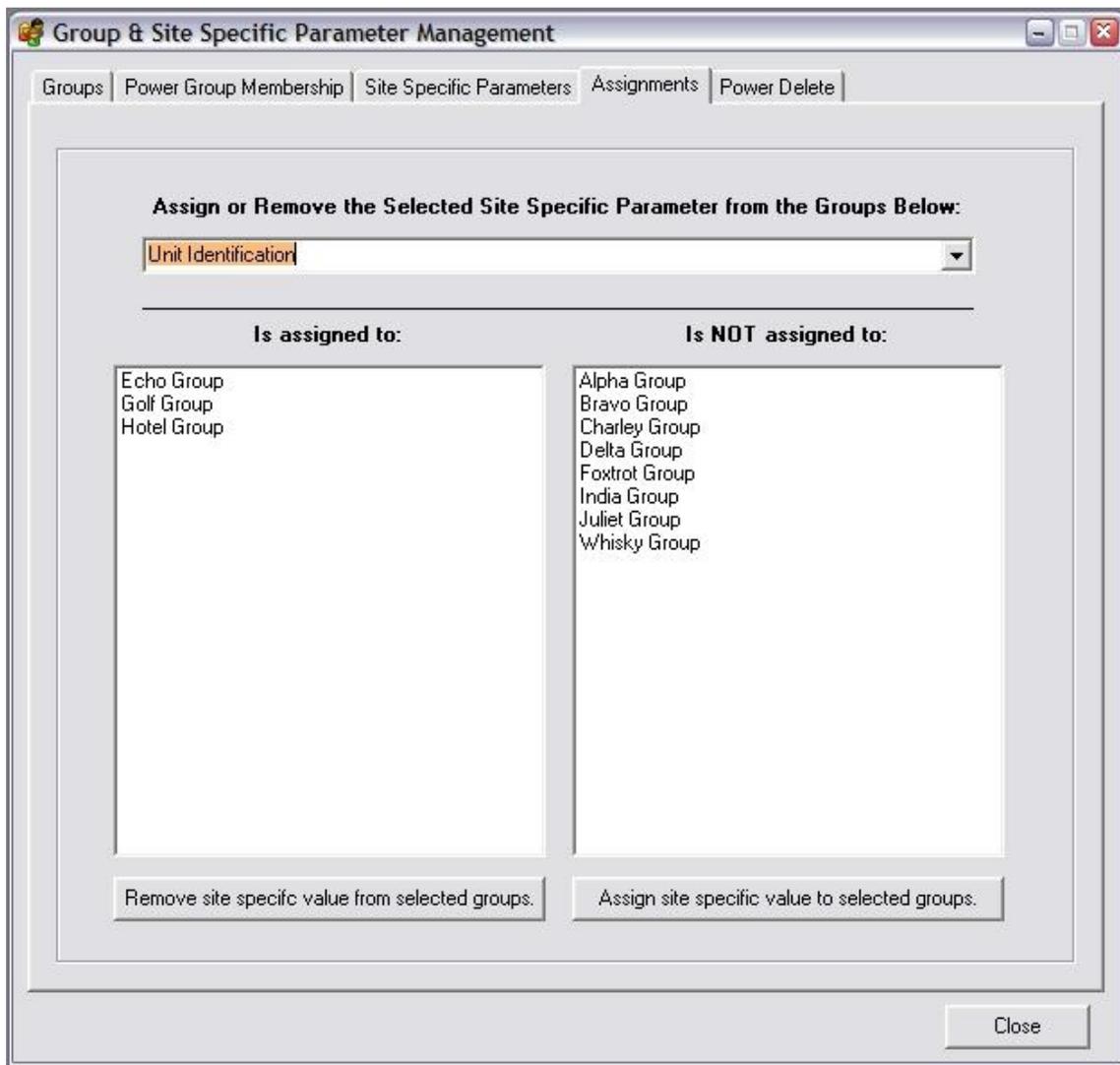
Suggested Name	Read Text	Description
Con Meth 0	conmeth0	Stores the result of the last connectivity test on the primary connection method
Con Meth 1	conmeth1	Stores the result of the last connectivity test on the secondary connection method
Con Meth 2	conmeth2	Stores the result of the last connectivity test on the tertiary connection method
ASY 1 BAUD	asy1baud	Reads the baud rate of ASY 1
Module Make	gprsmake	Reads the GSM/3G module manufacture's name
Current PPP 1 IP	ppp 1 status	Reads the current PPP 1 IP address
Signal Strength	modemcc 0 signal ?	Reads the current GSM/3G signal strength.
Module Firmware	modemcc 0 firmware ?	Reads the firmware version on the GSM/3G module.
ADSL Status #1	adslinfo 0	Reads the current ADSL modem status on legacy routers.
SA Count	sastat	Reads back details of the IPSEC security associations currently up and stores a count of these.
Up time	uptime	Reads the routers up-time the time since the last reboot
Flash Size	flashsize	Attempts to work out the flash size by adding flash used to flash free from the output of the dir command.
ADSL Status #2	adslst	Reads the current ADSL modem status on DR64x0 routers
ISDN ST	at\mibs=st.dstat	Reads the ISDN status

9.4 Assignments

The assignments screen allows each site-specific parameter to be assigned or removed from one or more groups.

First select the appropriate site-specific parameter in the drop down list. Any group that this parameter is assigned to will be displayed on the LHS. The groups that this parameter is not assigned to will be displayed on the RHS.

To assign or remove this parameter from a group or groups, make the appropriate selection(s) in the list and then click the “Assign site specific value to selected groups” or “Remove site specific value from selected groups” button as appropriate.



9.5 Power Delete

The “Power Delete” screen allows entire groups of units including all their history and statistics to be deleted from the Remote Manager database. Currently this option is enabled for expert users only and a special password is required.

- ✓ *Before you use this feature **PLEASE** take a back up of the database file. (The location of the database can be found in the “Database Path” field of the “Options” screen. If the “Database Path” field is greyed out instead check the Remote Manager application title bar.)*

Now that you have read the about how important it is to back up the database first, we will give you the password that you need to use power delete:

“goforit”

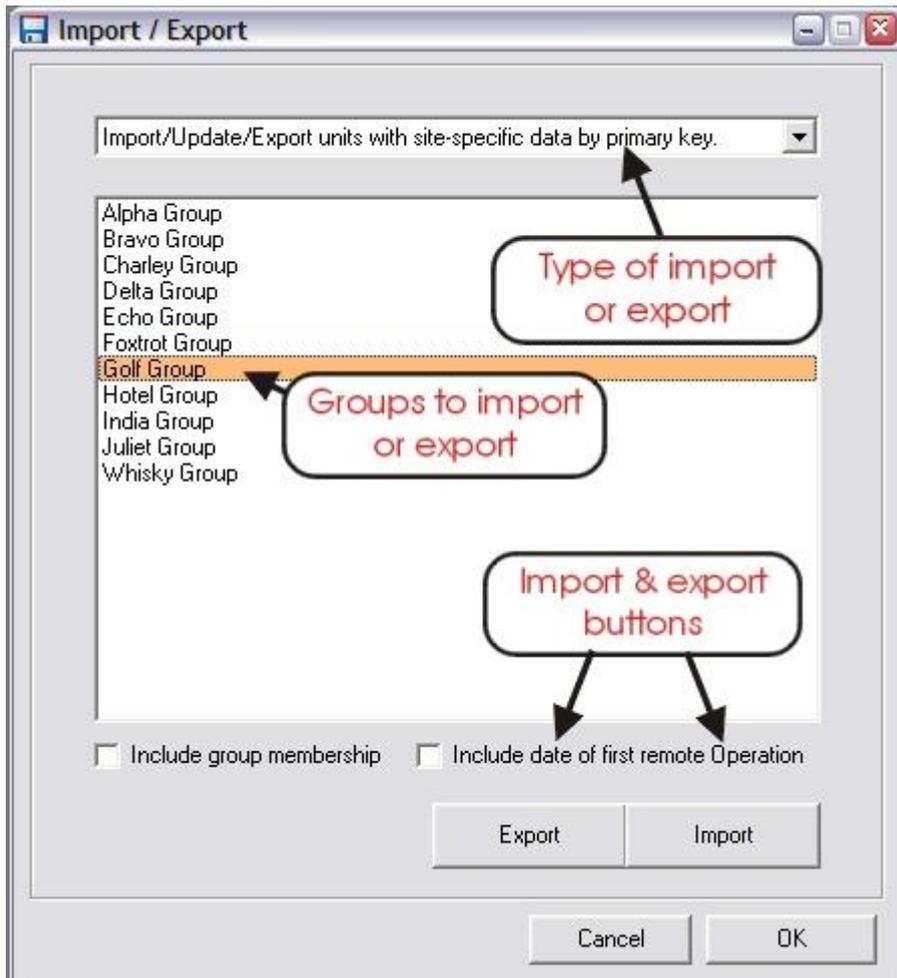
(one word no quotation marks)

10.0 IMPORTING AND EXPORTING UNITS

The Import and Export facilities can be accessed by clicking the “Import / Export” button on the main toolbar.

The Import and Export screen comprises:

- a drop down list where the type of import/export is selected
- a group list where the groups to be imported / exported are selected
- buttons to perform the import / export



The drop down list contains 2 default CSV import / export types:

- Import new units or update existing units by site number.
- Import/Update/Export units with site-specific data by primary key.

Depending upon the software version it may also contain other project-specific imports that can import or export to other types of file. The Import / Export buttons that are available depend upon the Import / Export type selected.

- ✓ *A **CSV** file is a **Comma Separated Value** file. This is a text file where commas are used to separate fields. This type of file is understood by most spreadsheets and some databases.*

10.1 Common procedures

The two most common reasons for using this feature are:

- To import a large number of units into the Remote Manager database for the first time. To achieve this, the recommend procedure is to first create a template and then import by site number. See section 10.2. However if it is necessary to also import the values of any site specific parameters, this can be achieved by importing by primary key, see section 10.3.
- To change the values of a large number of sites specific parameters in Remote Manager's database in order to later deploy these changes to the remote sites. See section 10.3.

10.2 Import by Site Number.

To perform this type of import, "Import new units or update existing units by site number" must be selected in the drop down list.

This import type does not support any sites specific data, *i.e.* importing the values of site-specific parameters.

This import / update facility will only import CSV files with the correct header (*i.e.* field titles). It is therefore recommended that the "Create Template" button is used to create a template CSV file with the correct header before hand.

Units imported by this method will be added to the database as new units if the following condition is met; a unit that is a member of the groups selected does not already exist in the database with an identical site number.

If a unit with the same site number is found in the database and that unit is a member of one of the selected groups then the unit's details will be updated with those from the CSV file entry.

To use this function:

- Select "Import new units or update existing units by site number" in the drop down list.
- Next click on the "Create Template" button and save the CSV template to disk.
- Open the CSV template in your chosen application (*e.g.* a spreadsheet) and make entries in the appropriate fields. Save the CSV file to disk.
- In Remote Manager, select the group or groups that you wish the imported units to be members of.
- Click the "Import" button and choose the CSV file you saved earlier.

The units in the CSV file will be imported into Remote Manager's database. A count of the units added and the units updated will be available at the bottom left hand side of the Import / Export screen.

10.3 Import or Export by Primary Key.

To perform this type of import, select "Import/Update/Export units with site-specific data by primary key" in the drop down list.

This import / export method does support importing or exporting values of site-specific parameters.

As the site-specific parameters available are dependant upon the groups that units are members of, the number of fields in any exported or imported CSV file is variable.

10.3.1 Exporting units with site-specific and or group data

To export units with site-specific data, select the group or groups containing the units that are to be exported.

Ensure that “Import/Update/Export units with site-specific data by primary key” is selected in the drop down list.

If the group membership is also to be exported, tick the Include group membership check box. (If ticked, a column will be created in the exported CSV file for every group selected on the Import / Export screen. If the exported unit is a member of any of these groups then a “Yes” entry will be made in the appropriate column for this unit, if not then a “No”)

Click on the “Export” button and save the “.txt” file to disk.

The txt file will contain a “Comma Separated Values” list of all the sites in the selected groups. The number of columns in the list will be dependant upon the groups selected and the site-specific parameters assigned to those groups.

✓ *It is important to make the exact same group selection and also that the site-specific parameters assigned to the groups have not changed if re-importing this list.*

Once the data has been saved to disk, it can be manipulated in spreadsheets and with other tools. New sites can be added and the values of any existing sites including the site-specific parameters can be changed. To add a new site, for the new row in the CSV file ensure that the primary key column is left blank. To change the data for an existing site, ensure that the primary key column is not changed from the value exported.

The primary key column is included to reduce the chance of accidentally updating the values of the wrong site when re-importing data. (Unlike the site number, the primary key will always be completely unique for each site in the Remote Manager database.) This does mean that the data cannot be imported into another Remote Manager database without first deleting the values in the Primary Key column.

If it is necessary to open this file in Microsoft Excel, it is recommended that following procedure be followed.

- Choose Open from Microsoft Excel’s file menu.
 - In the “Files of type” drop down list select “Text Files”
 - Navigate to the “txt” file exported from Remote Manager, select it and click “Open”.
 - Choose “Delimited” as the type of data and click “Next”.
 - Choose a comma as the type of separator and click “Next”.
 - Select all the columns and mark each column as “Text” format. (This is an important step!)
 - Click “Finish”
 - Finally resize the columns as necessary.
 - When saving the file, choose CSV as the file type.
- ✓ *In Microsoft Excel, opening the file as a CSV file can cause data corruption in some fields e.g. the ISDN number field. If a field contains no non-numeric characters, MS Excel will treat this field as if the field is of “Number Format”. If the ISDN number begins with a 0, the 0 will be deleted. The above procedure will avoid this problem.*
- ✓ *An Excel Macro could be written to speed up the import process*

10.3.2 Importing units with site-specific data

To import units with site-specific data, ensure that “Import/Update/Export units with site-specific data by primary key” is selected in the drop down list. Also if group membership is to be imported tick the “Include group membership” check box.

As the number of fields required in the CSV file changes with the number of site-specific parameters and also the groups selected (if group membership is included), it is advisable only to

attempt to import a file that is based closely on a file previously exported using this function. Also care should be taken to ensure that the same group or groups of units are selected for the import as were selected for the original export. If a different selection of groups is made and this group selection causes the units to have different site-specific parameters, Remote Manager will refuse to import the file.

To import the data:

- Select the groups that the imported units are to be members of.
- Click on the “Import” button and select the file to import.

If the “Include Group Membership” check box is ticked, then the units imported will only be made members of the selected groups if there is a “Yes” entry for that group in the CSV file. If the entry is not set to “Yes” then the units imported will be removed from this group if they are already a member.

If the “Include Group Membership” check box is NOT checked, then the units imported will all be made members of all the groups selected. In this case units imported will not be removed from any other groups of which they are already a member.

- ✓ *As detailed in the previous section 10.3.1, CSV file rows with a primary key value will update the values for units already in the database. CSV file rows where the primary key value is blank will be added to Remote Manager as new units.*

A count of the units added and the units updated will be available at the bottom left hand side of the Import / Export screen during and after the import.

11.0 OPTIONS

The Options screen can be accessed by clicking the “Options” button on the main toolbar. This facility consists of several tabbed panes.

11.1 General Standard

The general screen contains global options which affect the operation of Remote Manager.

11.1.1 ISDN Dial Prefix

The ISDN dial prefix is a digit which when set will be prefixed onto the ISDN number before dialling. This is useful when connected to a private exchange and an extra digit is required to access an outside line.

11.1.2 Analogue Dial Prefix

The analogue dial prefix is a digit which when set will be prefixed onto calls made through the analogue DUN connection. This is useful when Remote Manager’s modem is connected to a PABX and it is necessary to dial an extra digit to access an “outside line”.

11.1.3 FTP Up Timeout (s)

This is the maximum time in seconds that Remote Manager will allow for the FTP upload of a single file (e.g. during a file upgrade remote operation). If the file transfer of a single file takes any longer than this then an FTP timeout error will occur. The default value is 1800 seconds, which is 30 minutes. This value is suitable for firmware to be upgraded over very slow links.

11.1.4 FTP Down Timeout (s)

This is the timeout that is used when Remote Manager is downloading a file from an FTP host and network connectivity with the host is lost. This applies to a “Compare Files” poll. (See section x,x). The default value is 180 seconds which is 3 minutes.

11.1.5 DUN Pause

This feature is included for compatibility with Windows 95/98/Me. For all other operating systems the value should be set to 0. This is the value in milliseconds that Remote Manager will pause before launching a dial-up-networking (DUN) connection.

11.1.6 Local COMM Port

This is the PC communications port number that Remote Manger will use for remote connections.

11.1.7 Retry opening a comm Port time

This setting is used to specify the time in seconds that Remote Manager will wait whilst retrying to open a comm. port. This is useful in a scenario where Windows has not yet closed the comm. port from a previous dial-up-networking (DUN) attempt. This can occur occasionally when a remote unit does not answer. If you experience this problem then try a setting of 30 to 60 seconds in this field.

11.1.8 Retry Connection #

If an attempt at establishing a Telnet/SSH session with a remote unit has failed, Remote Manager will try to connect again the number of times specified by this parameter. If two IP addresses (separated by a “!” character) have been specified in the “IP Address” field in the site editor, then this value must be greater than “1” if a connection to the secondary IP address is to be attempted.

11.1.9 V120 Connect Time (s)

This is the maximum time in seconds that Remote Manager will wait for a v120 connection to be established. The default is 60 seconds.

11.1.10 Use %%% for v120

Usually, to establish a remote command session with a unit over a V120 ISDN call it is necessary to send the %%% characters before logging in. In some special configurations/firmware versions this is not required, for these situations un-tick the use %%% check box.

11.1.11 Web browser path

This is the location of the web browser that Remote Manager will launch after the “Connect Now” “Web” button has been clicked. Clicking on “Browse” allows an alternative web browser path to be selected.

11.1.12 Database path

This is the location of the database that Remote Manager is currently using. Clicking on “Browse” allows an alternative database to be selected. NB If Remote Manager is launched with a command line argument specifying the location of the database to use, then this field will be greyed out.

11.1.13 ISDN device for DUN connections

This is the name of the “Modem” (as found in Windows Control Panel) that will be used when ISDN DUN connections are created.

11.1.14 Analogue modem for DUN connections:

This is the name of the “Modem” (as found in Windows Control Panel) that will be used when analogue modem DUN connections are created.

11.2 General Advanced

11.2.1 External database for password and site specific parameters.

For security reasons some customers wish to store site passwords and values of sites specific parameters in a separate database to the main Remote Manager database. This functionally can be configured here.

11.2.2 Save Analyser Trace of Errors

When this feature is enabled, Remote Manager will connect to the unit specified here and save a snap shot of the analyser trace every time a remote operation fails. The analyser traces are saved in the “anatraces” subfolder of the Remote Manager installation folder.

11.2.3 X.25 Telnet Gateway / PPP Gateway

The X.25 Telnet Gateway can be used to allow Remote Manager to connect over X.25 to remote unit when the terminal adaptor connected directly to Remote Manager is not connected to an X.25 network. Instead of connecting via the local terminal adaptor, Remote Manager will access a remote ISDN device via Telnet.

These settings are also used for the “Direct IP via router PPP” connection method, see section 4.1.1 for details.

IP Address

This parameter contains the IP address of remote ISDN device with “D-Channel” X.25 access.

Username

This parameter contains the user name to use to authenticate with remote ISDN device in the Telnet session.

Password

This parameter contains the password to use to authenticate with remote ISDN device in the Telnet session.

PPP Instance #

The PPP instance number to program with the phone number, username and password to connect to the remote site.

X.25 Enabled

When this check box is checked, X.25 “D-Channel” connections will be attempted via the X.25 Telnet gateway rather than the locally connected terminal adaptor.

11.2.4 Always use rasdial

This setting will cause Remote Manager to always use the “rasdial” API call to launch dial up network connections. The alternate behaviour is to use Internet Explorer’s “Internet Dial” API (which shows the connection progress) for “Connect NOW” sessions and non multi active mode” remote operations. “rasdial” is always used for multi active mode remote operations and polling operations.

11.2.5 Use PORT (instead of PASV) mode for wininet FTP transfers

When using FTP to download files for a file “Compare Files” poll schedule, by default Remote Manager will use PASV mode. PASV mode has been found to work more reliably especially when connecting to many remote sites at once. Should you need to use PORT mode instead, then tick this check box.

11.2.6 Always use wininet.dll for FTP

This option is for debugging and should NOT be enabled normally.

11.2.7 Use FTP/SFTP to download files

During a “collect file” scheduled poll, this option dictates that FTP or SFTP should be used to download the file rather than the “type” command issued over a command session.

11.3 General SSH

SSH authorisation can use password mode, public key mode or public key failing back to password authentication preferences. The mode required can be set here.

When using public key authentication, the private key file and key pass phrase must be selected here. Use the freeware program PuTTYgGen to generate the private key.

11.4 Listening Options

The “Listening Options” screen contains setting that affect the behaviour of Remote Manger when operating in “Listening Mode”.

11.4.1 Maximum number of retries

This value determines the maximum number of times that Remote Manager will attempt an update on any one individual unit before giving up permanently.

11.4.2 Retry count for same IP address

This value determines the maximum number of times that Remote Manager will attempt an update on any one individual unit on a particular IP address. This is useful when units have dynamic IP addresses or are not necessarily accessible on the network at all times.

When this number of retries has occurred, Remote Manager will delete the IP address from the table above (but store it in the history) and wait for another UDP packet before making another attempt at the operation on this unit.

- ✓ *Only IP addresses specified as dynamic i.e. as accessed on the “Connection” screen of the “Site Editor” will be deleted.*

11.4.3 Minimum time in minutes between retries

This parameter determines the minimum time that Remote Manager will wait before retrying an operation on a remote unit via listening mode.

11.4.4 Time in minutes to consider an IP address valid

When set to a non-zero value, this parameter determines the amount of time in minutes to consider an IP address in the listening table valid. If this parameter were set to 5 for example, no updates would be attempted on any unit if a UDP packet has not been received within the last 5 minutes. This parameter is useful for units that have dynamic IP addresses.

11.4.5 Play sound upon receipt of UDP packet

If this check box is ticked, then Remote Manager will attempt to “play” a media file with the name “WHOOSH.WAV” located in the Remote Manager installation folder whenever a UDP packet is received.

11.4.6 Delete dynamic IP addresses after update

When checked, immediately after a successful listening mode operation, the dynamic IP address for the unit will be deleted from the listening table. (The IP address will be stored in the history however.)

Only IP addresses specified as dynamic *i.e.* as accessed on the “Connection” screen of the “Site Editor” will be deleted.

11.4.7 Update unit IP address with listen mode IP address after update

If this check box is checked, then after a successful operation, the unit IP address (as accessed from the site editor) will be updated with the IP address obtained during the listen mode operation. This is useful when the remote unit IP addresses were previously unknown but are static i.e. will not change.

11.5 Active Options

When a remote operation is run in active mode or multi active mode and retries are enabled, the number of times to retry a unit for each operation type and error condition is configurable.

To change the number of retries for a particular operation type and error condition:

- Select the operation in the operation drop down list
 - Select the error condition in the error condition drop down list
 - Change the number of retries for this operation by clicking on the spin arrows
- ✓ *The changes are immediately implemented in the underlying database and cannot be cancelled by clicking the cancel button.*

When the “Play success and failure sounds” check box is ticked, Remote Manager will attempt to play files called either pass.wav or fail.wav as appropriate after each remote operation. These files must be located in the Remote Manager installation folder.

11.6 Multi Active Settings

This page contains important configuration settings for multi active mode. Multi active mode is where Remote Manager simultaneously and actively connects to several remote units in order to perform the remote operations. For this to work with any connection method other than “Direct IP” it is necessary to configure Remote Manager to use as many different COMM ports as simultaneous operations are required. If this is to work with connection method “PPP ISDN B channel” then it is also necessary to configure Remote Manager to use as many ISDN devices as simultaneous operations are required. See section 2.3 for help with installing multiple ISDN devices.

11.6.1 Maximum Simultaneous Operations

Making an entry in this text field sets the maximum number of simultaneous operations that can be run in multi active mode. The maximum value that can be entered in here is 50 and the minimum is 1.

NB the maximum number of units that can be updated simultaneously over

- dial up networking connections
- v120 connections
- X.25 connections

is 10. 50 units can only be updated simultaneously when using the “Direct IP” connection method.

When this entry is less than 10, the ISDN devices/COMM ports will be used in order from the top of the screen to the bottom. For example, if the maximum simultaneous operations were set to the value 2. Only Connection 1 ISDN device, Connection 1 COMM port, Connection 2 ISDN device and Connection 2 COMM port would be used.

11.6.2 Connection ‘n’ ISDN Device

Select the appropriate ISDN device for each connection instance.

