IP Office

Using IP Office System Monitor

15-601019 Issue 03c - (01 March 2013)

Notice
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you.
"Designated Processor" means a single stand-alone computing device.
"Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

License types
Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
Units may be linked to a specific, identified Server.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity pecified for the Software. End User may not re-install or operate the software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software.
"Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/licenseinfo under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark.

Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product.

For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

1. System Monitor

2. Using the Screen Log

3. Logging to a File

4. Setting the Trace Options

5. Status Screens

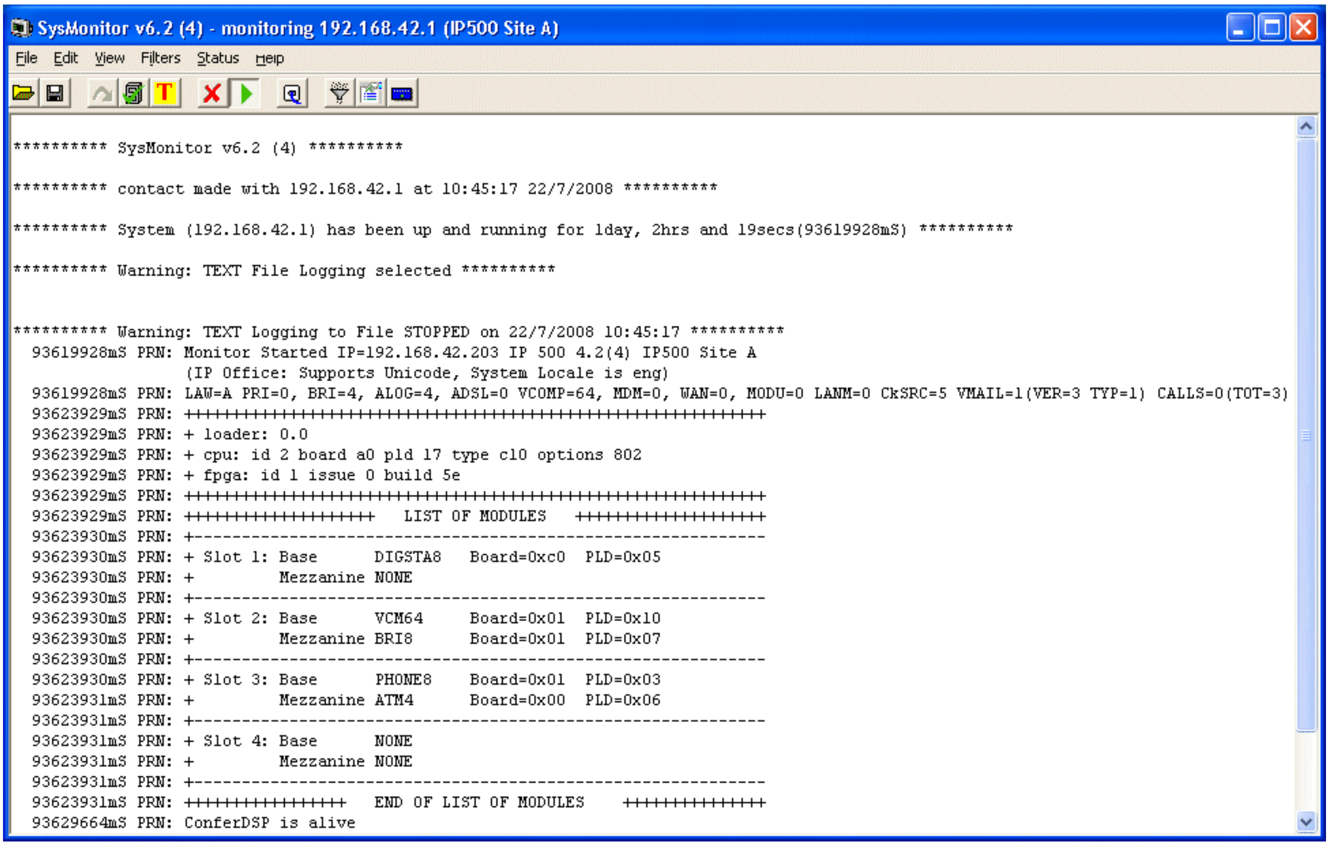
6. Example Monitor Settings

7. Addendum

Chapter 1.
System Monitor

1. System Monitor

System Monitor can assist in the detailed diagnosis of system problems. Through configuration of its trace options, it is able to display information on specific areas of a system's operation. It can also record that information as log files for later analysis.


SysMonitor v6.2 (4) - monitoring 192.168.42.1 (IP500 Site A)
File Edit View Filters Status Help

```
********** SysMonitor v6.2 (4) **********

********** contact made with 192.168.42.1 at 10:45:17 22/7/2008 **********

********** System (192.168.42.1) has been up and running for 1day, 2hrs and 19secs(93619928mS) **********

********** Warning: TEXT File Logging selected **********


********** Warning: TEXT Logging to File STOPPED on 22/7/2008 10:45:17 **********
  93619928mS PRN: Monitor Started IP=192.168.42.203 IP 500 4.2(4) IP500 Site A
                  (IP Office: Supports Unicode, System Locale is eng)
  93619928mS PRN: LAW=A PRI=0, BRI=4, ALOG=4, ADSL=0 VCOMP=64, MDM=0, WAN=0, MODU=0 LANM=0 CkSRC=5 VMAIL=1(VER=3 TYP=1) CALLS=0(TOT=3)
  93623929mS PRN: +++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
  93623929mS PRN: + loader: 0.0
  93623929mS PRN: + cpu: id 2 board a0 pld 17 type c10 options 802
  93623929mS PRN: + fpga: id 1 issue 0 build 5e
  93623929mS PRN: +++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
  93623929mS PRN: ++++++++++++++++++++   LIST OF MODULES   ++++++++++++++++++++
  93623930mS PRN: +------------------------------------------------------------
  93623930mS PRN: + Slot 1: Base      DIGSTA8   Board=0xc0  PLD=0x05
  93623930mS PRN: +         Mezzanine NONE
  93623930mS PRN: +------------------------------------------------------------
  93623930mS PRN: + Slot 2: Base      VCM64     Board=0x01  PLD=0x10
  93623930mS PRN: +         Mezzanine BRI8      Board=0x01  PLD=0x07
  93623930mS PRN: +------------------------------------------------------------
  93623930mS PRN: + Slot 3: Base      PHONE8    Board=0x01  PLD=0x03
  93623931mS PRN: +         Mezzanine ATM4      Board=0x00  PLD=0x06
  93623931mS PRN: +------------------------------------------------------------
  93623931mS PRN: + Slot 4: Base      NONE
  93623931mS PRN: +         Mezzanine NONE
  93623931mS PRN: +------------------------------------------------------------
  93623931mS PRN: +++++++++++++++++   END OF LIST OF MODULES    +++++++++++++++
  93629664mS PRN: ConferDSP is alive
```

- System Monitor is also known as "Monitor" or "SysMon".
- System Monitor is intended primarily for use by Avaya support and development staff. The settings within System Monitor and the information shown frequently change between software releases.
- Analysis of the information shown requires detailed data and telecommunications knowledge plus system knowledge and is not intended for general users.
- Despite the facts above, all persons maintaining systems need to be able to run System Monitor in order to capture logs for submission with fault reports even if they cannot interpret the logs themselves.

System Status Application

For general purpose monitoring of the status of a system and calls, use IP Office System Status Application rather than System Monitor. The System Status Application provides much easier to interpret data and information and is suitable for use by system maintainers and advanced system users.

1.1 Installing System Monitor

Avaya supply System Monitor on the IP Office Administrator Applications DVD. The installation process normally includes installation of System Monitor and the IP Office Manager application by default. However, if necessary you can install System Monitor separately.

System Monitor is a Windows application. Its interface runs in English only but does not require any licenses.

PC Requirements

Minimum PC Requirements	
RAM	128MB
Hard Disk Free Space	10GB
Processor:	
- Pentium	PIII 800MHz
- Celeron	Celeron 3 800Mhz
- AMD	Athlon B 650MHz

Operating System Support	
Server OS:	
2003 Server	Yes
2008 R2 Server	Yes
Client OS:	
XP Professional	Yes
Vista	Yes
Windows 7	Yes

- Vista support is only on Business, Enterprise and Ultimate versions.
- Windows 7 support is only on Professional, Enterprise and Ultimate versions.

Ports

By default, System Monitor connects to UDP port 50794 on the monitored system.

To install System Monitor:

1. Inserting the DVD into the PC's DVD drive. This starts the Installation Wizard.
2. Select the required language. Click **Next**.
3. Select the file path for the installed files. Click **Next**.
4. From the list of available applications, check that **System Monitor** is selected for installation. Be careful about de-selecting any other highlighted options, as this triggers their removal if already installed.
5. Click **Next**.
6. Click **Install**.

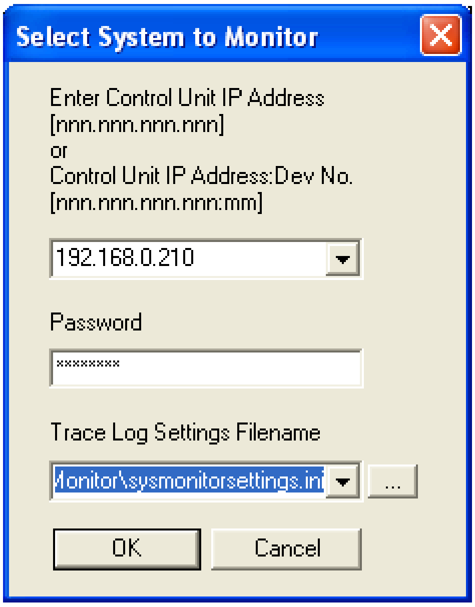
1.2 Starting System Monitor

You can run System Monitor from a PC on the same local IP subnet as the targeted system or it can run on a PC on a remote subnet.

- If the PC running the System Monitor and the targeted system are on the same subnet, then you can either use the system's IP address (eg. 192.168.42.1) or the local subnet broadcast address (eg. 192.168.42.255). If there is more than one system on the local subnet, then you must use the system's IP address.
- If the PC running the System Monitor and the targeted system are on the different subnets (these can be different local subnets or from a remote subnet) then you must use the system's unique IP address. It is also essential that bi-directional routing exists between the two subnets in question.

To start System Monitor:

1. Select **Start | Programs | IP Office | System Monitor**.
2. If System Monitor has run before, it automatically attempts to connect with the system that was previously being monitored. If otherwise or you want to monitor a different system, use the steps below to select the required system.
3. Select **File** and then **Select Unit**.



Enter Control Unit IP Address
[nnn.nnn.nnn.nnn]
or
Control Unit IP Address:Dev No.
[nnn.nnn.nnn.nnn:mm]

192.168.0.210

Password

****

Trace Log Settings Filename

Monitor\sysmonitorsettings.ini

4. Enter the **IP Address** and **Password** of the system that you want to monitor.
   - **Which Password?**
     Using IP Office Manager, it is possible to set a specific **Monitor Password**. If the system does not have a **Monitor Password** set, System Monitor uses the system's **System Password**. The **Monitor Password** and **System Password** are set within a system's security configuration settings.
5. If you want System Monitor to start with a previously saved set of trace options, use the **Trace Log Settings Filename** browse button to select the trace options settings file.
6. Click **OK**.
7. Once System Monitor has connected with a system, System Monitor displays the system's status report 12 and alarm log 13.

1.3 The System Status Report

The status report is output whenever System Monitor connects to a system. The information included varies depending on the type of system and the equipment installed with it. The example below is a typical output for an IP500 system.

The first few lines include the time, date plus the IP address of the system and up time of the monitored system.

```
********** SysMonitor v6.2 (4) **********
********** contact made with 192.168.42.1 at 10:45:17 22/7/2008 **********
********** System (192.168.42.1) has been up and running for 1day, 2hrs and 19secs(93619928mS) **********
  93619928mS PRN: System Monitor Started IP=192.168.42.203 IP 500 4.2(4) IP500 Site A
                  (IP Office: Supports Unicode, System Locale is eng)
  93619928mS PRN: LAW=A PRI=0, BRI=4, ALOG=4, ADSL=0 VCOMP=64, MDM=0, WAN=0, MODU=0 LANM=0 CkSRC=5 VMAIL=1(VER=3 TYP=1) CALLS=0(TOT=
  93623929mS PRN: +++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
  93623929mS PRN: + loader: 0.0
  93623929mS PRN: + cpu: id 2 board a0 pld 17 type c10 options 802
  93623929mS PRN: + fpga: id 1 issue 0 build 5e
  93623929mS PRN: +++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
  93623929mS PRN: ++++++++++++++++++++   LIST OF MODULES   ++++++++++++++++++++
  93623930mS PRN: +------------------------------------------------------------
  93623930mS PRN: + Slot 1: Base      DIGSTA8   Board=0xc0  PLD=0x05
  93623930mS PRN: +         Mezzanine NONE
  93623930mS PRN: +------------------------------------------------------------
  93623930mS PRN: + Slot 2: Base      VCM64     Board=0x01  PLD=0x10
  93623930mS PRN: +         Mezzanine BRI8      Board=0x01  PLD=0x07
  93623930mS PRN: +------------------------------------------------------------
  93623930mS PRN: + Slot 3: Base      PHONE8    Board=0x01  PLD=0x03
  93623931mS PRN: +         Mezzanine ATM4      Board=0x00  PLD=0x06
  93623931mS PRN: +------------------------------------------------------------
  93623931mS PRN: + Slot 4: Base      NONE
  93623931mS PRN: +         Mezzanine NONE
  93623931mS PRN: +------------------------------------------------------------
  93623931mS PRN: +++++++++++++++++   END OF LIST OF MODULES    +++++++++++++++
```

The next line gives information about various aspects of the system. This line is output at regular intervals, set through the file logging preferences 28.

```
  93619928mS PRN: LAW=A PRI=0, BRI=4, ALOG=4, ADSL=0 VCOMP=64, MDM=0, WAN=0, MODU=0 LANM=0 CkSRC=5 VMAIL=1(VER=3 TYP=1) CALLS=0(TOT=
```

LAW =	A-Law or U-law system.
PRI =	Number of PRI channels
BRI =	Number of BRI channels.
ALOG =	Number of Analog Trunk Channels
ADSL =	*Not Used.*
VCOMP =	Number of voice compression channels installed.
MDM =	Size of Modem Card Fitted
WAN =	Number of WAN Ports configured.
MODU =	Number of external expansion modules (excluding WAN3 modules) attached.
LANM =	Number of WAN3 external expansion modules attached.
CkSRC =	The current clock source being used for PRI/BRI trunks (0 = Internal Clock Source).
VMAIL =	Indicates whether the voicemail server is connected. 1 if connected, 0 if not connected.
VER =	The software version of the voicemail server if obtainable.
TYP =	The type of Voicemail Server: 0 = None. 1 = Voicemail Lite/Pro. 2 = Centralized Voicemail Pro. 3 = Embedded Voicemail. 4 = Group (3rd party) voicemail. 5 = Remote Audix Voicemail
CALLS =	Number of current calls
TOT =	Total number of calls made to date since last system reboot.

In addition, when System Monitor starts, the initial output may include the system's alarm log. See The Alarm Log 13.

1.4 The Alarm Log

When System Monitor connects to a system, the trace includes the system's alarm log. The alarms cannot be interpreted. However, if a site is the same repeated problem, Avaya may request the alarm log details.

The presence of alarms is not necessarily critical as each system keeps a record of the first 8 alarms since the alarm log was last cleared. However, once the alarm log is full, the system ignores additional alarms.

```
3003mS PRN: +++ START OF ALARM LOG DUMP +++
3019mS PRN: ALARM: 18/03/2004 13:07:56 IP 412 2.1(8) <Program Exception> CRIT RAISED addr=00000000 d=5 pc=00000000 0082eef0 0094d780
3019mS PRN: ALARM: 22/04/2004 07:26:44 IP 412 2.1(11) <Program Exception> CRIT RAISED addr=00000000 d=5 pc=00000000 0095dfe0 0095e27
3019mS PRN: ALARM: 22/04/2004 07:26:46 IP 412 2.1(11) <WATCHDOG> CRIT RAISED addr=00000000 d=0 pc=00000000 01e75750 01f983d4 0095e27
3004mS PRN: +++ END OF ALARM LOG DUMP +++
```

You can view the alarm log again at any time. You can also clear the alarm log to remove old alarms. See Alarms 79.

1.5 Adding Log Stamps

Using their phone, system users can access a log stamp function. This allows the user to insert a log stamp event into their system's monitor records. You can use this to have users indicate when an issue that you are trying to capture in the system log has occurred.

The log stamp record includes the date, time, user name and extension of the user who triggered the log stamp function. The system prefixes the record with **LSTMP: Log Stamped** and a log stamp number.

The system restarts the log stamp number from 000 whenever the system is restarted. Each time the log stamp function is used, the number increments, in a cycle from 000 to 999. However, a specific log stamp number can be assigned to a button or short code used to trigger the function. When triggered, the user's phone briefly displays the log stamp number.

A default system short code *55 is automatically added for new systems. For users with appropriate telephones, the log stamp function can also be assigned to a programmable button on the phone using the **Advanced | Miscellaneous | Stamp Log**.

To send a log using the default system short code:

1. When the event to be marked, dial ***55**. If already on a call, put that call on hold before dialing ***55**.

1.6 Monitor Icons

The System Monitor window contains a number of icons:

- **Open File**
  Open a previous monitor log file. See Opening a Log File 31.

- **Save Log As**
  Save the current monitor log to a text file. See Saving the Current Screen as a Log File 31.

- **Rollover Log**
  Force the current log file to rollover. System Monitor adds a date and time stamp to the log file name and a new log file started. See Manually Rolling Over the Log File 31.

- **Stop Logging**
  Stop logging to a file. See Stopping File Logging 30.

- **Start Logging**
  Start logging to a file. See Starting File Logging 30.

- **Text Log File**
  This icon indicates that System Monitor is currently set to log to a plain text file. Clicking the icon changes the mode to binary file logging (forcing a rollover of any current log file). See Switching Between Binary and Text Logging 30.

- **Binary Log File**
  This icon indicates that System Monitor is currently set to log to a binary file. Clicking the icon changes the mode to text file logging (forcing a rollover of any current log file). See Switching Between Binary and Text Logging 30.

- **Clear Screen Display**
  Clear the current log shown in the display. See Clearing the Screen Log 21.

- **Run Screen Display**
  Show the live monitor log in the display. See Starting the Screen Log 21.

- **Freeze Screen Display**
  Pause the live monitor log in the display. This does not stop the logging to file. See Pausing the Screen Log 21.

- **Reconnect**
  Connect to the system specified in the **Select Unit** options. See Reconnecting to the Monitored System 23.

- **Filter Trace Options**
  Set the filter options for what should be included in the logs. See Filtering the Screen Log 22.

- **Log Preferences**
  Set the format and destination for the monitor log file. See Setting the Log Preferences 29.

- **Select Unit**
  Set the details of the system to monitor. See Selecting the System to Monitor 23.

1.7 Keyboard Shortcuts

You can use the following keyboard shortcuts with System Monitor:

Function	Shortcut	
Select unit	Ctrl+U	See Selecting the System to Monitor 23.
Reconnect	Ctrl+E	See Reconnecting to the Monitored System 23.
Open file	Ctrl+O	See Opening a Log File 31.
Save screen log as	Ctrl+S	See Saving the Screen Log as a Log File 25.
Send to mail recipient	Ctrl+M	See Emailing the Screen Log 25.
Send to mail recipient as attachment	Ctrl+H	See Emailing the Screen Log 25.
Rollover log	Ctrl+R	See Manually Rolling Over the Log File 31.
Log preferences	Ctrl+L	See Setting the Log Preferences 29.
Clear the screen log	Ctrl+X	See Clearing the Screen Log 21.
Copy the screen log	Ctrl+C	See Copying Screen Log Information 25.
Select all	Ctrl+A	See Copying Screen Log Information 25.
Find	Ctrl+F	See Searching the Screen Log 22.
IP Calculate	Ctrl+D	See Converting IP Address Hex Values 22.
Log to screen (start/pause)	Ctrl+G	See Starting the Screen Log 21 and Pausing the Screen Log 21.
Trace options	Ctrl+T	See Setting the Trace Options 34.
US PRI Trunk status	Ctrl+I	See US PRI Trunks 97.
Filter screen log	F4	See Filtering the Screen Log 22.
Close System Monitor	Alt+F4	See Stopping System Monitor 17.

1.8 Closing System Monitor

Closing System Monitor ends screen and file logging. When System Monitor is next started, it attempts to reconnect to the same system that it was connected to when it was closed.

To close System Monitor:

1. Click the **X** icon at the top-right of the window. Alternatively, press ***Alt+F4*** or click **File** and select **Exit**.
2. The application is closed. All logging stops.

Chapter 2.
Using the Screen Log

2. Using the Screen Log

System Monitor uses its main display area to show records received from the connected system. Alternatively, it can display a previously saved logged file for study.

The records displayed in the screen log are not the raw records as received from the system, instead that are "interpreted" records. System Monitor applies various changes to aid the interpretation of the records. For example, a record containing the raw entry ***pcol=6*** is interpreted and displayed as ***pcol=6 (TCP)***.

2.1 Pausing the Screen Log

When System Monitor displays the trace from a connected system, you can pause the trace in order to inspect it.

To pause the screen log:

1. Click the ⏸ **Freeze Screen Logging** icon. Alternatively, press ***Ctrl+G***.
2. System Monitor displays a warning **Logging to Screen Stopped** as part of the log.
3. To restart the screen log, see Starting the Screen Log 21.

2.2 Starting the Screen Log

When System Monitor displays the records from a connected system, you may need to pause the output in order to inspect it. See Pausing the Screen Log 21. You can use the following option to restart displaying records received.

When you load a log file for display, any screen logging from a connected system is automatically paused. Restarting the screen log add records from the connected system when they are received.

To restart the screen log:

1. Click the ▶ **Log to Screen** icon. Alternatively, press ***Ctrl+G***.
2. System Monitor displays a warning **Logging to Screen Started** as part of the log.

2.3 Clearing the Screen Log

You can clear the currently displayed trace.

- If the trace was from a connected system, those records are lost unless the trace was also being logged to a file.
- Clearing the trace does not affect any trace records logged to a file.
- If the screen log was loaded from a previously saved log file, clearing the trace clears the screen log but does not erase records from the log file.

To clear the screen log:

1. Click the ✗ **Clear Display** icon. Alternatively, press **Ctrl+X**.

2.4 Filtering the Screen Log

System Monitor can display a filtered summary of the current screen log. You can base the filter on any selected part of the existing screen log, for example an IP address or extension number. System Monitor displays the filtered log as a separate window you can save to a text file.

To display a filtered screen log:

1. Using the cursor, highlight the part of the current screen log that you want used as the filter. If necessary, pause the screen in order to make the selection, see Pausing the Screen Log 21.
2. Press **F4**.
3. System Monitor displays a separate window that shows those records that contain matches to the filter.

To save a filtered screen log:

1. Filter the log using the process above.
2. In the filtered log window, click **File** and select **Save As**.
3. Enter a file name or select an existing file to overwrite.
4. Click **Save**.

To copy the filtered screen log:

1. Filter the log using the process above.
2. In the filtered log window, select the filter records that you want to copy.
3. Click **File** and select **Copy**.

2.5 Searching the Screen Log

You can search the screen log for records that contain text that match the search string you specify.

To search the screen log:

1. Optional: Selecting a piece of text in the screen log before starting search automatically makes that text the search string.
2. Click **Edit** and select **Find**. Alternatively, press ***Ctrl+F***.
3. Enter the search string for which you want to search the screen log.
4. Click **Find Next** to find the first match.
5. Click **Find Next** again to find the next match.

2.6 Converting IP Address Hex Values

Some values displayed in the screen log are Hex values. These are indicated by a 0x prefix to the number. Typically these are IP addresses. System Monitor can display the converted value. For example, ***0xff*** becomes ***0.0.0.255***.

To display the IP address conversion of a hex value:

1. In the screen log, select and highlight the value to be converted. It does not matter if you include the 0x in the selection or not.
2. Click **Edit** and select **IP Calculated (Selected Hex)**. Alternatively, press **Ctrl+D**.
3. System Monitor displays the converted value.

2.7 Selecting the System to Monitor

While already monitoring a system or viewing a log file, you can switch to receiving and displaying the log records from another system.

To select the system to monitor and start screen monitoring:

1. Click the **Select Unit** icon. Alternatively, press **Ctrl+U**.
2. Enter the **IP Address** and **Password** of the system that you want to monitor.
   - **Which Password?**
     Using IP Office Manager, it is possible to set a specific **Monitor Password**. If the system does not have a **Monitor Password** set, System Monitor uses the system's **System Password**. The **Monitor Password** and **System Password** are set within a system's security configuration settings.
3. Click **OK**.
4. Once System Monitor has connected to a system, System Monitor displays the system's status report 12 and alarm log 13.

2.8 Reconnecting to the Monitored System

System Monitor automatically attempts to reconnect to a system when it detects that the connection has been lost. However, if necessary you can manually select to reconnect.

To select the system to monitor and start screen monitoring:

1. Click the **Reconnect** icon. Alternatively, press **Ctrl+E**.
2. Once System Monitor has connected with a system, System Monitor displays the system's status report 12 and alarm log 13.

2.9 Setting the Trace Options

The output received from a system includes records for all activity. This can make it difficult to spot just those details needed to diagnose a particular issue. Therefore, System Monitor allows selection of which records are included in the current screen log and file logging. See Trace Options 34.

2.10 Viewing the System Alarms

This status menu displays the alarms records in the connected system's alarms log.

When System Monitor connects to a system, the trace includes the system's alarm log. The alarms cannot be interpreted. However, if a site is the same repeated problem, Avaya may request the alarm log details.

The presence of alarms is not necessarily critical as each system keeps a record of the first 8 alarms since the alarm log was last cleared. However, once the alarm log is full, the system ignores additional alarms.

```
3003mS PRN: +++ START OF ALARM LOG DUMP +++
3019mS PRN: ALARM: 18/03/2004 13:07:56 IP 412 2.1(8) <Program Exception> CRIT RAISED addr=00000000 d=5 pc=00000000 0082eef0 0094d78
3019mS PRN: ALARM: 22/04/2004 07:26:44 IP 412 2.1(11) <Program Exception> CRIT RAISED addr=00000000 d=5 pc=00000000 0095dfe0 0095e27
3019mS PRN: ALARM: 22/04/2004 07:26:46 IP 412 2.1(11) <WATCHDOG> CRIT RAISED addr=00000000 d=0 pc=00000000 01e75750 01f983d4 0095e27
3004mS PRN: +++ END OF ALARM LOG DUMP +++
```

To view the alarm log:

1. Click **Status** and select **Alarms**.

2. System Monitor displays the alarm records in a separate window.

To clear the alarm log:

1. View the alarm log using the process above.

2. Click **Clear Alarms**.

2.11 Viewing the Status Menus

In addition to the screen log, System Monitor can display a number of different status screens for different aspects of system operation.

To view a status screen:

1. Click Status and select the status screen required. See Status Screens 78.

2.12 Emailing the Screen Log

You can use the default email application configured on the PC to send an email copy of the current screen log.

You can send an email with the screen log either pasted into the email text or attached as a separate ***.txt*** file. Attaching as a file allows the recipient to easily load the log into their copy of System Monitor.

To email the screen log pasted into an email:

1. Click **File**, select **Send To** and then **Mail Recipient**. Alternatively, press ***Ctrl+M***.
2. The default email application displays a new email with the screen log pasted into the message text.
3. Complete the email details and click **Send**.

To email the screen log as an email attachment:

1. Click **File**, select **Send To** and then **Mail Recipient as Attachment**. Alternatively, press ***Ctrl+H***.
2. The default email application displays a new email with the screen log attached as a file.
3. Complete the email details and click **Send**.

2.13 Opening a Log File

You can use System Monitor to view an existing log file. Opening a log file automatically pauses the display of the screen log from the connected system.

To open a log file:

1. Click the **Open File** icon. Alternatively, press ***Ctrl+O*** or click **File** and select **Open File**.
2. Browse to and select the log file. Text log files end in ***.txt***. Binary log files end in ***.mon***.
3. Click **Open**.
4. The file opens in the System Monitor view.

2.14 Copying Screen Log Information

You can copy and paste the information shown in the screen log using the standard Windows methods.

To copy screen log information:

1. Using the cursor, select the section of the screen log to copy. Alternatively, press ***Ctrl+A*** to select the whole screen log.
2. System Monitor highlights the selected portion of the screen log.
3. Press ***Ctrl+C*** to copy the selected portion of the screen log.

2.15 Saving the Screen Log as a Log File

You can save the records displayed in the screen log as a text file.

- **Converting a Binary Log File**
  Using this option to open a binary log file and then save it as a plain text log file can be problematic if System Monitor displays a very large number of records. If that is the reason a plain text file is require, see Converting a Binary Log to a Text Log 32.

To save the current screen log as a file:

1. Click the **Save Screen Log As** icon. Alternatively, press ***Ctrl+S*** or click **Files** and select **Save Screen Log as**.
2. Enter a file name for the file.
3. Click **Save**.

2.16 Setting the Screen Font

You can select the default font used for displaying the logs.

To set the screen font:

1. Click **View** and select **Font**.
2. Select the font settings required.
3. Click **OK**.

2.17 Setting the Screen Background Colour

You can select the colour used for the background of the screen log.

To set the screen background colour:

1. Click **View** and select **Background Colour**.
2. Select the colour required.
3. Click **OK**.

2.18 Setting the Trace Colours

You can select a colour for a particular type of trace option. System Monitor then applies that colour to any matching records when added to the screen log.

To apply a colour to a trace option:

1. Click the **Trace Options** icon. Alternatively, press **Ctrl+T** or click **Filters** and select **Trace options**.
2. Select the tab showing the trace option for which you require a specific colour.
3. Right click on the name of the trace option.
4. Select the required colour.
5. Click **OK**.
6. System Monitor displays the trace option name in the selected colour.

Chapter 3.
Logging to a File

3. Logging to a File

In addition to displaying records in the screen log, System Monitor can copy records into a log file. You can view log files at a later time or send them for analysis by another person.

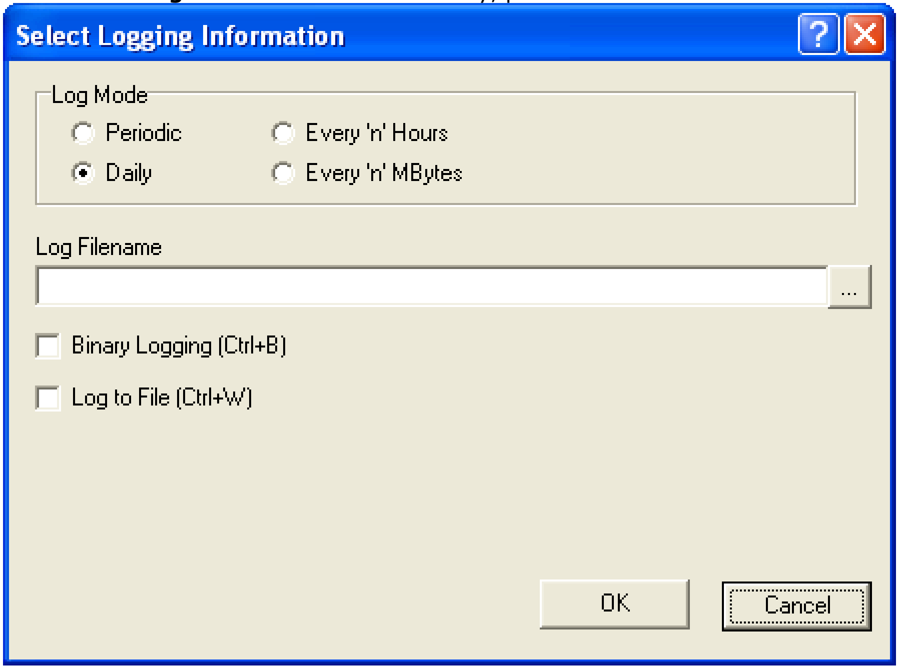
- Setting the log preferences 29
- Starting file logging 30
- Stopping file logging 30
- Opening a log file 31
- Saving the screen log as a log file 31
- Switching between binary and text logging 30
- Manually rolling over the log file 31
- Converting a binary log file to a plain text log file 32

3.1 Setting the Log Preferences

The settings below set where System Monitor stores log files and how often it starts a new log file.

To set the log preferences

1. Click the **Log Preferences** . Alternatively, press ***Ctrl+L*** or click **File** and select **Logging Preferences**.



Log Mode
○ Periodic ○ Every 'n' Hours
● Daily ○ Every 'n' MBytes

Log Filename

☐ Binary Logging (Ctrl+B)

☐ Log to File (Ctrl+W)

2. Select the **Log Mode** required. This setting controls when System Monitor saves the current log and starts a new log file. This is called "rolling over the log file".

   - **Periodic**
     Only rollover the log when the icon is pressed. See Manually Rolling Over the Log File 31.

   - **Daily**
     Rollover the log automatically at the end of each day.

   - **Every 'n' Hours**
     Rollover the log automatically every few hours. When selected, System Monitor displays an **Hours Interval** box to set the number of hours between each rollover.

   - **Every 'n' MBytes**
     Rollover the log automatically when it reaches a set size. When selected, System Monitor displays a **MBytes Interval** box to set the size limit.

3. Set the log file name and location using the Log Filename field. The default location is the System Monitor application program folder ***C:\Program Files\Avaya\IP Office\Monitor***. Each time file log stops or rolls over, System Monitor adds the date and time to the log file name.

4. Select whether you want binary logging. To select a binary log, select **Binary Logging**.

   - **Binary format**
     This is the raw format of records as received from the system. The records are not processed in any way by System Monitor other than being added to the log file.

   - **Text format**
     This is the interpreted format of records. System Monitor adds additional information. For example, a record containing the raw entry ***pcol=6*** is changed to ***pcol=6 (TCP)***.

     - **Recommended Format**
       When logging in text format or running the screen log, it is possible for some records to be lost due to the high number of packets that System Monitor has to interpret. Running a binary log and pausing the System Monitor screen log reduces the chances of such lost packets.

5. To start logging to file immediately, select **Log to File**. If not selected, logging to file is started manually when required. See Starting Logging 30. When selected, System Monitor adds any records added to the screen log to the file log.

6. Click **OK**.

3.2 Starting File Logging

You can manually start logging to file if file logging is not already running.

To start logging to file:

1. Click the ✓ **Start Logging to File** icon. Alternatively, press ***Ctrl+W***.
2. The records are logged to file using the settings defined for the log preferences. See Setting the Log Preferences 29 .
3. The icon changes to a ☒ icon that can be used to stop logging. See Stopping Logging 30.

3.3 Stopping File Logging

You can stop the file logging at any time. When logging is stopped, the log file is saved in the folder specified in the log preferences with the date and time appended to the file name.

To stop logging to file:

1. Click the ☒ **Stop Logging to File** icon. Alternatively, press ***Ctrl+W***.
2. The icon changes to a ✓ icon that can be used to stop logging. See Stopping Logging 30.

3.4 Switching Between Binary and Text Logging

You can switch logging between using binary or text formats. Switching format automatically rolls over the current log file.

- **Binary format**
  This is the raw format of records as received from the system. The records are not processed in any way by System Monitor other than being added to the log file.
- **Text format**
  This is the interpreted format of records. System Monitor adds additional information. For example, a record containing the raw entry ***pcol=6*** is changed to ***pcol=6 (TCP)***.
  - **Recommended Format**
    When logging in text format or running the screen log, it is possible for some records to be lost due to the high number of packets that System Monitor has to interpret. Running a binary log and pausing the System Monitor screen log reduces the chances of such lost packets.

To switch to binary logging:

1. Click the B **Binary Logging** icon. Alternatively, press **Ctrl+B**.
2. Any current log is saved as a text log file and a new log in binary format started.
3. The icon changes to a T icon.

To switch to text logging:

1. Click the T **Text Logging** icon. Alternatively, press **Ctrl+B**.
2. Any current log is saved as a binary log file and a new log in text format started.
3. The icon changes to a B icon.

3.5 Opening a Log File

You can use System Monitor to view an existing log file. Opening a log file automatically pauses the display of the screen log from the connected system.

To open a log file:

1. Click the **Open File** icon. Alternatively, press ***Ctrl+O*** or click **File** and select **Open File**.
2. Browse to and select the log file. Text log files end in ***.txt***. Binary log files end in ***.mon***.
3. Click **Open**.
4. The file opens in the System Monitor view.

3.6 Saving the Screen Log as a Log File

You can save the records displayed in the screen log as a text file.

- **Converting a Binary Log File**
  Using this option to open a binary log file and then save it as a plain text log file can be problematic if System Monitor displays a very large number of records. If that is the reason a plain text file is require, see Converting a Binary Log to a Text Log 32.

To save the current screen log as a file:

1. Click the **Save Screen Log As** icon. Alternatively, press ***Ctrl+S*** or click **Files** and select **Save Screen Log as**.
2. Enter a file name for the file.
3. Click **Save**.

3.7 Manually Rolling Over the Log File

The logging preferences can automatically rollover the log file; creating a new log file daily, every few hours or after a certain amount of data. When this occurs, System Monitor saves the log file with the date and time added to the file name and starts a new log file. See Setting the Log Preferences 29.

You can force System Monitor to rollover the log file at anytime. You can do this even if System Monitor is already set to automatically rollover the file.

To manually rollover the log file:

1. Click **File** and select **Rollover Log**. Alternatively, press the **Rollover Log** icon or press ***Ctrl+R***.
2. System Monitor saves the existing log file and starts a new log file.

3.8 Converting a Binary Log to a Text Log

You can use System Monitor to view binary log files (.mon files). However, it may sometimes be necessary to create a plain text copy of the log file. For example, so that it can be viewed in other applications.

- **Why not use Files | Save As**
  While you can save the current screen log to a text file 31 at any time, this can be potentially problematic if a very large number of records have been displayed. That would typically apply when a large binary log file is loaded. While the method below is more complex, it ensures that no records are lost.

To convert a binary log file to a plain text log file:

1. Start System Monitor.

2. Clear the current screen log:

   a. If logging to screen, click the **Freeze Screen Logging** icon. Alternatively, press ***Ctrl+G***.

   b. Clear any existing contents in the screen log by clicking the **Clear Display** icon. Alternatively, press **Ctrl+X** .

3. Configure System Monitor to a non existent IP address.

   a. Click the **Select Unit** icon. Alternatively, press **Ctrl+U**.

   b. Enter an IP address that is not used.

   c. Click **OK**.

4. Set System Monitor to capture the screen log records as they appear into a plain text log file.

   a. Click the **Log Preferences** icon. Alternatively, press ***Ctrl+L*** or click **File** and select **Logging Preferences**.

   b. Set the **Log Mode** to ***Daily***.

   c. Ensure the **Binary Logging** is not selected.

   d. Select the **Log to File** option.

   e. Click **OK**.

5. Open the binary log file:

   a. Click the **Open File** icon. Alternatively, press ***Ctrl+O*** or click **File** and select **Open File**.

   b. Browse to and select the log file.

   c. Click **Open**.

   d. The file opens in the screen log.

6. Due to the log preferences selected above, as System Monitor adds each binary log file record to the screen log, it also write the record into a plain text log file.

7. Once the binary log file has been fully loaded, rollover the log file.

   a. Click the **Rollover Log** icon. Alternatively, press ***Ctrl+R*** or click **File** and select **Rollover Log**

Chapter 4.
Setting the Trace Options

4. Setting the Trace Options

The trace options set which records System Monitor receives from the connected system. The settings affect both the screen log and logging to file.

4.1 Setting the Trace Options

To set the trace options

1. Click the **Trace Options** icon. Alternatively, press **Ctrl+T** or click **Filters** and select **Trace options**.
2. Click the setting to enable or disable it.
3. Click **OK**.

4.2 Saving Trace Options as a File

The current set of trace options can be exported to an .ini file. You can then reload the settings from that file at a later time or send them to another user to set the trace options of their application. See Loading Trace Options from a File 35.

- **Note**
  System Monitor does not save trace option colour settings as part of the trace options file.

To export the trace options:

1. Click the **Trace Options** icon. Alternatively, press **Ctrl+T** or click **Filters** and select **Trace options**.
2. Select **Save File**.
3. Enter the name for the file and select the location. Alternatively, select an existing file to overwrite.
4. Click **Save**.

4.3 Loading Trace Options from a File

You can import a previously saved set of trace options. See Saving Trace Options as a File 35.

To load a set of trace options:

1. Click the **Trace Options** icon. Alternatively, press **Ctrl+T** or click **Filters** and select **Trace options**.
2. Select **Load File**.
3. Locate and select the file to load.
4. Click **Open**.

4.4 Colouring Individual Trace Options

You can select a colour for a particular type of trace option. System Monitor then applies that colour to any matching records when added to the screen log.

To apply a colour to a trace option:

1. Click the **Trace Options** icon. Alternatively, press **Ctrl+T** or click **Filters** and select **Trace options**.
2. Select the tab showing the trace option for which you require a specific colour.
3. Right click on the name of the trace option.
4. Select the required colour.
5. Click **OK**.
6. System Monitor displays the trace option name in the selected colour.

4.5 Colouring Tab Trace Options

For some tabs, in addition to applying colours to individual trace options (see Colouring Individual Trace Options 36), a single colour selection can be used to apply a colour to all trace options on the tab. This selection overrides any existing individual trace option colour selections, however those selections can be reapplied.

To colour the tab trace options:

1. Click the **Trace Options** icon. Alternatively, press **Ctrl+T** or click **Filters** and select **Trace options**.
2. Select the tab. The Call 41, H.323 50 and System 69 tabs support this option.
3. Click on **Trace Colour**.
4. Select the required colour and
5. Click **OK**.

4.6 Clearing a Trace Options Tab

You can clear all the currently selected trace options on the currently displayed trace options tab.

To clear the current trace options tab:

1. Click the **Trace Options** icon. Alternatively, press **Ctrl+T** or click **Filters** and select **Trace options**.
2. Select the tab that you want to clear.
3. Click **Tab Clear All**.

4.7 Setting a Trace Options Tab

You can set all the options on the currently displayed trace options tab.

To clear the current trace options tab:

1. Click the **Trace Options** icon. Alternatively, press **Ctrl+T** or click **Filters** and select **Trace options**.
2. Select the tab on which you want to set all the options.
3. Click **Tab Set All**.

4.8 Clearing All the Trace Options

You can clear all selected trace options.

To clear all trace options:

1. Click the **Trace Options** icon. Alternatively, press **Ctrl+T** or click **Filters** and select **Trace options**.
2. Click **Clear All**.
3. System Monitor displays a warning. To continue with the defaulting, click **Yes**.

4.9 Defaulting the Trace Options

You can default the trace options. This defaults both the selected trace options and the trace option colour settings.

To default all the trace options:

1. Click the **Trace Options** icon. Alternatively, press **Ctrl+T** or click **Filters** and select **Trace options**.
2. Click **Default All**.
3. System Monitor displays a warning. To continue defaulting the trace options, click **Yes**.

The Default Trace Options

Trace Options Tab	Default Selected Trace Options
ATM	• *None*
Call	• **Call**, **Call Delta**, **Call Logging**, **Extension**, **Targeting**, **ARS**, **LRQ,** **Extension Send**, **Extension Receive**, **Extension TxP**, **Extension RxP**, **Line Send**, **Line Receive**.
Directory	• *None*
DTE	• *None*
EConf	• *None*
Frame Relay	• **Frame Relay Events**, **Management Events**.
GOD	• *None*
H.323	• **H.323**
Interface	• **Interface Queue**, **TCP**, **UDP**, **ARP**, **MultiCast**.
ISDN	• **Layer 1**, **Layer 2**, **Layer 3**.
Jade	• *None*
Key/Lamp	• *None*
Media	• **Map**.
PPP	• **Err Msg**
R2	• **CAS**, **Channel**, **Dialler**, **DSP**, **Line**.
Routing	• *None*
SCN	• *None*
Services	• *None*
SIP	• **SIP Rx**, **SIP Tx**.
System	• **Error**, **Print**, **Prefix YYYY-MM-DD hh:mm:ss:mss**, **Resource Status Prints**, **Licencing**.
T1	• *None*
VPN	• **SSL VPN: Session** and **Session State**.
WAN	• **WAN Events**.

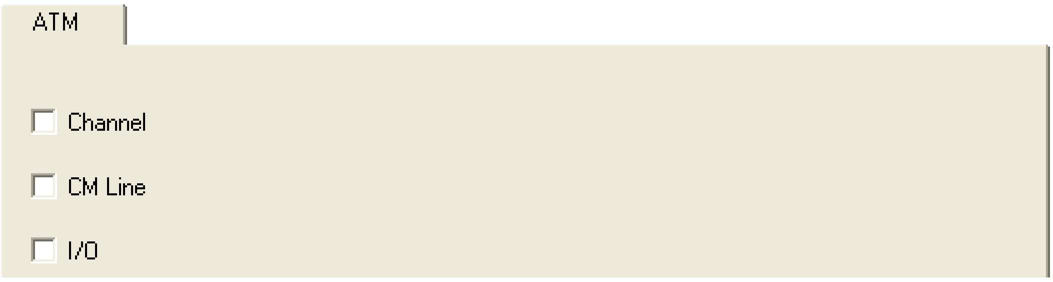
4.10 Trace Option Menus

The trace options are grouped onto the following tabs:

- **ATM** 40
  Monitor analog trunk traffic and events.
- **Call** 41
  Monitoring of extensions and calls.
- **Directory** 44
  Monitor LDAP traffic and events.
- **DTE** 45
  Monitoring of the system's DTE port.
- **EConf** 47
  Monitor IP Office Conferencing Center events.
- **Frame Relay** 48
  Monitor Frame Relay traffic and events.
- **GOD** 49
  Monitor messages between the modules in a system.
- **H.323** 50
  Monitoring of H.323 VoIP calls.
- **Interface** 52
  Monitoring IP data interfaces such as NAT and the Firewall.
- **ISDN** 54
  Monitor ISDN traffic and events.
- **Jade** 56
  For Linux based systems, monitor the call media services.
- **Key/Lamp** 57
  Monitor appearance functions.
- **Media** 58
  Monitor the media support provided by the system.
- **PPP** 59
  Monitor PPP traffic and events.
- **R2** 61
  Monitor R2 trunk traffic and events.
- **Routing** 62
  Monitor IP traffic and events.
- **SCN** 64
  Monitor Small Community Network traffic and information.
- **Services** 65
  Monitor SNMP alarms events.
- **SIP** 67
  Monitor SIP trunks and connections.
- **SSI** 68
  Monitor the system's SSI connections.
- **System** 69
  Monitor internal events.
- **T1** 70
  Monitor T1 traffic and events.
- **VComp** 72
  Monitor the system's voice compression channels.
- **VPN** 74
  Monitor VPN events.
- **WAN** 76
  Monitor WAN traffic and events.

4.10.1 ATM

This tab provides trace options for monitoring the system's analog trunks.



ATM

□ Channel

□ CM Line

□ I/O

- **Channel**
  If selected, this option logs information relating to the Analog Trunk state machine.
- **CM Line**
  If selected, this option logs information relating to the interaction between the Line Handler and the Call Manager (CM).
- **I/O**
  If selected, this option logs events on the Line or in the DSP.

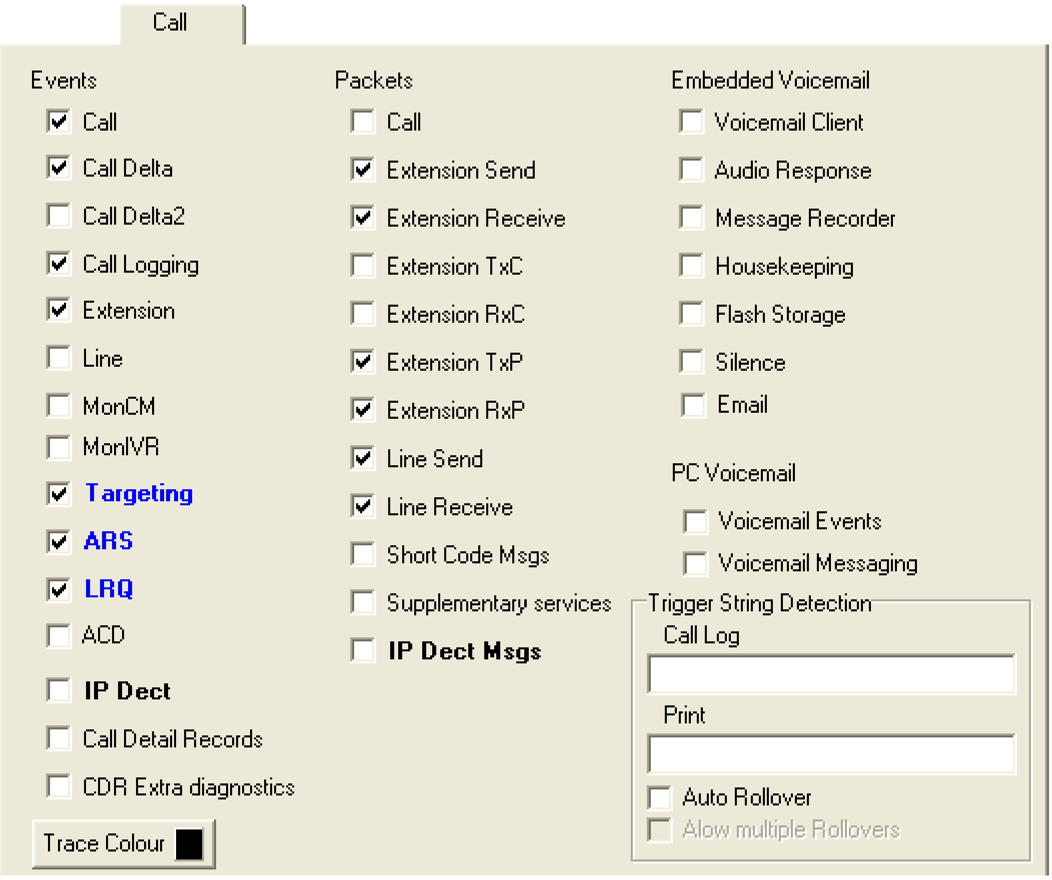
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- *None*.