- ✓ *It is important that the ISDN device selected uses the same COMM port as is set in the adjacent COMM port 'n' text field.*

11.6.3 Connection 'n' COMM Port

Select the appropriate COMM port for each connection instance.

- ✓ *It is important that this entry matches the COMM port selected for the ISDN device in the adjacent ISDN device setting.*

11.6.4 Set-up Delay

In order to work correctly with Microsoft Windows™, it is necessary for Remote Manager to pause slightly in between creating the DUN connections. If Remote Manager attempts to create several DUN connections simultaneously then problems usually occur. This setting ensures that Remote Manager will wait for the specified number of milliseconds in between creating a DUN connection. The default value is 5000 milliseconds.

11.6.5 Launch Delay

In order to work correctly with Microsoft Windows™, it is necessary for Remote Manager to pause slightly in between launching DUN connections. If Remote Manager attempts to launch several DUN connections simultaneously then problems usually occur. This setting ensures that Remote Manager will wait for the specified number of milliseconds in between launching a DUN connection. The default value is 8000 milliseconds. This will not impact on the time taken to upgrade a large number of units it just offsets the launch of the Remote Operations. *i.e.* As soon as the first remote operation is complete, the free communications port will be used immediately to perform an operation on the next unit in the list.

11.7 User Interface

The user interface tab changes the behaviour of various sections of the Remote Manager user interface. Some users may prefer behaviour that is different to the default.

11.7.1 Site Editor

Prompt For Save When Loading a new unit if modified

When this option is selected, if a new unit is loaded into the site editor and if any of the data in the site editor has been modified, the user will be prompted to save any changes made to the database.

Bring to front after double click on a search result

When this option is selected, if a unit is loaded into the site editor by the user double clicking on a search result in the Find dialog box, the site Editor will be brought to the front of all the child windows.

11.7.2 Find Utility

Display site parameters in fields when result is single clicked

If this option is checked, whenever the user single clicks on a result in the Find dialog, the search fields of the find dialog box will be populated with the values from the selected unit.

11.8 Users

The users screen allows Remote Manager users to be added, edited or deleted from the currently loaded Remote Manager database. It also allows the permission's of the users to be changed. This screen is only visible if the currently selected user has "Super" permission level.

Entering a username and password and ticking the "Enable automatic login" check box will cause RM to automatically enter this username and password at program launch. The login screen is effectively bypassed when Remote manager is launched. This means that a computer can be configured to load remote manger automatically at start up and no human needs to be present to enter a username and password. Holding down shift whilst launching Remote Manager will disable this feature.

If "Use RM login credentials to connect to sites" is ticked, when connecting to remote sites, instead of using the username and password stored in the site editor, RM will use the username and password that the user used when logging in to Remote Manager at program launch. Also, the password used when the user logs into Remote Manager at program launch is not actually checked against Remote Manager's internal database. This is useful when a centralised authentication server is used and the remote sites are configured to check all authorisations against a centralised server via TACACS+ or RADIUS.

If "Force login with Windows username" is ticked, this will force the user to use the same username they used to log into Windows to log into Remote Manager.

If "Prevent Termination" is ticked, Remote Manager will not allow the user to exit the program.

11.9 Permissions

This screen allows a super user to set the permission level required to perform each remote operation. Double click on a Remote Operation to change the permission required to run that operation.

11.10 Email

Remote Manager can send automatic emails containing reports. This section is where the mail delivery is configured.

11.10.1 SMTP Server

The IP Address of the SMTP server.

11.10.2 SMTP Port

The TCP port number that the SMTP service is listening on. Usually this is 25.

11.10.3 Mail From Address

The email address that Remote Manager will claim to have when sending the email.

11.10.4 Use SMTP Authentication.

If the SMTP server requires authentication, tick this check box and fill out the username and password fields below.

11.10.5 SMTP Username

If the SMTP server requires authentication, enter the username here.

11.10.6 SMTP Password

If the SMTP server requires authentication, enter the password here.

11.11 Report Options

Use German Range Format

If the local settings are Germany, MS Excel reports require slightly different syntax to generate correctly.

Use Office 2007 compatible file names

If using Office 2007 and later, tick the check box “Use Office 2007 compatible file names” or the automated reports will not generate correctly. For Office 2003 and earlier un-tick this check box.

Use MapPoint North America

If the North American version of MapPoint is installed instead of the European version, it is necessary to tick this check box.

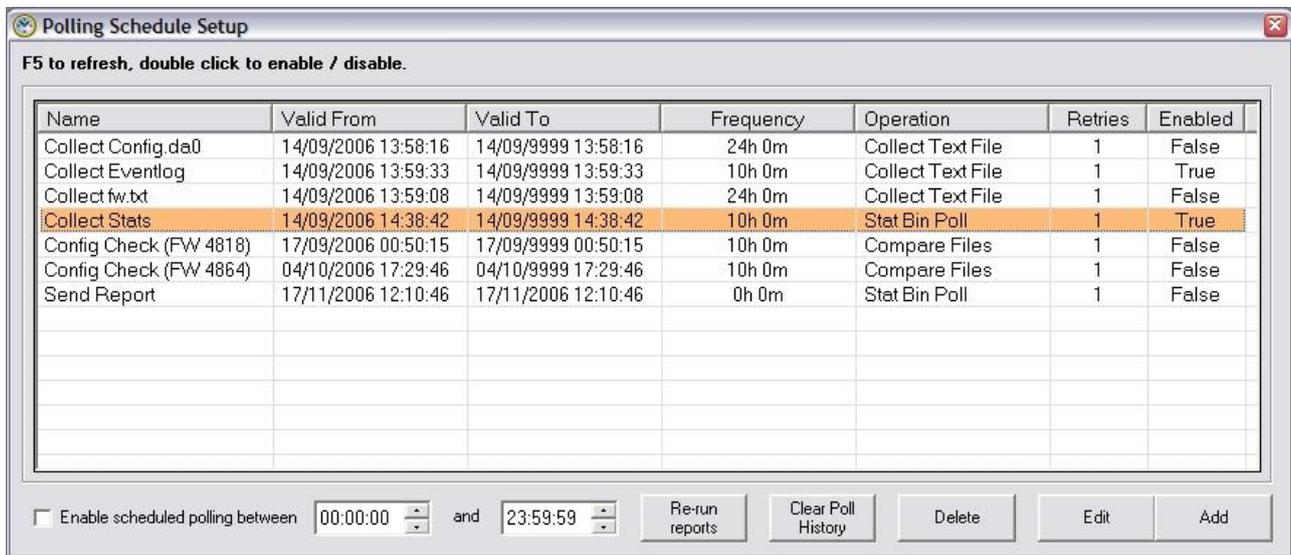
12.0 POLLING

The “Polling Schedule Setup” screen is where scheduled polls are set up. Scheduled polls are special remote operations that are run on a regular basis. They can be used to:

- Collect Statistics
- Generate and optionally email reports
- Collect text files (such as eventlog.txt or ana.txt) and optionally zip them up and email them
- Check configuration files (such as config.da0, fw.txt and sregs.dat). The files on all remote units will be compared with a base configuration file, if differences are found that are not due to site specific settings these will be highlighted in a report. The report can optionally be automatically emailed.

12.1 Polling Principles

Clicking the “Poll Schedules” button on the toolbar will display the Polling Schedule Setup screen:



A new polling schedule is added using the “Add” button.

A polling schedule can run only between the dates and times specified in the “Valid From” and “Valid To” columns.

Once a poll has run, it will not be valid to run again for the time specified in the “Frequency” column. Usually it is appropriate to run a poll every 24 hours. If it is required that the poll runs at the exact same time each day (*i.e.* the polling time does not drift) then it is recommended that a frequency of less than 24 hours is specified as the polling interval and also that a polling window is configured. The polling window specifies the time of day at which Remote Manager is allowed to run polls. This is configured by ticking the check box “Enable scheduled polling between” and specifying a start and end time. For example, to ensure that a poll will occur at exactly 02:00hrs every day, configure the polling window to be from 02:00hrs to 09:00hrs and configure the “Frequency” in the schedule to 8 hours. Thus when 02:00hrs comes Remote Manager will run the poll. Once the poll is complete it will not be valid to run again for another 8 hours. In another 8 hours the polling window will have expired and so no further polling will take place until exactly 02:00hrs the next morning.

A schedule can be enabled and disabled by double clicking the entry.

12.1.1 Re-Run Reports

The “Re-Run Reports” button can be used to re-create the reports for the selected schedule entry. This includes emailing the report if the schedule is configured to send reports generated by email. Note that this button does not cause Remote Manager to re-poll units, any reports generated will be based upon information already in the database.

12.1.2 Clear Poll History

The “Clear Poll History” button causes Remote Manager to “forget” that it has ever polled any schedules. Thus all schedules become valid for polling immediately. Provided that the polling window times are set appropriately and scheduled polling is enabled, clicking this will cause Remote Manager to immediately commence polling all enabled schedules.

12.1.3 Delete

The delete button will delete the currently selected polling schedule.

12.1.4 Edit

The edit button will cause the currently selected polling schedule to be loaded into the site editor.

12.1.5 Add

The add button will create a new polling schedule and load it into the schedule editor.

12.2 Creating a Polling Schedule

To create a new polling schedule click on the “Add” button. Give the schedule an appropriate name and tick the “Schedule Enabled” tick box.

12.2.1 Schedule valid between dates & times

Next in the “Schedule valid between dates & times” set the start time and end time. If you need the first poll to occur at a particular date and time select this under “Start:”. If not then leave the default settings which is the time you created the new schedule entry. For the end time, if there is a date and time in the future after which you no longer wish this polling scheduled to be run, set this as the end date under “End:”. Otherwise highlight the year part of the date under “End” and change it to “9999”.

12.2.2 Polling Settings

Set the poll frequency in hours and minutes to the frequency at which you wish the poll to be run.

Set number of retries?

Usually it is appropriate to run a poll every 24 hours. If it is required that the poll runs at the exact same time each day (*i.e.* the polling time does not drift) then it is recommended that a frequency of less than 24 hours is specified as the polling interval and also that a polling window is configured. See section 12.1 above.

12.2.3 Operation

Under operation the drop down list is used to select the type of poll. Changing this setting also determines which other tabbed panes are visible in the “Edit Schedule” screen.

Stat Bin Poll

Selecting “Stat Bin Poll” causes Remote Manager to collect statistics from the remote units. The statistics to be collect are configured in the “Stat Setup” screen and also under the “Stats” tab in the site editor. Various PPP bin and TPAD bin reports can be selected for polls of this type.

Download Files

Selecting “Download Files” causes Remote Manager to collect a text file with the name specified in the “File name to collect” field. Immediately after collecting the text file, Remote Manager can optionally issue a command to the remote unit. To issue such a command, make an entry in the “Command to issue” field. For example if collecting file ana.txt, a suitable command to issue might be “ana 0 anaclr”. This would clear the analyser trace and prevent the TransPort/Sarian from retrieving the same data on the next poll attempt.

If the filename to collect is eventlog.txt Remote Manager will automatically look for “outages” in the eventlog whilst collecting the file. It is thus possible to configure RM to generate an “Eventlog Outage Report”. See section 12.1 for more details.

Collected files will automatically be saved in a “collected_files” sub folder of the Remote Manager installation folder.

Compare Files

Selecting “Compare Files” will display the “Configuration Differ” tab. Using the configuration differ feature Remote Manager can connect to a remote site, download the configuration files (by FTP) and compare them to base configuration files stored on the PC. A report can then be generated highlighting any differences found. See section 12.6 for details.

12.2.4 Report Save Location

This location must be set to a valid path on the PC and is the location at which any reports generated by the schedule will be stored. *i.e.* PPP reports, TPAD reports, Eventlog Outage Reports and File Difference Reports.

- ✓ *Note that any files collected are not stored in this location, but rather in the collected_files sub folder of the Remote Manager installation folder.*

12.2.5 Email

Any reports generated or files collected can be automatically emailed to recipients specified in this list. Multiple email addresses can be entered here and separated with a semi-colon.

To enable this feature also tick the check box “Email report & charts to:”

- ✓ *Files collected and certain large reports will automatically be zipped up before being attached to the email. Please ensure that any SPAM detection or other software your company uses is not configured to delete or bounce emails with such attachments.*

12.2.6 Groups

For all polling operations, the groups of units to run the operation on must be selected in the “Groups” tab.

12.2.7 Further Details

For further details on the reports and poll types, see the sections that follow.

12.3 PPP Reports

To use the PPP reports (only visible when a Stat Bin Poll operation is selected - section 12.2.3), it

is first necessary to configure the remote TransPort/Sarian units to collect data on the network performance. This is usually achieved by configuring the remote TransPort/Sarian's UDP echo client to send UDP packets on a regular basis to a UDP echo server at the head-end location. Next a firewall rule is required to configure the TransPort/Sarian to collect stats on these packets and store the data in hourly bins. See section 17.0 for help with this.

Each PPP bin (one stored per hour) contains the following information:

Stat Name	Description
Bin Start Time	Start date and time of bin period.
Minimum Latency	The shortest round trip time measured in the hour.
Maximum Latency	The longest round trip time measured in the hour.
Average Latency	The average round trip time over the hour.
Transaction Count	The number of UDP packets sent in the hour.
Drop Count	The number of UDP packets to which no response was received in the hour.
Out of service count	The number of times that the interface was put out of service and/or deactivated due to the specified number of packets in a row being dropped.
Signal strength	The signal strength at the start of the hour.
Up time	The total number of seconds that the interface was "up" for in the hour.
TX Bytes	The total number of bytes transmitted on the interface in the hour.
RX Bytes	The total number of bytes received on the interface in the hour.

12.3.1 SLA Report

An SLA Report is a Microsoft Word™ document report based upon the weighted latencies and weighted average transaction times of all the units in the groups selected for the report. The report can contain data from several days.

Units that exceed specified latencies and packet loss thresholds are listed in the report.

On the "SLA Report" tab which is on the "PPP Reports" tab the following settings can be made

SLA Report (daily)

Tick this check box to generate an SLA report every day reporting on the previous day's data.

SLA Report (last day of month)

Tick this check box to generate an SLA report on the first day of every month, reporting on the previous month's data.

SLA Report (last day of week)

Tick this check box to generate an SLA report every week reporting on the previous week's data.

Include site without 24 bins per day

If this box is ticked then all sites that Remote Manager has any data for during the report period will be included in the report. If this tick box is not ticked, then any sites that Remote Manager has not managed to collect a full set of data for will be excluded from the report.

SLA/Sporadic Start hours

It is possible to configure certain periods of the day out of the SLA report. For example you may not be concerned about the performance at night time when your sites are not being used (Night time is often the time when network maintenance is performed). This setting specifies the start time for the first bin to be included in the report. To include the full 24 hours worth of data in the report set this to 00:00:00. This setting is shared with the "Sporadic Site Report".

SLA/Sporadic End Hours

It is possible to configure certain periods of the day out of the SLA report. For example you may not be concerned about the performance at night time when your sites are not being used. (Night time is often the time when network maintenance is performed.) This setting specifies the start time for the last bin to be included in the report. To include the full 24 hours worth of data in the report set this to 23:00:00. This setting is shared with the "Sporadic Site Report".

SLA Max Latency

This is the threshold at which if the daily average latency is exceeded, a unit will be highlighted in the report.

SLA Max Packet Loss

This is the threshold at which, if the daily average packet loss exceeds, a unit will be highlighted in the report.

Low Latency Defaults

Clicking the "Low Latency Defaults" setting will load suitable thresholds for monitoring a GPRS network with low latency.

High Latency Defaults

Clicking the "High Latency Defaults" setting will load suitable thresholds for monitoring a GPRS network with high latency.

An SLA example report follows:

SLA report from 13 Mar 2005 to 17 Mar 2005

(Hours of operation: 00:00:00 to 00:00:00)

Highlights of the Period

Total number of routers in service	31
Average latency for period	1517ms
Average packet loss for period	0.54%

Latency

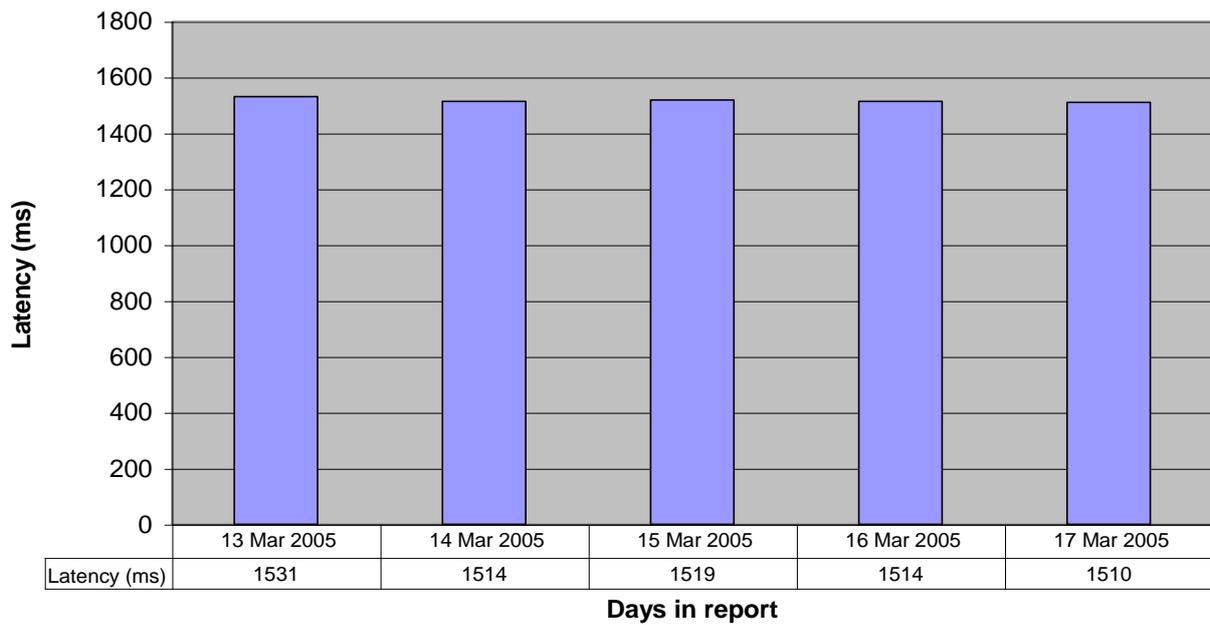
Average latency for network over period (5 days)	1517ms
--	---------------

Average latency for network per day of period

Day 1	13 Mar 2005	1531ms
Day 2	14 Mar 2005	1514ms
Day 3	15 Mar 2005	1519ms
Day 4	16 Mar 2005	1514ms
Day 5	17 Mar 2005	1510ms

Graphical representation of latency over period

Average Network Latency Per Day



List of sites with daily latency higher than specified value (1700ms)

Day	Date	Agent ID	IP Address	Latency (ms)
3	15-Mar-2005	Murray Store (1029)	10.19.36.254	2132
4	16-Mar-2005	Murray Store (1029)	10.19.36.254	1802
1	13-Mar-2005	Inn (1286)	10.18.75.254	2492
2	14-Mar-2005	Inn (1286)	10.18.75.254	2143
3	15-Mar-2005	Dale's House (3326)	10.18.44.254	1755
5	17-Mar-2005	Dale's House (3326)	10.18.44.254	1864
1	13-Mar-2005	The Pink Hotel (16-01101-1)	10.22.49.254	1719
5	17-Mar-2005	The Pink Hotel (16-01101-1)	10.22.49.254	1755

Packet Loss

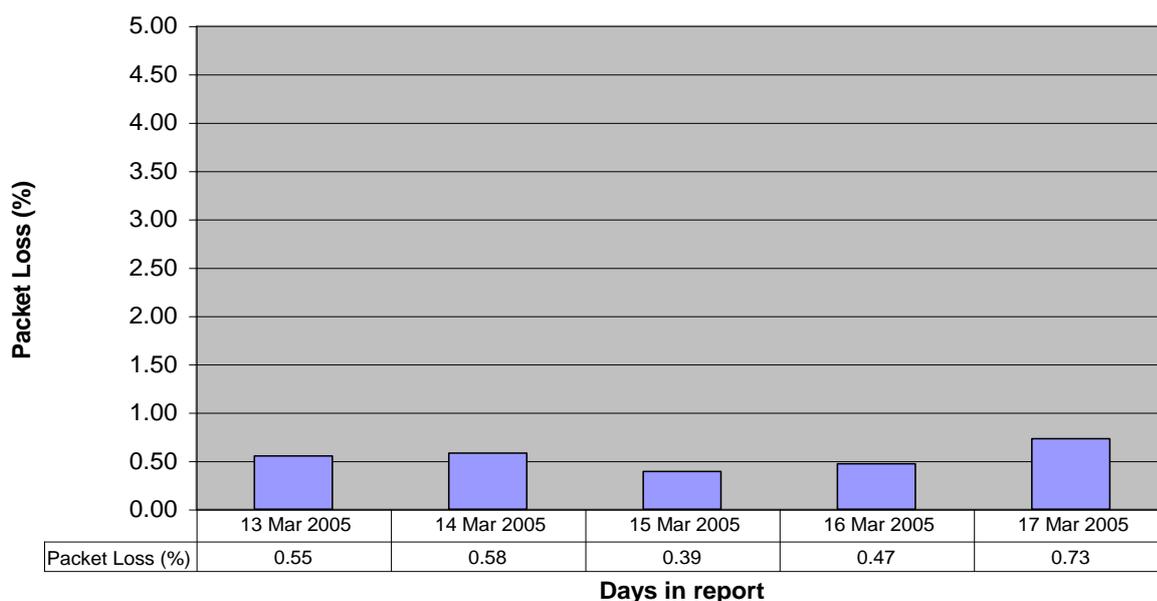
Average packet loss over period (5 days)	0.54%
--	--------------

Average packet loss for network per day of period

Day 1	13 Mar 2005	0.55%
Day 2	14 Mar 2005	0.58%
Day 3	15 Mar 2005	0.39%
Day 4	16 Mar 2005	0.47%
Day 5	17 Mar 2005	0.73%

Graphical representation of packet loss over period

Network Packet Loss Per Day



List of sites with daily packet loss higher than specified value (1%)

Day	Date	Agent ID	IP Address	Packet Loss (%)
3	15-Mar-2005	Murray Store (1029)	10.27.36.254	1.7
4	16-Mar-2005	Murray Store (1029)	10.27.36.254	2.2
2	14-Mar-2005	Bloom Supermarket (9238)	10.27.54.254	1.4
3	15-Mar-2005	Bloom Supermarket (9238)	10.27.54.254	1.1
4	16-Mar-2005	Bloom Supermarket (9238)	10.27.54.254	1.2
5	17-Mar-2005	Broad (2324)	10.27.115.254	1.0
2	14-Mar-2005	Cart Horse (2245)	10.27.11.254	2.3
3	15-Mar-2005	Cart Horse (2245)	10.27.11.254	1.1
1	13-Mar-2005	Kings Wash (2001)	10.27.24.254	1.0
4	16-Mar-2005	Kings Wash (2001)	10.27.24.254	1.3
5	17-Mar-2005	Kings Wash (2001)	10.27.24.254	1.4
1	13-Mar-2005	Inn (1286)	10.27.84.254	9.7
2	14-Mar-2005	Inn (1286)	10.27.84.254	8.5
4	16-Mar-2005	Inn (1286)	10.27.84.254	1.9
5	17-Mar-2005	Inn (1286)	10.27.84.254	1.1
1	13-Mar-2005	Dale's House (3326)	10.27.22.254	1.0
3	15-Mar-2005	Dale's House (3326)	10.27.22.254	1.2
4	16-Mar-2005	Dale's House (3326)	10.27.22.254	1.1
5	17-Mar-2005	Dale's House (3326)	10.27.22.254	5.5