4.10.2 Call

This tab provides trace options for monitoring the system's calls including the use of voicemail.



Call

Events
- ☑ Call
- ☑ Call Delta
- ☐ Call Delta2
- ☑ Call Logging
- ☑ Extension
- ☐ Line
- ☐ MonCM
- ☐ MonIVR
- ☑ Targeting
- ☑ ARS
- ☑ LRQ
- ☐ ACD
- ☐ IP Dect
- ☐ Call Detail Records
- ☐ CDR Extra diagnostics

Trace Colour ■

Packets
- ☐ Call
- ☑ Extension Send
- ☑ Extension Receive
- ☐ Extension TxC
- ☐ Extension RxC
- ☑ Extension TxP
- ☑ Extension RxP
- ☑ Line Send
- ☑ Line Receive
- ☐ Short Code Msgs
- ☐ Supplementary services
- ☐ IP Dect Msgs

Embedded Voicemail
- ☐ Voicemail Client
- ☐ Audio Response
- ☐ Message Recorder
- ☐ Housekeeping
- ☐ Flash Storage
- ☐ Silence
- ☐ Email

PC Voicemail
- ☐ Voicemail Events
- ☐ Voicemail Messaging

Trigger String Detection

Call Log

Print

- ☐ Auto Rollover
- ☐ Allow multiple Rollovers

Events

- **Call**
  If selected, this option logs changes of state for the call (Aend and Bend).

- **Call Delta**
  If selected, this option logs information on general call state changes.

- **Call Delta2**

- **Call Logging**
  If selected, this option logs ACD status messages, CALL message giving statistics of call and SERVICE message giving statistics of service.

- **Extension**
  If selected, this option logs changes of state for the extension plus console print on setting bchan.

- **Extension Cut**
  If selected, this option logs changes of 'cut' state for the extension (mapping connections).

- **Line**
  Currently this option does not provide any trace messages. It is included for possible future use only.

- **MonCM**
  If selected, this option logs all received call control messages (NOT Short Code messages) and some additional console print messages - adjustcount, ringback.

- **MonIVR**
  If selected, this option logs up to date information on the messages in a user’s voicemail box.

- **Targeting**
  If selected, this option logs information concerning call routing (targeting).

- **ARS**

- **LRQ**

- **ACD**

- **IP Dect**

- **Call Detail Records**

- **CDR Extra Diganostics**

Packets

- **Call**
  If selected, this option logs all received call control messages and contents.

- **Extension Send**
  If selected, this option logs all call control messages and contents transmitted to an extension.

- **Extension Receive**
  If selected, this option logs all call control messages and contents received from an extension.

- **Extension TxC**
  If selected, this option logs all call control messages and contents transmitted to the call object. Note: this message is actually received from the extension.

- **Extension RxC**
  If selected, this option logs all call control messages and contents received from the call object. Note: this message is actually sent to the extension.

- **Extension TxP**
  If selected, this option logs all call control messages and contents transmitted to a partner (eg. phone manager). Also enables ***CMExtnCopyProcessMsg***, ***CMExtnCopyProcessCallMsg***, ***CMExtnConfCopyProcessCallMsg***, ***CMExtnCopySendCallMsg*** and ***CMExtnCopyCallLostMsg*** messages.

- **Extension RxP**
  If selected, this option logs all call control messages and contents received from a partner application such as IP Office SoftConsole or Phone Manager.

- **Line Send**
  If selected, this option logs all call control messages and contents sent to a line. Also enables ***CMCallReleaseStart***, ***CMCallReleaseEnd*** and ***CMCallLostRecord Timeout*** messages.

- **Line Receive**
  If selected, this option logs all call control messages and contents received from a line. Also enables Incoming ***Call Waiting***, ***CallRefused Incoming Blocked*** and ***CallRefused*** because channels are in use messages.

- **Short Code Msgs**
  If selected, this option logs short code messages associated with the selected **Extension Send**, **Extension Receive** and **MonCM** trace options.

- **Supplementary services**

- **IP Dect Msgs**

Embedded Voicemail

- **Voicemail Client**
- **Audio Response**
- **Message Recorder**
- **Housekeeping**
- **Flash Storage**
- **Silence**
- **Email**

PC Voicemail

- **Voicemail Events**
- **Voicemail Messaging**

Trigger String Detection

These options are only available when the **Development Tracing** option is selected in the **Trace Options | System** 69 menu. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

- **Call Log**
- **Print**
- **Auto Rollover**
- **Allow Multiple Rollovers**

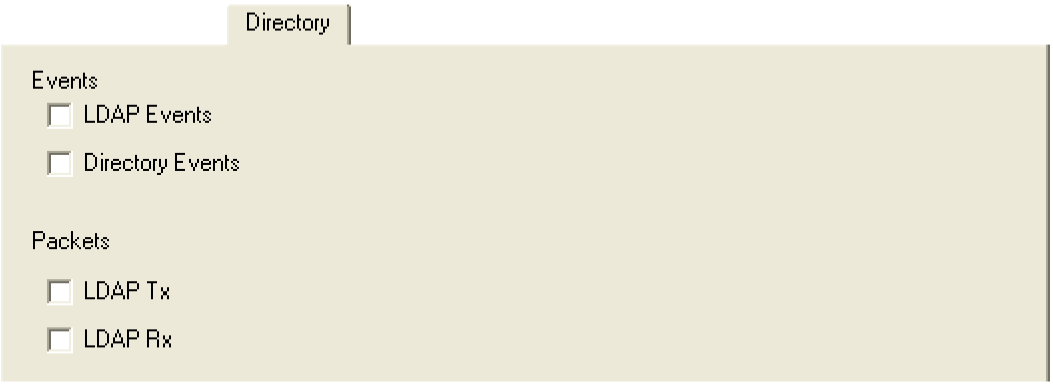
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- **Call**, **Call Delta**, **Call Logging**, **Extension**, **Targeting**, **ARS**, **LRQ,** **Extension Send**, **Extension Receive**, **Extension TxP**, **Extension RxP**, **Line Send**, **Line Receive**.

4.10.3 Directory

This tab provides trace options for monitoring the system's directory requests.



Directory

Events

□ LDAP Events

□ Directory Events

Packets

□ LDAP Tx

□ LDAP Rx

Events

- **LDAP Events**
  If selected, this option logs information on the status of the system’s LDAP "software" state machine and associated events.

Packets

Use the following options with caution as they produce a prolific amount of records. For both, if **Packets In** (see Interface 52) is also selected, System Monitor also adds the packet information to the end of a packet.

- **LDAP Tx**
  If selected, this option logs a breakdown of any transmitted LDAP data packets.
- **LDAP Rx**
  If selected, this option logs a detailed breakdown of any received LDAP data packets.

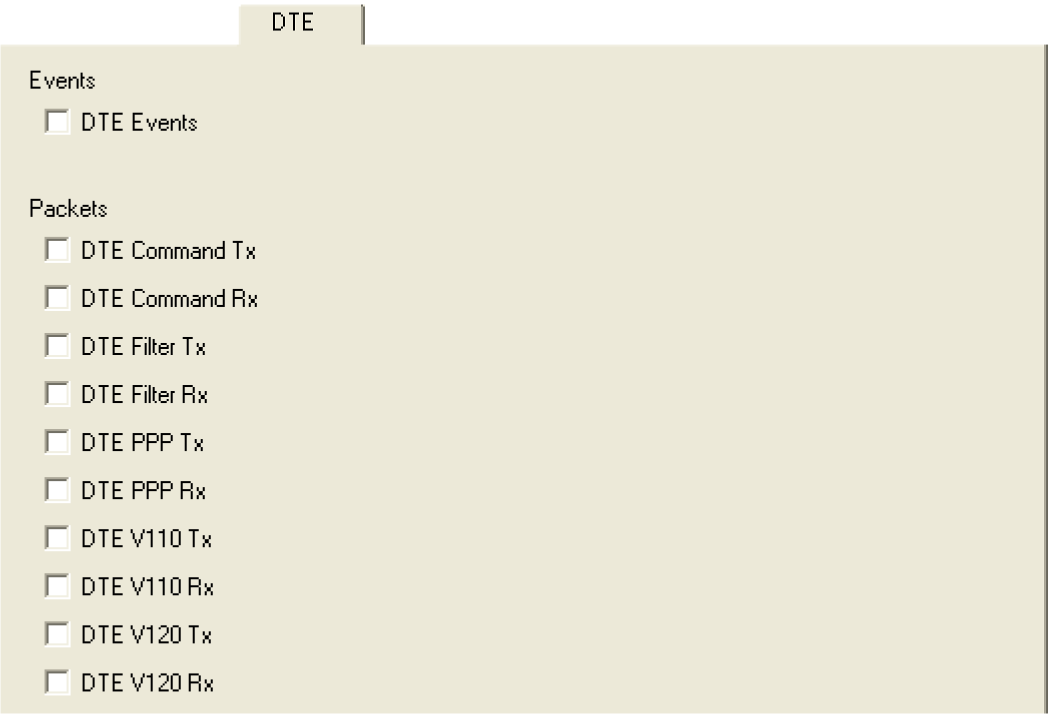
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- *None*.

4.10.4 DTE

This tab provides trace options for monitoring the system's DTE port.



DTE

Events

□ DTE Events

Packets

□ DTE Command Tx

□ DTE Command Rx

□ DTE Filter Tx

□ DTE Filter Rx

□ DTE PPP Tx

□ DTE PPP Rx

□ DTE V110 Tx

□ DTE V110 Rx

□ DTE V120 Tx

□ DTE V120 Rx

Events

- **DTE Events**
  If selected, this option logs on the status of Flow Control, Modem Controls (DTR, DCD, etc), Baud Rate changes on the DTE port, etc.

Packets

- **DTE Command Tx**
  If selected, this option logs the Hayes AT commands send out of the DTE interface.

- **DTE Command Rx**
  If selected, this option logs the Hayes AT commands received from the DTE interface.

- **DTE Filter Tx**
  If selected, this option logs serial data transmitted out of the DTE interface once connected.

- **DTE Filter Rx**
  If selected, this option logs serial data received from the DTE interface once connected.

- **DTE PPP Tx**
  If selected, this option logs Framed PPP packets Transmitted to the DTE interface if the Hayes ATB0 option is set on the port.

- **DTE PPP Rx**
  If selected, this option logs Framed PPP packets received from the DTE interface if the Hayes ATB0 option is set on the port.

- **DTE V110 Tx**
  If selected, this option logs Framed V.110 packets received from the DTE interface if the Hayes ATB3 option is set on the port.

- **DTE V110 Rx**
  If selected, this option logs Framed V.110 packets received from the DTE interface if the Hayes ATB3 option is set on the port.

- **DTE V120 Tx**
  If selected, this option logs Framed V.120 packets received from the DTE interface if the Hayes ATB2 option is set on the port.

- **DTE V120 Rx**
  If selected, this option logs Framed V.120 packets received from the DTE interface if the Hayes ATB2 option is set on the port.

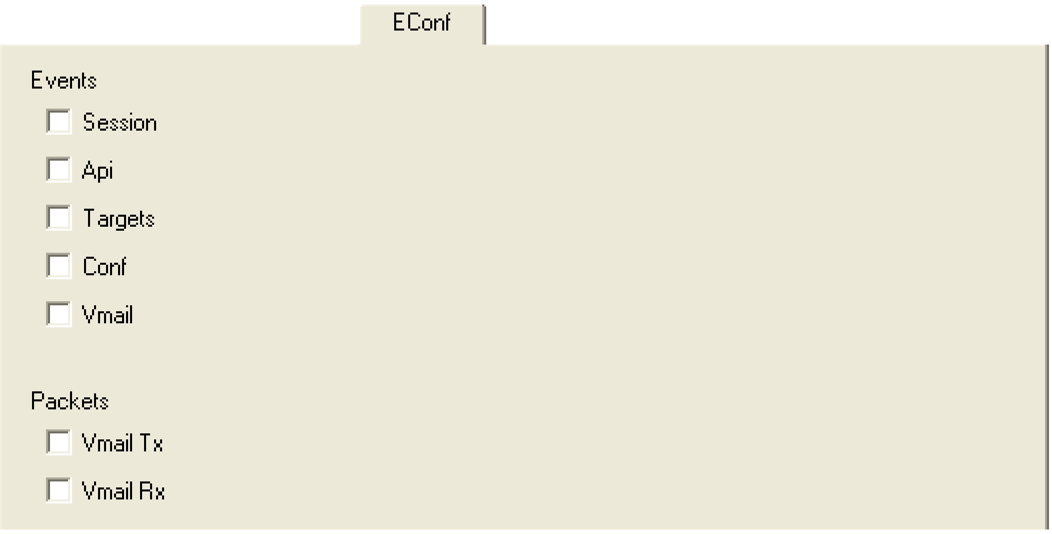
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- *None*.

4.10.5 EConf

This tab provides trace options for monitoring the IP Office Conferencing Center application.



Events

□ Session

□ Api

□ Targets

□ Conf

□ Vmail

Packets

□ Vmail Tx

□ Vmail Rx

Events

- **Session**
  If selected, this option logs incoming and outgoing messages to/from the conferencing server. It also shows the session being established between the system and the conferencing server.

- **Api**
  If selected, this option logs state changes of the various EConf resources used.

- **Targets**
  If selected, this option logs the targeting information, as calls try to enter an enhanced conference.

- **Conf**
  If selected, this option logs events happening to ***CMConference*** object. It displays information on the creation/deletion of conferences, as well as calls being added/removed.

- **Vmail**
  If selected, this option logs information on the call as it arrives at the system from the voicemail server. It displays the GUID's that the server has given for the calls transfer into the conference and it shows the voicemail server making announcements into the conference.

Packets

- **Vmail Tx**
  If selected, this option logs messages which show the contents of IP packets transmitted to the voicemail server that are specifically associated with the IP Office Conferencing Centre.

- **Vmail Rx**
  If selected, this option logs messages which show the contents of IP packets received from the voicemail server that are specifically associated with the IP Office Conferencing Centre.

Report

- **Report**
  The **Report** button gives an instant snapshot of the state of all the resources in the EConf system. It shows what states all the EConferences and EChannels are in, and what CMConferences and CMCalls are associated with them at that time. It also shows you how many free reserved resources are available. When this button is clicked, a series of PRN: traces are output to the log. Note that the **Print** 69 option must be enabled.

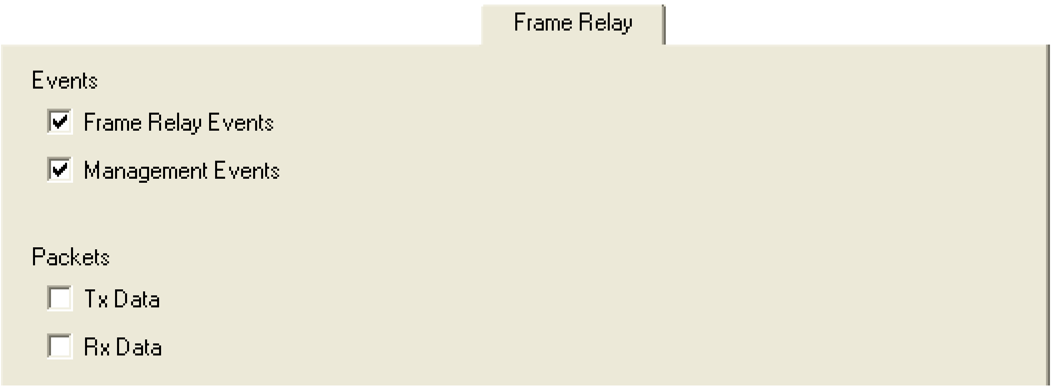
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- *None*.

4.10.6 Frame Relay

This tab provides trace options for monitoring the system's frame relay services.



Frame Relay

Events

☑ Frame Relay Events

☑ Management Events

Packets

□ Tx Data

□ Rx Data

Events

- **Frame Relay Events**
  If selected, this option logs Frame Relay events be it data in, data out, management, status etc.

- **Management Events**
  If selected, this option logs Management events/packets, ie. SE/FSE packets and management status.

Packets

- **Tx Data**
  If selected, this option logs transmitted packets on a Frame Relay link - both data & management.

- **Rx Data**
  If selected, this option logs received packets on a Frame Relay link - both data & management.

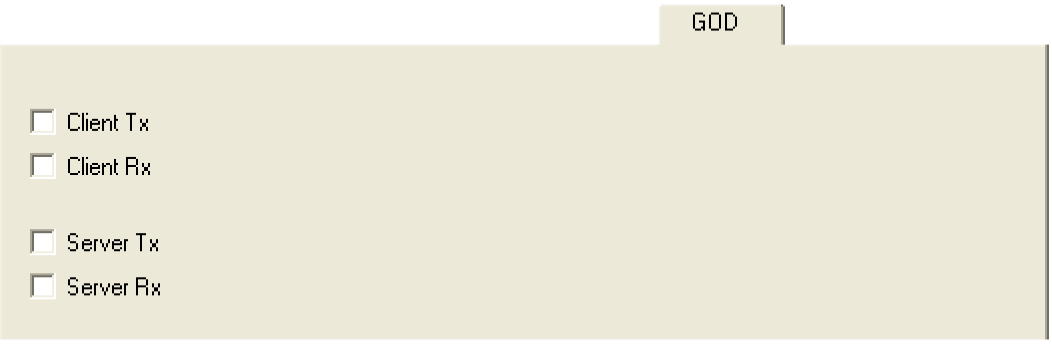
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- **Frame Relay Events**, **Management Events**.

4.10.7 GOD

This tab provides trace options for monitoring the system's communications between individual modules.



□ Client Tx

□ Client Rx

□ Server Tx

□ Server Rx

- **Client Tx**
  If selected, this option logs Inter-Unit protocol messages sent by the unit, other those from the Gatekeeper.
- **Client Rx**
  If selected, this option logs Inter-Unit protocol messages received by the unit, other those to the Gatekeeper.
- **Server Tx**
  If selected, this option logs Inter-Unit protocol messages sent by the Gatekeeper.
- **Server Rx**
  If selected, this option logs Inter-Unit protocol messages received by the Gatekeeper.

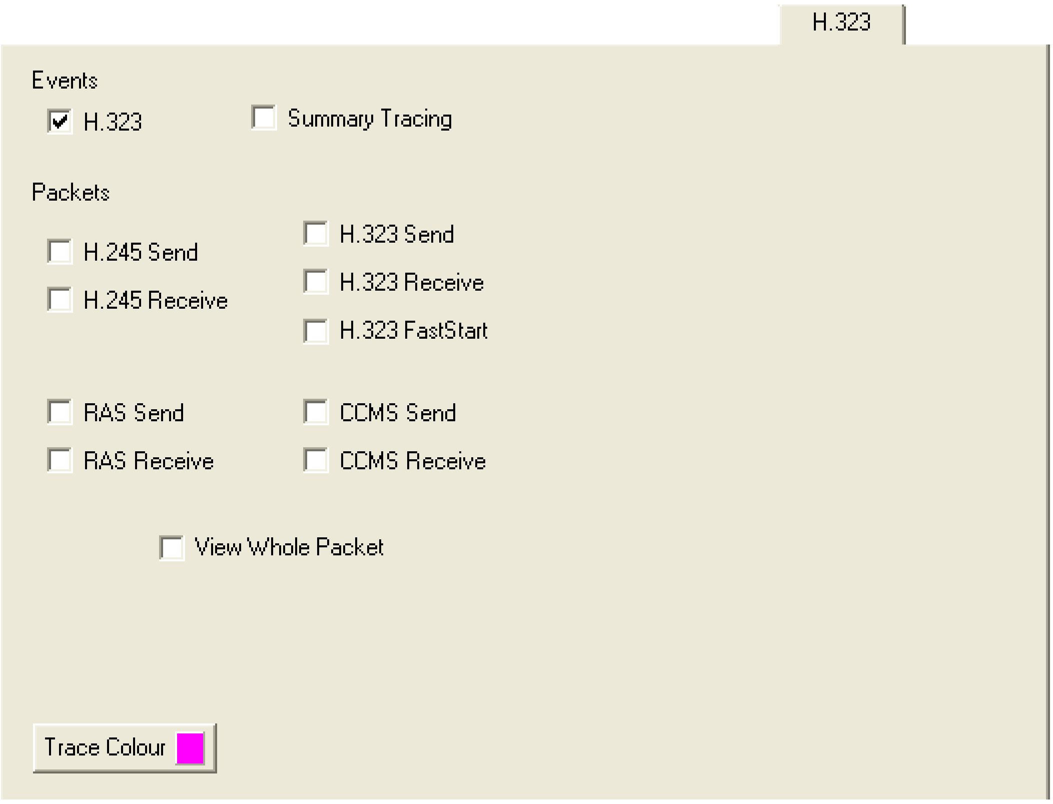
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- *None*.

4.10.8 H.323

This tab provides trace options for monitoring H.323 and H.245 events related to VoIP calls.



H.323

Events

☑ H.323 □ Summary Tracing

Packets

□ H.245 Send □ H.323 Send

□ H.245 Receive □ H.323 Receive

□ H.323 FastStart

□ RAS Send □ CCMS Send

□ RAS Receive □ CCMS Receive

□ View Whole Packet

Events

- **H.323**
  If selected, this option logs the state changes of the H.323 call.

Packets

- **H.245 Send**
  If selected, this option logs H.245 messages sent to an H.323 endpoint (IP phone or IP trunk).
- **H.245 Receive**
  If selected, this option logs H.245 messages received from an H.323 endpoint (IP phone or IP trunk).
- **H.323**
  If selected, this option logs the state changes of the H.323 call.
- **H.323 Send**
  If selected, this option logs the H.323 messages sent to an H.323 endpoint (IP phone or IP trunk).
- **H.323 Receive**
  If selected, this option logs H.323 messages received from an H.323 endpoint (IP phone or IP trunk).
- **H.323 Fast Start**
  If selected, this option logs H.323 fast-start messages send to/received from an H.323 endpoint (IP phone or IP trunk).
- **RAS Send**
  If selected, this option logs RAS (registration, admission and status) messages sent to an IP phone.
- **RAS Receive**
  If selected, this option logs RAS messages received from an IP phone.
- **CCMS Send**
  If selected, this option logs the CCMS (Control Channel Message Set) messages sent to an H.323 endpoint (IP phone or IP trunk).
- **CCMS Receive**
  If selected, this option logs CCMS messages received from an H.323 endpoint (IP phone or IP trunk).
- **View Whole Packet**
  If selected, the full H.323 message is decoded and included in the trace. If not selected, the trace only includes the first two lines of the H.323 message.