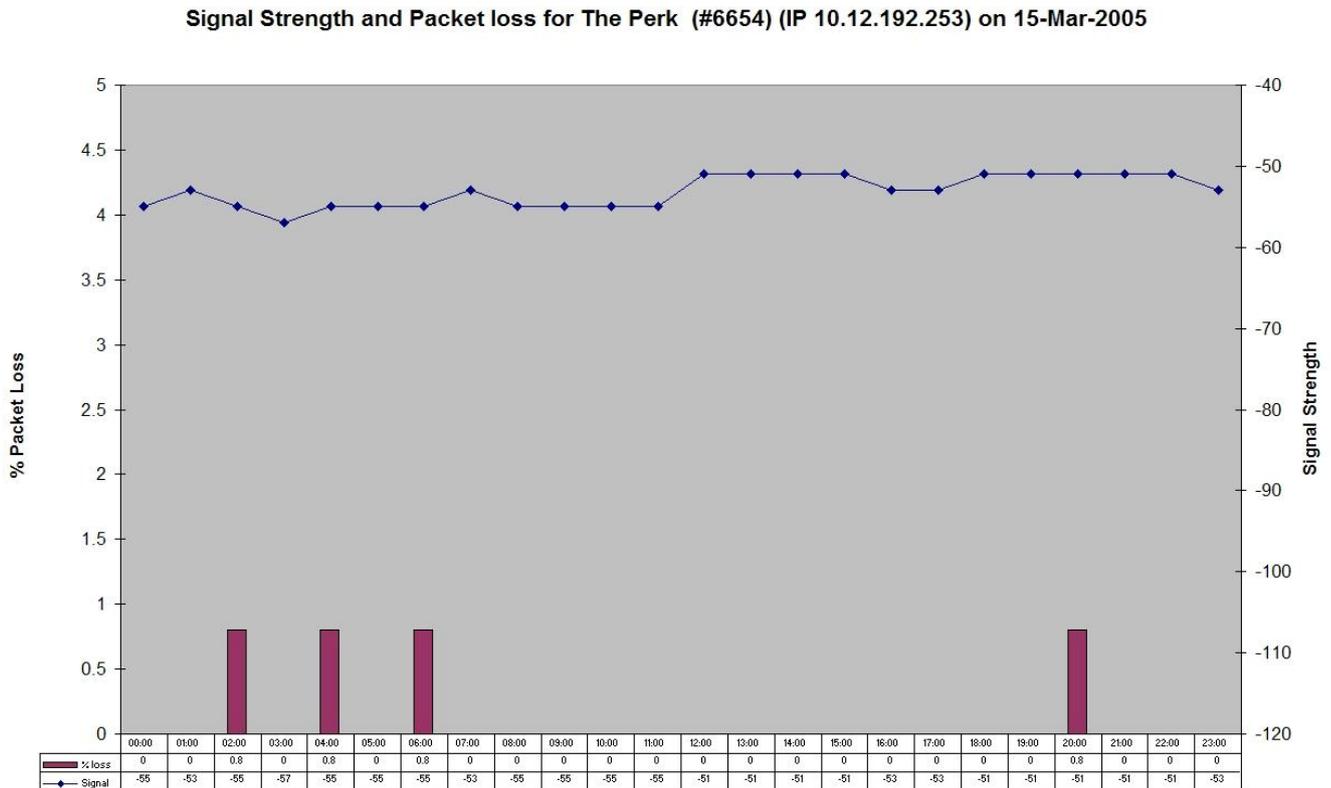
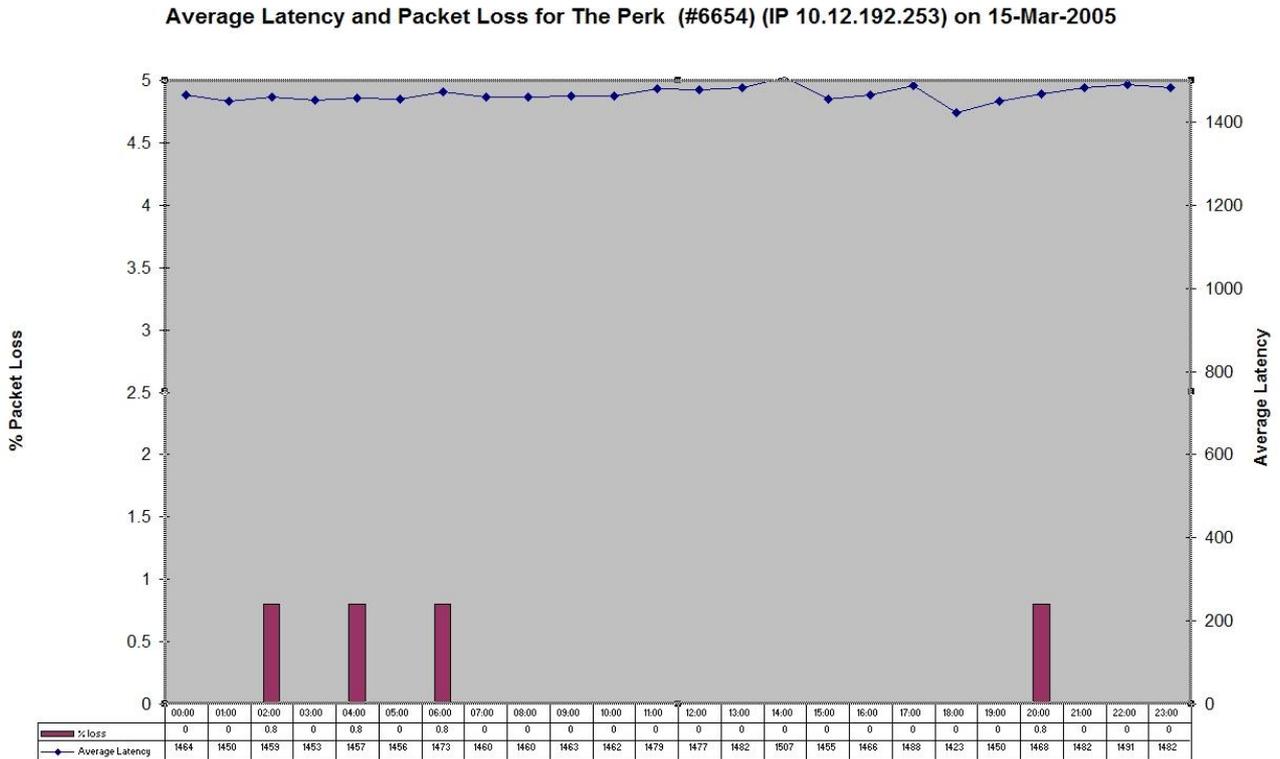
12.3.2 Latency & Loss Graphs

Latency and loss graphs are Excel workbooks containing various data such as packet loss, signal strength and latency plotted against time.

Individual Latency & Loss (daily)

If ticked, for every site in the groups selected, a Microsoft Excel™ workbook will be created containing a data sheet and two charts. One chart shows packet loss and latency against time for the previous day. The other chart shows packet loss and signal strength against time for the previous day.

Example charts follow:

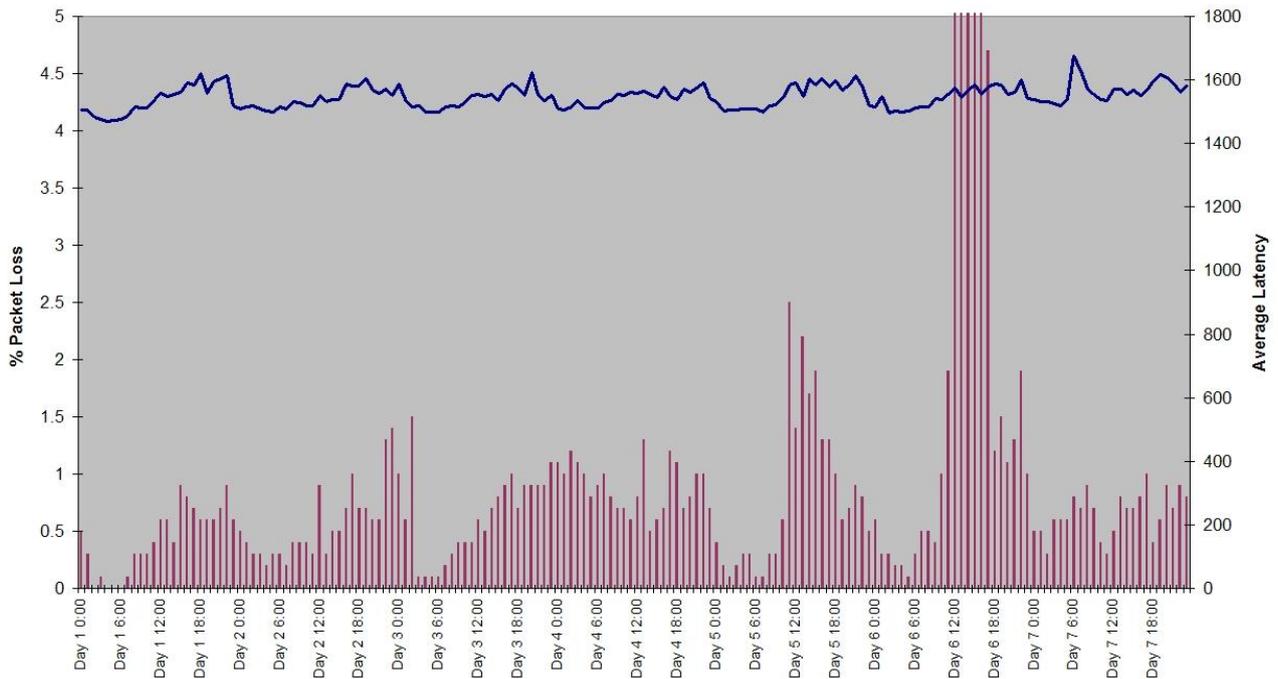


Latency & Loss (last day of week)

If ticked, a Microsoft Excel™ workbook will be created containing a chart showing the average latency and packet loss over all the sites in the selected groups for the previous week.

An example follows:

Average Latency and Packet Loss per hour from 13 Mar 2005 to 19 Mar 2005.
(Average values across many sites.)



Latency & Loss (last day of month)

If ticked, a Microsoft Excel™ workbook will be created containing a chart showing the average latency and packet loss over all the sites in the selected groups for the previous month.

Page Per Site Performance Report (Require MS Access 2003 or later)

This is the most powerful performance report. It shows all performance data collected from the PPP bins over the number of days specified in the “Days in page per site report” parameter below.

This report generates a single page of graphs and other data for each site in the selected groups.

- ✓ *A user familiar with Microsoft Access 2003™ should find it possible to completely customise this report e.g. add new charts, delete existing charts or even include their own data along side (from another data source). To achieve this open the “report_template.mdb” file in the Remote Manager installation folder with Microsoft Access 2003™ or later and modify the “PagePerSiteSummary” report and “bins” query as appropriate.*

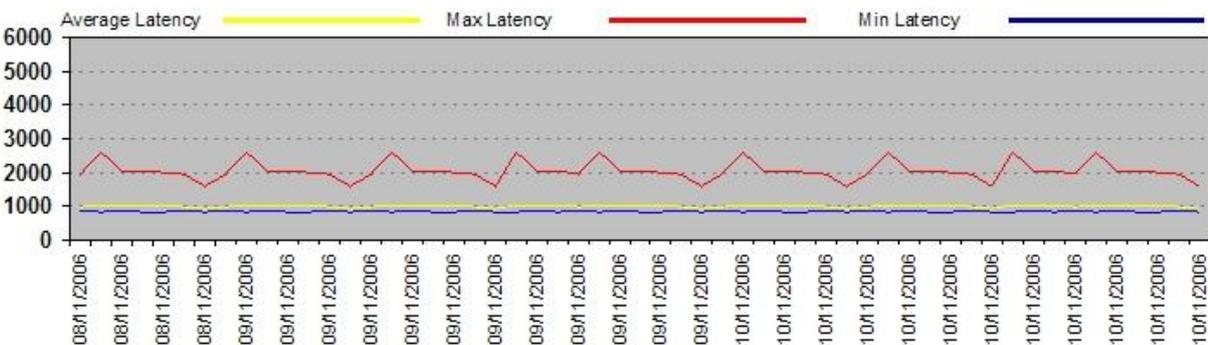
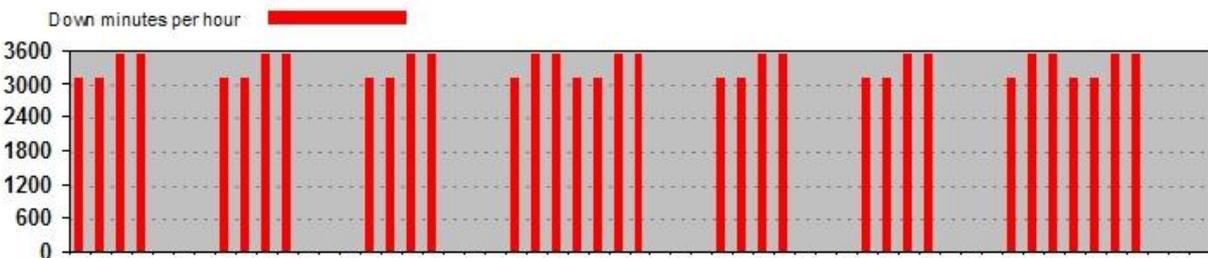
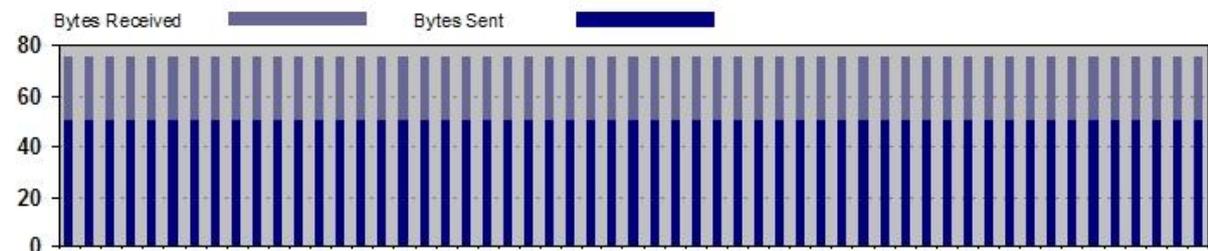
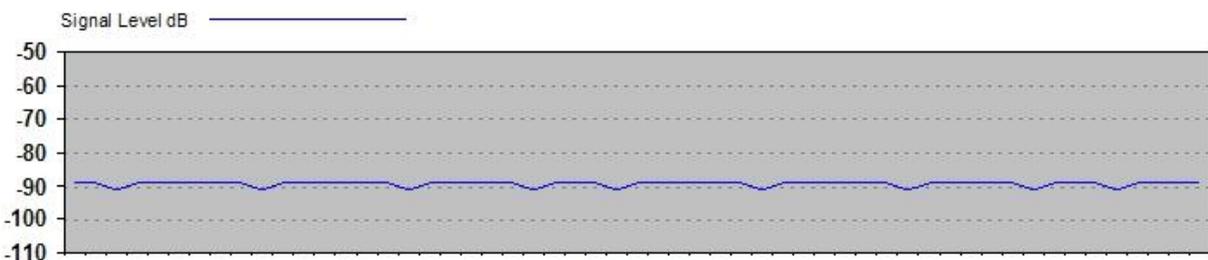
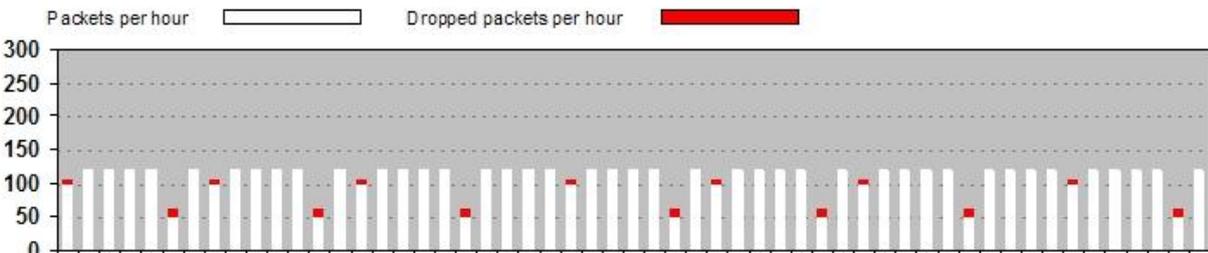
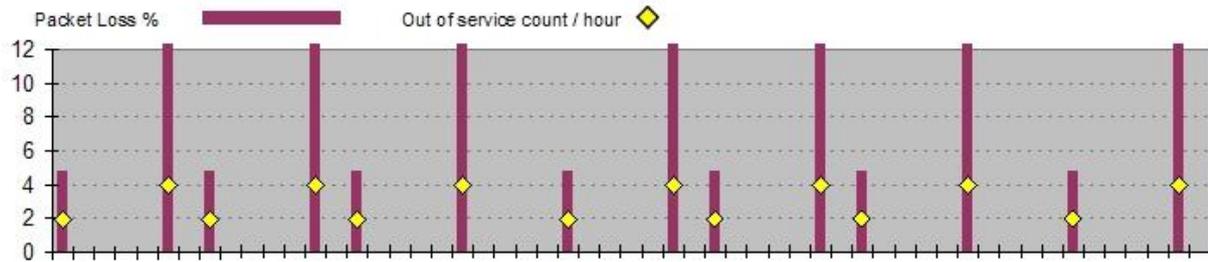
An example report is shown below:

- ✓ *The report contains fictitious data, it is not representative of real data.*

Manchester

0001

IP Address: 192.168.9.99 Total Packets Sent: 6075 Avg Packet Loss: 0.017 % OOS Count: 42



Email all PPP BINS daily

When this option is ticked an access “allbins.mdb” file containing all the PPP bin data for the last 7 days will be emailed to the address configured on the General tab.

12.3.3 Sporadic Site Report

The sporadic site report is a Microsoft Word TM document report containing a list of sites where the data in any hourly bin or daily average exceeds certain configurable trigger levels. The intention of this report is to quickly highlight problem sites allowing the user to concentrate on studying the Latency & Loss graphs or Page per site summary report for these problem sites only.

The following trigger levels can be set:

Trigger Name	Description
Hourly Loss	The % packet loss in any one hour has exceeded this % value
OOS Max	The number of out of service counts/interface deactivations due to packet loss in any one day has exceeded this value.
Hourly max latency	The maximum latency in any one hour has exceeded this value in milliseconds.
Daily Loss	The average weighted packet loss over one day has exceeded this % value
Daily avg latency	The average weighted latency over one day has exceeded this value.
Hourly avg latency	The average hourly latency over one day has exceeded this value.

Low Latency Defaults

Clicking the “Low Latency Defaults” button will load suitable default settings for use with low latency GPRS networks.

High Latency Defaults

Clicking the “High Latency Defaults” button will load suitable default settings for use with high latency GPRS networks.

12.3.4 Byte Count & Down Time

The byte count & down time report is a Microsoft Excel TM Workbook that contains charts showing:

- Data transferred per day (sum across all sites in the selected groups)
- Data transferred per site (sum per site over the period of the report)
- Down minutes per site over the period of the report (This may not be 100% accurate because if Remote Manager doesn't have PPP bin data to show that a site was up, it assumes it was down).

Byte count & down time report (daily)

Generates a daily report covering a period of one day.

Byte count & down time report (last day of week)

Generate a weekly report covering a period of one week (Sunday-sat?).

Byte count & down time report (last day of month)

Generate a monthly report covering a period of one calendar month.

Report Settings

Selecting Bytes, KiloBytes or MegaBytes will cause the report to be generated using the appropriate units.

12.4 TPAD Reports

If the TPAD entity is used in your TransPort/Sarian for transactions/authorisations, Remote Manager can automatically collect statistics on this transactions and store them in hourly bins *i.e.* one new bin is created each hour and the statistics for the transactions in that hour are stored in the bin.

Unlike the default behaviour of PPP, all TPAD instances write their stats to the same set of bins (each PPP instance has its own set of bins up until a certain number is reached).

Each TPAD bin (one stored per hour) contains the following information:

Stat Name	Description
Bin Start Time	Start date and time of bin period.
Minimum transaction time	The shortest total transaction time
Maximum transaction time	The longest total transaction time
Average transaction time	The average total transaction time
Minimum host response time	Shortest time taken for the unit to receive a response from the host after sending a transaction request.
Maximum host response time	Longest time taken for the unit to receive a response from the host after sending a transaction request
Average host response time	Average time taken for the unit to receive a response from the host after sending a transaction request.
Minimum layer 3 connection time	Shortest time for a L3 connection to be made (typically an X.25 call). This time excludes the time taken for lower layers (e.g. L2) to connect.
Maximum layer 3 connection time	Longest time for a L3 connection to be made (typically an X.25 call). This time excludes the time taken for lower layers (e.g. L2) to connect.
Average layer 3 connection time	Average time for a L3 connection to be made (typically an X.25 call). This time excludes the time taken for lower layers (e.g. L2) to connect.
Minimum layer 2 connection time	Number of successful L2 (typically LAPB) connections
Maximum layer 2 connection time	Longest time for a L2 connection to be made. This time excludes the time taken for lower layers (e.g. L1) to connect.
Average layer 2 connection time	Average time for a L2 connection to be made. This time excludes the time taken for lower layers (e.g. L1) to connect.
Minimum layer 1 connection time	Shortest time for a L1 connection (e.g. ISDN) to be made
Maximum layer 1 connection time	Longest time for a L1 connection (e.g. ISDN) to be made.
Average layer 1 connection time	Average time for a L1 connection (e.g. ISDN) to be made.
Number of host responses	The number of times a response was received from the host after sending a transaction request
Number of "no response from host"	The number of times a response was NOT received a response from the host after sending a transaction request.
Layer 1 connection failures	Number of times L1 failed to connect.
Layer 2 connection failures	Number of times L2 failed to connect.
Layer 3 connection failures	Number of times L3 failed to connect.
Number of backups	The number of times a backup connection has been made.
Count of SLA exceptions	Number of service level agreement exceptions. The SLA time is the time configured into the TPAD 'tsla' parameter. The time measured is the time to receive a response from the host.
Number of layer 3 connections	Number of successful L3 (typically X.25) connections.
Number of layer 2 connections	Number of successful L2 (typically LAPB) connections.

Number of transactions received from terminal	Number of transaction requests received from the local terminal.
Number of transactions sent to host	Number of transaction requests sent to host

12.4.1 TPAD SLA Report

An SLA Report is a Microsoft Word™ document report based upon the average total transaction time per day, the transaction failure rate per day and the count of SLA exceptions per day.

Units that exceed the daily specified average transaction times, failed transaction rates or SLA count threshold are listed in the report.

On the “SLA Report” tab which is on the “TPAD Reports” tab the following settings can be made:

SLA report (daily)

When ticked an SLA report covering one day’s worth of data and all the sites in the selected groups will be generated every day.

SLA report (last day of month)

When ticked an SLA report covering one month’s worth of data and all the sites in the selected groups will be generated every month.

SLA report (last day of week)

When ticked an SLA report covering one week’s worth of data and all the sites in the selected groups will be generated every week.

SLA Start hours

It is possible to configure certain periods of the day out of the SLA report. For example you may not be concerned about the performance at night time when your sites are not being used. (Night time is often the time when network maintenance is performed.) This setting specifies the start time for the first bin to be included in the report. To include the full 24 hours worth of data in the report set this to 00:00:00.

SLA End Hours

It is possible to configure certain periods of the day out of the SLA report. For example you may not be concerned about the performance at night time when your sites are not being used (Night time is often the time when network maintenance is performed). This setting specifies the start time for the last bin to be included in the report. To include the full 24 hours worth of data in the report set this to 23:00:00.

SLA Max Tran time

If the daily average transaction time for site exceeds this value (in milliseconds), it will be listed in the report.

SLA Max & Failure

If the daily % transaction failure rate for a site exceeds this value (in percent), it will be listed in the report.

SLA Exception Threshold

If the daily count of SLA exceptions exceeds this value then the site will be listed in the report. An SLA exception is where the host response time is greater than the value configured in the TPAD parameter "SLA Tran Time (ms)" (tpad x tsla)

Include site without 24 bins per day

If this box is ticked then all sites that Remote Manager has any data for during the report period will be included in the report. If this tick box is not ticked, then any sites that Remote Manager has not managed to collect a full set of data for will be excluded from the report.

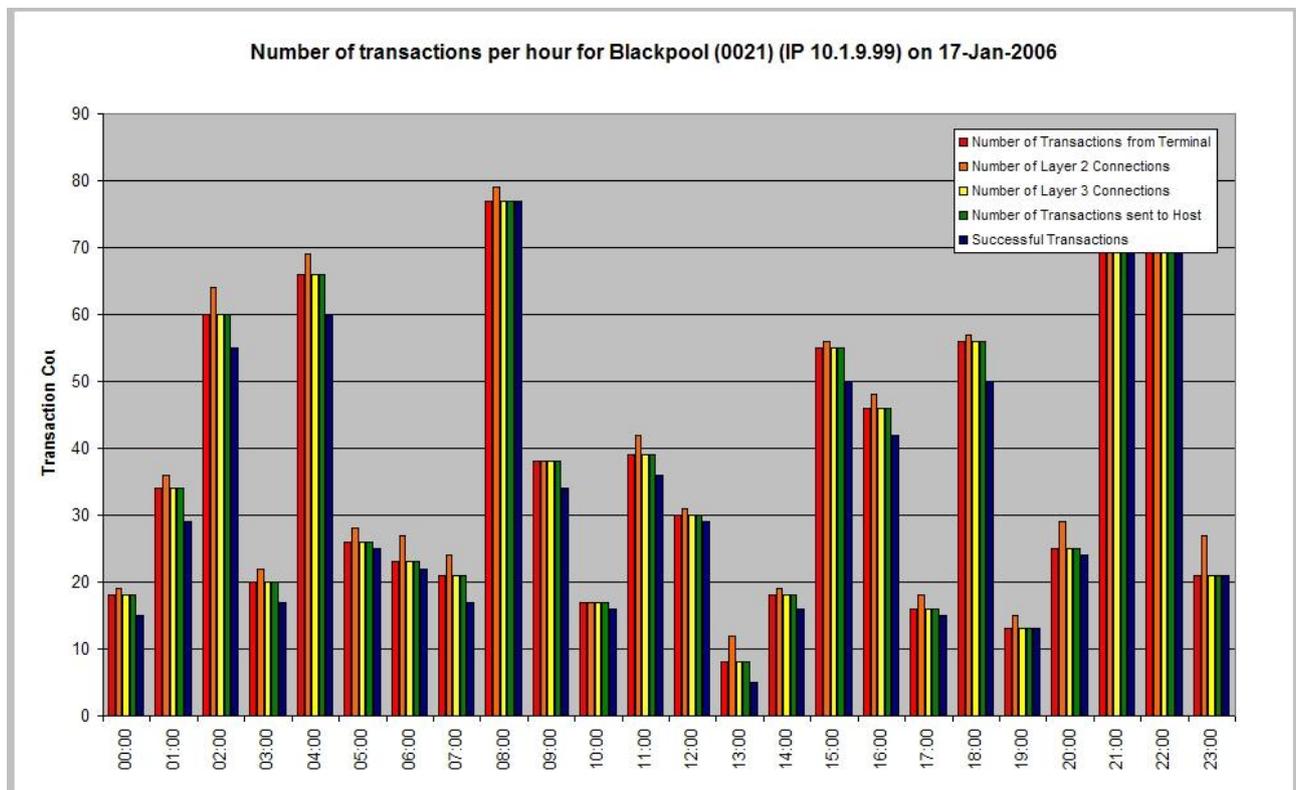
12.4.2 TPAD Charts

The following TPAD chart reports can be enabled

Detailed stats per hour yesterday (1 workbook per site)

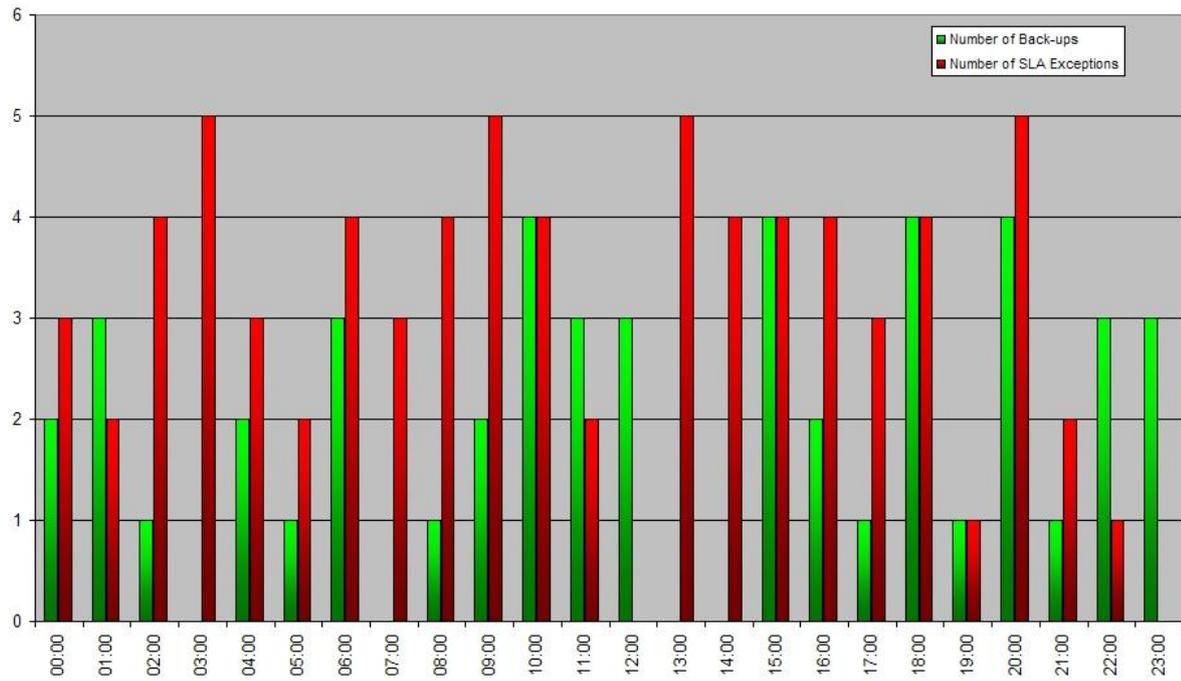
The detailed site report is an Excel workbook with data in for just one site for a 24 hour period. It currently contains 1 date sheet and 6 charts.

Number of transactions per hour

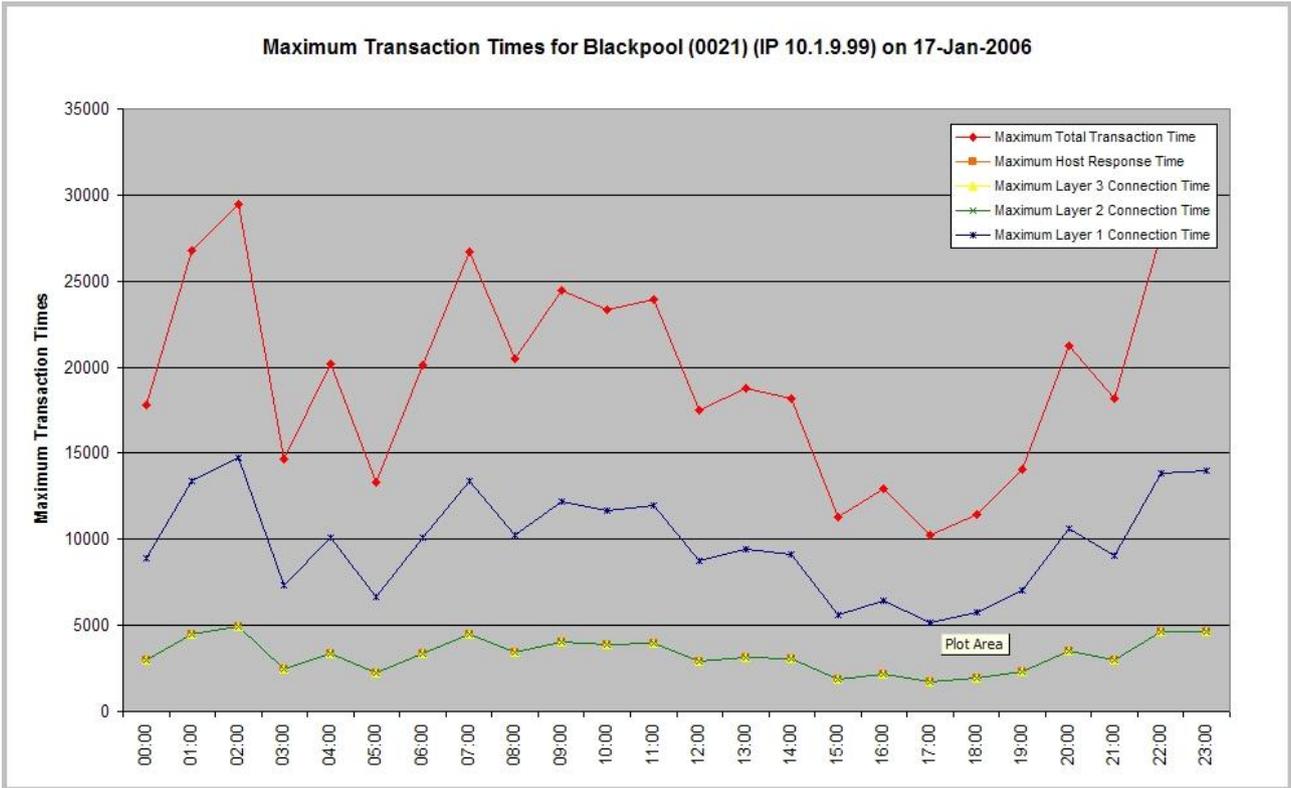


SLA Exceptions and Automatic Back-ups

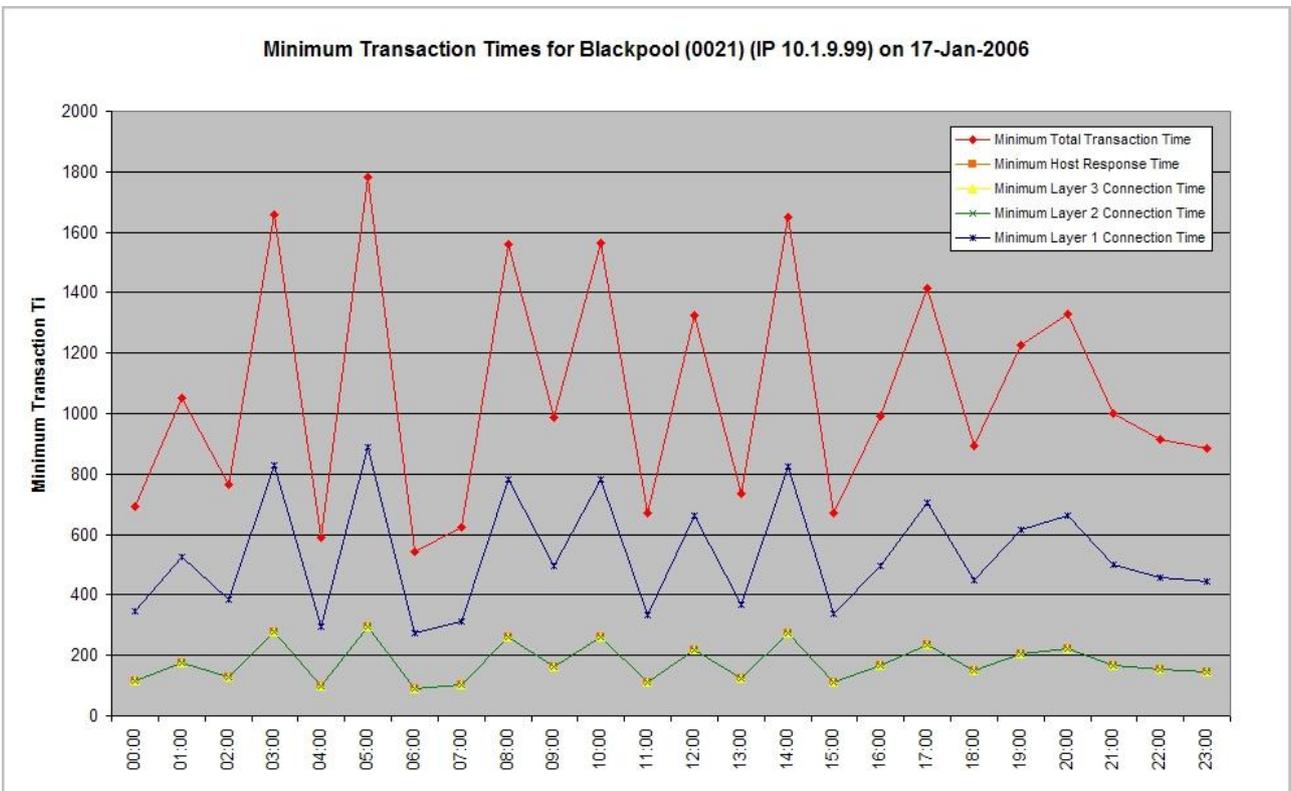
SLA Exceptions and Automatic Back-ups for Blackpool (0021) (IP 10.1.9.99) on 17-Jan-2006



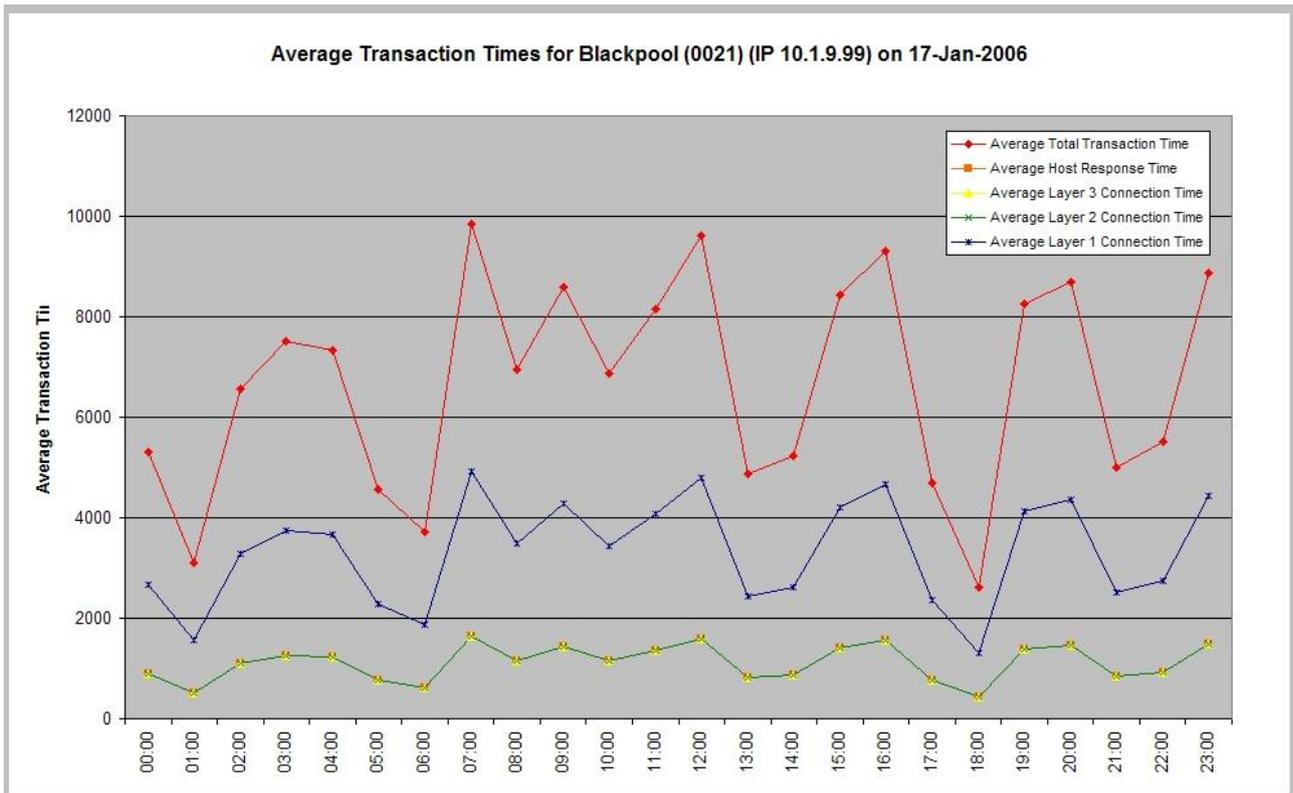
Maximum Transaction Times



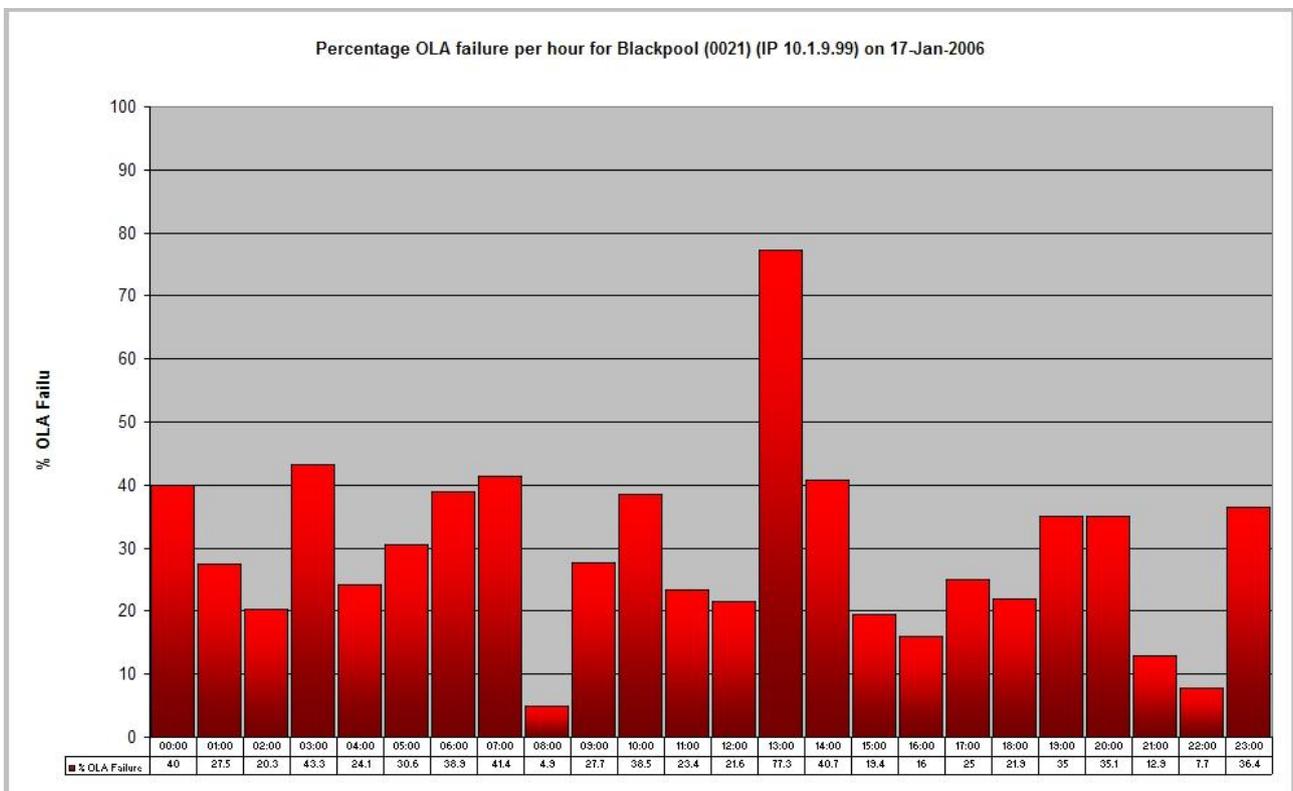
Minimum Transaction Times



Average Transaction Times



Percentage OLA failure per hour



Raw Data

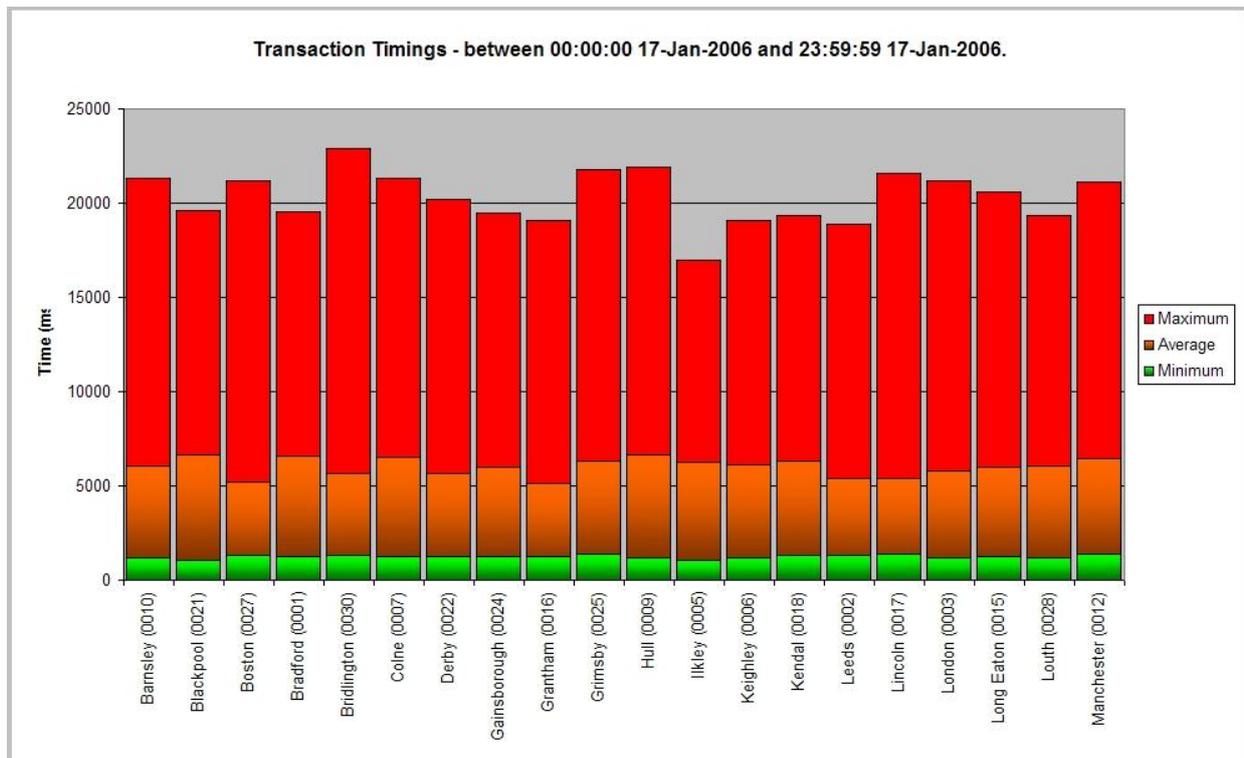
Microsoft Excel - Book1

File Edit View Insert Format Tools Data Window Help

128 = 21

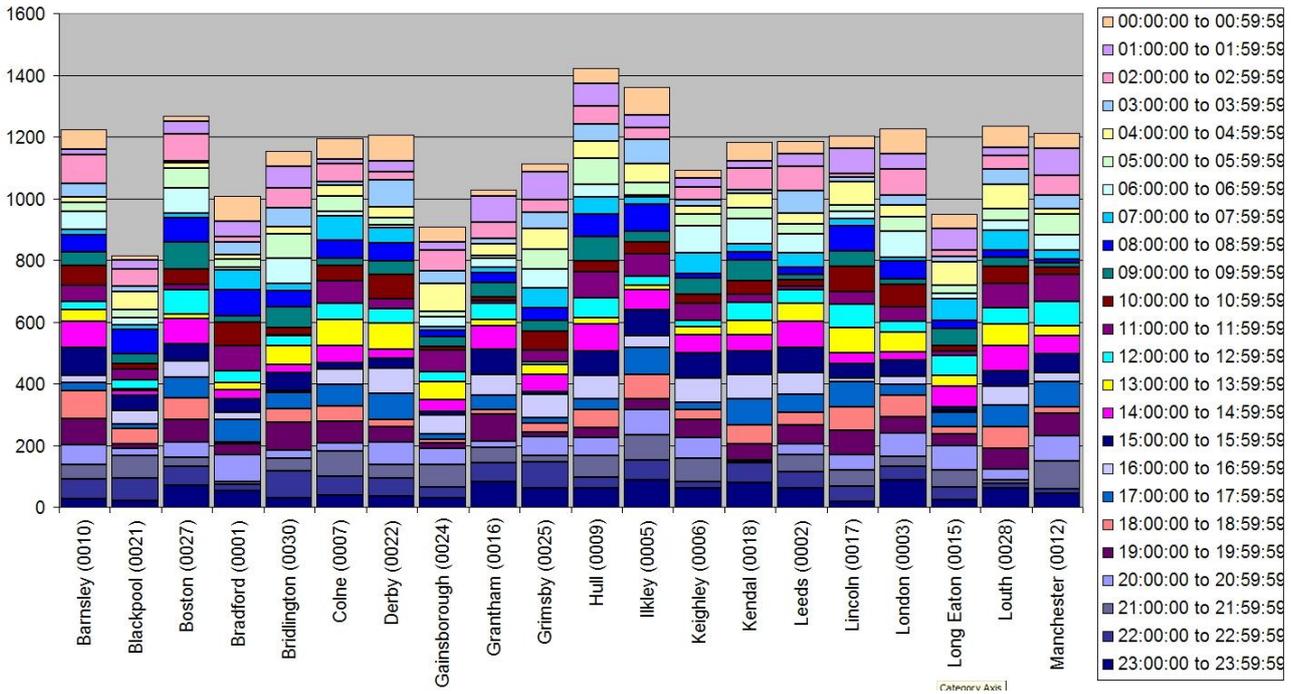
	A	B	C	D	E	F	G	H	I	J
1	Blackpool (0021)	00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00	08:00
2	% OLA Failure	40	27.5	20.3	43.3	24.1	30.6	38.9	41.4	41.4
3	Minimum Total Transaction Time	692	1052	766	1656	588	1780	544	624	156
4	Maximum Total Transaction Time	17804	26796	29498	14681	20175	13297	20130	26736	2045
5	Average Total Transaction Time	5320	3105	6571	7504	7323	4557	3722	9855	695
6	Minimum Host Response Time	115	175	127	276	98	296	90	104	26
7	Maximum Host Response Time	2967	4466	4916	2446	3362	2216	3355	4456	340
8	Average Host Response Time	886	517	1095	1250	1220	759	620	1642	115
9	Minimum Layer 3 Connection Time	115	175	127	276	98	296	90	104	26
10	Maximum Layer 3 Connection Time	2967	4466	4916	2446	3362	2216	3355	4456	340
11	Average Layer 3 Connection Time	886	517	1095	1250	1220	759	620	1642	115
12	Minimum Layer 2 Connection Time	115	175	127	276	98	296	90	104	26
13	Maximum Layer 2 Connection Time	2967	4466	4916	2446	3362	2216	3355	4456	340
14	Average Layer 2 Connection Time	886	517	1095	1250	1220	759	620	1642	115
15	Minimum Layer 1 Connection Time	346	526	383	828	294	890	272	312	78
16	Maximum Layer 1 Connection Time	8902	13398	14749	7340	10087	6648	10065	13368	1022
17	Average Layer 1 Connection Time	2660	1552	3285	3752	3661	2278	1861	4927	347
18	Number of Layer 2 Connections	19	36	64	22	69	28	27	24	7
19	Number of Layer 3 Connections	18	34	60	20	66	26	23	21	7
20	Successful Transactions	15	29	55	17	60	25	22	17	7
21	Number of Layer 1 Connection Failures	4	1	2	3	5	3	3	1	
22	Number of Layer 2 Connection Failures	2	3	3	5	5	5	6	4	
23	Number of Layer 3 Connection Failures	1	2	4	2	3	2	4	3	
24	Number of Back-ups	2	3	1	0	2	1	3	0	
25	Number of SLA Exceptions	3	2	4	5	3	2	4	3	
26	Number of None-responses from Host	3	5	5	3	6	1	1	4	
27	Number of Transactions from Terminal	18	34	60	20	66	26	23	21	7
28	Number of Transactions sent to Host	18	34	60	20	66	26	23	21	7
29										
30										