Default Settings

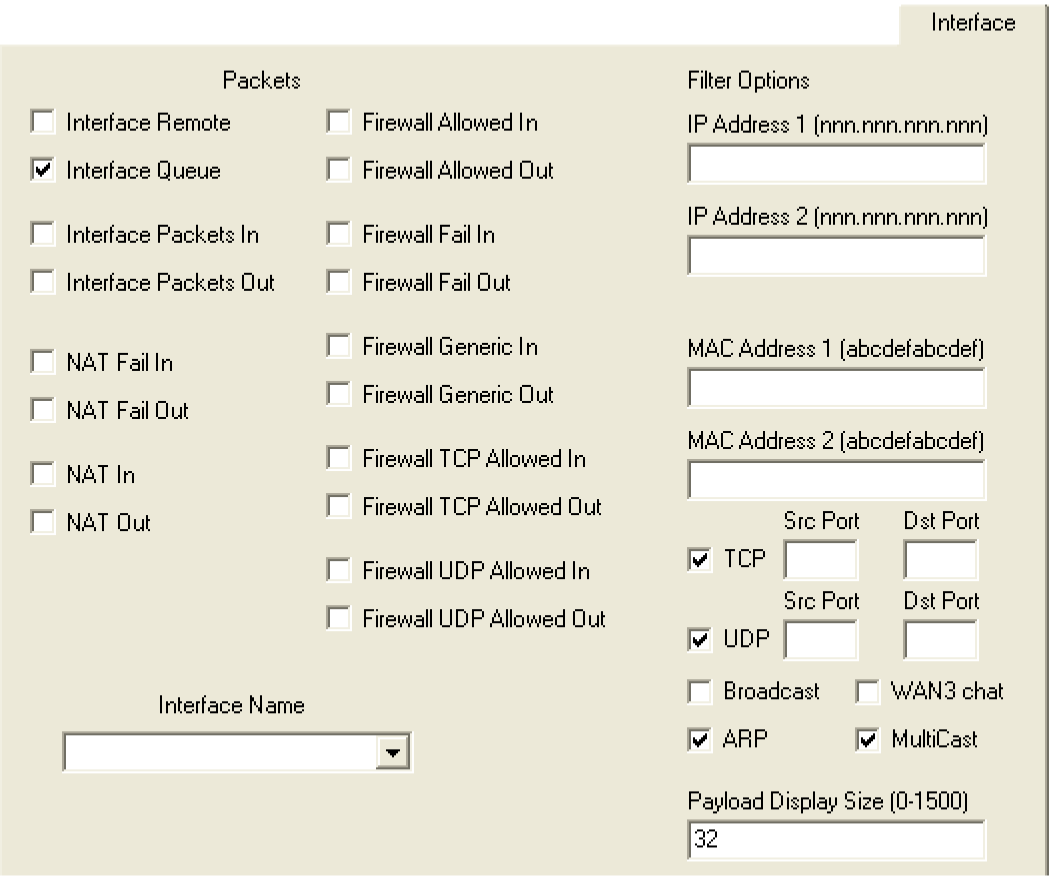
The following trace options are enabled by default (see Defaulting the Trace Options 38):

The default settings also apply the colour pink to the whole tab.

- **H.323**

4.10.9 Interface

This tab provides trace options for monitoring the system's data network interfaces. An interface can be a physical interface like a LAN port or a configuration interface, like a data connection to a remote system or a Dial-In User.



Packets

- ☐ Interface Remote
- ☑ Interface Queue
- ☐ Interface Packets In
- ☐ Interface Packets Out
- ☐ NAT Fail In
- ☐ NAT Fail Out
- ☐ NAT In
- ☐ NAT Out
- ☐ Firewall Allowed In
- ☐ Firewall Allowed Out
- ☐ Firewall Fail In
- ☐ Firewall Fail Out
- ☐ Firewall Generic In
- ☐ Firewall Generic Out
- ☐ Firewall TCP Allowed In
- ☐ Firewall TCP Allowed Out
- ☐ Firewall UDP Allowed In
- ☐ Firewall UDP Allowed Out

Interface Name:

Filter Options

IP Address 1 (nnn.nnn.nnn.nnn):

IP Address 2 (nnn.nnn.nnn.nnn):

MAC Address 1 (abcdefabcdef):

MAC Address 2 (abcdefabcdef):

☑ TCP Src Port: Dst Port:

☑ UDP Src Port: Dst Port:

☐ Broadcast ☐ WAN3 chat

☑ ARP ☑ MultiCast

Payload Display Size (0-1500): 32

Packets

- **Interface Remote**
  If selected, this option logs traffic tunneled through to any externally connected WAN3 modules.

- **Interface Queue**
  If selected, this option logs packets being queued at an interface. Especially useful for determining what packet, and therefore which IP address on the internal network, caused an outgoing data call to be made.

The following trace options provide information on either the whole system or on the specific interface specified in the **Interface Name** field, see below.

- **Interface Packets In**
  If selected, this option logs all packets received.

- **Interface Packets Out**
  If selected, this option logs all packets transmitted.

- **NAT Fail In**
  If selected, this option logs all NAT (Network Address Translation) packets received that have failed to pass through the firewall

- **NAT Fail Out**
  If selected, this option logs all NAT (Network Address Translation) packets transmitted that have failed to pass through the firewall.

- **NAT In**
  If selected, this option logs all NAT (Network Address Translation) packets received.

- **NAT Out**
  If selected, this option logs all NAT (Network Address Translation) packets transmitted.

- **Firewall Allowed In**
  If selected, this option logs all packets received that have successfully passed through the firewall.

- **Firewall Allowed Out**
  If selected, this option logs all packets transmitted that have successfully passed through the firewall.

- **Firewall Fail In**
  If selected, this option logs all packets received that have failed to pass through the firewall.

- **Firewall Fail Out**
  If selected, this option logs all packets transmitted by the system that have failed to pass through the firewall.

- **Firewall Generic In**
  If selected, this option logs all packets received (except UDP, TCP and ICMP) that have successfully passed through the firewall.

- **Firewall Generic Out**
  If selected, this option logs all packets transmitted (except UDP, TCP and ICMP) that have successfully passed through the firewall.

- **Firewall TCP Allowed In**
  If selected, this option logs all TCP packets received that have successfully passed through the firewall.

- **Firewall TCP Allowed Out**
  If selected, this option logs all TCP packets transmitted that have successfully passed through the firewall.

- **Firewall UDP Allowed In**
  If selected, this option logs all UDP packets received that have successfully passed through the firewall.

- **Firewall UDP Allowed Out**
  If selected, this option logs all UDP packets transmitted that have successfully passed through the firewall.

- **Interface Name**
  This option can be used to limit the information shown for the fields above to those associate with a selected service. A blank entry matches all services.

Filters

These options are used in conjunction with the other options on the tab to limit the number of packets displayed or to display packets from a range of devices.

- **IP Address 1**
  If set, only packets to and from the IP address are logged.

- **IP Address 2**
  If set, this field is used in conjunction with **IP Address 1** to display only packets between the pair of addresses.

- **MAC Address 2**
  If set, only packets to and from the MAC are logged.

- **MAC Address 2**
  If set, this field is used in conjunction with **MAC Address 1** to display only packets between the pair of MAC addresses.

- **TCP**
  - **Src Port**
  - **Dst Port**

- **UDP**
  - **Src Port**
  - **Dst Port**

- **Broadcast**
  If set, this option logs all broadcast packets except ARP broadcasts.

- **WAN3 chat**
  This option allows you to filter out the continuous dialogue which takes place between an system's control unit and an associated WAN3 module.

- **ARP**
  If selected, this option logs ARP packets.

- **MultiCast**
  If selected, this option logs MultiCast packets (i.e. packets with either a source or destination address of 224.0.0.0).

- **Payload Display Size**
  This option limits the size of the IP packet displayed. Displayed payload can be set to anything between 0 and 1500 bytes. The default setting is 32 bytes.

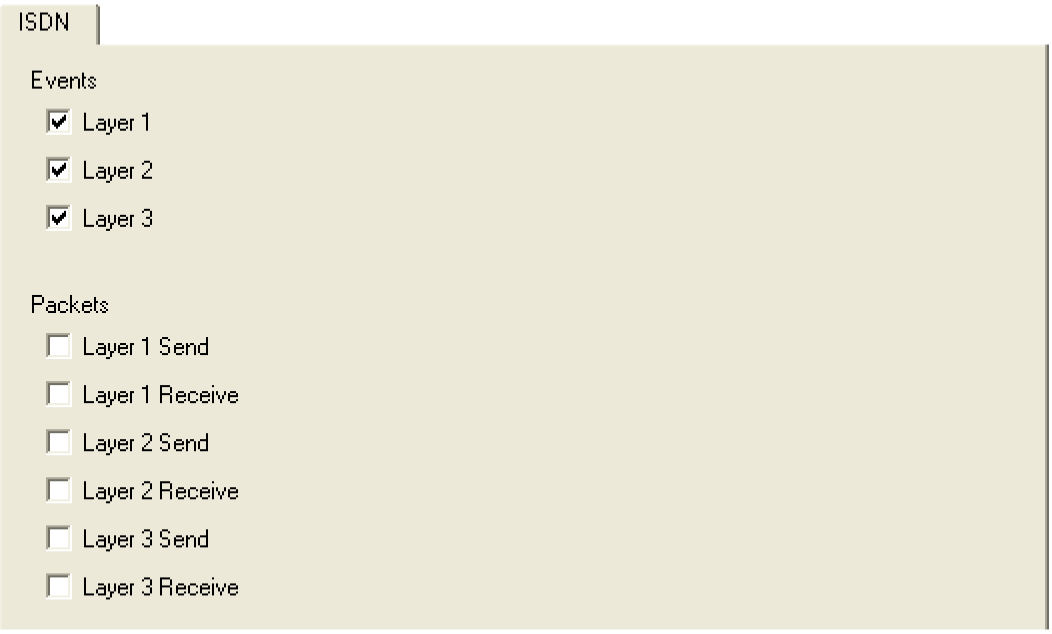
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- **Interface Queue**, **TCP**, **UDP**, **ARP**, **MultiCast**.

4.10.10 ISDN

This tab provides trace options for monitoring the system's ISDN digital trunks (BRI and PRI).



ISDN

Events

☑ Layer 1

☑ Layer 2

☑ Layer 3

Packets

□ Layer 1 Send

□ Layer 1 Receive

□ Layer 2 Send

□ Layer 2 Receive

□ Layer 3 Send

□ Layer 3 Receive

Events

- **Layer 1**
  If selected, this option logs information on the status of the system’s ISDN Layer 1 software state machine and associated events.
- **Layer 2**
  If selected, this option logs information on the status of the system’s ISDN Layer 2 software state machine and associated events.
- **Layer 3**
  If selected, this option logs information on the status of the system’s ISDN Layer 3 software state machine and associated events.

Packets

- **Layer 1 Send**
  If selected, this option logs the actual data packets transmitted at the ISDN Layer 1 level.
- **Layer 1 Receive**
  If selected, this option logs the actual data packets received at the ISDN Layer 1 level.
- **Layer 2 Send**
  If selected, this option logs the actual data packets transmitted at the ISDN Layer 2 level.
- **Layer 2 Receive**
  If selected, this option logs the actual data packets received at the ISDN Layer 2 level.
- **Layer 3 Send**
  If selected, this option logs the actual data packets transmitted at the ISDN Layer 3 level.
- **Layer 3 Receive**
  If selected, this option logs the actual data packets received at the ISDN Layer 3 level.

Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- **Layer 1**, **Layer 2**, **Layer 3**.

The following messages are output when ISDN/Events/Layer1 are selected:

```
ISDNL1Evt: v=[line_no.] peb=[hardware device no.], [new state] [old state]
```

where the state values shown are:

Value	Definition
F1	Inactive.
F2	Sensing.
F3	Deactivated.
F4	Awaiting signal.
F5	Identifying input.
F6	Synchronised.
F7	Activated.
F8	Lost framing.

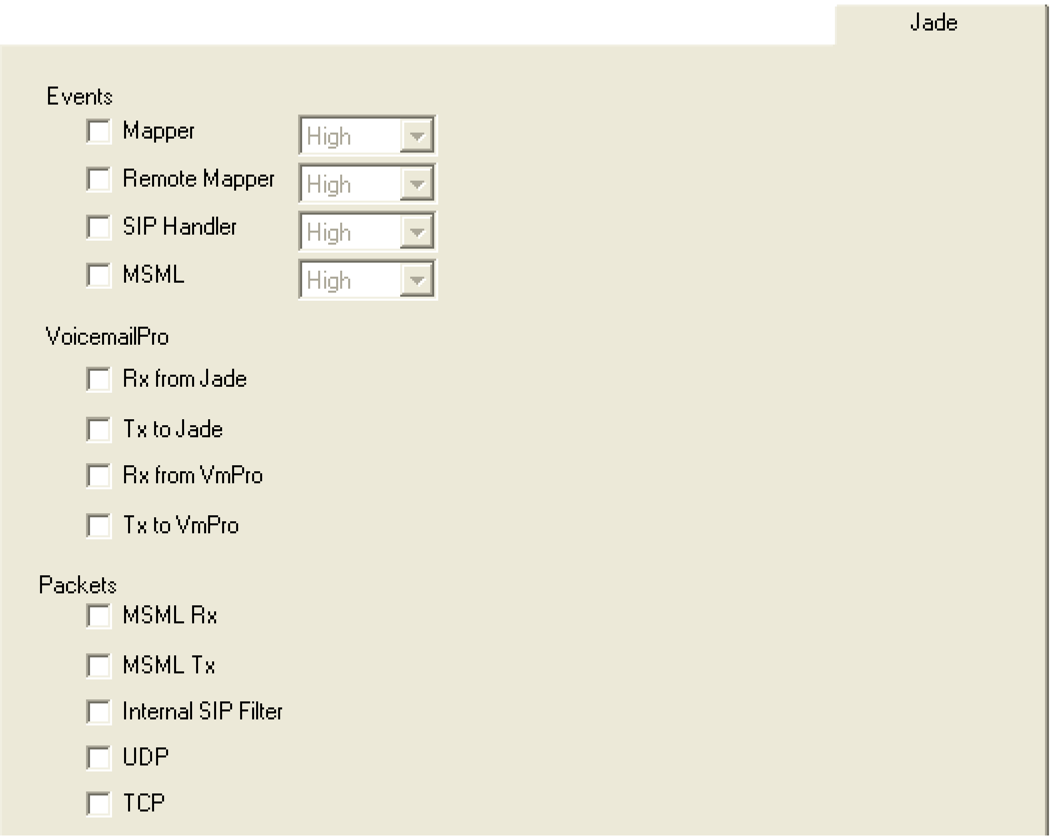
```
ISDNL1Evt: v=[line_no.] peb=[hardware device no.], [message]
```

where message value are:

Value	Definition
PHAI	Physical Activate Indication (i.e. Line is UP)
PHDI	Physical Deactivate Indication (Line is DOWN)
T3TO	T3 timeout has occurred
TxErr	A Transmit error has occurred
UnLocked	The system is not able to lock its clock to this line
Locked	The system and the clock extracted from this line are locked together.

4.10.11 Jade

This tab provides trace options for monitoring the Jade service used by Linux base systems.



Jade

Events

- □ Mapper High
- □ Remote Mapper High
- □ SIP Handler High
- □ MSML High

VoicemailPro

- □ Rx from Jade
- □ Tx to Jade
- □ Rx from VmPro
- □ Tx to VmPro

Packets

- □ MSML Rx
- □ MSML Tx
- □ Internal SIP Filter
- □ UDP
- □ TCP

Events

- **Mapper**
- **Remote Mapper**
- **SIP Handler**
- **MSML**

Voicemail Pro

- **Rx from Jade**
- **Tx to Jade**
- **Rx from VmPro**
- **Tx to VmPro**

Packets

- **MSML Rx**
- **MSML Tx**
- **Internal SIP Filter**
- **UDP**
- **TCP**

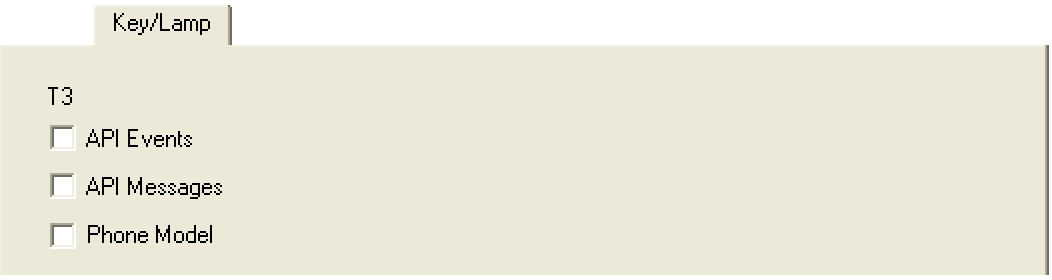
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- *None*.

4.10.12 Key/Lamp

This tab provides trace options for monitoring the events for T3 Series telephones.



Key/Lamp

T3

□ API Events

□ API Messages

□ Phone Model

T3

- **API Events**
- **API Messages**
- **Phone Model**

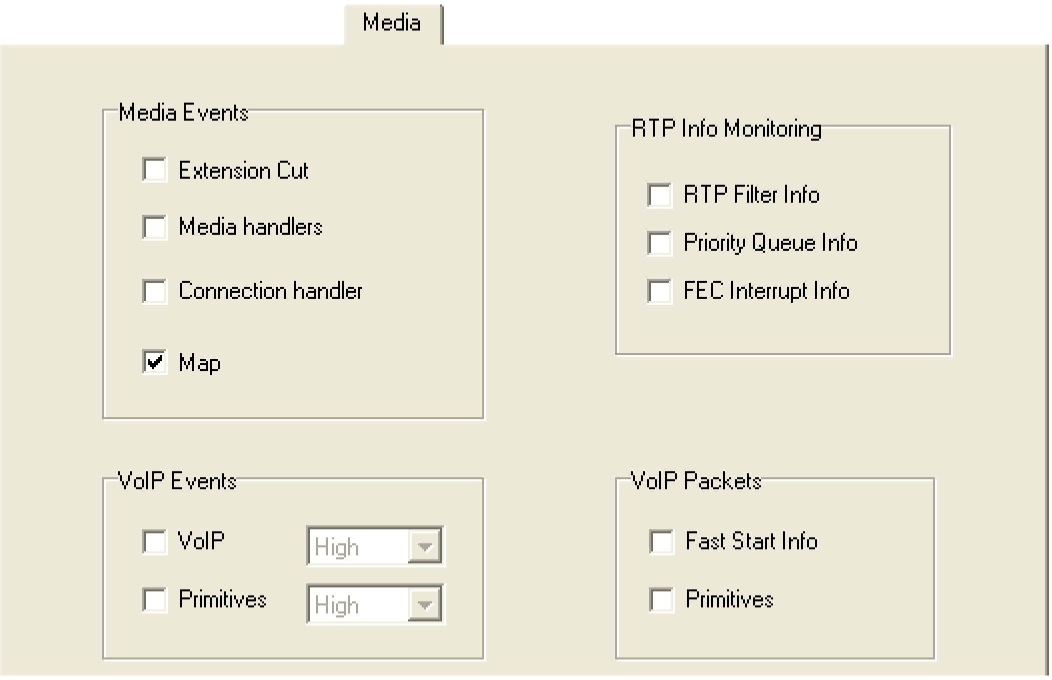
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- *None*.

4.10.13 Media

This tab provides trace options for monitoring the system's media service.



Media

Media Events
- □ Extension Cut
- □ Media handlers
- □ Connection handler
- ☑ Map

RTP Info Monitoring
- □ RTP Filter Info
- □ Priority Queue Info
- □ FEC Interrupt Info

VoIP Events
- □ VoIP High
- □ Primitives High

VoIP Packets
- □ Fast Start Info
- □ Primitives

Media Events

- **Extension Cut**
- **Media handlers**
- **Connection handle**
- **Map**

VoIP Events

- **VoIP**
- **Primitives**

RTP Info Monitoring

- **RTP Filter Info**
- **Priority Queue Info**
- **FEC Interrupt Info**

VoIP Packets

- **Fast Start Info**
- **Primitives**

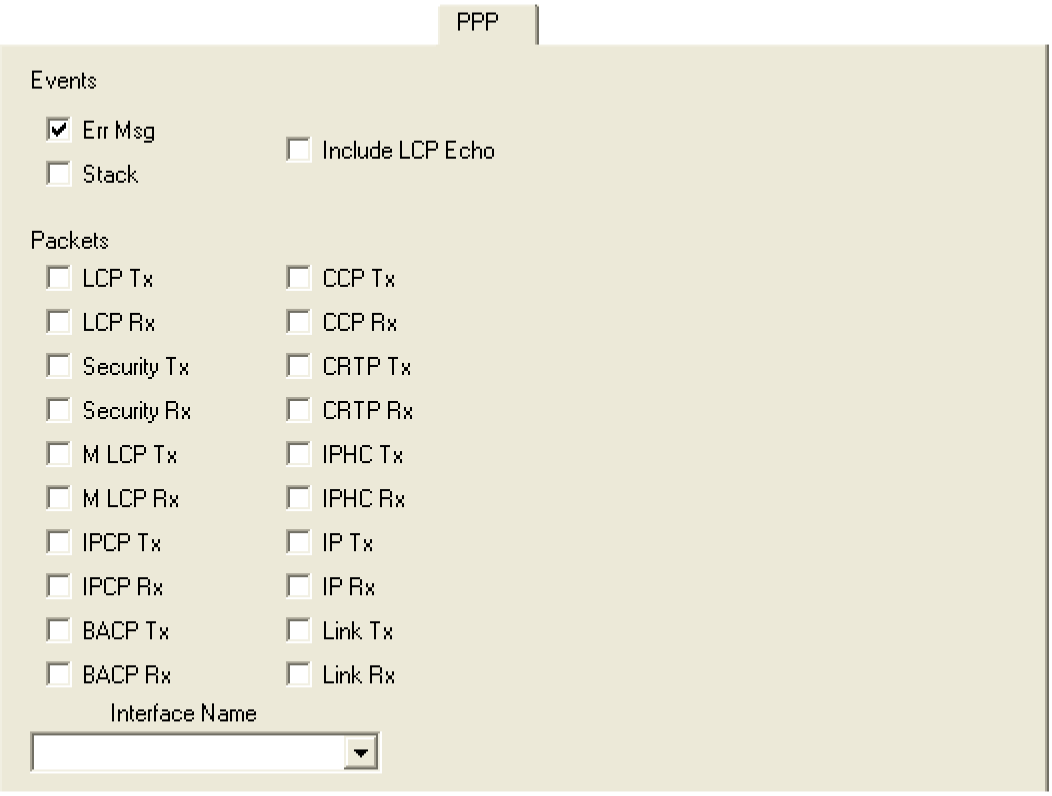
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- **Map**.

4.10.14 PPP

This tab provides trace options for monitoring the system's PPP service events.



PPP

Events

☑ Err Msg

□ Stack

□ Include LCP Echo

Packets

□ LCP Tx
□ LCP Rx
□ Security Tx
□ Security Rx
□ M LCP Tx
□ M LCP Rx
□ IPCP Tx
□ IPCP Rx
□ BACP Tx
□ BACP Rx

□ CCP Tx
□ CCP Rx
□ CRTP Tx
□ CRTP Rx
□ IPHC Tx
□ IPHC Rx
□ IP Tx
□ IP Rx
□ Link Tx
□ Link Rx

Interface Name

Events

- **Err Msg**
  Currently this option does not provide any trace messages. It is included for possible future use only.

- **Stack**
  If selected, this option logs interface utilisation and bandwidth allocation increase/decrease messages.

- **Include LCP Echo**
  If selected, this option logs all LCP Echo and LCP Echo Reply packets received and transmitted.

Packets

- **LCP Tx**
  If selected, this option logs all LCP (Link Control Protocol) packets transmitted.

- **LCP Rx**
  If selected, this option logs all LCP (Link Control Protocol) packets received.

- **Security Tx**
  If selected, this option logs all PAP (Password Authentication Protocol) and/or CHAP (Control Handshake Authentication Protocol) packets transmitted.

- **Security Rx**
  If selected, this option logs all PAP (Password Authentication Protocol) and/or CHAP (Control Handshake Authentication Protocol) packets received.

- **M LCP Tx**
  If selected, this option logs all MLCP (Multilink Layer Control Protocol messages) packets transmitted.

- **M LCP Rx**
  If selected, this option logs all MLCP (Multilink Layer Control Protocol messages) packets received.

- **IPCP Tx**
  If selected, this option logs all IPCP (Internet Protocol Control Protocol) packets transmitted.

- **IPCP Rx**
  If selected, this option logs all IPCP (Internet Protocol Control Protocol) packets received.

- **BACP Tx**
  If selected, this option logs all BACP (Bandwidth Allocation Control Protocol) packets transmitted.

- **BACP Rx**
  If selected, this option logs all BACP (Bandwidth Allocation Control Protocol) packets received.

- **CCP Tx**
  If selected, this option logs all CCP (Compression Control Protocol) packets transmitted.
- **CCP Rx**
  If selected, this option logs all CCP (Compression Control Protocol) packets received.
- **CRTP Tx**
  If selected, this option logs all CRTP (Compressed Real Time Protocol) packets transmitted.
- **CRTP Rx**
  If selected, this option logs all CRTP (Compressed Real Time Protocol) packets received.
- **IPHC Tx**
  If selected, this option logs all IPHC (IP Header compression) packets transmitted.
- **IPHC Rx**
  If selected, this option logs all IPHC (IP Header compression) packets received.
- **IP Tx**
  If selected, this option logs all IP (Internet Protocol) packets transmitted.
- **IP Rx**
  If selected, this option logs all IP (Internet Protocol) packets received.
- **Link Tx**
  If selected, this option logs all packets transmitted.
- **Link Rx**
  If selected, this option logs all packets received.
- **Interface Name**
  This option can be used to limit the information shown for the fields above to those associate with a selected service. A blank entry matches all services.