Max/Min/Avg transaction timings yesterday (20 sites per chart)



Number of transactions yesterday (20 sites per chart)

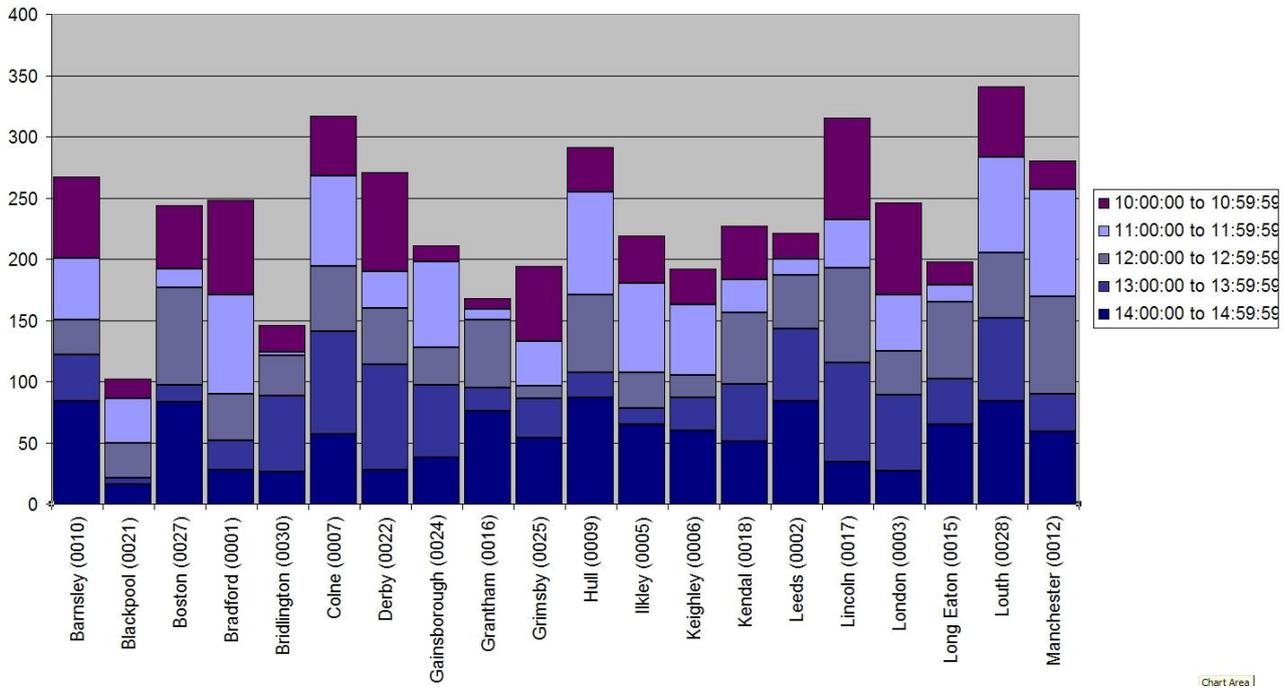
Number of transactions per hour for 24 hours from 00:00:00 17-Jan-2006.



Number of transactions in the last XX hours.

This is the same report has above, only containing data for a shorter time period.

Number of transactions per hour for 5 hours from 10:00:00 17-Jan-2006.



12.5 Eventlog Outage Report

If Remote Manager is configured to collect eventlogs on a regular basis, it can also be configured to monitor routes going in and out of service in the eventlogs and from this generate a report on the

outages an estate of TransPort/Sarian routers have experienced in the last 24 hours.

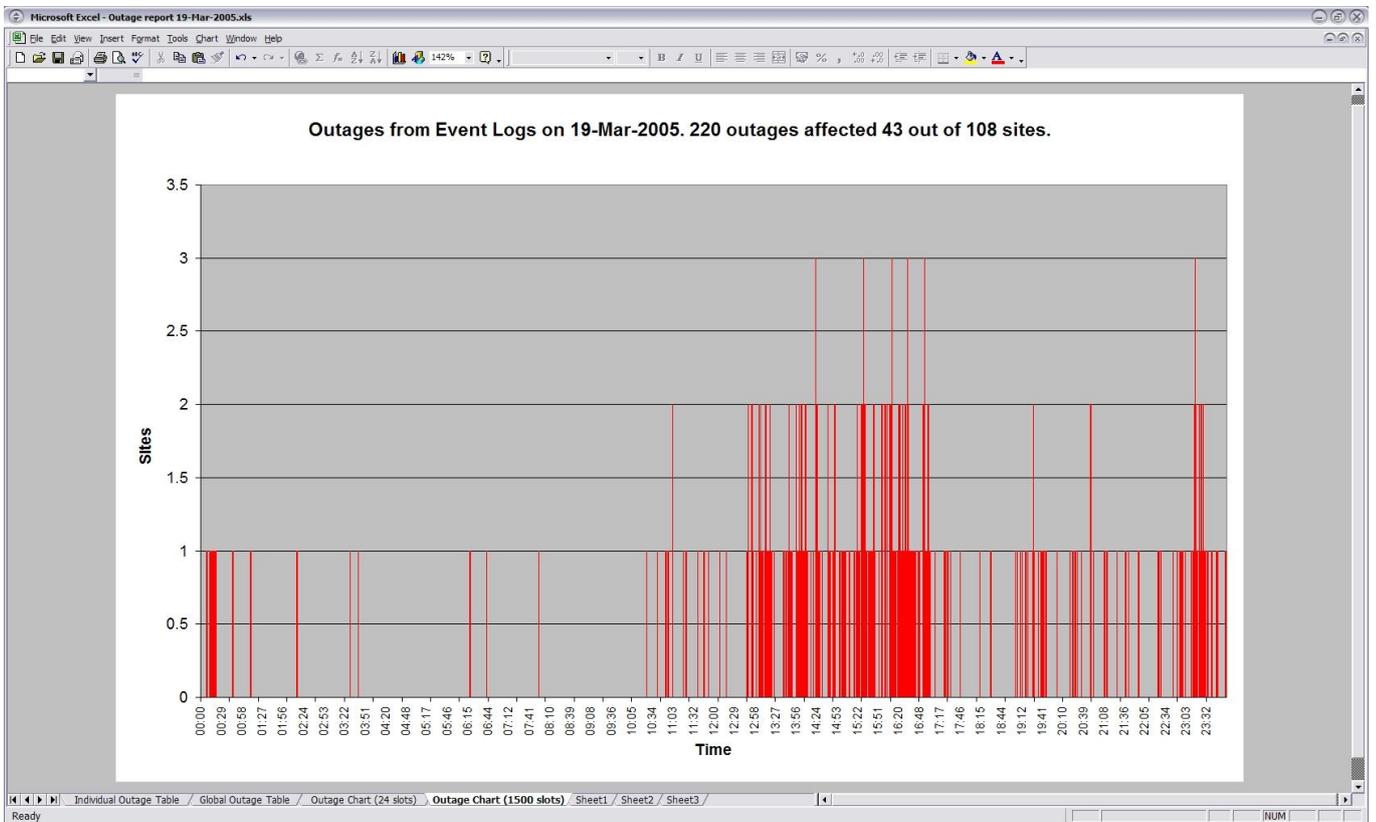
This report can never be perfect *i.e.* show every single outage as sometimes events will occur rapidly filling up the eventlog such that even if Remote Manager collects the eventlog once a day some events will be missed. To configure this feature, follow the steps below.

1. This report is only appropriate for monitoring PPP interfaces that are configured as always on. So ensure that the PPP interface you wish to monitor is configured as always on.
 2. This report actually monitors routes rather than interfaces, so configure a default route *e.g.* default route 0 to point at the PPP interface you wish to monitor.
 3. On the PPP instance you are using, set the parameter “Go out of service if first AODI connection fails” to “On”. This will ensure that the route will go out of service if the TransPort/Sarian is rebooted or power cycled (as the first PPP connection attempt after a power up or reboot will fail – at least for wireless interfaces). Thus a power up or reboot will be seen in the outage report. (If this step is not possible for whatever reason, then a second return to service text parameter must be added, instead – see step 7).
 4. Tick the “Generate outage report daily” check box on the “Eventlog Outage Report” tab.
 5. Assuming default route 0 was chosen in step 2, enter “Default Route 0 Out Of Service” in the “out of service text 1” field.
 6. Assuming default route 0 was chosen in step 2, enter “Default Route 0 Available” in the “Return to service text 1” field.
 7. If (and ONLY IF) it was not possible to set the parameter “Go out of service if first AODI connection fails” to “On” or if you are using ISDN or some other interface that allows the first attempt at raising PPP after a power cycle to be successful, it is necessary to add some text to the “Return to service text 2” field. If we are monitoring PPP 1 then add “PPP 1 UP”. This is in order that the following scenario will work:
 - default route 0 goes out of service
 - TransPort/Sarian is power cycled
 - default route 0 return to service event does NOT occur when PPP 1 comes up because default route 0 never went out of service after the power cycle
- There are some disadvantages to adding this extra return to service parameter, so only do this if you cannot use “Go out of service if first AODI connection fails”.
8. Filter out from the eventlog any events that occur on a regular basis and are not important to you. For example the “GP Socket connected event” can quickly fill up the eventlog when using the UDP echo client. To filter out an event, find the event number for the event you wish to filter out and add it to “Event Filter Codes” list on the Configure → Event Handler web page in the TransPort/Sarian.
 9. Unless monitoring multiple interfaces, leave all other return to service and out of service text fields blank.
 10. Set “Outage Start” to 00:00:00 and “Outage End” to “23:59:59”

Include only outages between

The “Outage Start” and “Outage End” settings can be used to filter out (of the report) any outages that do not occur within the specified time window. For example you may not be interested in outages that occur during the night.

Example pages from the event log outage reports follow:



Note that detail for individual outages is also available in table form. You can see:

- All outages
- All outages for a selected site
- All outages in a selected hour

e.g. selected site: “The Old House” is selected

	A	B	C	D	E	F	G
	Time slot	Site Name	Site Number	IP Address	Out of service time	Return to service time	Duration (s)
155	17:00 to 18:00	The Old House	4298	10.38.48.254	19/03/2005 17:01:03	19/03/2005 17:01:13	10
156	17:00 to 18:00	The Old House	4298	10.38.48.254	19/03/2005 17:01:23	19/03/2005 17:01:43	20
157	17:00 to 18:00	The Old House	4298	10.38.48.254	19/03/2005 17:01:53	19/03/2005 17:02:03	10
158	17:00 to 18:00	The Old House	4298	10.38.48.254	19/03/2005 17:02:13	19/03/2005 17:02:23	10
223							

e.g. selected hour: 17:00 to 18:00 is selected

Microsoft Excel - Outage report 19-Mar-2005.xls

File Edit View Insert Format Tools Data Window Help

A223

	A	B	C	D	E	F	G
1	Time slot	Site Name	Site Number	IP Address	Out of service time	Return to service time	Duration (s)
152	17:00 to 18:00	Charles	3332	10.50.33.254	19/03/2005 17:03:58	19/03/2005 17:04:08	10
153	17:00 to 18:00	Charles	3332	10.50.33.254	19/03/2005 17:24:58	19/03/2005 17:27:18	140
154	17:00 to 18:00	Charles	3332	10.50.33.254	19/03/2005 17:29:08	19/03/2005 17:30:28	80
155	17:00 to 18:00	The Old House	4298	10.6.48.254	19/03/2005 17:01:03	19/03/2005 17:01:13	10
156	17:00 to 18:00	The Old House	4298	10.6.48.254	19/03/2005 17:01:23	19/03/2005 17:01:43	20
157	17:00 to 18:00	The Old House	4298	10.6.48.254	19/03/2005 17:01:53	19/03/2005 17:02:03	10
158	17:00 to 18:00	The Old House	4298	10.6.48.254	19/03/2005 17:02:13	19/03/2005 17:02:23	10
159	17:00 to 18:00	The Limp	2256	10.50.79.254	19/03/2005 17:04:19	19/03/2005 17:04:20	1
160	17:00 to 18:00	The Limp	2256	10.50.79.254	19/03/2005 17:04:21	19/03/2005 17:05:52	91
161	17:00 to 18:00	The Old Horse	2778	10.50.44.254	19/03/2005 17:12:05	19/03/2005 17:12:11	6
162	17:00 to 18:00	The Old Horse	2778	10.50.44.254	19/03/2005 17:12:11	19/03/2005 17:12:23	12
163	17:00 to 18:00	The Old Horse	2778	10.50.44.254	19/03/2005 17:33:12	19/03/2005 17:33:18	6
164	17:00 to 18:00	The Old Horse	2778	10.50.44.254	19/03/2005 17:33:18	19/03/2005 17:33:30	12
165	17:00 to 18:00	The White Mouse	5477	10.50.20.254	19/03/2005 17:02:08	19/03/2005 17:03:18	70
166	17:00 to 18:00	The White Mouse	5477	10.50.20.254	19/03/2005 17:46:58	19/03/2005 17:47:08	10

12.6 Configuration Differ

When the poll schedule operation type is set to “Compare Files” (see section 12.2.3), the “Configuration Differ” tab will appear.

The compare files/configuration differ feature enables Remote Manager to regularly connect to all the remote sites in the selected groups, FTP download the configuration files and compare them to the base or master configuration files on the PC.

To use the configuration differ drag the base configuration files into the Window using Windows Explorer™.

The base configuration files can usually be taken from one of your live sites if you know that the configuration is correct.

Any file that is present on the remote units can be compared, but it only usually makes sense to use one of the following configuration files.

Filename	Description	Default compare type
config.da0	The main configuration file.	config.dax
sregs.dat	The serial port settings (baud rate etc)	binary
fw.txt	The firewall configuration file	binary
x3prof	X.25 PAD profile settings	binary
logcodes.txt	Event logger definitions file.	binary
ospf.conf	OSPF configuration file	binary
Bgp.conf?	BGP configuration file?	Binary?

There are two different compare types. The compare type can be changed by right clicking on the file in the configuration differ window and then left clicking on the desired compare type.

12.6.1 Binary

Binary compare type is where the file from the remote unit is compared byte by byte with the base configuration file. Any change whatsoever will result in the files being flagged as different.

12.6.2 Config.dax

With the config.dax compare type, the comparison is made more intelligently. For example the order in which lines appear in the config.dax file is not important to Remote Manager because it is not important to the TransPort/Sarian. Also any configuration lines that start with the “set text” of a site specific parameter (see section 9.3) are ignored in the first part of the comparison and checked separately later. The following list explains how this comparison works

1. Every line present in the base config.da0 file that does not start with the “set text” of a site specific parameter defined for this unit is checked for in the config.da0 file from the remote unit. If such a line does not appear somewhere in the config.da0 file from the remote, then the file will be flagged as different and the reason recorded.
2. Every line present in the config.da0 file from the remote that does not start with the “set text” of a site specific parameter defined for this unit is checked for in the base config.da0 file. If such a line does not appear somewhere in the config.da0 file from the remote, then the file will be flagged as different and the reason recorded.
3. The values of the site specific parameters in the running configuration of the remote units are compared with the values stored for the same site specific parameters in Remote Manager’s database. If any difference is found then the file will be flagged as different and the reason recorded.

✓ *As soon as the first difference is found, the reason for this difference is recorded and the comparison aborted. i.e. you will not receive a list of every difference found in the config.dax file, just the first difference found.*

12.6.3 Example Report

As with all the reports generated after polling, the reports will be saved to the hard drive and optionally also emailed to the email distribution list.

	A	B	C	D	E
1	Site Name	Site Number	File Name	Result	Reason
2	Smith's Street	0001	config.da0	Different	udpecho 0 dstip "10.9.107.47"
3	Smith's Street	0001	fw.txt	Identical	
4	Smith's Street	0001	Site specific parameter mismatch	Different	EPIN
5	Smith's Street	0001	sregs.dat	Identical	
6	Albert Road	0002	config.da0	Identical	
7	Albert Road	0002	fw.txt	Identical	
8	Albert Road	0002	Site specific parameter mismatch	Different	EPIN
9	Albert Road	0002	sregs.dat	Different	binary
10					
11					
12					

Row 2 shows a difference found in the config.da0 file.

Rows 4 & 8 show differences found when checking the value of a site specific parameter.

Row 9 shows a difference found in the sregs.dat file with a binary compare.

Note that you can click on any of the drop down lists (for example the “Result” drop down and “Site name” drop down arrows are highlighted by a red circle) to filter the rows displayed by the value selected. Clicking on the “Result” drop down and selecting “Different” for example will then display

all the rows and only the rows where a difference has been found.

13.0 REPORTS

All the reports except the “Eventlog Outage Report” can be produced on demand by clicking the “Reports” button to access the “Report Wizard”.

Generally speaking the reports produced via the wizard are slightly more flexible than those produced automatically by a polling schedule. This is mainly because the period that the report covers and the units in the reports can be controlled more precisely.

13.1 Date and time selection

The first screen of the report wizard allows you to select a start and end date and time for the report.

13.1.1 Start and end date

Use the start and end date to select the period of time that the report should cover.

By default the start and end date will be both be yesterday – this is the correct setting if you want the report to cover just one full day *i.e.* the day of yesterday (usually the most recent day the database will have a full day of data for).

13.1.2 Start and end time

The start and end time selectors can have different meanings for different reports. Usually they refer to the start time for the first bin and last bin (respectively) to include in the report for all the days included in the report.

For example, often it is required that an SLA report only shows data taken from working hours. If working hours are from 09:00 to 17:00, then set the start time to 09:00 and the end time to 16:00. Note that the end time is set to 16:00 as this is the bin start time for the bin that covers the period of 16:00 – 17:00. To include the full days data (*i.e.* 24 hours data per day) in the report set the start time to 00:00:00 and the end time to 23:00:00.

Some reports may ignore the start and end times.

13.2 Group Selection

On the group selection screen, select the group or groups that contain the units that are to be included in the report. Click Next.

13.3 Unit Selection

The “Unit Selection” screen will contain the units found in the group selection made on the previous screen. To include all these units in the report click the “Select All” button, otherwise make individual selections as appropriate. Click Next.

13.4 Report Selection

On the report selection screen select the type of report you wish to generate and then click the “Draw” button. This screen will not automatically close so you can generate multiple reports for the selections made on the previous screens.

13.5 TPAD Reports

TPAD reports are the reports that can be generated based upon the data collected from the remote unit's TPAD bins.

13.5.1 SLA Report

A TPAD SLA Report is a Microsoft Word™ document report based upon the average total transaction time per day, the transaction failure rate per day and the count of SLA exceptions per day.

Units that exceed the daily specified average transaction times, failed transaction rates or SLA count threshold are listed in the report.

13.5.2 Detailed stats per hour

The detailed stats per hour option will generate 1 workbook per day per site. *i.e.* the number of workbooks = number of sites x number of days in report period. Each workbook contains the following charts:

- Number of transactions per hour
- SLA Exceptions and Automatic Back-ups
- Maximum Transaction Times
- Minimum Transaction Times
- Average Transaction Times
- Percentage OLA failure per hour
- Raw Data

For example of these charts see section 12.4.2

13.5.3 Max/Min/Avg timings

This chart shows the maximum, minimum and average transaction times per report period for each site in the report. (20 sites per page arranged alphabetically by site name).

For an example chart see section 12.4.2

13.5.4 Transactions/ Hour

This chart shows the number of transactions per hour for the report period for each site in the report. (20 sites per page arranged alphabetically by site name).

For an example chart see section 12.4.2

13.6 PPP Reports

PPP reports are the reports that can be generated based upon the data collated from the remote unit's PPP bins.

13.6.1 SLA Report

A PPP SLA Report is a Microsoft Word™ document report based upon the weighted latencies and weighted average transaction times of all the units in the groups selected for the report. The report can contain data from several days.

Units that exceed specified latencies and packet loss thresholds are listed in the report. When the “Draw” button is clicked, the user is prompted for the latency and packet loss thresholds to use whilst generating the report.

See section 12.3.1 for more details and an example report.

13.6.2 Detailed stats per hour

The detail stats per hour report is a Microsoft Excel™ workbook containing plots of packet loss & latency per hour and packet loss & signal strength per hour. See section 12.3.2 for some example reports.

The reports produced vary based upon the number of sites selected and the answer to the question “Do you want an individual graph for each site and day?” which will appear when you click “Draw”.

Single Site Selected

If a single site was selected in section 13.3 and you ask for an individual report for each site and day, then multiple Excel workbooks will be created, one for each day.

If a single site is selected and you answer “No” to the question about individual sites and day. A single workbook will be created covering the entire period of the report. This is a special case and this report will be treated as a “soak test report”. A text box will be added to the report stating whether or not the unit passes the test based upon the following criteria. NB The following criteria is very strict and not recommended for most projects. Currently the criteria cannot be edited. For most projects it is recommend that the performance report is used instead and the soak criteria specified in section 13.6.6.

- Total number of packets sent must be > **some value** and < **some value** (The “**some value**” is determined by the number of days the report covers and assumes packets are sent at 15 second intervals.)
- Instances of packet loss \geq 2% over each 24 hour period is not greater than 0.
- Instances of packet loss \geq 5% in any one hour is not greater than 0.
- Instances of packet loss \geq 5% and \leq 10% in any one hour is not greater than 2.
- Instances of packet loss \geq 2% and \leq 5% for more than 2 hours in day is not greater than 0.
- Instances of average latency \geq 850ms in a day is not greater than 0 (referral not fail)
- Instances of average latency \geq 1200ms in an hour is not greater than 0 (referral not fail)
- Instances of average latency \geq 850ms and < 1200 ms in an hour is not greater than 2 (referral not fail)
- Instances of >0 oos counts in any one day is not greater than 0 (referral not fail)

- Instances of >1 oos counts in any one day is not greater than 0
- Instances of signal strength less than -85 dBm is not greater than 0 (referral not fail)
- Average signal strength - standard deviation > -80dBm (referral not fail)
- Report lasts at least 2 days

For the soak test results to be meaningful,

- The remote unit must be monitoring UDP echo packets generated at a frequency of exactly 15 second intervals
- The unit must have been collecting these results for at least two full days.

Multiple Sites Selected

If multiple sites are selected and you ask for an individual report for each site and day, one report will be generated for each day and each site *i.e.* number of Excel workbooks = number of sites x number of days. If a large number of workbooks are to be generated then it is recommend that you answer yes to the subsequent question (do you want to save the Excel workbooks to disk).

If multiple sites are selected and you do NOT ask for an individual report for each site and day, then a single workbook will be generated containing:

- A graph for each day showing the average values across all the sites in the report'
 - A single graph covering the whole time period showing average values across all the sites in the report.
- ✓ *In such a graph, if a selection other than 00:00:00 to 23:00:00 was made on the time selectors in section 13.1.2, then non-working hours will still be visible in the report but greyed out. On a large estate of units this report is useful for seeing global performance issues i.e. problems that affect most or all sites on the network.*

13.6.3 Data per day & down time

The data per day & down time report is a Microsoft Excel™ Workbook that contains charts showing:

- Data transferred per day (sum across all sites it the selected groups).
- Data transferred per site (sum per site over the period of the report).
- Down minutes per site over the period of the report (This may not be 100% accurate because if Remote Manager doesn't have PPP bin data to show that a site was up, it assumes it was down).

13.6.4 Sporadic sites report

The sporadic site report is a Microsoft Word™ document report containing a list of sites where the data in any hourly bin or daily average exceeds certain configurable trigger levels. The intention of this report is to quickly highlight problem sites allowing the user to concentrate on studying the Latency & Loss graphs or Page per site summary report for these problem sites only.

The following trigger levels can be set when the "Draw" button is clicked.

Trigger Name	Description
Hourly Loss	The % packet loss in any one hour has exceeded this % value
OOS Max	The number of out of service counts/interface deactivations due to packet loss in any one day has exceeded this value.
Hourly max latency	The maximum latency in any one hour has exceeded this value in milliseconds.
Daily Loss	The average weighted packet loss over one day has exceeded this % value
Daily avg latency	The average weighted latency over one day has exceeded this value.
Hourly avg latency	The average hourly latency over one day has exceeded this value.

13.6.5 Outage Report

Not yet supported in the Report Wizard.

13.6.6 Performance Report

The performance report also known as the “Page Per Site Summary Report” is the most powerful report. It shows all performance data collected from the PPP bins over the number of days in the report.

This report generates a single page of graphs and other data for each site in the selected groups.

It is possible for the end user to completely customise this report, e.g. add new charts, delete existing charts or even include their own data along side (from another data source). To achieve this open the “report_template.mdb” file in the Remote Manager installation folder with Microsoft Access 2003™ or later and modify the “PagePerSiteSummary” report and “bins” query as appropriate.

For most projects where a commission test is performed by means of sending UDP traffic for a period of time (usually known as a soak test) it is recommended that this report is used to judge the performance of the site. The following is an example of some criteria that could be used:

- There must be more than x packets sent over the period.
- There must be less than x% packet loss over the period.
- There must be less than x out of service counts over the period.
- Average signal strength is -85dBm or better (-51dBm is the strongest possible signal).

In all cases “x” must be adjusted to suit the project and rate at which the packets are sent. As a general rule though, more than 2 out of service counts per day would indicate some kind of problem that should be addressed.

See section 12.3.2 for an example of this report.

General advice on signal strength

Signal quality is actually much more important than signal strength but signal quality is not easily measured on GPRS. The signal strength is only a rough guide to the signal quality as reflections off buildings and electromagnetic interference can affect the signal quality without affecting the signal strength.

During installation ensure that the signal strength is better than -80dB. If -75dB can be achieved (e.g. by fitting an external antenna etc) then it is well worth any extra effort.

We have seen units working well with a signal strength as low as -95dB – however this should not be expected as it is an unusual occurrence.

If you are installing a large number of units we recommend the use of the UDP echo generator in conjunction with stat collection from our management package Remote Manager. Remote Manager includes a "soak test" facility which is basically a 24 or 48 hour report on the GPRS performance of the unit. This can be used to verify that an installation has been successful.

14.0 STAT SETUP

The “Stat Setup” screen is where Statistic Classes are created. These statistics classes can be bound or mapped to each individual site using the site editor.

14.1 Adding a Statistics Class

If PPP bin or TPAD bin statistics are to be collected, it is necessary to add a “Statistics Class”.

To add a “Statistics Class” click the “Add” button. In the description field type a name for the class. (This is the name that will appear under the “Stats” tab of the site editor.) For “Class Type” either “PPP bin” or “TPAD bin” (depending upon the type of statistics you wish to collect). Please note that PPP bin and TPAD bin are the only class types supported at this time.

Finally click “Add Instance #”. This refers to the instance number of the TransPort/Sarian entity that the stats will be collected from. Normally the WAN interface on a TransPort/Sarian is PPP instance 1. So normally click on “Add Instance #” and enter “1” for the instance number when prompted.

For TPAD stats, all the TPAD instances share the same BIN, so the instance number you select here is not important. (As long as a TPAD instance exists with this number on the remote unit – so choose a lower instance number e.g. 0-3)

14.2 Always use direct IP

The “Always use direct IP connection method for stat polling” check box can be used to override the connection method in the site editor for all sites whilst polling. If this check box is ticked then direct IP will be used for all sites whilst polling. *i.e.* collecting stats, collecting text files or running a configuration difference report

14.3 Tidy Bins

On occasion a remote TransPort / Sarian unit may create more than one bin of data covering the same time period. As an example, this can happen when the unit’s firmware is upgraded and the contents of the NVRAM are lost. Clicking the “Tidy Bins” button will cause Remote Manager to look for any such duplicate bins and if found consolidate the data into a single bin.

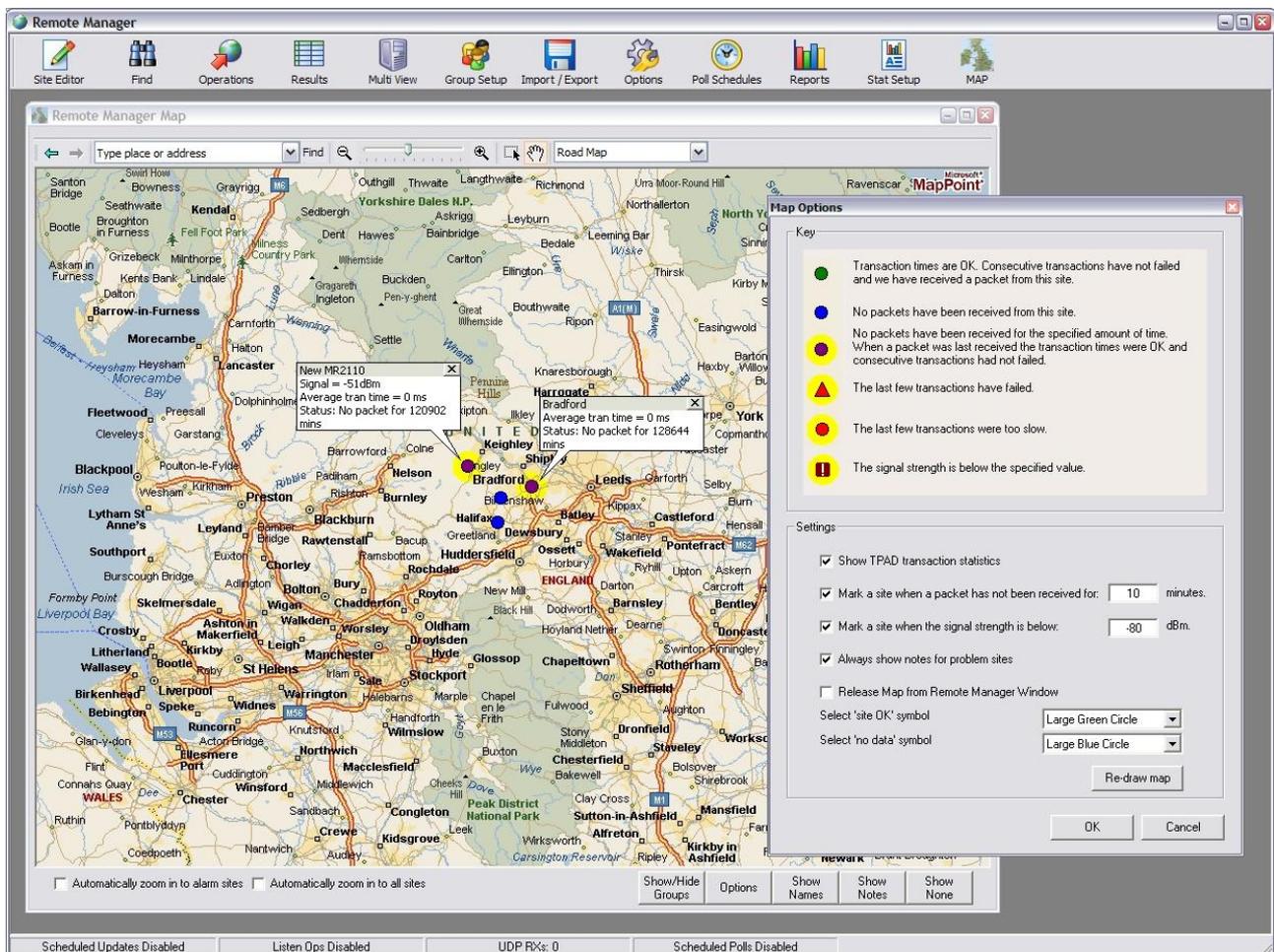
15.0 MAP – REAL TIME PERFORMANCE MONITORING

For always-on-furn style networks Remote Manager can be configured to receive UDP packets from remote sites in real time.

To use this feature

- Microsoft MapPoint™ must be installed on the Remote Manager PC.
- The sites must be configured to send a UDP heartbeat packet to Remote Manager on a regular basis. This can be achieved by configuring the TransPort/Sarian PPP or Eth parameters “Heartbeat interval (s)” and “Heartbeat destination” parameters. (These are the same UDP packets that are used in order for Remote Manager to operate in listening mode.)

15.1 Map View



Each site on the map can be displayed as a simple dot with no name, a dot with site name or a dot with site notes. The site notes will contain the most up to date detailed information Remote Manager has received from the UDP packets, e.g. TPAD performance or current signal strength.

To show notes for all sites click the “Show Notes” button.

To show just the names for all sites click the “Show Names” button.

To show just the dots for all sites click the “Show None” button.

Ticking the “Automatically Zoom in to alarm sites” check box, means that Remote Manager will automatically zoom into any problem sites when one of the follow two event happen.

- Receipt of a UDP packet with information about a problem (e.g. poor signal strength or poor TPAD performance).
- A UDP packet is not received for the amount of time specified in the map options.

Ticking the “Automatically zoom in to all sites” check box will cause Remote Manager to zoom into every site every time it receives a UDP packet from the remote site.

In order for a site to be visible in the map, it must have either a post code or Latitude and Longitude setting defined in the “Address/Notes” tab of the site editor. After making changes to these fields in the site editor it is necessary to click the “Re-draw map” button on the “Map Options” screen to see the new locations of the sites.

15.2 Show / Hide Groups

Clicking on the “Show/Hide Groups” screen allows groups of sites to be filtered in and out of the map view.

15.3 Non-contactable sites

Remote Manager can highlight sites on a map that it has not received data from in a configurable time period. Thus problem sites (e.g. sites that have lost their WAN connection) can be identified nearly immediately, rather than having to wait for the reports to come through the next day.

To configure this time period, click the “Options” button on the “Map” screen. Change the parameter “Mark a site when a packet has not been received for XX minutes” to an appropriate setting.

15.4 TPAD sites

If the site is also configured for TPAD performance measurement then these UDP packets will include information on the average transaction time of the last few transactions. This allows sites with poor performance to be highlighted on the map in real time.

Also if a site is configured for TPAD performance measurement, if a specified number of transactions in a row fail then the site can be highlighted in real time.

These settings can be found by clicking the “Options” on the “Map” screen. If your sites are not using TPAD then un-tick the “Show TPAD transaction statistics” check box.

The remote TransPort/Sarian devices must also be configured correctly. On the remote unit navigate to Configure → TPAD → TPAD Statistics and configure suitable values for:

- Number of most recent transaction times to average
- Generate event after this many consecutive failures
- Generate event after average transaction time exceeds (ms)

15.5 GSM/3G Sites

If your sites are connected via a wireless network such as GPRS, Edge, UMTS or HSDPA, then the current signal strength can be found in the UDP heartbeat packet. Remote Manager can be

configured to highlight any sites where the signal strength goes below a certain value. This value is configured in the “Mark a site when the signal strength is below XX dBm” section.

15.6 GPS data

If the remote routers have GPS, they can be configured to include GPS data in the UDP heartbeats. If this is the case then the position of the site on the map will be automatically updated every time a GPS packet is received. Note that the serial number for the site must be programmed into the site editor and there must be no duplicates.

15.7 Map Options

Map Options

Key

- We have received a packet from this site.
- No packets have been received from this site.
- No packets have been received for the specified amount of time.

Map Settings

- Show TPAD transaction statistics
- Mark a site when a packet has not been received for: minutes.
- Mark a site when the signal strength is below: dBm.
- Always show notes for problem sites
- Release Map from Remote Manager Window
- Select 'site OK' symbol:
- Select 'no data' symbol:
-

HTML Export

- Export an HTML copy of the map every minutes, x pixels, y pixels
- Enter the location to save the files to:
- IP Address: Remote Folder: Username: Password: FTP Enabled

Other Settings

- Email the site contact (in the site editor Address tab) when a heart beat has not been received from the site for the number of minutes specified above or a site goes below the signal strength threshold.

15.7.1 Key

The key shows the various symbols that can be displayed on the map to represent a site and the meanings of those symbols.

15.7.2 Show TPAD transaction statistics

Ticking or clearing this check box as appropriate will determine whether Remote Manager will attempt to display information relating to the TPAD performance of sites on the map. The “key” will be updated automatically when this selection is changed.

15.7.3 Mark a site when a packet has not been received

If this check box is ticked, Remote Manager can highlight a site that from which it has not received a UDP packet for the specified amount of time. The key is updated automatically when this setting is changed.

15.7.4 Mark a site when the signal strength is below

If this check box is ticked, Remote Manager can highlight any sites that have a signal strength below the value specified in the adjacent text field. The key is updated automatically when this value is changed.

15.7.5 Always show notes for problem sites

Ticking this check box will cause Remote Manager to always show the notes field for sites that are highlighted with a problem. This will override the “Show None” button on the main mp screen.

15.7.6 Release Map from Remote Manager Window

Ticking this check box will cause the map to have its own Window. The default behaviour is for the map to appear as a child window inside the Remote Manager MDI. This setting is useful if you wish to display the map by itself say on a second monitor or projector in a control room.

It is necessary to re-start Remote Manager when this setting is changed.

15.7.7 Select site OK symbol

Allows the map symbol for a site with no problems to be changed to:

- Large green dot
- Small green dot
- None

15.7.8 Select “no data” symbol

Allows the map symbol for a site from which Remote Manager has **never** received any UDP packets for to be changed to:

- Large blue dot
- Small blue dot
- None

15.7.9 HTML export

The HTML Export settings can be configured to export an HTML copy of the map which includes a GIF on a regular basis. A full version of Microsoft MapPoint must be installed for this to work.

The IP address, Remote Folder, Username, Password and “FTP Enabled” settings allow Remote Manager to be configured to upload this map via FTP to a server every time it is updated.

15.7.10 Other Settings

The check box enables a feature whereby Remote Manager will email the site contact (email address from the address tab in the site editor) if the heart beat packet has not been received for the specified number of minutes, or the sites goes below the signal strength threshold.

16.0 EXAMPLE I - UPDATING FIRWARE AND CONFIGURATION

This example explains how to use Remote Manager to upgrade the firmware and configuration on a group of remote units.

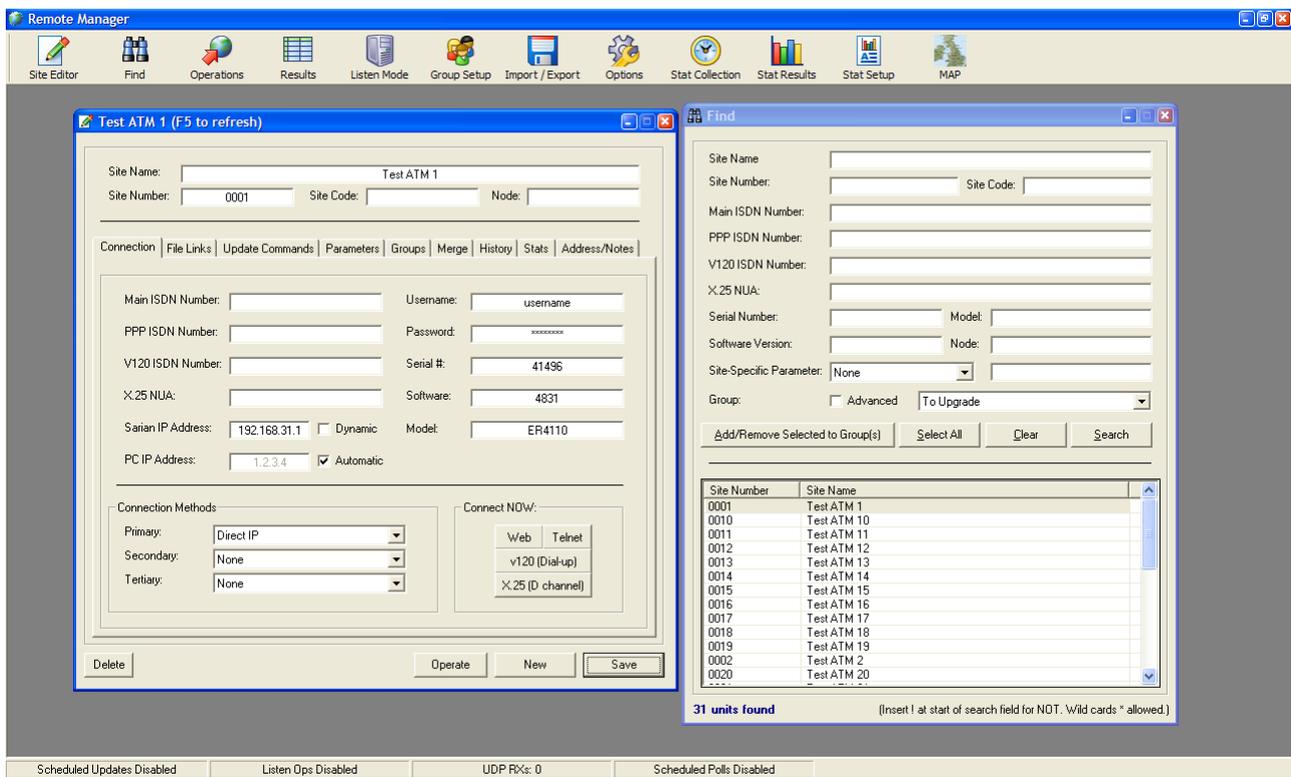
16.1 Starting Point

In this example a configuration change and firmware upgrade will be made to all the units that are in the “To Upgrade” group.

It is assumed that the units are already programmed into the database, they are all of the same model (hence requiring the same set of firmware files) and that these units are already a member of the “To Upgrade” group.

16.2 File Links

First use the find utility to load a single unit that is a member of the “To Upgrade” group into the Site Editor:



Next click on the “File Links” tab in the site editor and use Windows Explorer to drag all the firmware and configuration files into the File Links.

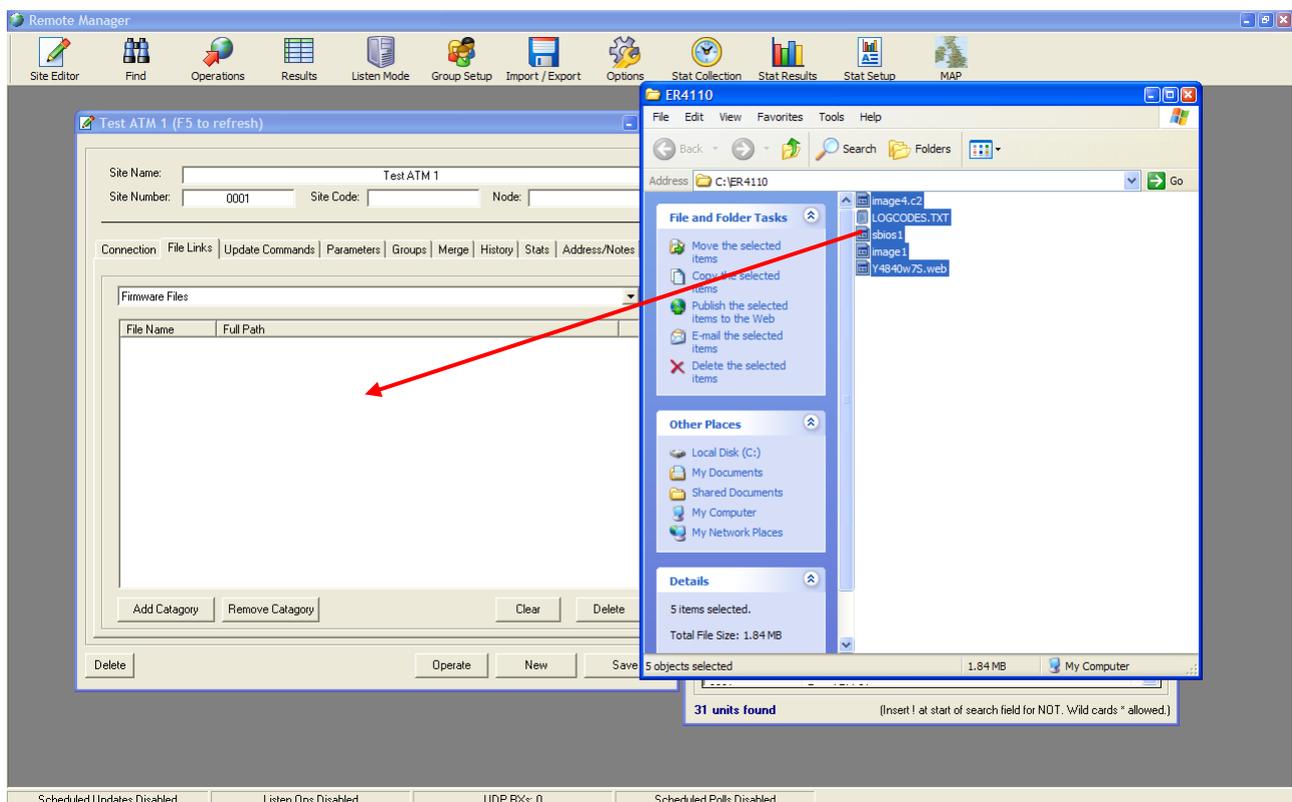
A typical set of firmware and configuration file names follow:

Y4848w7S.web
image1
image4.c2
LOGCODES.TXT
sbios1
config.da0

Note that `config.da0` is the configuration file and optional for the purpose of this example. Usually configurations will be changed by issuing update commands and changing site specific parameter values. But sometimes it is more efficient to replace a `config.da0` file. One example of such a situation is when commissioning a site for the first time and you may not be sure of exactly what is in the configuration of the remote unit.

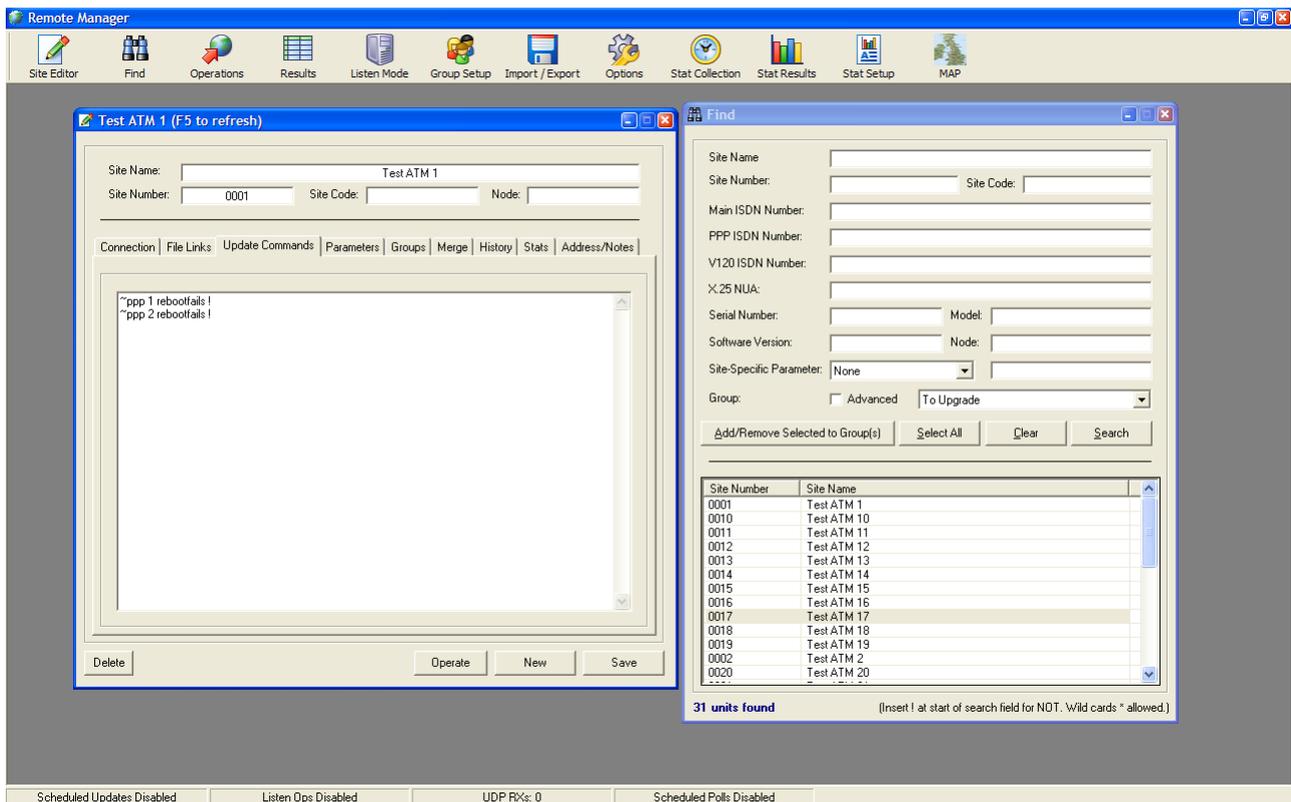
Note that the boot loader (sbios) is actually called `sbios1` and the main application (image) is actually called `image1`. The files are renamed to `image1` and `sbios1` to instruct Remote Manager to FTP the new firmware files on first BEFORE deleting the old files. This reduces the risk incurred during the firmware upgrade.