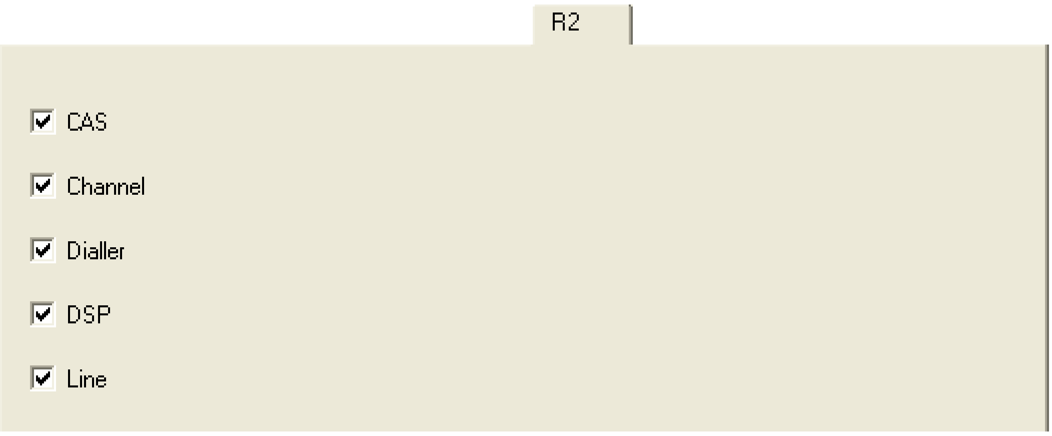
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- **Err Msg**

4.10.15 R2

This tab provides trace options for monitoring the system's E1-R2 trunks.



☑ CAS

☑ Channel

☑ Dialler

☑ DSP

☑ Line

- **CAS**
  If selected, this option logs the common-channel Channel Associated Signaling (CAS) being transmitted and received on all of the channels.
- **Channel**
  If selected, this option logs the events, messages and status changes on the lower level signaling handlers being used on each channel.
- **Dialler**
  If selected, this option logs Dialler events and state changes on all channels. This includes outgoing and incoming digits, MFC dialer state transitions and translations of transmitted and received MFC tones into the correct meanings.
- **DSP**
  If selected, this option logs all significant events, digits and MFC tones being processed by the DSP on the R2 card.
- **Line**
  If selected, this option logs the events, messages and status changes on the line in general, and of "upper level" channel events, messages and status changes, which are independent of the lower level signaling handler being used on each channel.

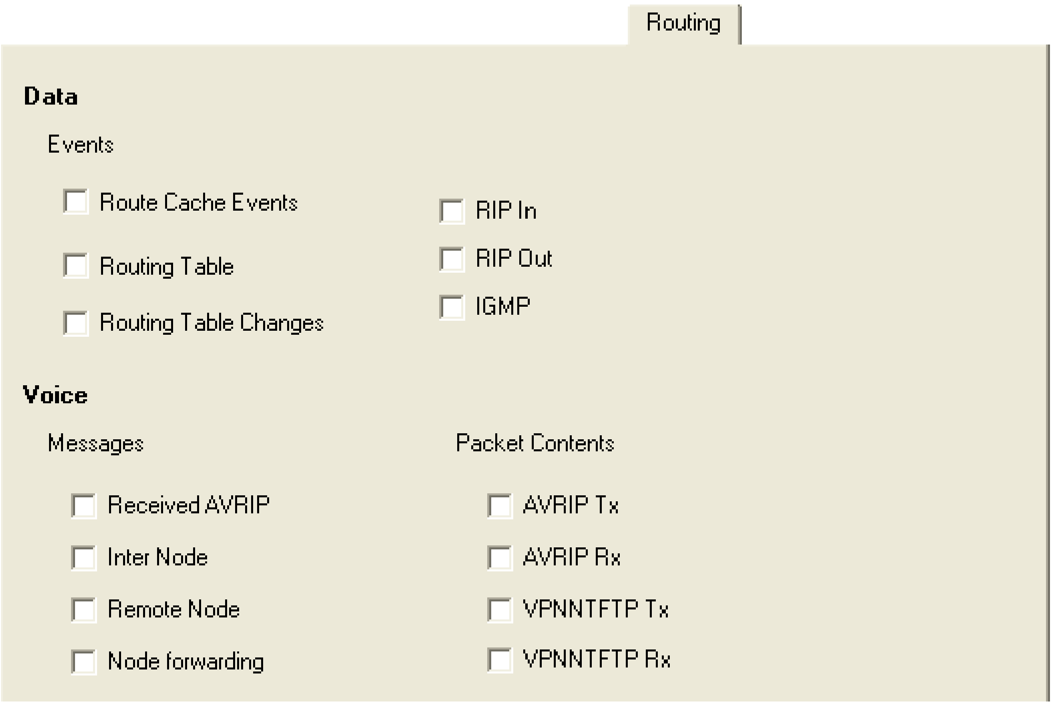
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- **CAS**, **Channel**, **Dialler**, **DSP**, **Line**.

4.10.16 Routing

This tab provides trace options for monitoring the system's IP data routing events for data and for voice.



Routing

Data

Events

- □ Route Cache Events
- □ Routing Table
- □ Routing Table Changes
- □ RIP In
- □ RIP Out
- □ IGMP

Voice

Messages

- □ Received AVRIP
- □ Inter Node
- □ Remote Node
- □ Node forwarding

Packet Contents

- □ AVRIP Tx
- □ AVRIP Rx
- □ VPNNTFTP Tx
- □ VPNNTFTP Rx

Data

The event options under this heading are used to display information pertinent to the IP Routing activities on the system. They provide information on the system's Route Cache, Routing Table, and any RIP updates it receive or transmits.

Events

- **Route Cache Events**
  If selected, this option logs information on the current state of the system's route cache.
- **Routing Table**
  If selected, this option logs information on the system's Routing table.
- **Routing Table Changes**
  If selected, this option logs changes made to the system's Routing Table.
- **RIP In**
  If selected, this option logs received RIP packets.
- **RIP Out**
  If selected, this option logs transmitted RIP packets.
- **IGMP**
  If selected, this options logs IGMP packets.

Voice

The options under this heading are used to display event information pertinent to the Small Community Networking (SCN) Voice Routing activities on the system. These activities include information on SCN messages sent between Adjacent Nodes, and the actual information contained within those message packets.

Messages

- **Received AVRIP**
  If selected, this option logs, when enabled, traces the received AVRIP messages which are sent every 10 seconds during user activity and stop after 11 when idle. They can be used to check what nodes are active in a network. (If you want to see the actual messages then enable Voice/Packets/AVRIP Tx)
- **Inter Node**
  If selected, this option logs general Small Community Networking (SCN) messages which may help in the diagnosis of problem networks.
- **Remote Node**
  If selected, this option logs information on the establishment (or breakdown) of remote nodes in a SCN. These messages can be used to check what nodes are active in a network (note that a remote node is 2 or more hops away).

- **Node Forwarding**
  If selected, this option logs information about how this node is forwarding information about adjacent nodes to other adjacent nodes. Note that in a star network, the central node receives a large number of forwarding messages.

Packet Contents

An AVRIP packet contains information about the voicemail status of that node and information about what other nodes can be reached (IP address and number of hops and voicemail status). VPN TFTP packets contain information on the nodes User configuration data, User VoiceMail message counts, extension BLF status, call information.

- **AVRIP Tx**
  If selected, this option logs all transmitted SCN AVRIP packets from the Node being monitored.
- **AVRIP Rx**
  If selected, this option logs all received SCN AVRIP packets from Nodes adjacent to the one being monitored.
- **VPN TFTP Tx**
  If selected, this option logs all transmitted SCN TFTP packets from the Node being monitored.
- **VPN TFTP Rx**
  If selected, this option logs all received SCN TFTP packets from Nodes adjacent to the one being monitored.

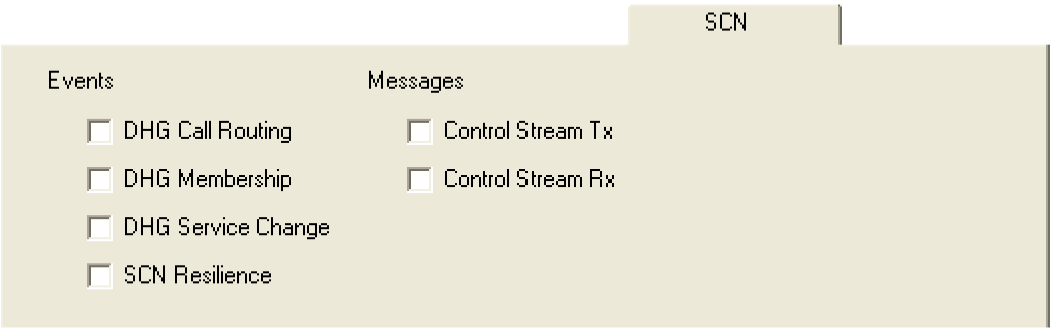
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- *None*.

4.10.17 SCN

This tab provides trace options for monitoring the system's Small Community Network events.



SCN

Events

☐ DHG Call Routing

☐ DHG Membership

☐ DHG Service Change

☐ SCN Resilience

Messages

☐ Control Stream Tx

☐ Control Stream Rx

Events

- **DHG Call Routing**
- **DHG Membership**
- **DHG Service Change**
- **SCN Resilience**

Messages

- **Control Stream Tx**
- **Control Stream Rx**

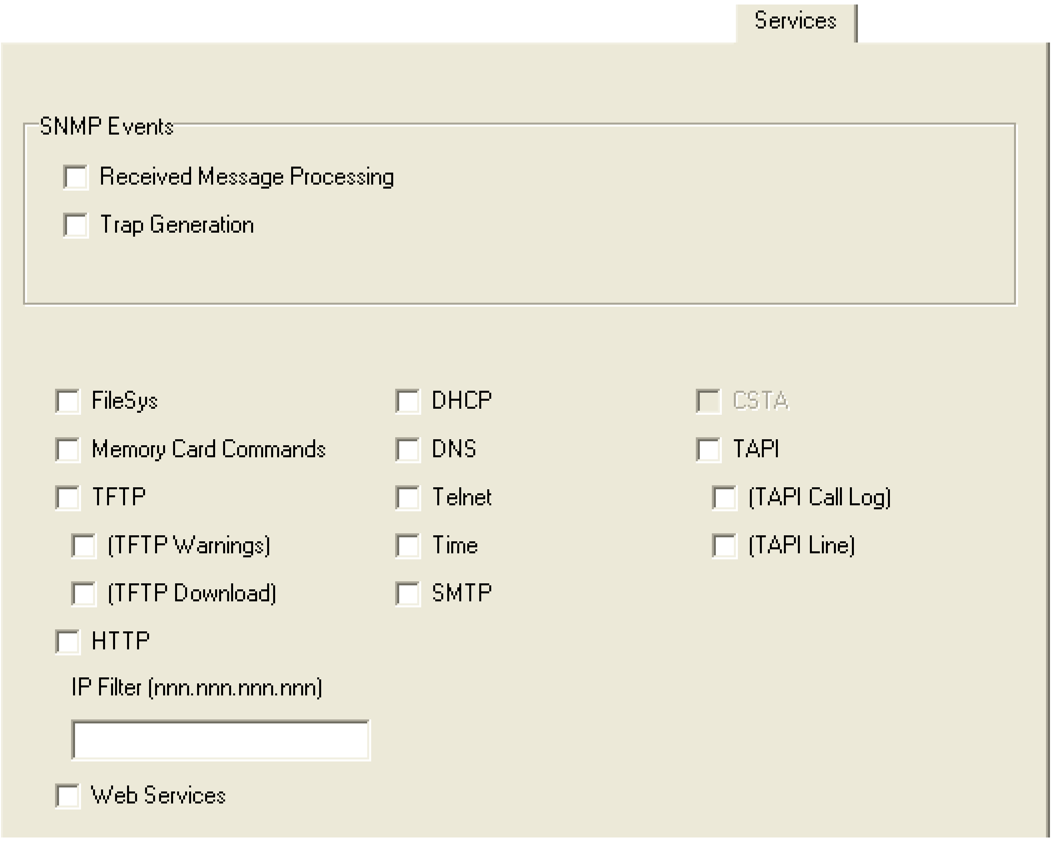
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- *None*.

4.10.18 Services

This tab provides trace options for monitoring various services provided by the system.



Services

SNMP Events

□ Received Message Processing

□ Trap Generation

□ FileSys

□ Memory Card Commands

□ TFTP

□ (TFTP Warnings)

□ (TFTP Download)

□ HTTP

IP Filter (nnn.nnn.nnn.nnn)

□ Web Services

□ DHCP

□ DNS

□ Telnet

□ Time

□ SMTP

□ CSTA

□ TAPI

□ (TAPI Call Log)

□ (TAPI Line)

SNMP Events

- **Received Message Processing**
  If selected, this option logs SNMP requests (Get, Get-Next, Set) received by the system and the responses if valid or associated errors if invalid.

- **Trap Generation**
  If selected, this option logs SNMP trap events sent by the system.

- **Var Bind Processing**
  This option is available when either of the above SNMP trace options are selected. If selected, this option logs a decode of SNMP Var Binds processed in received requests, returned Var Bind for Get-Next requests, and Var Binds sent out in Traps.

Others

- **FileSys**
  If selected, this option logs file requests received by the system.

- **Memory Card Commands**
  If selected, this option logs memory card commands and actions.

- **TFTP**
  If selected, this option logs TFTP file requests to the system and by the system.

  - **TFTP Warnings**
    If selected, this option logs TFTP warnings that occur in response to file requests.

  - **TFTP Download**
    If selected, this option logs the progress of TFTP downloads.

- **HTTP**
  If selected, this option logs HTTP requests.

- **DHCP**
  If selected, this option logs DHCP requests.

- **DNS**
  If selected, this option logs DNS requests.

- **Telnet**
  If selected, this option logs Telnet activity.

- **Time**
  If selected, this option logs time and date requests and responses to the system and between the system and its configured time server.

- **SMTP**
  If selected, this option logs SMTP activity on the system.

- **CSTA**
  If selected, this option logs CSTA messages and responses.

- **TAPI**
  If selected, this option logs TAPI messages.

  - **TAPI Call Log**
    If selected, this option logs TAPI Call Log messages.

  - **TAPI Line**
    If selected, this option logs TAPI Line messages.

- **IP Filter**
  The value in this field can be used to only show only messages to and from the specified IP address. The filter is applied to all the other selected trace options on the tab.

- **Web Services**
  If selected, this option logs web service messages.

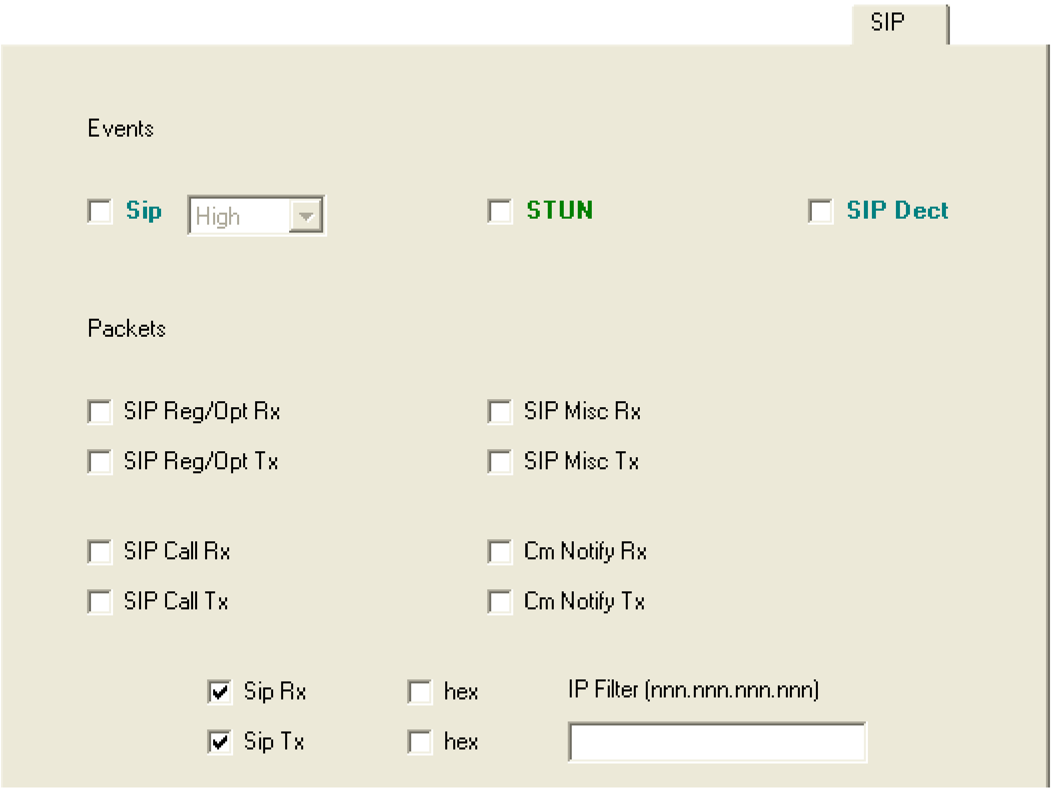
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- *None*.

4.10.19 SIP

This tab provides trace options for monitoring the system's SIP events.



SIP

Events

□ Sip High

□ STUN

□ SIP Dect

Packets

□ SIP Reg/Opt Rx

□ SIP Reg/Opt Tx

□ SIP Misc Rx

□ SIP Misc Tx

□ SIP Call Rx

□ SIP Call Tx

□ Cm Notify Rx

□ Cm Notify Tx

☑ Sip Rx □ hex

☑ Sip Tx □ hex

IP Filter (nnn.nnn.nnn.nnn)

Events

- **SIP**
- **STUN**
- **SIP Dect**

Packets

- **SIP Reg/Opt Rx**
- **SIG Reg/Opt Tx**
- **SIP Call Rx**
- **SIP Call Tx**
- **SIP Misc Rx**
- **SIP Misc Tx**
- **Cm Notify Rx**
- **Cm Notify Tx**
- **Sip Rx**
- **Sip Tx**
- **IP Filter**

Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

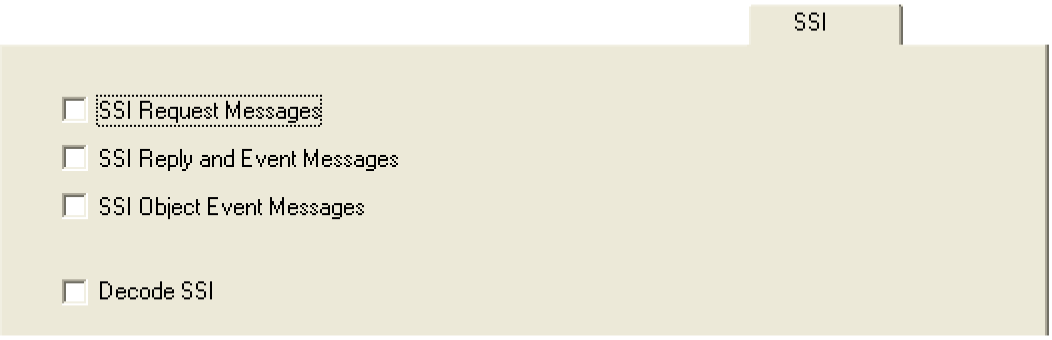
- **SIP Rx**, **SIP Tx**.

4.10.20 SSI

This tab provides trace options for monitoring the system's SSI connections. SSI is used for the IP Office Customer Call Reporter and IP Office System Status applications.

These options are only available when the **Development Tracing** option is selected in the **Trace Options | System** 69 menu. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.



□ SSI Request Messages

□ SSI Reply and Event Messages

□ SSI Object Event Messages

□ Decode SSI

- **SSI Request Messages**
- **SSI Reply and Event Messages**
- **SSI Object Event Messages**
- **Decode SSI**

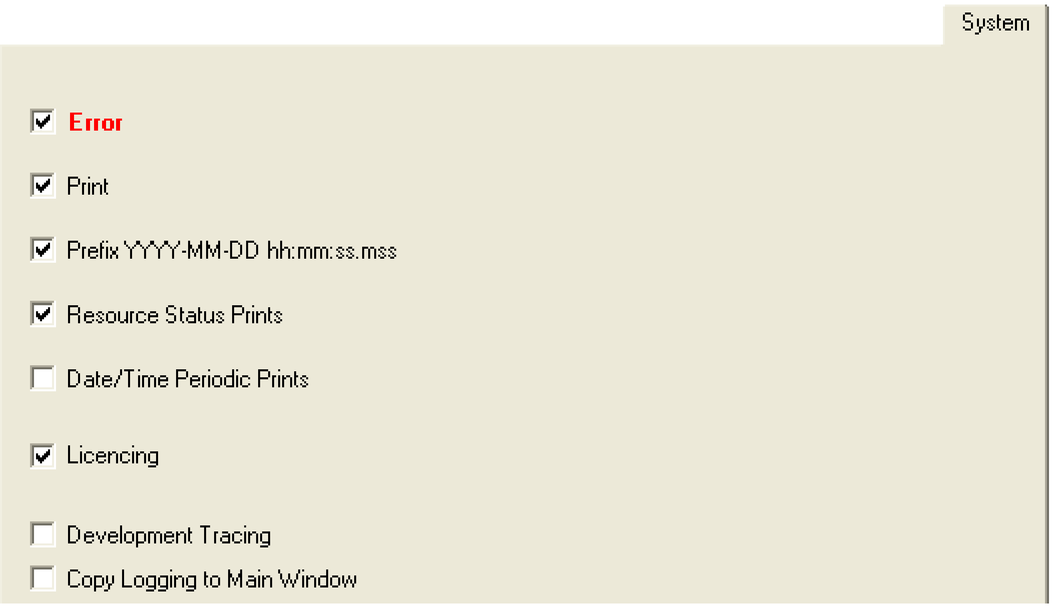
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- *None*.

4.10.21 System

This tab provides general trace options.



System

☑ Error

☑ Print

☑ Prefix YYYY-MM-DD hh:mm:ss.mss

☑ Resource Status Prints

□ Date/Time Periodic Prints

☑ Licencing

□ Development Tracing

□ Copy Logging to Main Window

- **Error**
  If selected, this option logs all messages that are tagged with ***[ERROR:]***.

- **Print**
  If selected, this option logs all messages that are tagged with ***[PRN:]***. These are messages relating to major events or changes in status of the software modules running.

- **Prefix YYY-MM-DD hh:mm:ss**
  If selected, each record received is prefixed with the current date and time.

- **Resource Status Prints**
  If selected, once every 20 seconds the trace includes a summary of the system memory resources and the number of connections. The messages are tagged with ***[RES:]***.

- **Date/Time Periodic Prints**
  If selected, once a minute the trace includes a record of the date and time plus details of the connected system name and IP address. This is useful in a trace if the **Prefix YYY-MM-DD hh:mm:ss** trace option is not selected.

- **Licencing**
  If selected, this option logs messages relating to the verification of system licenses. Licensing messages are tagged with ***[LIC:]***.

- **Development Tracing**
  This option should only be selected when advised to do so by Avaya. When is selected, System Monitor has access to additional trace option tabs for SSI 68 and VComp 72 and a number of additional status screens, see Status Screens 78.