- ✓ *Some models do not have enough flash space to allow two copies of the image, on these models the file to link should be named "image" and not "image1".*
- ✓ *The boot loader file to link to Remote Manager must ALWAYS be named sbios1 or the boot loader will not be upgraded.*



16.3 Update Commands

In order to ensure that a unit configured to reboot itself automatically will not do so until the upgrade is complete (very important if there is some kind of GPRS problem) click on the update commands tab and enter the text "`~ppp 1 rebootfails !`". This must be done for every PPP instance on the TransPort/Sarian that has the "rebootfails" parameter set to a non-zero value.



In a “File & Configuration” update operation, any command preceded with the “~” character will be issued to the remote unit BEFORE the file update starts. This means that if the unit loses its GPRS connection and is unable to reconnect it will therefore NOT reboot itself.

When the unit is rebooted after the file upload the configuration will revert to that in the config.da0 file so the “reboothails” setting will be restored.

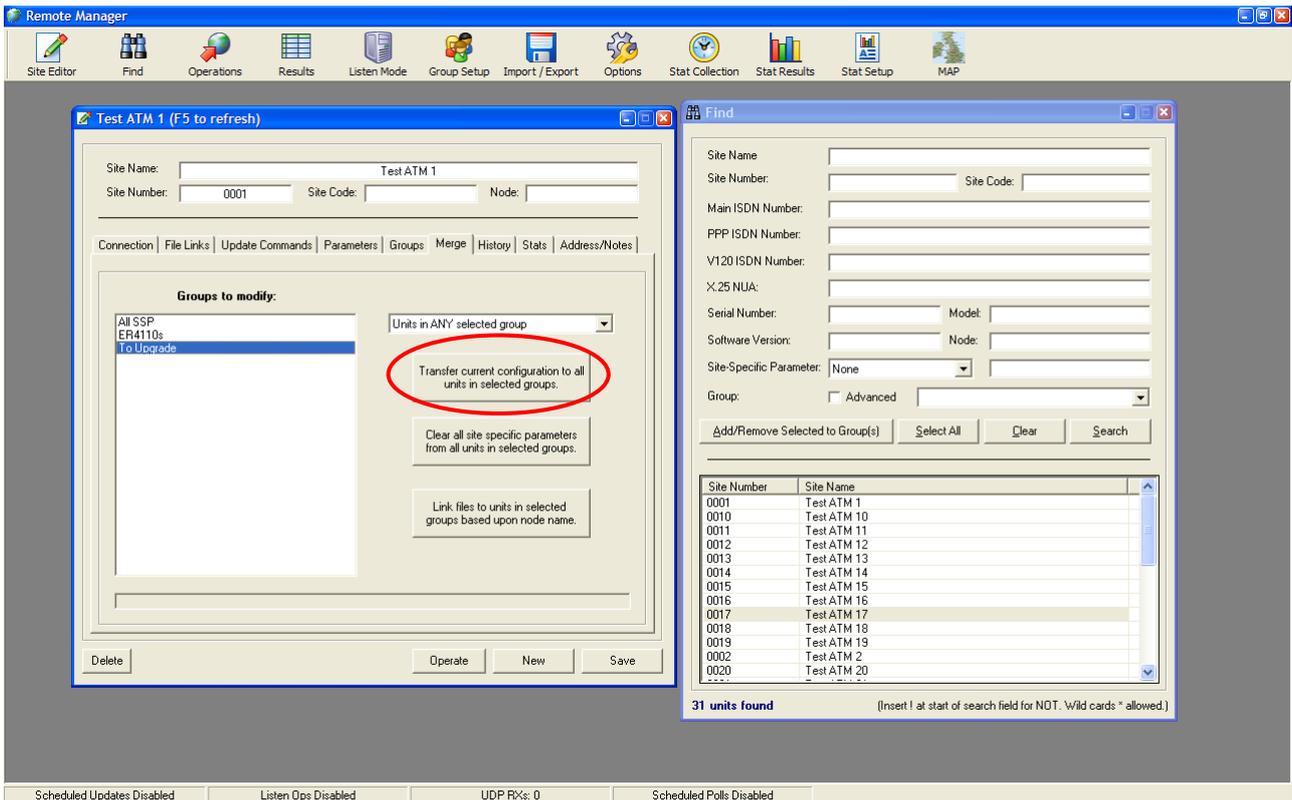
✓ *It is especially important that a TransPort/Sarian cannot reboot itself if the main application is named image and not image1.*

Any extra update commands added here not preceded by the “~” character will be issued and saved to the TransPort/Sarian after the file update is complete and the TransPort/Sarian has been rebooted. This is a useful way of changing the configuration if you did not include a config.da0 file in the files you uploaded.

16.4 Merge the file links with the other units in the group.

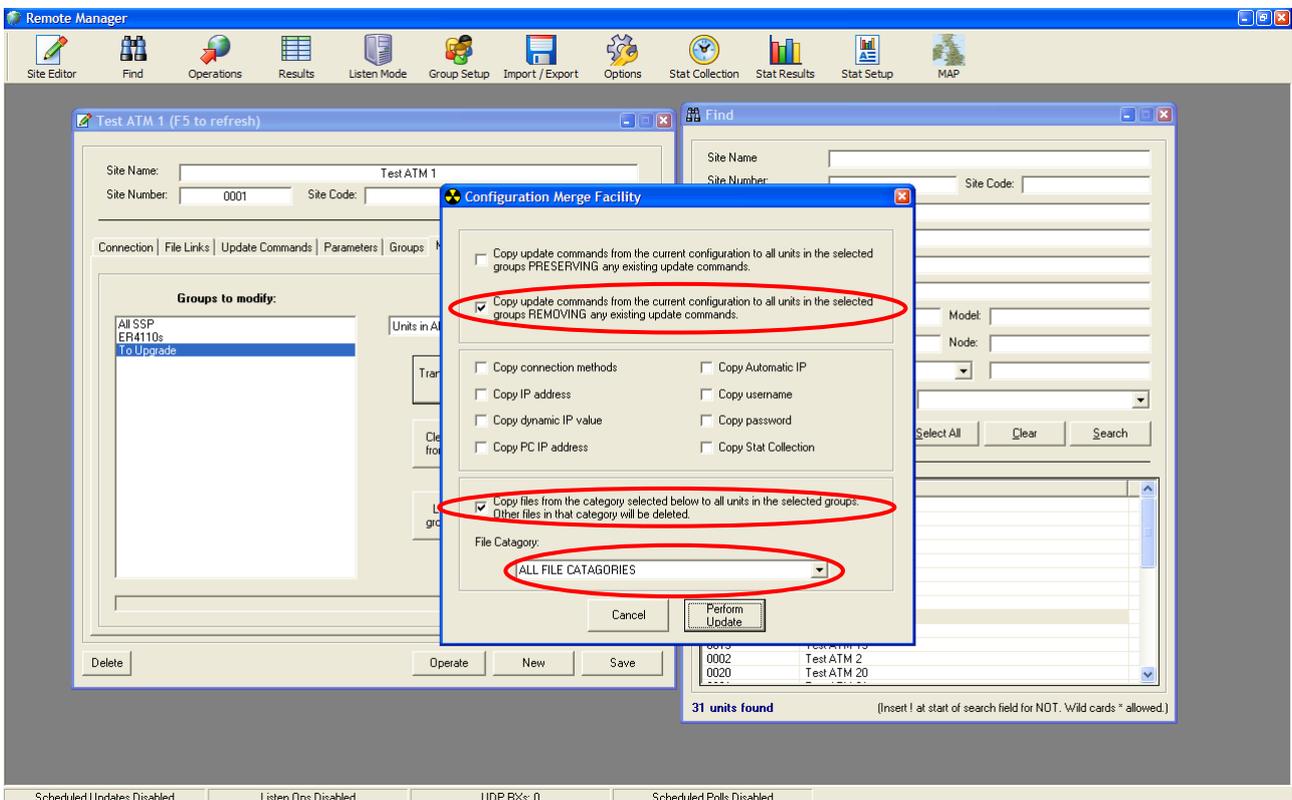
The next step is to select the “Merge” tab and “Merge” these configurations with the other members of the “To Upgrade” group

In the Site Editor click on the “Merge” tab.



Select the group to modify, in this case “To Upgrade”.

Next Click the button “Transfer current site configuration to all units in selected groups.”



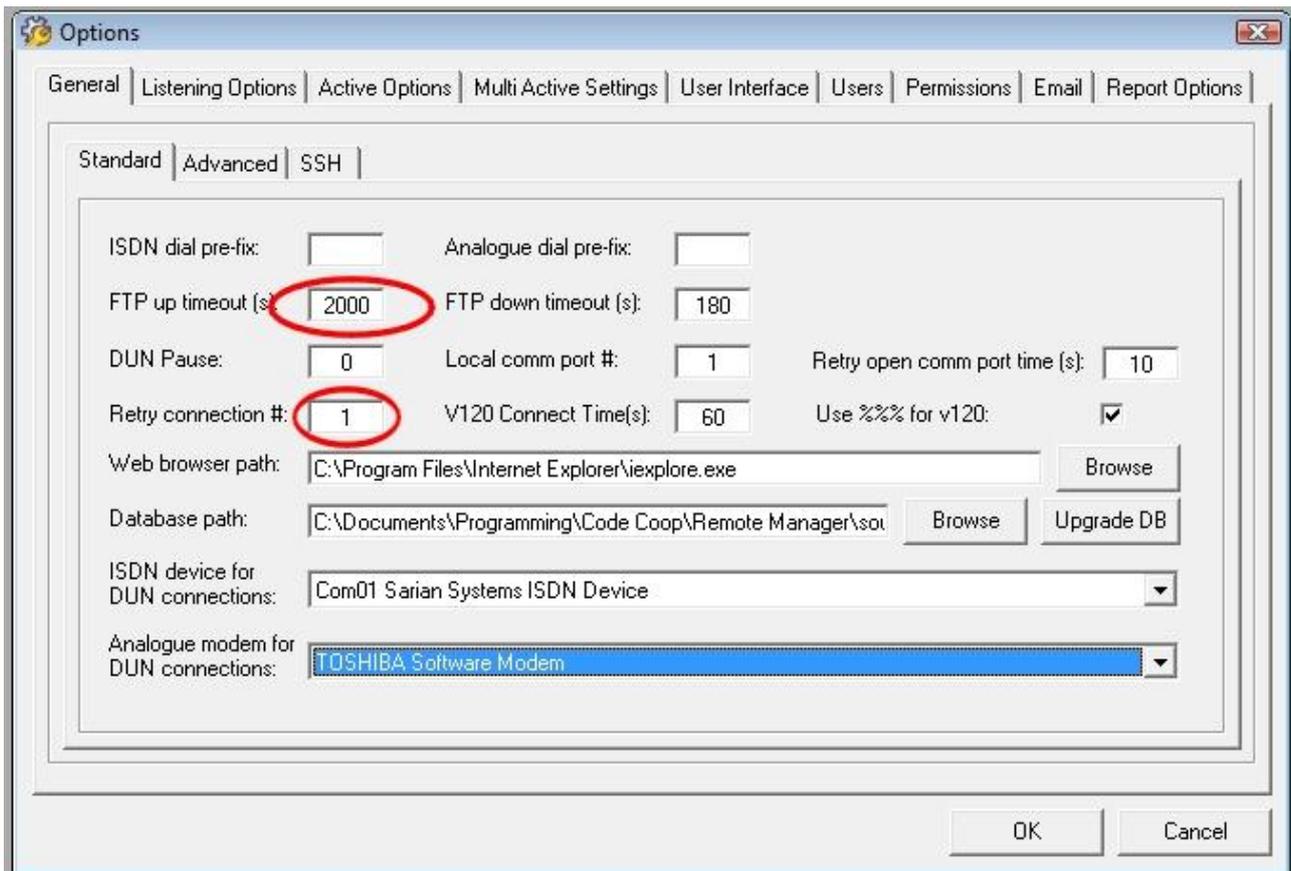
1. *****Tick the check box “Copy update commands from the current configuration to all the selected groups **REMOVING** any existing update commands”

2. Also, tick the check box “Copy file from the category selected below to all units in the selected groups...”
3. Ensure that “ALL FILE CATAGORIES” is selected in the drop down list.
4. Click on “Perform Update”.

All the file links will now be copied across to other members of the Alpha group.

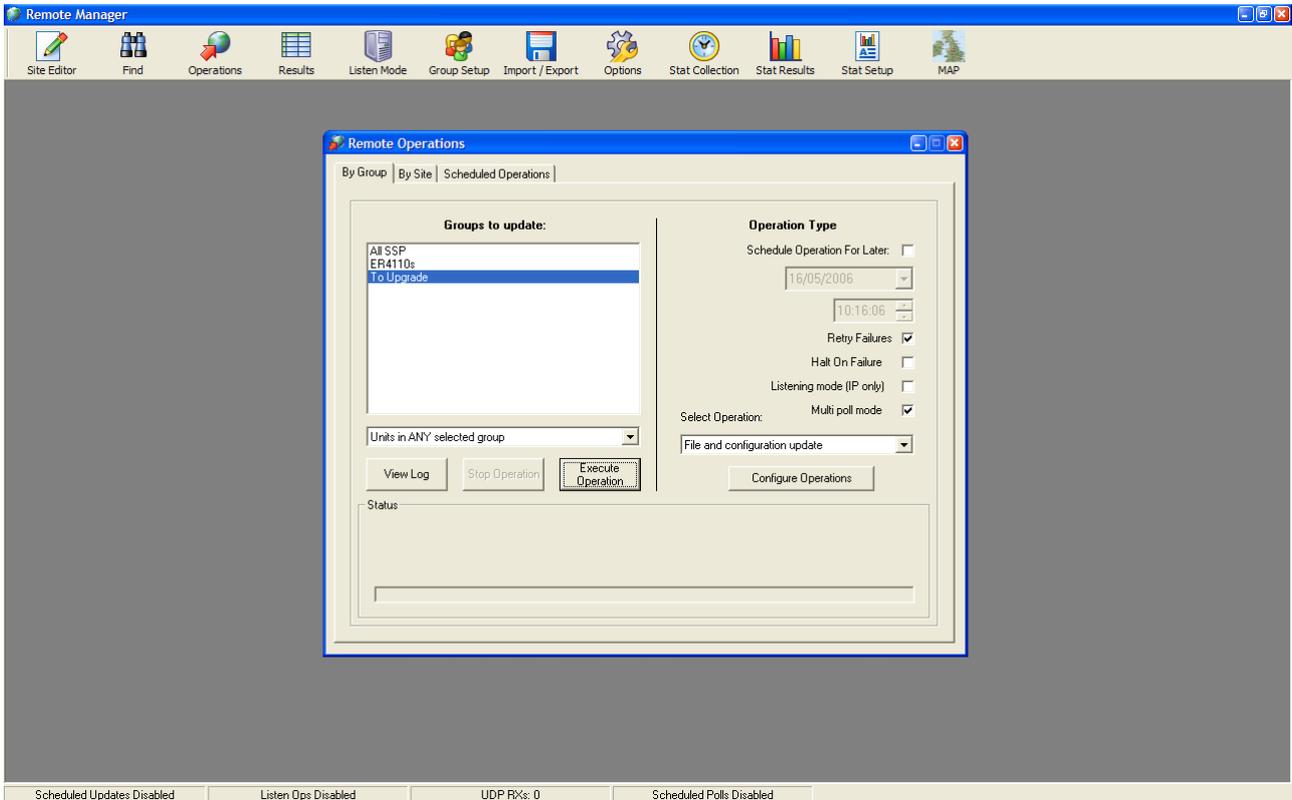
16.5 General Options

Click on the “Options” button on the tool bar and ensure your settings match those circled in red. These settings are very important for GPRS upgrades.

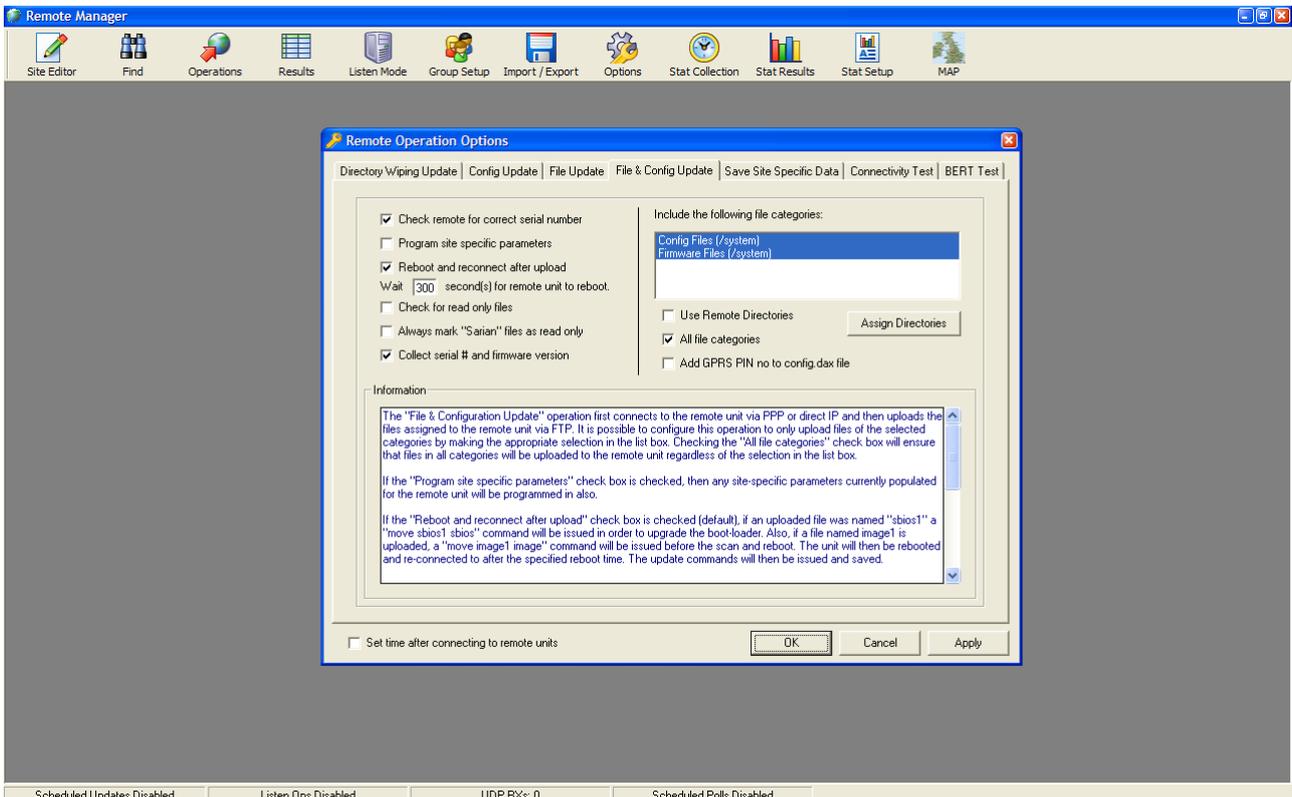


16.6 Remote File & Configuration Update Options

Click on the “Operations” button on the tool bar and select the “File Update” operation.



Click on the Configure Operations button and ensure the settings match those **exactly** in the screen shot below:



- ✓ *Allow 300 seconds for the remote unit to reboot, sometimes GPRS units can take longer than expected to come back on-line. 300 seconds seems to work well with GPRS units.*

Click the OK Button.

IF as well as the firmware, you are also replacing the config.da0 file

AND

(your SIM cards are protected by **different** PIN numbers OR you have a **different** PPP 1 usernames or passwords on your sites)

You will need to take the following extra steps:

- 1) On this screen tick "Add GPRS pin number to config.daX file"
- 2) In the config.da0 file you upload, ensure you have the following entry:

```
modemcc 0 epin *
```

and optionally the following entries:

```
ppp 1 epassword *
```

```
ppp 1 username *
```

- 3) Ensure that the config.da0 file is also linked to all sites in the file links tab of the site editor.

Remote Manager will then copy the existing values of these parameters into the config.da0 files before uploading it to the site. Please contact Technical Support if you need further assistance with this specialised feature.

16.7 Performing the Upgrade

On the "Operations" screen select the group you want to perform the operation on, in the "By Group" tab. Ensure that "Retry Failures" and "Multi Active mode" are ticked.

(The type of operation should still be "File and configuration update")

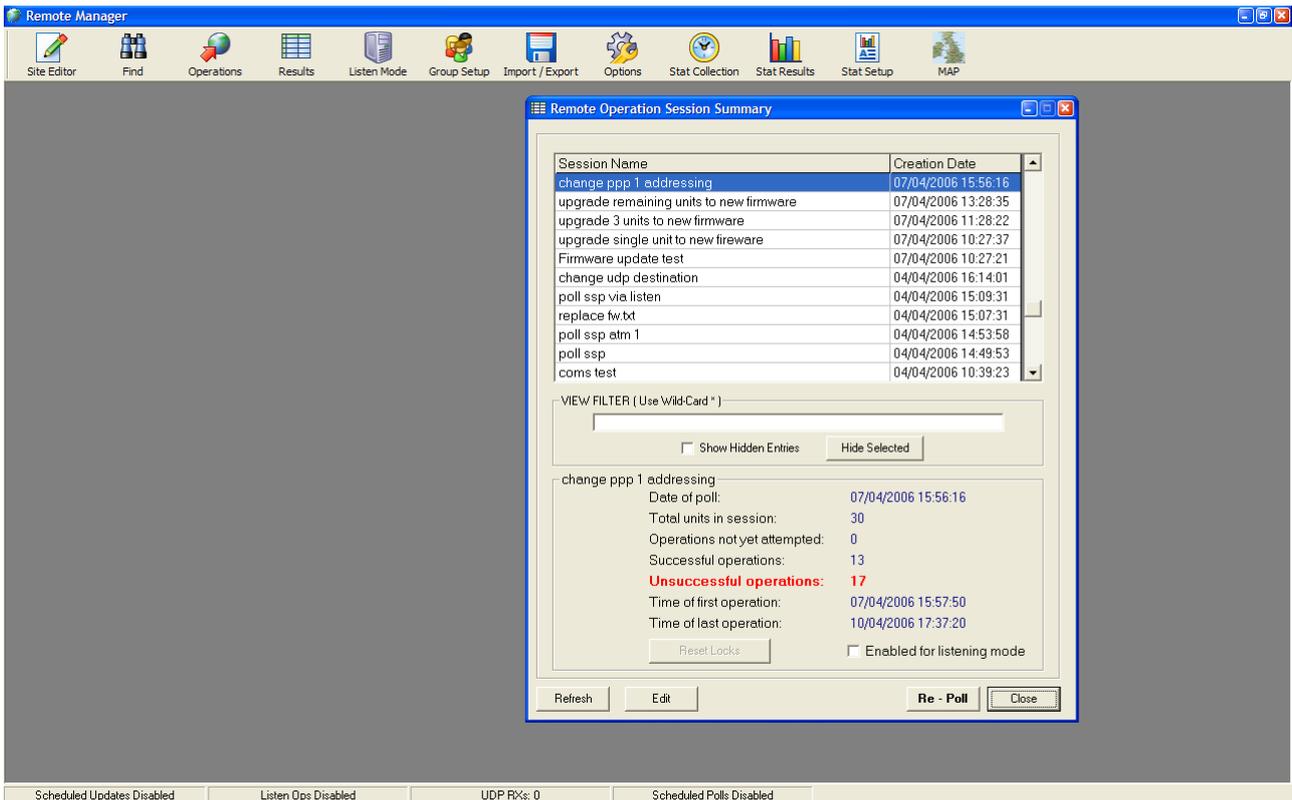
Click on the "Execute Operation" button and give the operation a name.