- **Copy Logging to Main Window**

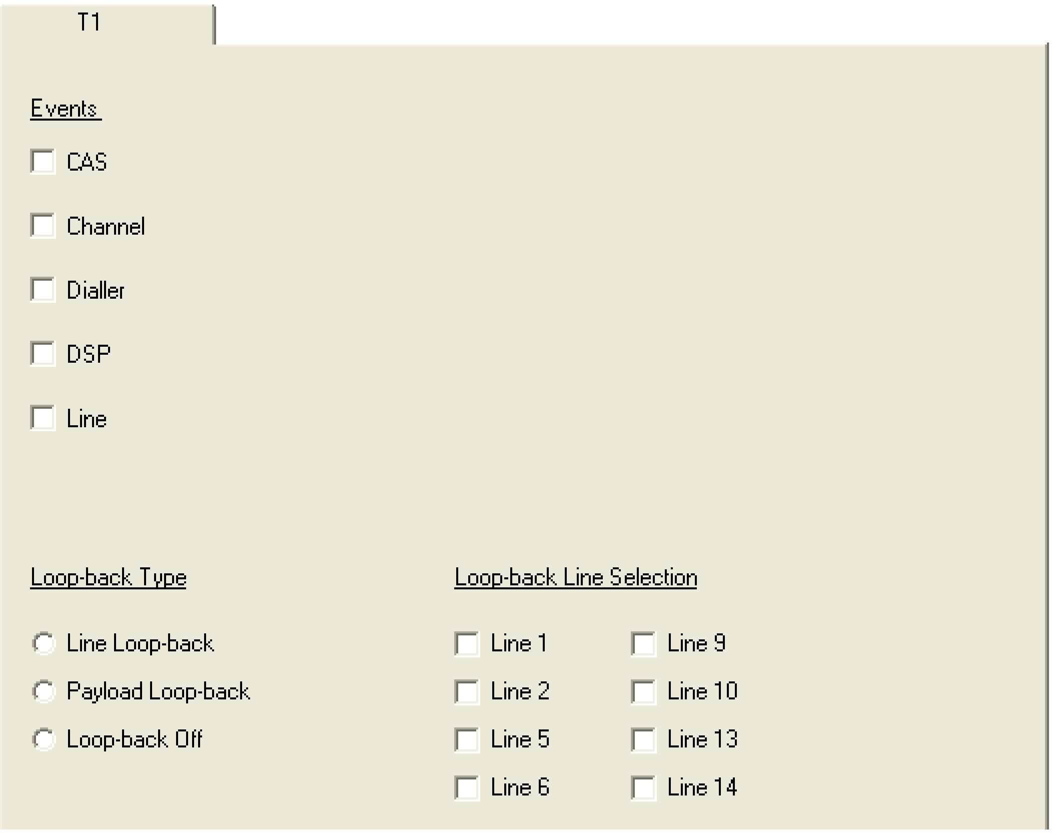
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- **Error**, **Print**, **Prefix YYYY-MM-DD hh:mm:ss:mss**, **Resource Status Prints**, **Licencing**.

4.10.22 T1

This tab provides trace options for monitoring the system's T1 trunks.



T1

Events

□ CAS

□ Channel

□ Dialler

□ DSP

□ Line

Loop-back Type

○ Line Loop-back

○ Payload Loop-back

○ Loop-back Off

Loop-back Line Selection

□ Line 1 □ Line 9

□ Line 2 □ Line 10

□ Line 5 □ Line 13

□ Line 6 □ Line 14

Events

- **CAS**
  If selected, this option logs the robbed-bit Channel Associated Signaling (CAS) being transmitted and received on all of the channels.

- **Channel**
  If selected, this option logs the events, messages and status changes on the lower level signaling handlers being used on each channel.

- **Dialler**
  If selected, this option logs "Dialler" events and state changes on all channels. This includes outgoing and incoming digits.

- **DSP**
  If selected, this option logs all significant events and digits being processed by the DSP on the T1 card.

- **Line**
  If selected, this option logs the events, messages and status changes on the T1 line in general, and "upper level" channel events, messages and status changes, which are independent of the lower level signaling handler being used on each channel.

Loop-back

These options are used to set loop-back operation. First select the line on which loop-back is required and then the type of loop-back. The settings are applied after clicking OK.

Loop-back Type

- **Line Loop-back**
  This loop-back type loops back the entire received signal to the far end of the line without the signal entering the system at all.

- **Payload Loop-back**
  This loop-back type allows the received signal into the line driver chip-set. The signal payload is extracted from the incoming framed signal and transmitted back to the line with new framing.

- **Loop-Back Off**
  This option disables any loop-back operation currently applied to the selected line.

Loop-back Line Selection

- **Loop-back Line Selection**
  These settings are used to select the lines to which the selected Loop-back Type are applied.

Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

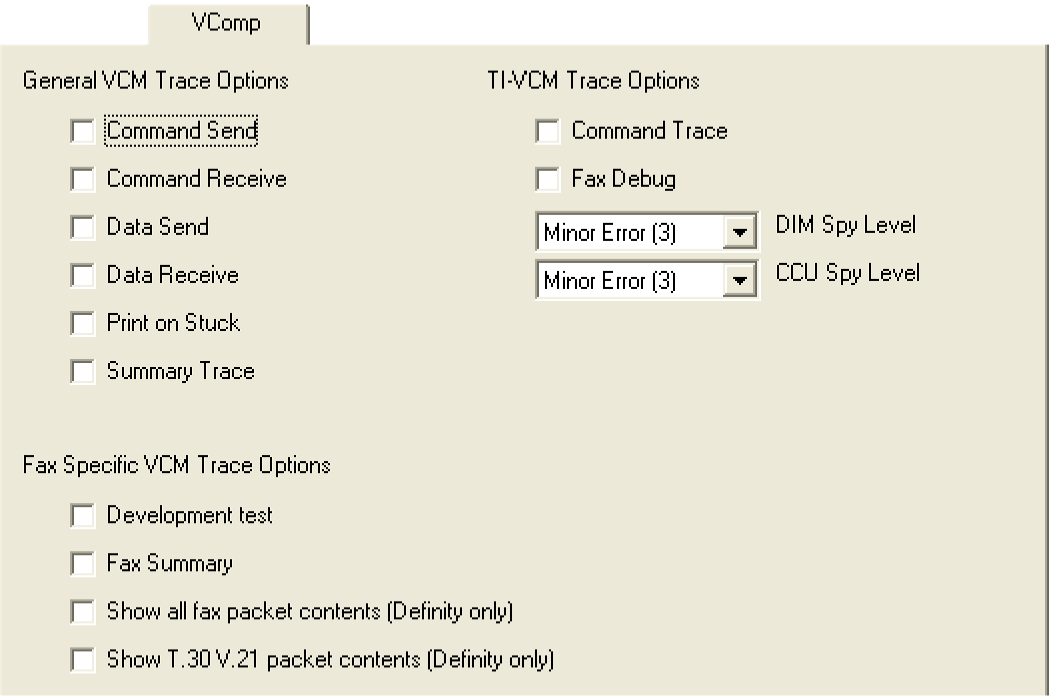
- *None*.

4.10.23 VComp

This tab provides trace options for monitoring the system's voice compression channels. Note that these options produce a large amount of trace records and so should be used with caution.

These options are only available when the **Development Tracing** option is selected in the **Trace Options | System** 69 menu. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.



General VCM Trace Options

- □ Command Send
- □ Command Receive
- □ Data Send
- □ Data Receive
- □ Print on Stuck
- □ Summary Trace

TI-VCM Trace Options

- □ Command Trace
- □ Fax Debug
- DIM Spy Level: Minor Error (3)
- CCU Spy Level: Minor Error (3)

Fax Specific VCM Trace Options

- □ Development test
- □ Fax Summary
- □ Show all fax packet contents (Definity only)
- □ Show T.30 V.21 packet contents (Definity only)

General VCM Trace Options

- **Command Send**
  If selected, this option logs details of commands transmitted to the voice compressor chip.
- **Command Receive**
  If selected, this option logs details of commands received from the voice compressor chip.
- **Data Send**
  If selected, this option logs details of data transmitted to the voice compressor chip (additional detail from the Command Send option).
- **Data Receive**
  If selected, this option logs details of data received from the voice compressor chip (additional detail from the Command Receive option).
- **Print on Stuck**
  This option produce the summary trace but only if the system detects a severe problem.
- **Summary Trace**
  If selected, this option logs the commands to and from all the voice compressor chips (multiple occurrences are counted to reduce output) and the output is controlled so as not to swamp the system. Care should be exercised when selecting this option - especially if multiple VoIP calls are in progress.

Fax Specific VCM Trace Options

- **Development Test**
  Used when debugging private variations of Development s/w.
- **Fax Summary**
  If selected, this option logs the V.21 and T.30 messages.
- **Show all fax packet contents (Definity only)**
  Display the contents of ALL fax packets - including the actual fax data (only when connected to a Definity).
- **Show T.30 V.21 packet contents (Definity only)**
  Display the contents of T.30 and V.21 packet (only when connected to a Definity).

TI-VCM Trace Options

- **Command Trace**

- **Fax Debug**
- **DIM Spy Level**
- **CCU Spy Level**

Default Settings

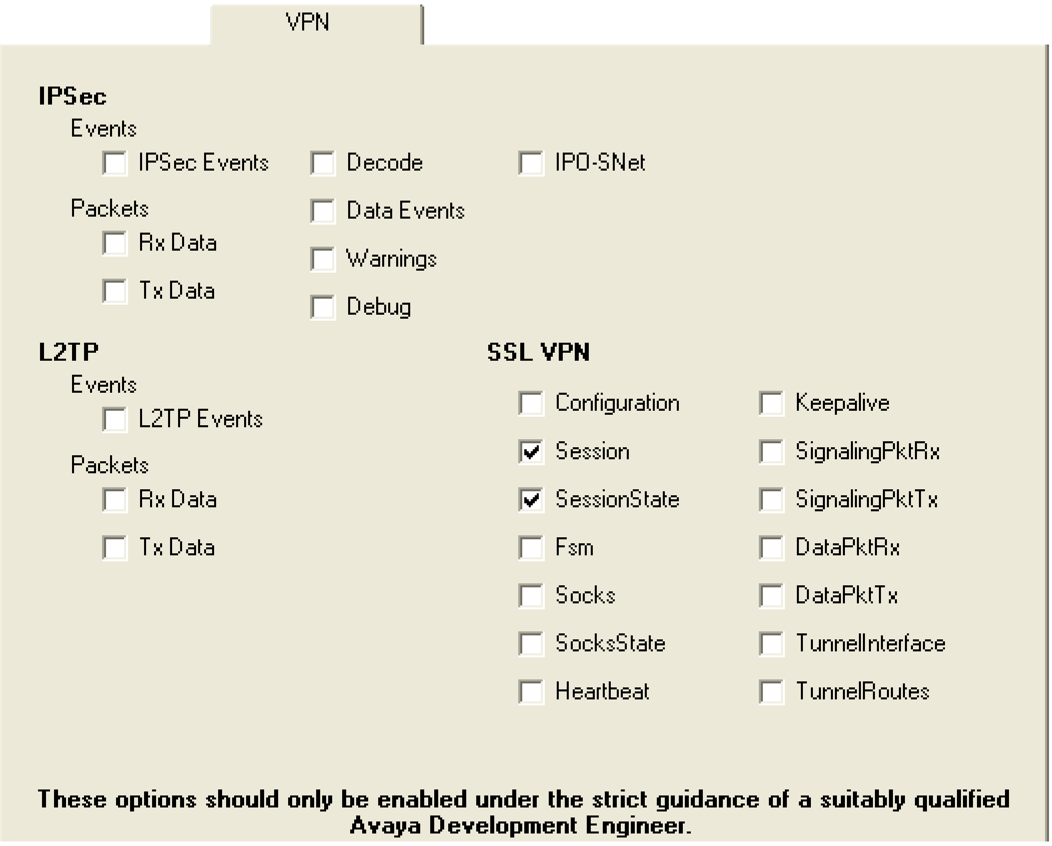
The following trace options are enabled by default (see Defaulting the Trace Options 38):

- *None*.

4.10.24 VPN

This tab provides trace options for monitoring the systems VPN connections.

These options should only be used under the guidance of an authorized Avaya development engineer.



IPSec

Events

□ IPSec Events

□ Decode

□ IPO-SNet

Packets

□ Rx Data

□ Tx Data

□ Data Events

□ Warnings

□ Debug

L2TP

Events

□ L2TP Events

Packets

□ Rx Data

□ Tx Data

SSL VPN

□ Configuration

☑ Session

☑ SessionState

□ Fsm

□ Socks

□ SocksState

□ Heartbeat

□ Keepalive

□ SignalingPktRx

□ SignalingPktTx

□ DataPktRx

□ DataPktTx

□ TunnelInterface

□ TunnelRoutes

These options should only be enabled under the strict guidance of a suitably qualified Avaya Development Engineer.

IPSec

Events

- **IPSec Events**
  If selected, this option logs primary events when bringing up and tearing down IPSec tunnels. It also indicates when packets are being discarded, etc.

- **Decode**
  If selected, this option logs the decrypted IKE packets.

- **IPO-SNet**
  Not currently used.

- **Data Events**
  If selected, this option logs when packets are encrypted into and out of tunnel. It does not display the actual packet contents, they can be logged using the **Interface** 52 tab options **Interface Packets In** and **Interface Packets Out**.

- **Warnings**
  If selected, this option logs information relating to faults in the IPSec processing.

- **Debug**
  If selected, this option logs special engineering trace information.

Packets

- **Rx Data**
  If selected, this option logs the content of received ESP encrypted packets before decryption.

- **Tx Data**
  If selected, this option logs the content of sent ESP encrypted packets after encryption.

L2TP

Events

- **L2TP Events**
  If selected, this option logs the establishment of the L2TP tunnel (the stage underneath the PPP). You really need to include the appropriate PPP tracing additionally to this to see the complete picture.

Packets

- **Rx Data**
  Currently not used.
- **Tx Data**
  Currently not used.

SSL VPN

- **Configuration**
- **Session**
- **Session State**
- **Fsm**
- **Socks**
- **SocksState**
- **Heartbeat**
- **Keepalive**
- **SignalingPktRx**
- **SignalingPkTx**
- **DataPktRx**
- **DataPktTx**
- **TunnelInterface**
- **TunnelRoutes**

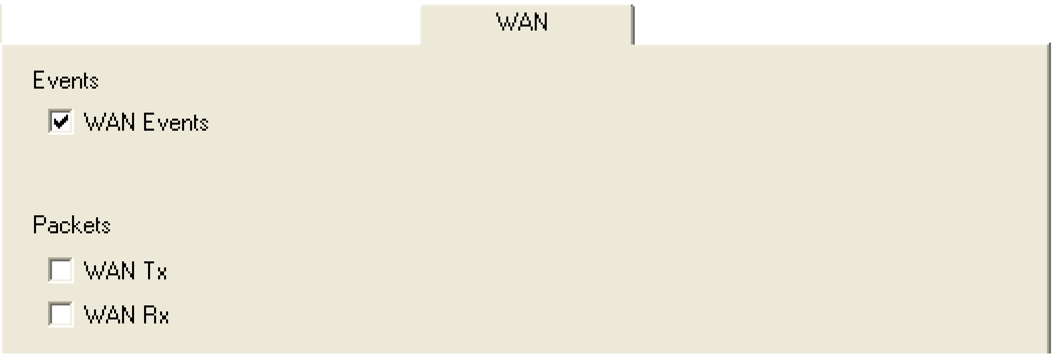
Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- **SSL VPN: Session** and **Session State**.

4.10.25 WAN

This tab provides trace options for monitoring the system's WAN ports.



Events

☑ WAN Events

Packets

□ WAN Tx

□ WAN Rx

Events

- **WAN Events**
  If selected, this option logs messages that are associated with changes to the software state machine controlling the WAN link on the selected unit.

Packets

- **WAN Tx**
  If selected, this option logs all IP data packets transmitted on the WAN ports of the selected unit.

- **WAN Rx**
  If selected, this option logs all IP data packets received on the WAN ports of the selected unit.

Default Settings

The following trace options are enabled by default (see Defaulting the Trace Options 38):

- **WAN Events**.

Chapter 5.
Status Screens

5. Status Screens

In addition to screen logging, System Monitor can display a number of status screens that show additional information about the connected system. These are accessed by clicking Status and selecting the required status menu.

- **US PRI Trunks** 97
- **RTP Sessions** 91
- **Voicemail Sessions** 98
- **SCN Licence** 92
- **IPV6 Config** 83
- **Small Community Networking** 95
- **Partner Sessions** 89
- **Alarms** 79
- **Map Status** 85
- **Conference Status** 81
- **Network View** 88
- **H.323 Phone Status** 83
- **SIP Phone Status** 93
- **SIP TCP User Data** 94
- **TCP Streams Data** 96

The following additional status menus are accessible if the **Development Tracing** trace option is selected. See System Trace Options 69.

- **Performance Data** 90
- **Memory Data** 86
- **Buffer Data** 80
- **DHCP Data** 82
- **Voice Compression** 99
- **Voice Compression (TI)** 100
- **IPO-SNet** 83
- **DSS Status** 82
- **Logging** 84
- **NAPT Status** 87

5.1 Alarms

This status menu displays the alarms records in the connected system's alarms log.

When System Monitor connects to a system, the trace includes the system's alarm log. The alarms cannot be interpreted. However, if a site is the same repeated problem, Avaya may request the alarm log details.

The presence of alarms is not necessarily critical as each system keeps a record of the first 8 alarms since the alarm log was last cleared. However, once the alarm log is full, the system ignores additional alarms.

```
3003mS PRN: +++ START OF ALARM LOG DUMP +++
3019mS PRN: ALARM: 18/03/2004 13:07:56 IP 412 2.1(8) <Program Exception> CRIT RAISED addr=00000000 d=5 pc=00000000 0082eef0 0094d780
3019mS PRN: ALARM: 22/04/2004 07:26:44 IP 412 2.1(11) <Program Exception> CRIT RAISED addr=00000000 d=5 pc=00000000 0095dfe0 0095e27
3019mS PRN: ALARM: 22/04/2004 07:26:46 IP 412 2.1(11) <WATCHDOG> CRIT RAISED addr=00000000 d=0 pc=00000000 01e75750 01f983d4 0095e27
3004mS PRN: +++ END OF ALARM LOG DUMP +++
```

To view the alarm log:

1. Click **Status** and select **Alarms**.
2. System Monitor displays the alarm records in a separate window.

To clear the alarm log:

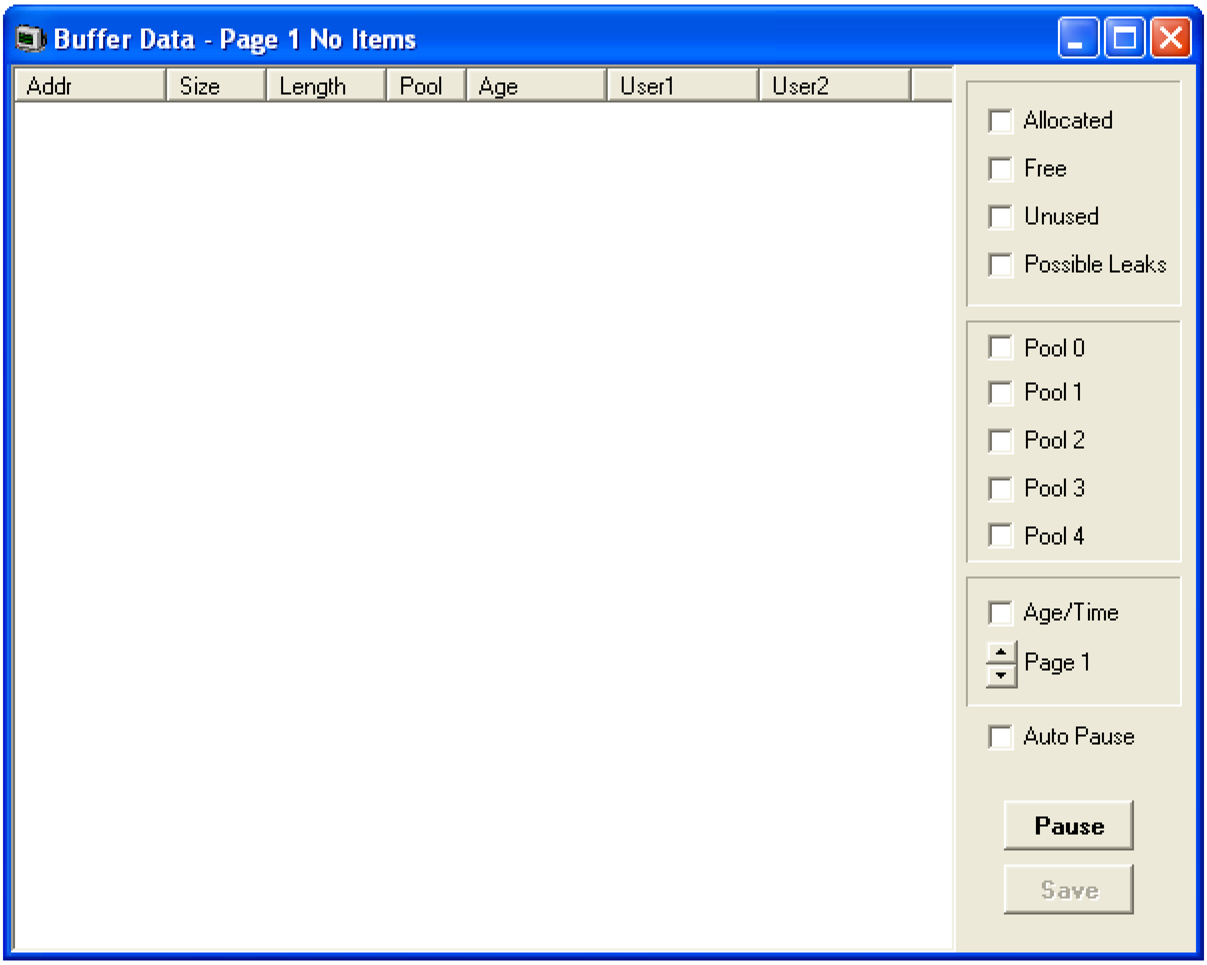
1. View the alarm log using the process above.
2. Click **Clear Alarms**.

5.2 Buffer Data

This status menu displays data about the system's memory buffers.

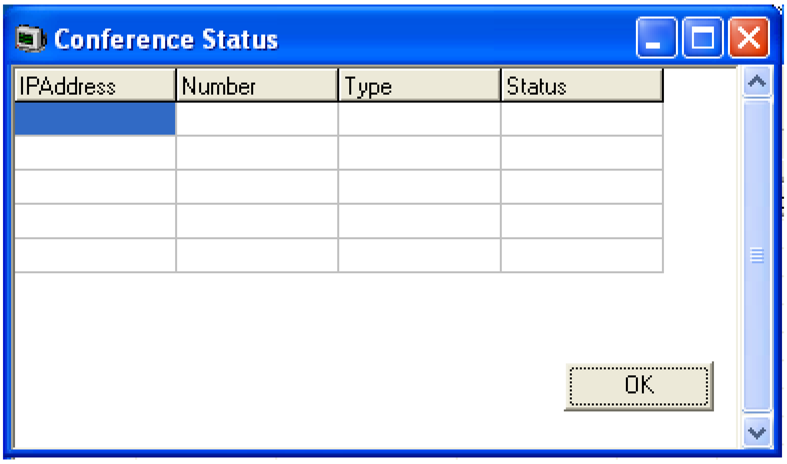
These options are only available when the **Development Tracing** option is selected in the **Trace Options | System** 69 menu. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.



5.3 Conference Status

This status menu displays the status of conference's being supported by the system.



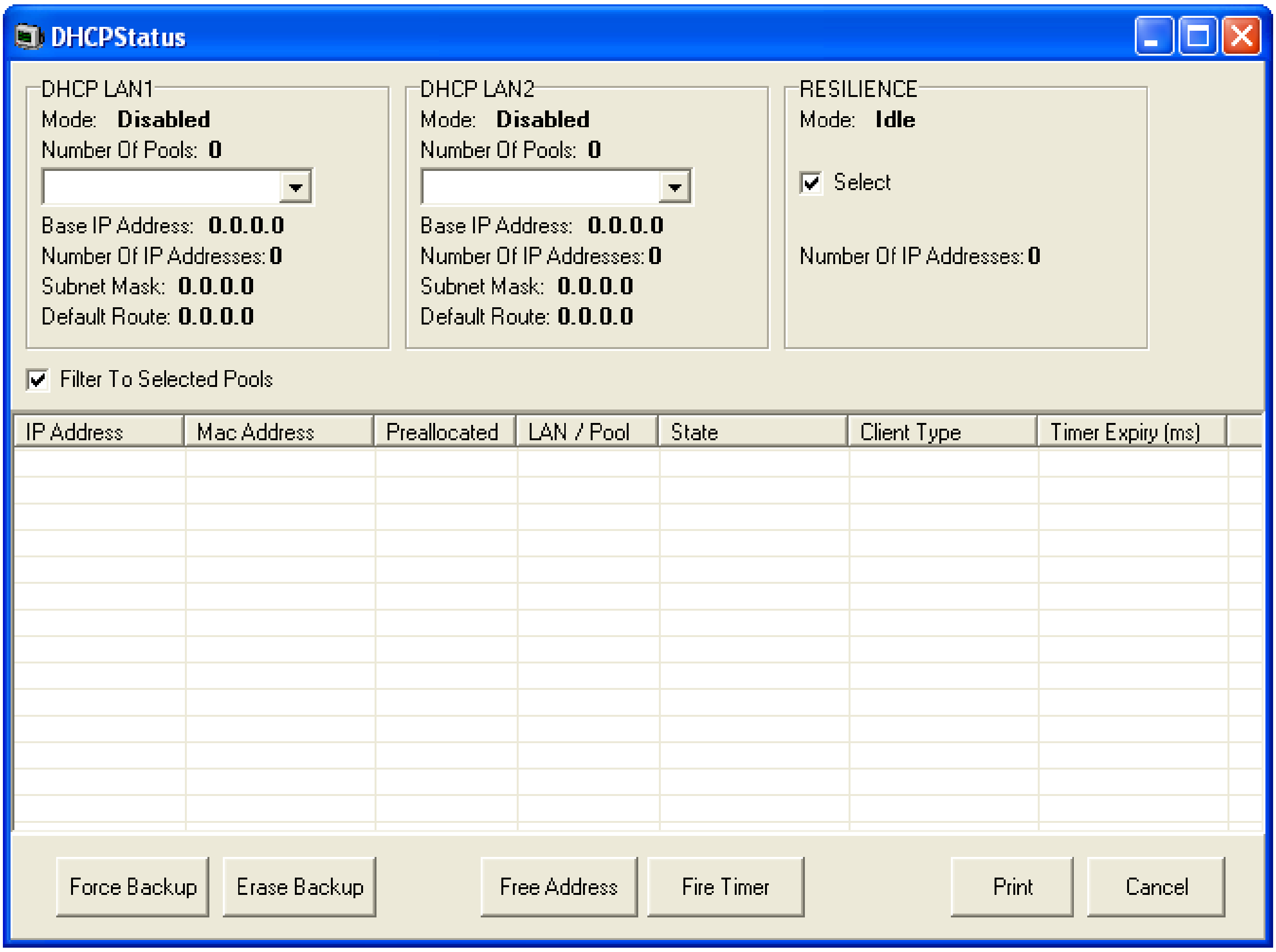
IPAddress	Number	Type	Status

5.4 DHCP Data

This status menu displays details of the system's DHCP server settings and the DHCP clients being supported by the system.

These options are only available when the **Development Tracing** option is selected in the **Trace Options | System** 69 menu. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.



DHCP LAN1
Mode: **Disabled**
Number Of Pools: **0**
Base IP Address: **0.0.0.0**
Number Of IP Addresses: **0**
Subnet Mask: **0.0.0.0**
Default Route: **0.0.0.0**

DHCP LAN2
Mode: **Disabled**
Number Of Pools: **0**
Base IP Address: **0.0.0.0**
Number Of IP Addresses: **0**
Subnet Mask: **0.0.0.0**
Default Route: **0.0.0.0**

RESILIENCE
Mode: **Idle**
☑ Select
Number Of IP Addresses: **0**

☑ Filter To Selected Pools

IP Address	Mac Address	Preallocated	LAN / Pool	State	Client Type	Timer Expiry (ms)

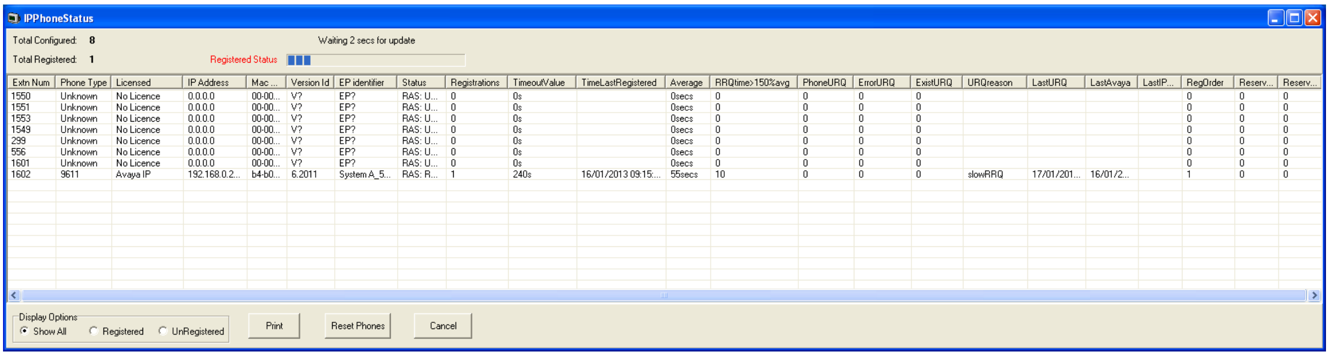
5.5 DSS Status

These options are only available when the **Development Tracing** option is selected in the **Trace Options | System** 69 menu. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

5.6 H.323 Phone Status

This status menu displays details of the H.323 end points known by the system.



Total Configured: **8**

Total Registered: **1**

Waiting 2 secs for update

Registered Status

Extn Num	Phone Type	Licensed	IP Address	Mac ...	Version Id	EP identifier	Status	Registrations	TimeoutValue	TimeLastRegistered	Average	RRQtime>150%avg	PhoneURQ	ErrorURQ	ExistURQ	URQreason	LastURQ	LastAvaya	LastIP...	RegOrder	Reserv...	Reserv...
1550	Unknown	No Licence	0.0.0.0	00-00...	V?	EP?	RAS: U...	0	0s		0secs	0	0	0	0					0	0	0
1551	Unknown	No Licence	0.0.0.0	00-00...	V?	EP?	RAS: U...	0	0s		0secs	0	0	0	0					0	0	0
1553	Unknown	No Licence	0.0.0.0	00-00...	V?	EP?	RAS: U...	0	0s		0secs	0	0	0	0					0	0	0
1549	Unknown	No Licence	0.0.0.0	00-00...	V?	EP?	RAS: U...	0	0s		0secs	0	0	0	0					0	0	0
299	Unknown	No Licence	0.0.0.0	00-00...	V?	EP?	RAS: U...	0	0s		0secs	0	0	0	0					0	0	0
556	Unknown	No Licence	0.0.0.0	00-00...	V?	EP?	RAS: U...	0	0s		0secs	0	0	0	0					0	0	0
1601	Unknown	No Licence	0.0.0.0	00-00...	V?	EP?	RAS: U...	0	0s		0secs	0	0	0	0					0	0	0
1602	9611	Avaya IP	192.168.0.2...	b4-b0...	6.2011	System A_5...	RAS: R...	1	240s	16/01/2013 09:15:...	55secs	10	0	0	0	slowRRQ	17/01/201...	16/01/2...		1	0	0

Display Options: ● Show All ○ Registered ○ UnRegistered

5.7 IPO-SNet

These options are only available when the **Development Tracing** option is selected in the **Trace Options | System** 69 menu. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

5.8 IPV6 Config

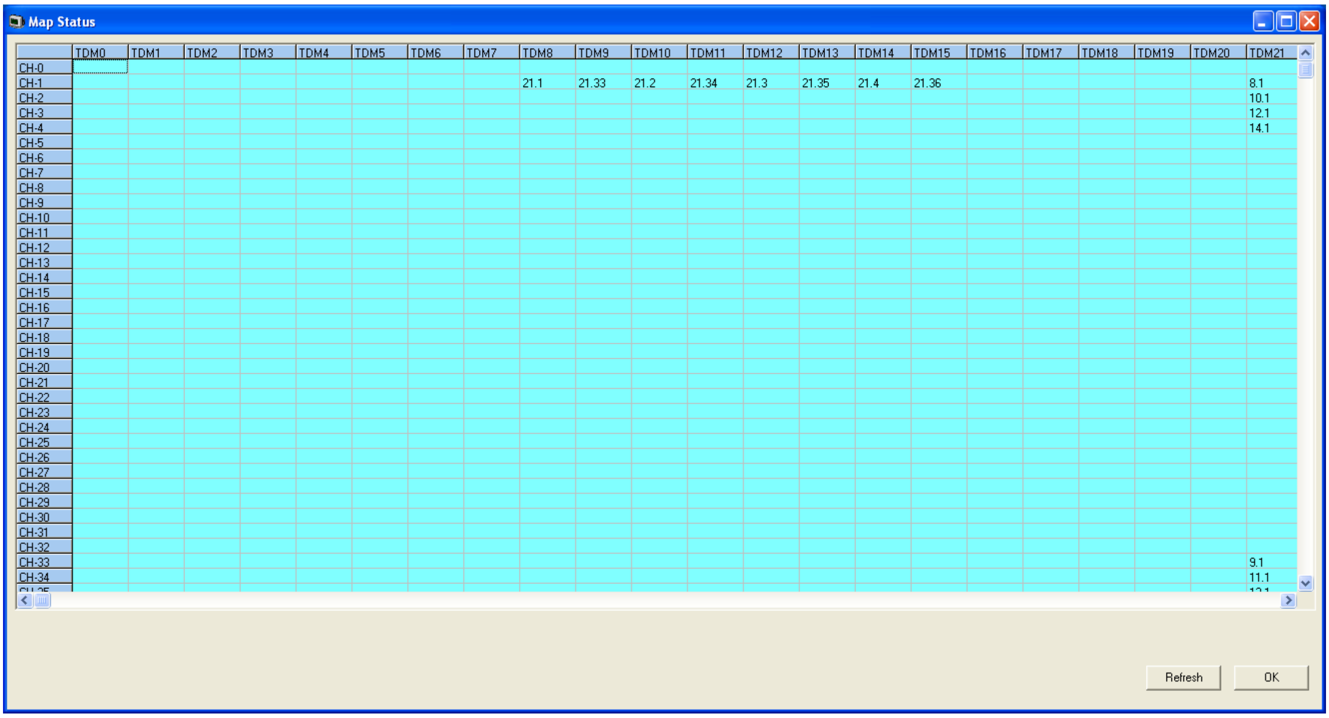
This status menu is not currently used.

5.9 Logging

These options are only available when the **Development Tracing** option is selected in the **Trace Options | System** 69 menu. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

5.10 Map Status



	TDM0	TDM1	TDM2	TDM3	TDM4	TDM5	TDM6	TDM7	TDM8	TDM9	TDM10	TDM11	TDM12	TDM13	TDM14	TDM15	TDM16	TDM17	TDM18	TDM19	TDM20	TDM21
CH-0																						
CH-1									21.1	21.33	21.2	21.34	21.3	21.35	21.4	21.36						8.1
CH-2																						10.1
CH-3																						12.1
CH-4																						14.1
CH-5																						
CH-6																						
CH-7																						
CH-8																						
CH-9																						
CH-10																						
CH-11																						
CH-12																						
CH-13																						
CH-14																						
CH-15																						
CH-16																						
CH-17																						
CH-18																						
CH-19																						
CH-20																						
CH-21																						
CH-22																						
CH-23																						
CH-24																						
CH-25																						
CH-26																						
CH-27																						
CH-28																						
CH-29																						
CH-30																						
CH-31																						
CH-32																						
CH-33																						9.1
CH-34																						11.1

5.11 Memory Data

These options are only available when the **Development Tracing** option is selected in the **Trace Options | System** 69 menu. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

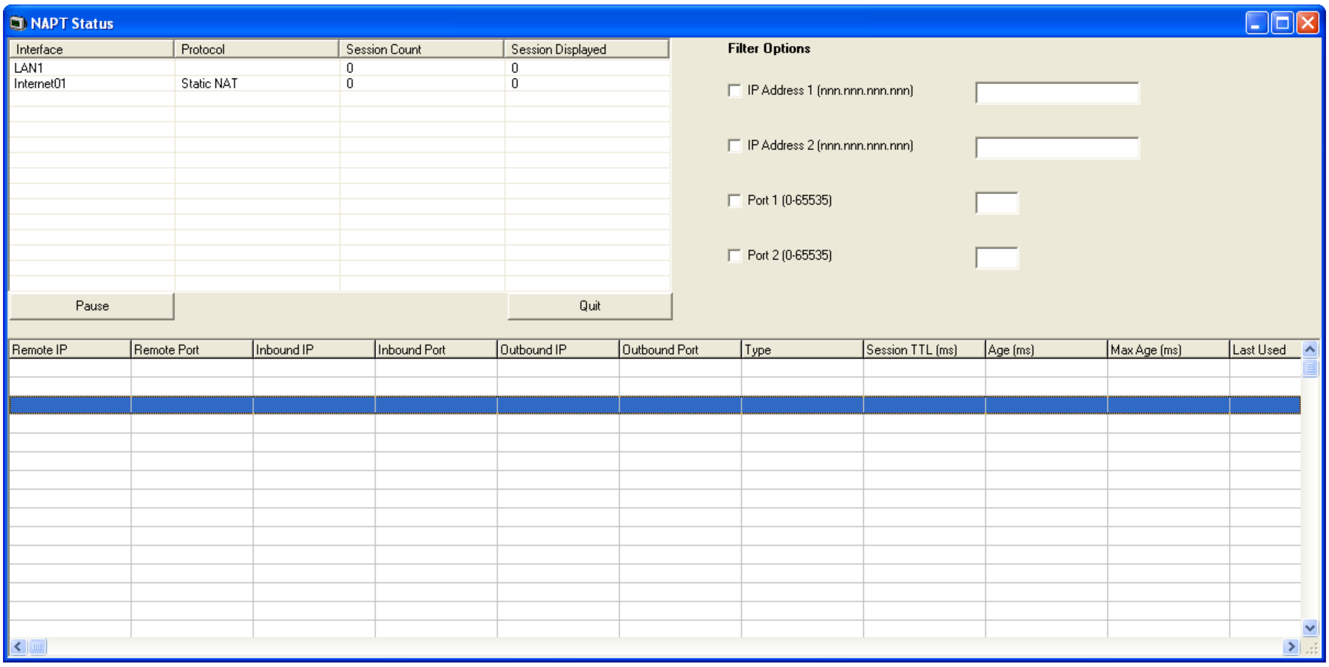
These options should only be used under the guidance of an authorized Avaya development engineer.

5.12 NAPT Status

This status menu displays the status of NAPT sessions being supported by the system.

These options are only available when the **Development Tracing** option is selected in the **Trace Options | System** 69 menu. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.



NAPT Status

Interface	Protocol	Session Count	Session Displayed
LAN1		0	0
Internet01	Static NAT	0	0

Filter Options

□ IP Address 1 (nnn.nnn.nnn.nnn)

□ IP Address 2 (nnn.nnn.nnn.nnn)

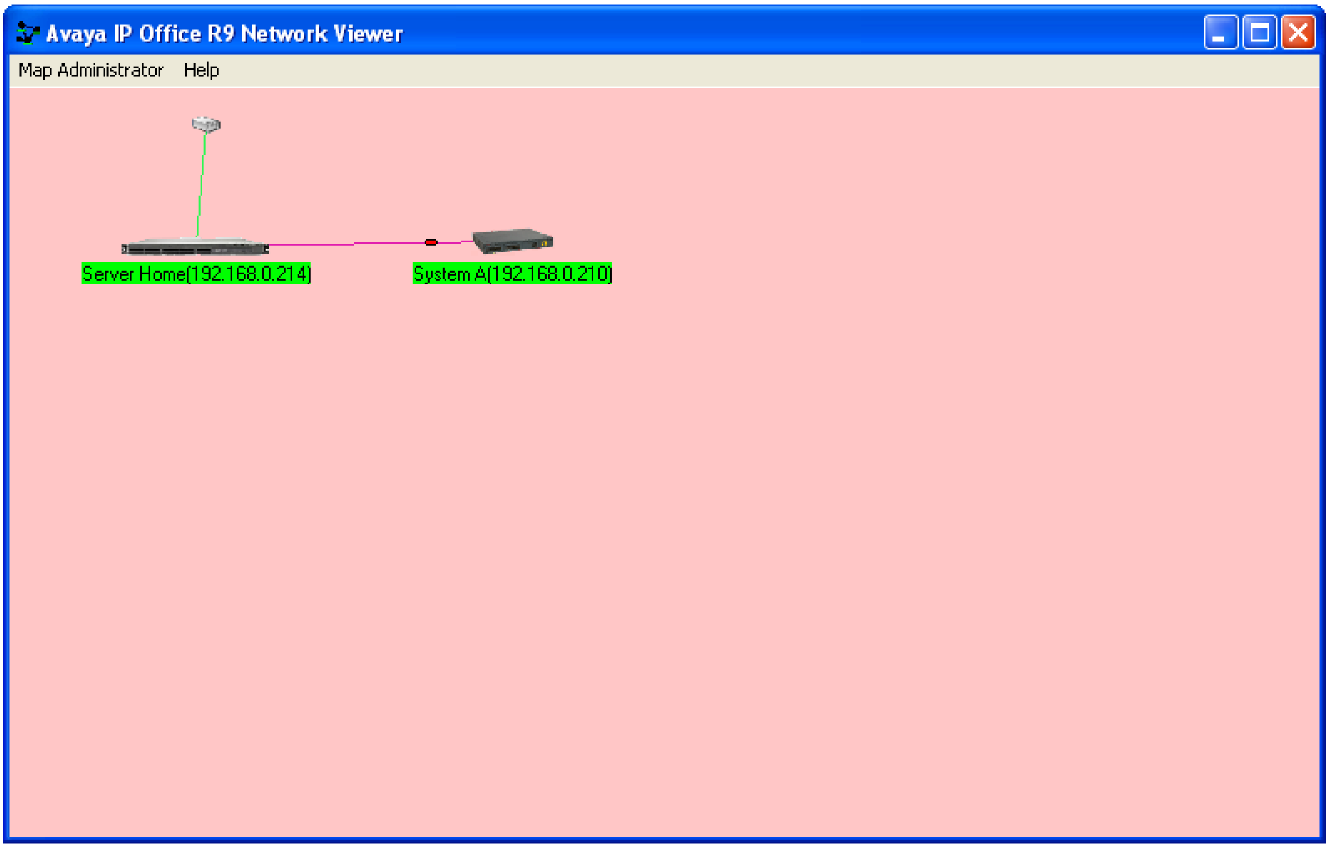
□ Port 1 (0-65535)

□ Port 2 (0-65535)

Remote IP	Remote Port	Inbound IP	Inbound Port	Outbound IP	Outbound Port	Type	Session TTL (ms)	Age (ms)	Max Age (ms)	Last Used

5.13 Network View

This status menu displays a view of the multisite network of which the system is a part. It can also display calls between the sites.



5.14 Partner Sessions

5.15 Performance Data

These options are only available when the **Development Tracing** option is selected in the **Trace Options | System** 69 menu. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

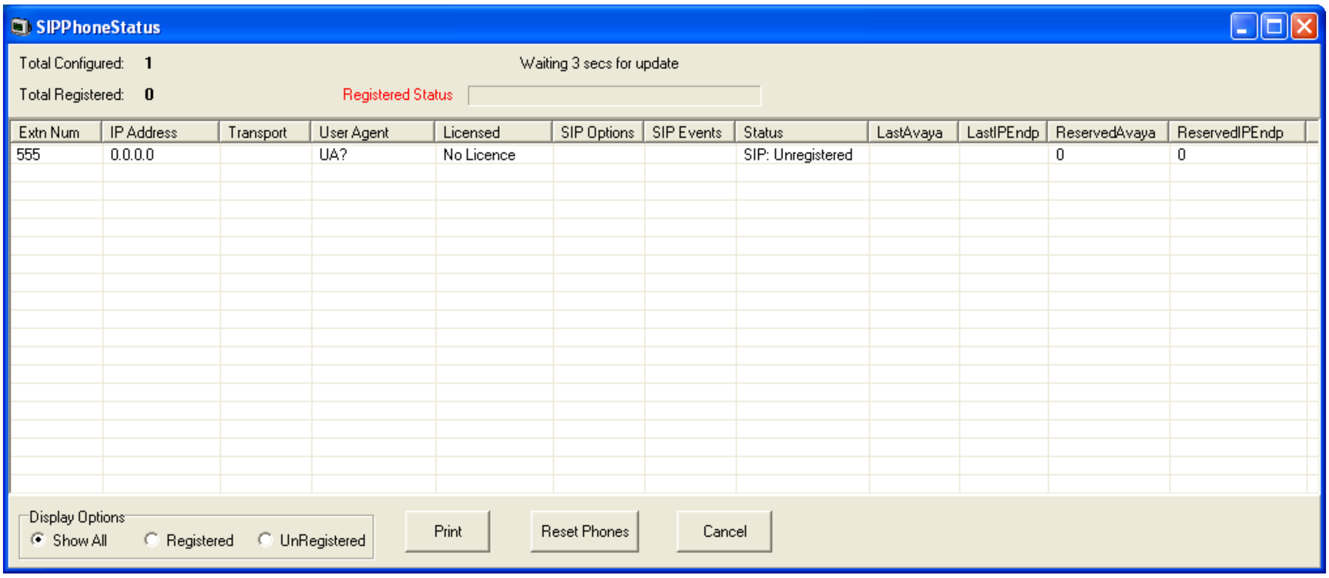
5.16 RTP Sessions

This status menu displays details of the RTP sessions being supported by the system.

5.17 SCN Licence

5.18 SIP Phone Status

This status menu displays the status of the SIP end points known by the system.



Total Configured: 1

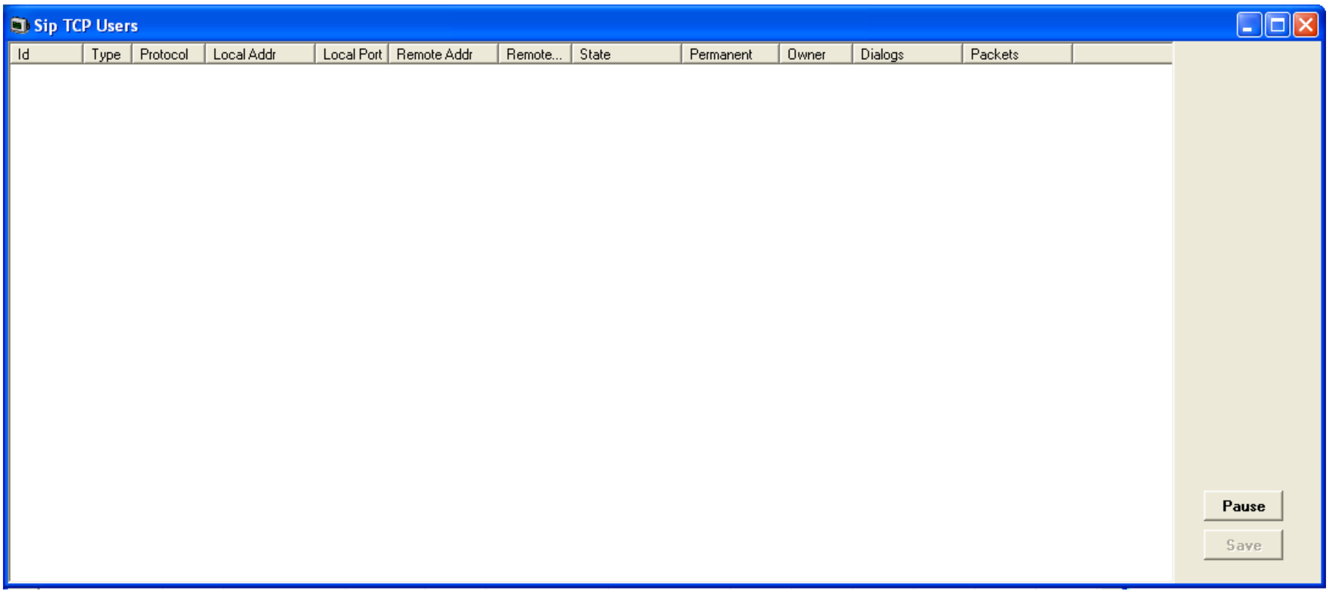
Total Registered: 0

Waiting 3 secs for update

Extn Num	IP Address	Transport	User Agent	Licensed	SIP Options	SIP Events	Status	LastAvaya	LastIPEndp	ReservedAvaya	ReservedIPEndp
555	0.0.0.0		UA?	No Licence			SIP: Unregistered			0	0