Now Remote Manager will connect to the remote sites (up to 50 sites at once (10 is the default) in multi active mode) and perform any updates required. The results are printed in the log display as well as recorded in the database.

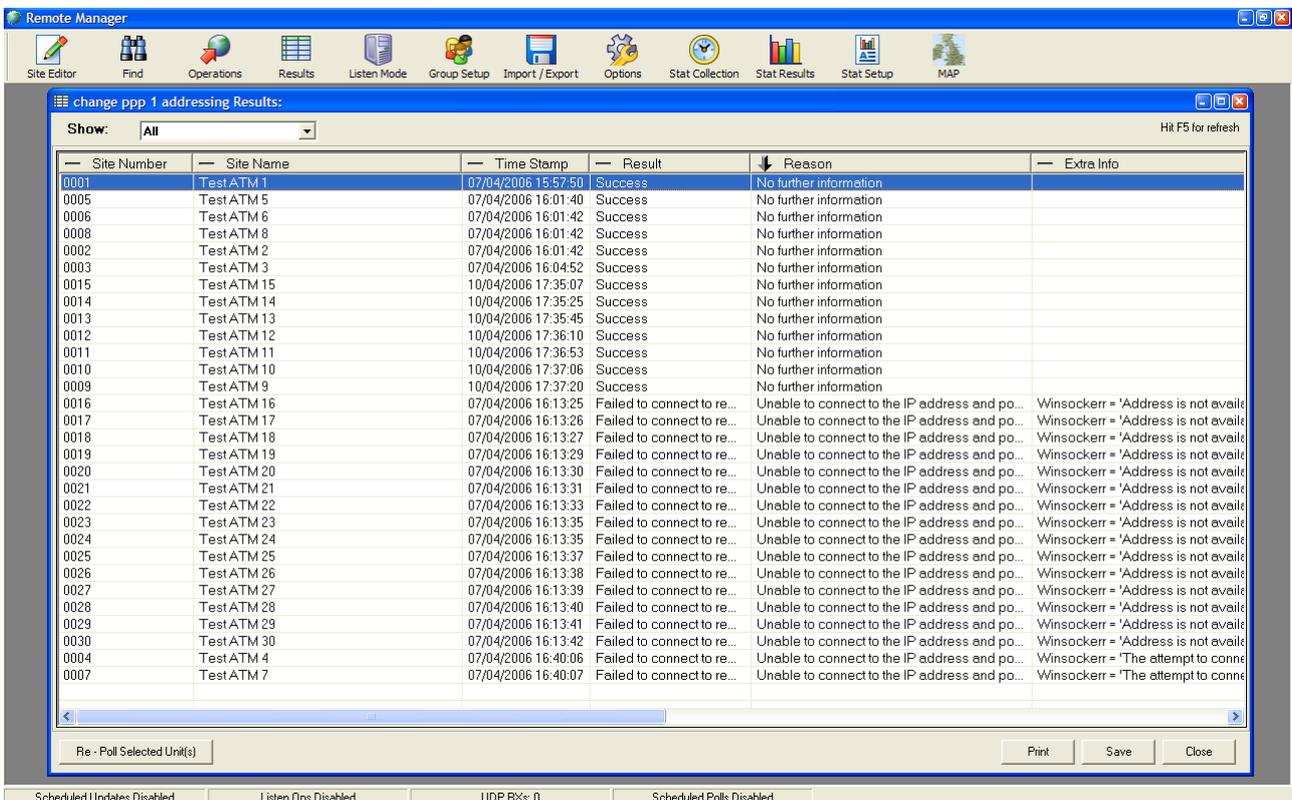
16.8 Viewing the results.

You can click "View Log" to view the details in the normal log (with red, green and black text). If you want to save this information you must click on "Save Log", before you shut down Remote Manager (or before it does any automated polling).

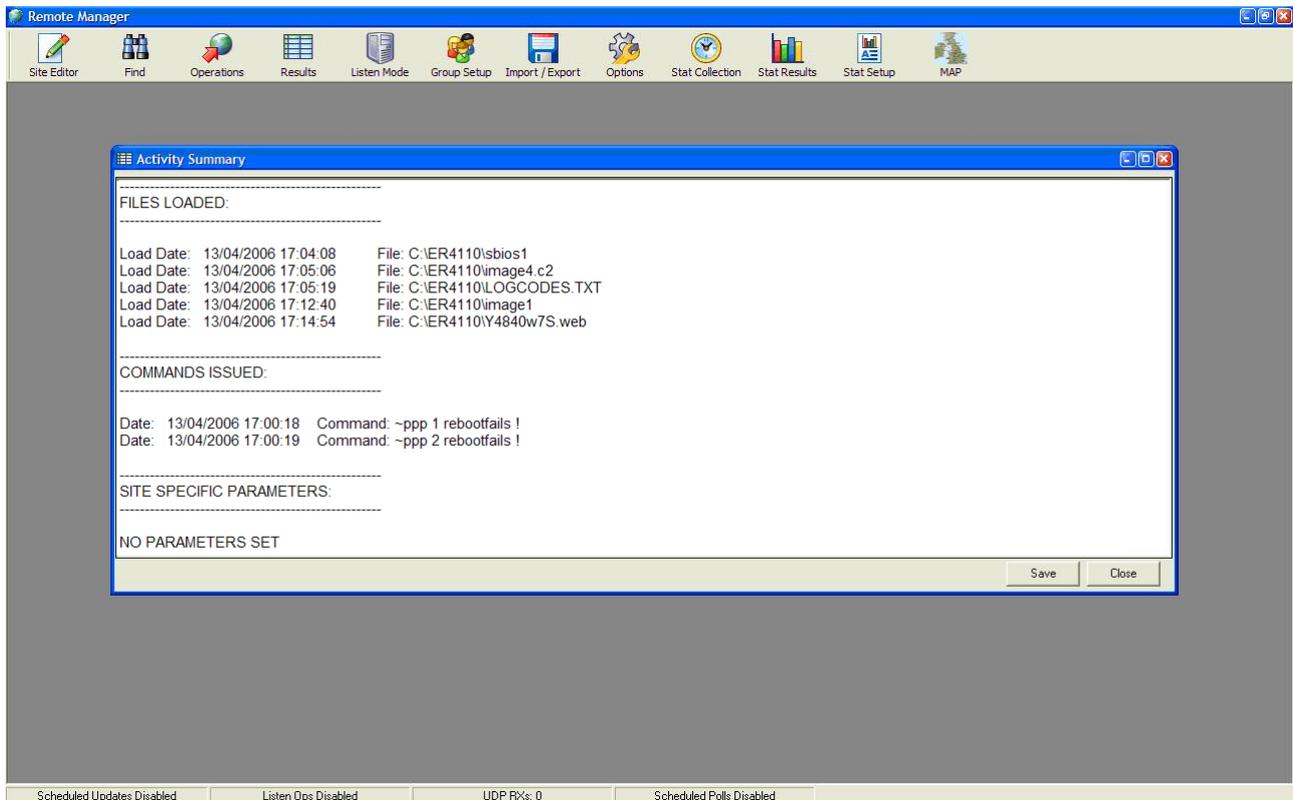
However the **final** (after any retries) result of the update is stored in the database and can be viewed by clicking on the "Results" toolbar button.



A summary of the results of the “Remote Operation Session” selected can be seen in the bottom half of the “Remote Operation Session Summary” screen. It is possible to initiate a retry of any unsuccessful polls by clicking the “Re-Poll” button. Double clicking the highlighted “Remote Operation Session” will display unit-by-unit results:



“Double Clicking” on an individual unit will display a summary of the files loaded, update commands issued or site specific parameters set:



This information is also accessible from the history tab of the site editor.

17.0 EXAMPLE II – MONITORING THE PERFORMANCE OF A GPRS/3G/UMTS/HSDPA NETWORK

17.1 Outline

This example explains how to

- Configure a GPRS/3G/UMTS/HSDPA TransPort/Sarian to collect stats on GPRS performance by sending UDP packets to a UDP echo server.
- Configure the Remote Manager program to collect these stats and produce graphs and reports every day.

17.2 Router Configuration

The firewall “stat” keyword can be used to collect various transaction style statistics on TCP and UDP traffic that the TransPort/Sarian routes. When used in conjunction with the UDP echo server and Remote Manager this is especially useful on GPRS/EDGE/UMTS/HSDPA networks as it allows the performance of the network to be monitored and automated reports to be generated every day. This feature can be used to police an SLA (Service Level Agreement).

This section explains how to configure the GPRS/Edge TransPort/Sarian to send UDP packets to an echo server which will echo the packets back. It also explains how to configure a TransPort/Sarian to be the echo server.

Also covered is the use of the firewall in the GPRS/Edge TransPort/Sarian to log statistics from these UDP packets.

17.2.1 Configuring the UDP echo client

On **Configuration** → **Common applications** → **UDP echo client/server** → **UDP echo client/server 0**

If using the old style web interface then browse to **Configure** → **UDP Echo Client/Server** → **UDP Echo 0**

Set the following parameters:

Destination IP address

This is the address to send the UDP packets to. Normally this would be a TransPort/Sarian running the Echo server. It could be any PC at the head-end as long as the PC is configured to echo the UDP packets back to the TransPort/Sarian. If an IPSEC tunnel is in use it is advisable to set the destination address to an address that will cause the UDP packets to go through the tunnel. The **Configure**→ **General** “GP sockets use IP from interface” and “GP sockets use IP from interface #” parameters can be used to set the source IP address of the UDP packets to an Ethernet interface to ensure that they go through the tunnel.

Destination port

This can be any valid unused port number if the destination IP address is another TransPort/Sarian. If the destination is a PC then the echo port number should be used which is 7.

Echo request interval (s)

Configure this to a suitable interval. A popular value would be between 30 to 80 seconds but any value is acceptable.

The more packets you send the higher the resolution of the graphs and the reports, but the more it will cost if you are charged for every byte of data sent.

Use routing code to determine echo interface:

Set to "Yes".

Exclude data from UDP packet

Set to "Yes" if you wish to make the UDP packet as small as possible in order to cut down on GPRS data charges.

Selecting the correct source IP address

If the TransPort/Sarian is configured to use IPSEC, then it is recommended that UDP packets are sent over the IPSEC tunnel. By default, the TransPort/Sarian will use the IP address of the Interface through which the UDP packets are being sent as the source IP address. In order to ensure that the packets go through an IPSEC tunnel it will usually be necessary to explicitly configure the TransPort/Sarian to use the IP address of an Ethernet interface (*i.e.* the Ethernet interface with the private IP address matching the Eroute's local subnet.).

To set the source IP address to be the IP address of Ethernet 0, navigate to **Configuration - System > General** (if using the old web interface **Configure → General**) and set the following parameters:

Parameter	Setting
GP sockets use IP from interface	Ethernet
GP sockets use IP from interface #	0

Remember to ensure that the destination IP address (on **Configure → UDP Echo Client/Server → UDP Echo 0**) is also an address that matches the Eroute's remote subnet.

Configuring the UDP Echo Server

If you are using a TransPort/Sarian as the echo server at the head end, then navigate to **Configure → UDP Echo Client/Server → UDP Echo 0** and configure the parameter "Local Port" to be the port number you choose as "Destination Port" in the remote TransPort/Sarian.

Configuring the Firewall

On the echo client remote TransPort/Sarian, ensure that the firewall is turned on for the appropriate WAN interface. Enter a firewall rule similar to the following:

```
pass out break end on ppp 1 proto udp from any to <Echo server IP address> port = 7 inspect-state oos 1 t=60 c=5 d=5 stat
```

And a second rule to allow other traffic to route:

```
pass
```

The firewall rule will cause the TransPort/Sarian to collect the following statistics based upon the performance of the UDP stat bins.

Successful Transaction Count	0
Dropped Transaction Count	0
Route OOS Count	0
Minimum Transaction Time (ms)	0
Maximum Transaction Time (ms)	0
Average Transaction Time (ms)	0

These stats can be seen on the Statistics → PPP → PPP 1 web page.

Ensure that you can see “Successful Transactions” on this web page before configuring Remote Manager.

Statistic Bins

In addition to the stats visible on the web page, the TransPort/Sarian will automatically store these same statistics and more in the statistic bins.

A single statistic bin contains one hours worth of data. Every hour on the hour a new bin is created. This allows the TransPort/Sarian to keep a historical record of the performance of the network hour by hour. Remote Manager can be used to collect the data in the stat bins and draw graphs and reports.

Statistic bins are encrypted but can be accessed via the “statbin.enc” file.

17.3 Remote Manager Configuration

17.3.1 Using Remote Manager Statistics outside of the United Kingdom

Currently if you wish to use Remote Manager on a PC running a non UK English version of Microsoft Windows™ and/or Microsoft Office™ you must follow the instructions below (Support for other locals may be added upon request).

In Microsoft Windows™ navigate to the control panel and open up the “Regional and Language Options” applet. Under “Standards and formats” on the “Regional Options” tab select “English (United Kingdom)”.

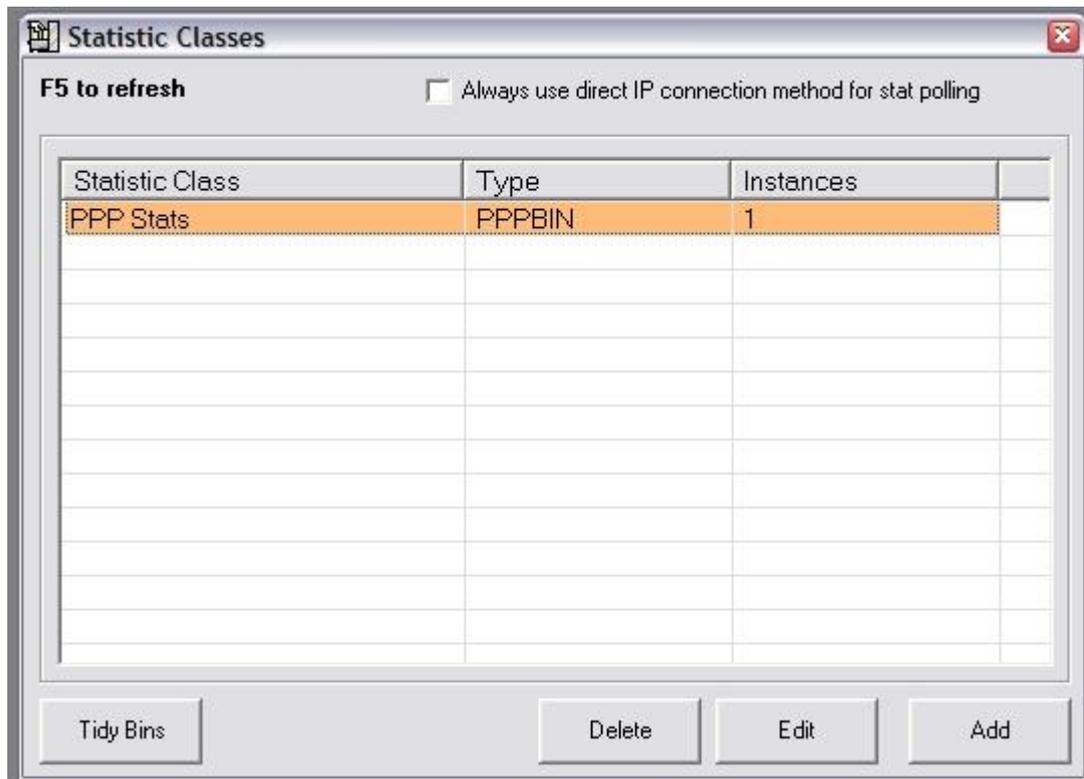
If you are running a non-English version of Microsoft Office, in a sub folder of the Office installation folder find the Excel™ document used as a template (XL8GALRY.XLS) for the built in chart types and open it in Excel. For example open:

“C:\Program Files\Microsoft Office\OFFICE11\1033\XL8GALRY.XLS”

Locate the work sheet called “Line - Column on 2 Axes” (translated to your language for example “Linie - Sule auf zwei Achsen” in German). Right click on this name and select rename. Rename it to the English title “Line - Column on 2 Axes”. Save XL8GALRY.XLS.

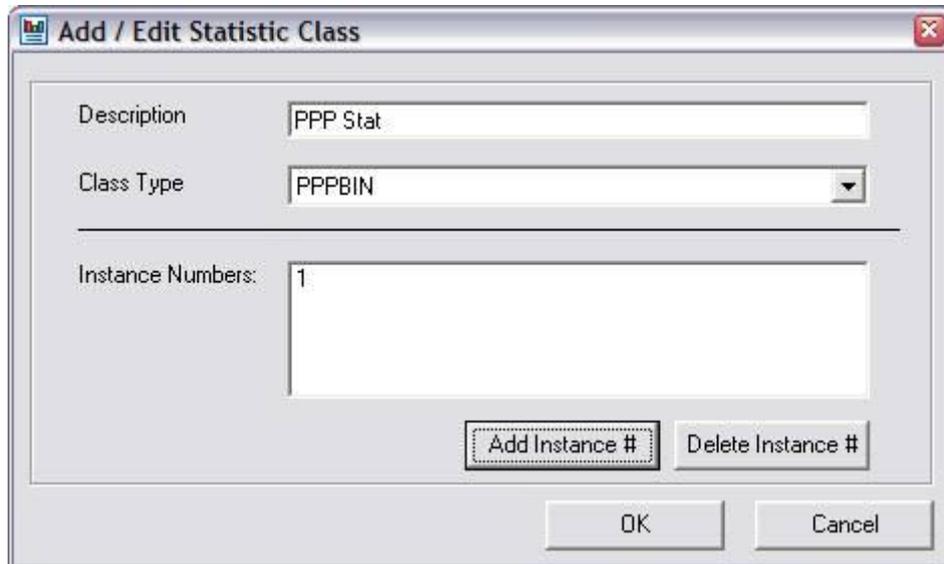
17.3.2 Global Statistic Settings

Once you have your stats working in the TransPort/Sarians, in Remote Manager click on the "Stat Setup" button:

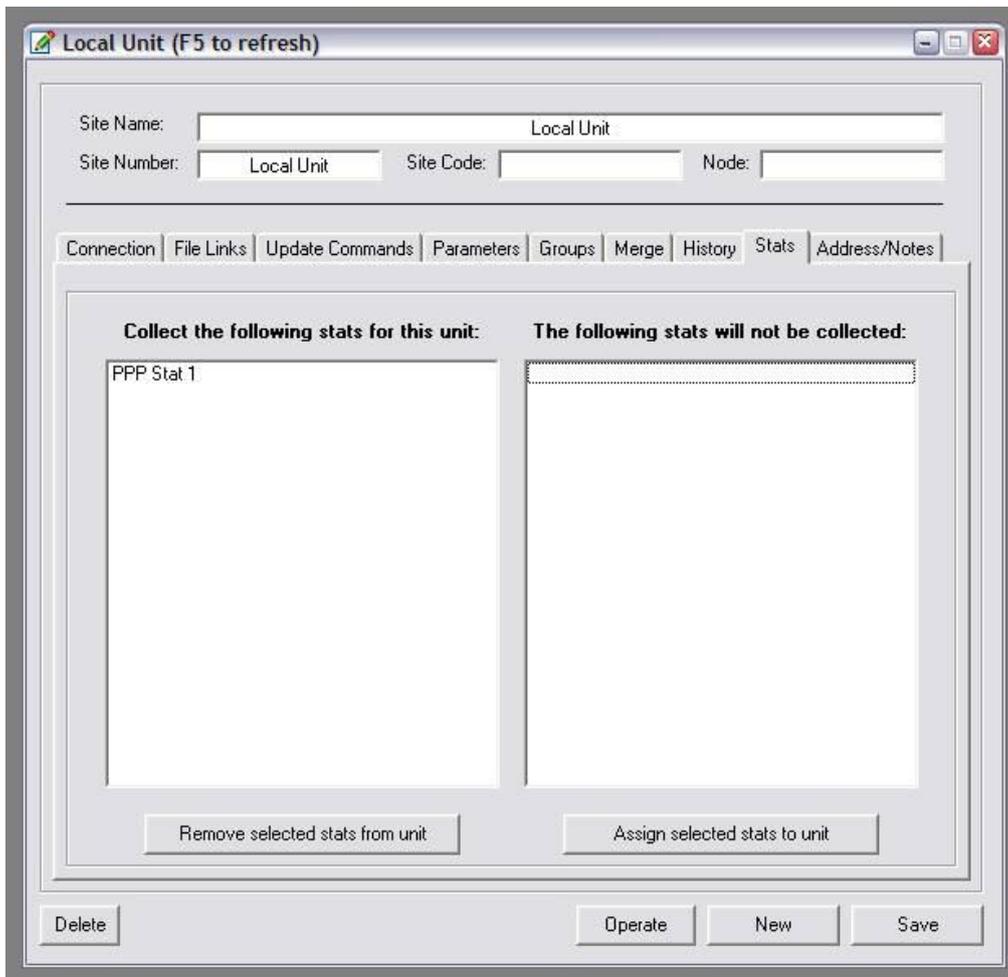


Then click on "Add"

Give it a name such as "PPP Stat", select the type to be "PPP Bin" and then click "Add Instance #" and enter "1".



Then click "OK"



Then click on the "Merge" tab.

Select the Group that you want to collect stats from and then click on the "Transfer current configuration to all units in selected groups" button.

Tick the check box "Copy Stat Collection" and then click "Perform Update"

Now all the units in the group you selected should have "PPP Stat 1" assigned to them in the "Stats" tab of the site editor.

17.3.4 Regular Collection of Statistics

Next Click on the "Poll Schedules" button.

Click the "Add" button and then:

- 1) Give the Schedule a name such as "Stat Collection"
- 2) Tick Schedule Enabled

General

Go to the General tab

- 3) In the "Schedule valid between dates & times" enter today's date for the start and some date a long time in the future for the End" (e.g. next year)

- 4) For the operation select "Stat Bin Poll"
- 5) Enter a suitable location to save the reports in the "Report Save Location"
- 6) Tick the "Email reports & charts to" check box and add your email address to the list below.
- 7) Enter a poll frequency of 1 hour (eventually you will want 10, 12 or 24 hours in this field)
- 8) Set the Retries setting to "1"

Groups

Go to the "Groups" tab

- 1) Select the group or groups that contain the units you want to collect the stats from.

PPP Reports

Go to the PPP Reports tab.

SLA Report

Go to the SLA Report sub-tab.

- 1) Tick "SLA report (daily)"
- 2) Tick "SLA report (last day of week)"
- 3) Click "Hi Latency Defaults"

Latency & Loss Graphs

Go to the "Latency & Loss Graphs" sub-tab.

- 1) Tick "Individual Latency & Loss (daily)"
- 2) Tick "Latency & Loss (last day of week)"
- 3) Tick "Page Per Site Performance Report"
- 4) Enter "7" days per site

Sporadic Site Report

Go to the "Sporadic Site Report" tab.

- 1) Tick "Generate sporadic failure report daily"
- 2) Click on "Hi Latency Defaults"

Outage Report

Go to Eventlog Outage Report sub-tab. Didn't get this tab, not sure if my RM was set up right for it to 'appear' unless this is not called 'Byte Count and Down Time'

- 1) Tick on "Generate outage report daily"

If you need to poll them again click on "Clear Poll History" and Remote Manager will "forget" it has ever polled these sites and so poll them again.

Note that the graphs and reports emailed to you today will be yesterday's graphs and therefore probably blank. To see today's graphs:

- 1) Click on "Stat Results"
- 2) Click "Next"
- 3) Select the group contain the units you are collecting stats from and click Next
- 4) Click "Select All" and click "Next"
- 5) Select "Performance Report"
- 6) To the question "Do you want an individual graph for each site and day" click "Yes"
- 7) To the next question decide the answer yourself and click Yes or No

17.4 Ensure that polling occurs at a specific time

It is recommended that you eventually set the poll interval for each schedule to a value of 10 hours. By means of "Enable Scheduled polling between" start and end time on the "Stat Collection" page restrict the polling window to less than 10 hours in a day. This will ensure that the polling occurs at exactly the same time every day, once every 24 hours.

For example.

In each schedule set the polling interval to 10 hours.

On the "Stat Collection" page set the polling window to 02:00 hrs to 11:00 hrs *i.e.* "Enable Scheduled Polling Between 02:00:00 and 11:00:00"