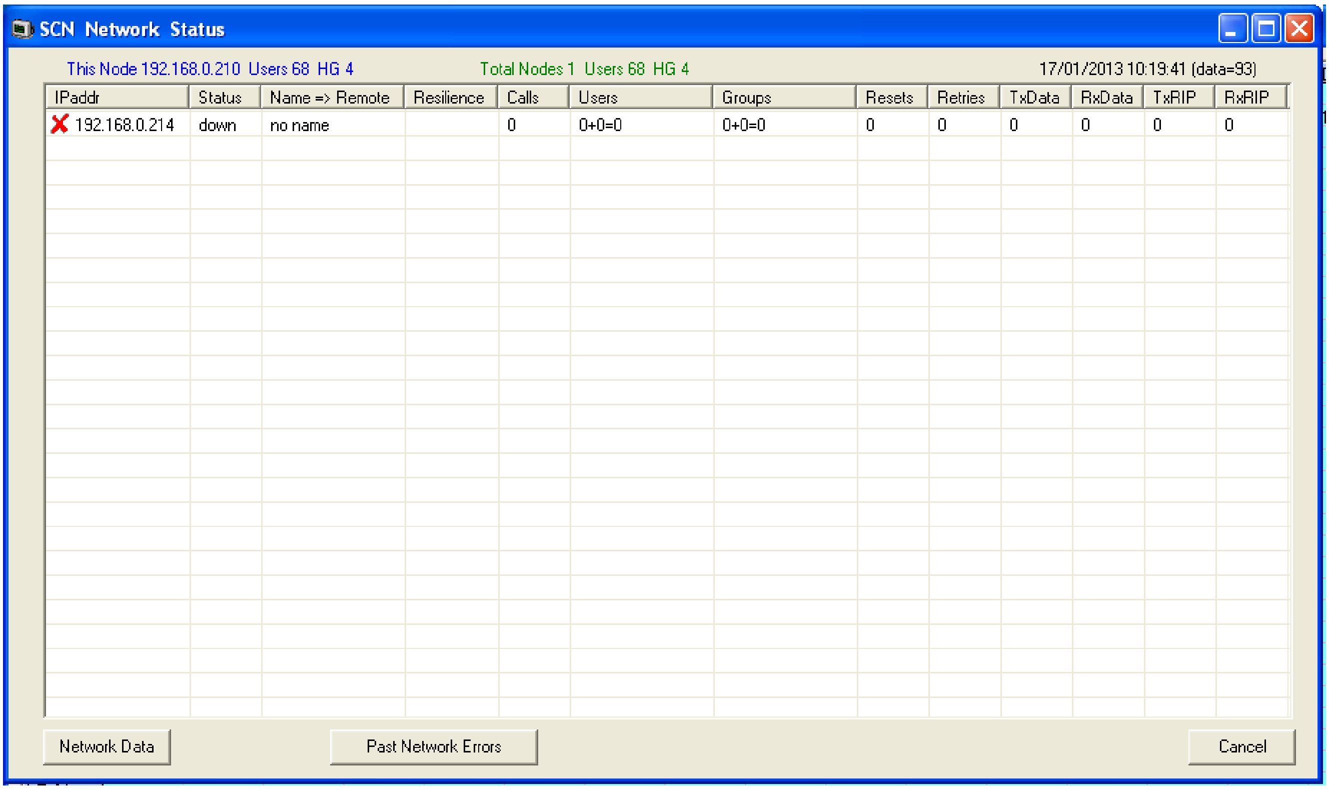
Display Options
● Show All ○ Registered ○ UnRegistered

5.19 SIP TCP User Data



5.20 Small Community Networking

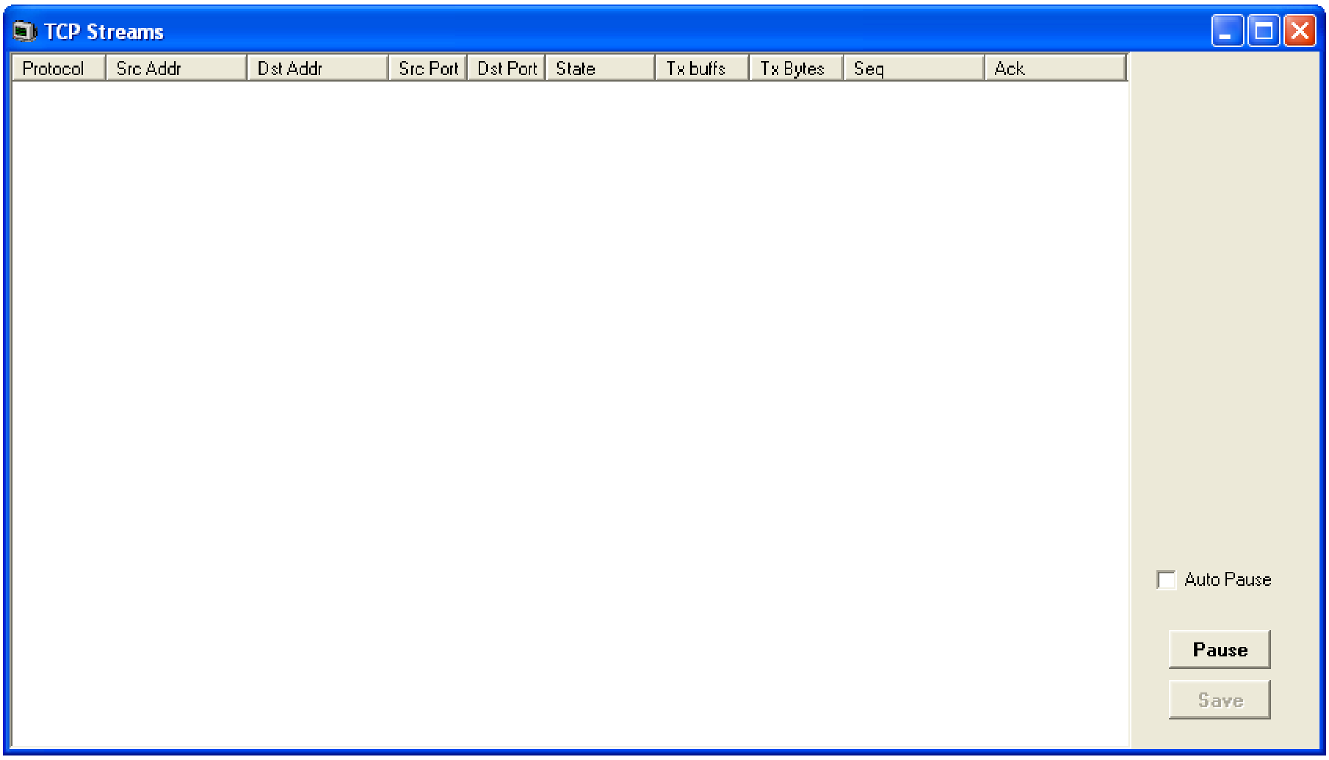
This status menu displays the status of the system's multisite network connections.



This Node 192.168.0.210 Users 68 HG 4 Total Nodes 1 Users 68 HG 4 17/01/2013 10:19:41 (data=93)

IPaddr	Status	Name => Remote	Resilience	Calls	Users	Groups	Resets	Retries	TxData	RxData	TxRIP	RxRIP
✗ 192.168.0.214	down	no name		0	0+0=0	0+0=0	0	0	0	0	0	0

5.21 TCP Streams Data



5.22 US PRI Trunks

This status menu displays the status of the system's US PRI trunk channels.

5.23 Voicemail Sessions

This status screen displays a summary of the voicemail service connections.

5.24 Voice Compression

This status menu displays the status of the voice compress channels provided by voice compression components not based on the TI chipset.

These options are only available when the **Development Tracing** option is selected in the **Trace Options | System** 69 menu. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

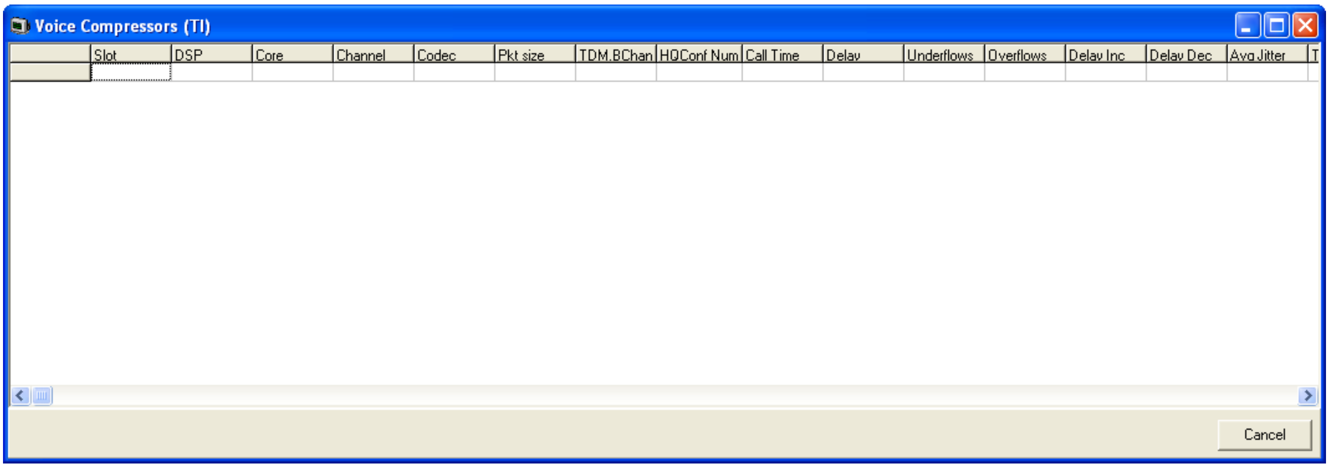
These options should only be used under the guidance of an authorized Avaya development engineer.

5.25 Voice Compression (TI)

This status menu displays the status of the voice compress channels provided by voice compression components based on the TI chipset.

These options are only available when the **Development Tracing** option is selected in the **Trace Options | System** 69 menu. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.



	Slot	DSP	Core	Channel	Codec	Pkt size	TDM.BChan	HQConf Num	Call Time	Delay	Underflows	Overflows	Delay Inc	Delay Dec	Avg Jitter	T

Chapter 6.
Example Monitor Settings

6. Example Monitor Settings

This document gives examples of the typical monitor settings to provide useable traces in different test and diagnosis scenarios.

Interpretation of the resulting traces is not covered in detail as this requires in depth data and telecoms experience.

Scenarios covered are:

6.1 Analog Trunk Caller ID

The following is an example trace from an analogue trunk that supports ICLID/CLI.

```
108691mS PRN: AtmTrunk1: StateChange CLIPossibleIncoming->Idle
108692mS PRN: AtmIO1: Block Forward OFF
108692mS PRN: AtmIO1: CLI Detection ON Equaliser ON
109703mS PRN: AtmTrunk1: CLI Message Rx'd:
109703mS PRN: 0x4500
109704mS PRN: 0x3031
109704mS PRN: 0x3134
109704mS PRN: 0x3136
109704mS PRN: 0x3035
109705mS PRN: AtmTrunk1: CLI Message Rx'd:
109705mS PRN: 0x4980
109706mS PRN: 0x3031
109706mS PRN: 0x3730
109706mS PRN: 0x372d
109706mS PRN: 0x3339
109706mS PRN: 0x3033
109707mS PRN: 0x3931
109707mS PRN: AtmTrunk1: CLI Message Rx'd:
109707mS PRN: 0x5800
09708mS PRN: AtmIO1: CLI Detection OFF Equaliser OFF
109708mS PRN: AtmTrunk1: StateChange CLIAwaitData->CLIDataSettle
109911mS PRN: AtmTrunk1: StateChange CLIDataSettle->CLIAwaitSecondRing
110191mS PRN: AtmTrunk1: StateChange CLIAwaitSecondRing->PossibleIncoming
```

Explanation
`108691mS PRN: AtmTrunk1: StateChange CLIPossibleIncoming->Idle` • The Line interface is primed ready for the possibility of an incoming ICLID/CLI message.
`108692mS PRN: AtmIO1: Block Forward OFF` • AtmIO1 = Line Number 1.
`108692mS PRN: AtmIO1: CLI Detection ON Equaliser ON` • CLI detection has been enabled for trunk 1.
`109703mS PRN: AtmTrunk1: CLI Message Rx'd:` • The first part of a ICLID message on trunk 1 has been detected.
`109703mS PRN: 0x4500` • 4500 = Date and time information. The info then follows in the 4 byte words.

`109704mS PRN: 0x3031`
`109704mS PRN: 0x3134`
`109704mS PRN: 0x3136`
`109704mS PRN: 0x3035`
• The call date and time is 16:05 on 14th January.
  • Month: 30 (hex) = 0 (ASCII), 31 (hex) = 1 (ASCII) > 01 (January)
  • Day: 31 (hex) = 1 (ASCII), 34 (hex) = 4 (ASCII) > 14th.
  • Hours: 31 (hex) = 1 (ASCII), 36 (hex) = 6 (ASCII) > 16:00.
  • Minutes: 30 (hex) = 0 (ASCII), 35 (hex) = 5 (ASCII) > 00:05.

`109705mS PRN: AtmTrunk1: CLI Message Rx'd:` • The second part of the ICLID message on trunk 1 has been detected.
`109705mS PRN: 0x4980` • 4980 = Calling Party Number information.

`109706mS PRN: 0x3031`
`109706mS PRN: 0x3730`
`109706mS PRN: 0x372d`
`109706mS PRN: 0x3339`
`109706mS PRN: 0x3033`
`109707mS PRN: 0x3931`
• The Calling Party Number is 01707-390391
  • 30 (hex) = 0 (ASCII), 31 (hex) = 1 (ASCII) > 01
  • 37 (hex) = 7 (ASCII), 30 (hex) = 0 (ASCII) > 70
  • 37 (hex) = 7 (ASCII), 2d (hex) = - (ASCII) > 7-
  • 33 (hex) = 3 (ASCII), 39 (hex) = 9 (ASCII) > 39
  • 30 (hex) = 0 (ASCII), 33 (hex) = 3 (ASCII) > 03
  • 39 (hex) = 9 (ASCII), 31 (hex) = 1 (ASCII) > 91

`109707mS PRN: AtmTrunk1: CLI Message Rx'd:` • The third part of the ICLID message on trunk 1 has been detected.
`109707mS PRN: 0x5800` • 5800 = End of ICLID.
`09708mS PRN: AtmIO1: CLI Detection OFF Equaliser OFF` • ICLID dectection has been disabled.

`109708mS PRN: AtmTrunk1: StateChange CLIAwaitData->CLIDataSettle`
`109911mS PRN: AtmTrunk1: StateChange CLIDataSettle->CLIAwaitSecondRing`
`110191mS PRN: AtmTrunk1: StateChange CLIAwaitSecondRing->PossibleIncoming`

- Line state changes from receiving ICLID to awaiting the incoming audio call.

6.2 ISDN Trunk Caller ID

1. On the PC running IP Office Manager, click the Windows Start icon and select Programs|IP Office|Monitor.
2. On the System Monitor, click **Trace Options** to select the trace settings.
3. On the **Call** tab, make sure the **Line Receive** check box is ticked.
4. Click **OK**.
5. In the System Monitor window, look for trace codes similar to the following:

```
22984658mS ISDNL3Rx: v=5 peb=5
            ISDN Layer3 Pcol=08(Q931) Reflen=2 ref=272F(Remote)
            Message Type = Setup
                InformationElement = BearerCapability
             0000 04 03 80 90 a2                                 .....
                InformationElement = CHI
             0000 18 03 a1 83 95                                 .....
                InformationElement = CallingPartyNumber
             0000 6c 0c 21 83 36 31 38 37 30 39 33 39 39 31       l.!.6187093991
                InformationElement = CalledPartyNumber
             0000 70 08 c1 36 34 36 37 31 33 31                  p..6467131
                InformationElement = HigherLayerCompat
             0000 7d 02 91 81                                    }...
```

- The Calling Party Number is [6187093991]
- The Called Party Number is [6467131]

6.3 ISDN Calls Disconnecting

Enable the following trace option settings:

Tab	Trace Options
ISDN	Layer 1, Layer 2, Layer 3, Layer 1 Send, Layer 1 Receive, Layer 2 Send, Layer 2 Receive, Layer 3 Send and Layer 3 Receive.
Call	Extension Send, Extension Receive, Extension TxP, Extension RxP, Line Send, Line Receive, Targetting and Call Logging.
System	Error, Print and Resource Status Prints.

This following is a sample trace of an PRI line going down, cutting off the calls in progress and then the line coming back up:

```
1072151mS ISDNL1Evt: v=0 peb=5,F2 F1
1072651mS ISDNL1Evt: v=0 peb=5,PHDI ?
1072651mS ISDNL3Evt: v=0 p1=0,p2=1001,p3=5,p4=127,s1=
1072651mS ISDNL3Evt: v=0 stacknum=0  State, new=NullState, old=Active id=4
1072652mS ISDNL3Evt: v=0 stacknum=0  State, new=NullState, old=Active id=24
1072653mS ISDNL3Evt: v=0 p1=0,p2=1001,p3=5,p4=0,s1=
1072656mS CMLineRx: v=5
          CMReleaseComp
          Line: type=Q931Line 5 Call: lid=5 id=4 in=1
          Cause=38, NetworkOOO
1072658mS CALL:2000/11/2408:40,00:00:17,033,01732464420,I,300,027624,,,,0
1072682mS CMLineRx: v=5
          CMReleaseComp
          Line: type=Q931Line 5 Call: lid=5 id=24 in=1
          Cause=38, NetworkOOO
1072684mS CALL:2000/11/2408:36,00:04:12,004,01689839919,I,300,027624,,,,0
1075545mS ISDNL1Evt: v=0 peb=5,F1 F2
1075595mS ISDNL1Evt: v=0 peb=5,PHAI ?
```

Explanation
`1072151mS ISDNL1Evt: v=0 peb=5,F2 F1` • PRI Line 5 (peb=5) has gone from the F1 state (normal Operational state) to the F2 state (Fault condition 1 state - receiving RAI or receiving CRC errors).
`1072651mS ISDNL1Evt: v=0 peb=5,PHDI ?` • Line 5 (peb=5) is now in the Disconnected state (PHDI – Physical Deactivate Indication).
`1072651mS ISDNL3Evt: v=0 p1=0,p2=1001,p3=5,p4=127,s1=` • ISDN Layer 3 event which gives current status of line 5 (p3=5)   • P1=0 -> ISDN Stacknum = 0.   • P2=1001 ->Line Disconnecting.   • P3=5 -> Internal reference number.   • P4=127 ->TEI = 127.   • S1= ->not used.
`1072651mS ISDNL3Evt: v=0 stacknum=0  State, new=NullState, old=Active id=4` • ISDN Layer 3 event which indicates that call with id 4 (id=4) on the first ISDN stack (stacknum=0) has changed from being Active (old=Active) to No Call exists (new=NullState).
`1072652mS ISDNL3Evt: v=0 stacknum=0  State, new=NullState, old=Active id=24` • ISDN Layer 3 event which indicates that call with id 24 (id=24) on the first ISDN stack (stacknum=0) has changed from being Active (old=Active) to No Call exists (new=NullState).
`1072653mS ISDNL3Evt: v=0 p1=0,p2=1001,p3=5,p4=0,s1=` • ISDN Layer 3 event which gives current status of line 5 (p3=5)   • P1=0 -> ISDN Stack number = 0.   • P2=1001 ->Line Disconnecting.   • P3=5 ->Internal reference number.   • P4=0 ->TEI = 0.   • S1= ->not used.

`1072656mS CMLineRx: v=5`
`          CMReleaseComp`
`          Line: type=Q931Line 5 Call: lid=5 id=4 in=1`
`          Cause=38, NetworkOOO`
• The incoming call (in=1) on line 5 (lid=5), with an internal call id of 4 (id=4) has been dropped. Clear code is 38 – Network Out Of Order (refer to ISDN Clear codes on our web site). There is no ISDNL3RX trace information as the call is dropped by the PBX NOT by the local exchange (due to the fact that we are no longer in communication with the Local Exchange!).

`1072658mS CALL:2000/11/2408:40,00:00:17,033,01732464420,I,300,027624,,,,0` • The Incoming call from 01732464420 to [02083]027624 (Extn300) has been disconnected.

`1072682mS CMLineRx: v=5`
`          CMReleaseComp`
`          Line: type=Q931Line 5 Call: lid=5 id=24 in=1`
`          Cause=38, NetworkOOO`

Explanation
• The incoming call (in=1) on line 5 (lid=5), with an internal call id of 24 (id=24) has been dropped. Clear code is 38 – Network Out Of Order (refer to ISDN Clear codes on our web site). Again there is no ISDNL3RX trace information as the call is dropped by the PBX NOT by the local exchange (due to the fact that we are no longer in communication with the Local Exchange!).
`1072684mS CALL:2000/11/2408:36,00:04:12,004,01689839919,I,300,027624,,,,0` • The incoming call from 01689839919 to [02083]027624 (Extn300) has been disconnected.
`1075545mS ISDNL1Evt: v=0 peb=5,F1 F2` • Line 5 (peb=5) has gone from the F2 state (Fault condition 1 state i.e. receiving RAI or receiving CRC errors) to the F1 state (normal Operational state).
`1075595mS ISDNL1Evt: v=0 peb=5,PHAI ?` • Line 5 (peb=5) has now fully recovered and is in the Connected state (PHAI – Physical Activate Indication).

6.4 System Rebooting

Enable the following trace option settings:

Tab	Trace Options
Call	Line Send, Line Receive, Extension Send, Extension Receive, Extension RxP, Extension TxP, Call Delta, Map, Targetting and Call Logging
System	Error, Print and Resource Status Prints.

You should also capture the data that is output on the DTE port on the back of the system control unit. This is necessary as the unit sends information to the DTE port during a reboot that is not seen by System Monitor as it cannot make contact with the unit via the LAN until after the reboot is completed.

If you are experiencing a rebooting problem then it is very important that both traces are provided in order to make an effective investigation into the problem.

Both traces should cover the period before and after the reboot occurs.

A reboot can be easily seen in the System Monitor application by the following:

```
== 25/4/2000 14:27 contact lost - reselect = 1
******************************************************************

******************** From: 192.168.27.1 (13597) ********************
== 25/4/2000 14:27 contact made
```

As a System Reboot can be easily located, all you have to do is search the trace for [contact lost].

6.5 ISDN Problems (T1 or E1 PRI connections)

Enable the following trace option settings. These provide information about the ISDN line itself and any calls in progress.

Tab	Trace Options
ISDN	Layer 1, Layer 2, Layer 3, Layer 1 Send, Layer 1 Receive, Layer 2 Send, Layer 2 Receive, Layer 3 Send and Layer 3 Receive.
Call	Extension Send, Extension Receive, Extension TxP, Extension RxP, Line Send, Line Receive, Targetting and Call Logging.
System	Error, Print and Resource Status Prints.

If the problem is with a specific ISDN line then the System Monitor can record info for a specific line only. This is done by entering an ISDN line number in the "Port Number" field. ISDN line numbers range from 0 – 8. The Line number is shown in the Configuration Lines List. A blank entry means all ISDN lines are monitored.

6.6 ISP & Dial-Up Data Connection Problems

Enable the following trace option settings:

Tab	Trace Options
ISDN	Later3 Tx and Layer3 Rx.
Call	Line Send, Line Receive, Targetting and Call Logging
Interface	Interface/Interface Queue
PPP	LCP Tx, LCP Rx, Security Tx, Security Rx, IPCP Tx and IPCP Rx.
System	Error, Print and Resource Status Prints.

If the problem is to a specific destination then System Monitor can record information pertinent to that connection only. This is done by entering the appropriate service name in the **Interface Name** field in the PPP trace option settings. A blank entry means monitor all data connections.

You should also look for things like PAP/CHAP password failure. This indicates that the "Service" configuration is not correct.

6.7 Remote Site Data Connection Problems over Leased (WAN) Lines

Enable the following trace option settings:

Tab	Trace Options
WAN	WAN Tx, WAN Rx and Events.
PPP	LCP Tx, LCP Rx, Security Tx, Security Rx, IPCP Tx, IPCP Rx, IP Tx and IP Rx.
System	Error, Print and Resource Status Prints.

- If the line is connected via the WAN port on the system's control unit, System Monitor should be configured to monitor the IP address of the system.
- If the line is connected via a WAN port on a WAN3 module, System Monitor should be configured to monitor the IP address of the WAN3 unit.

If the Leased Line problem is to a specific destination, System Monitor can record information pertinent to that connection only. This is done by entering the service name in the **Interface Name** field in PPP trace options settings. A blank entry means all data connections (Services) are monitored.

You should also look for things like PAP/CHAP password failure. This indicates that the service configuration is not correct.

Note that the WAN Tx and WAN Rx information is in raw hex format only. An in-depth knowledge of the IP Packet make-up is required to manually decode these messages – it is not done automatically.

6.8 Frame Relay Links

Enable the following trace option settings:

Tab	Trace Options
Frame Relay	Events, Tx Data, Tx Data Decode, Rx Data, Rx Data Decode, Tx Data and Mgmt Events (if Management enabled on link)

Please note that the following PPP options may also be required if using PPP over Frame Relay as the connection method :-

Tab	Trace Options
PPP	LCP Tx, LCP Rx, Security Tx, Security Rx, IPCP Tx, IPCP Rx, IP Tx and IP Rx

6.9 Speech Calls Dropping

ISDN or QSIG Line

Enable the following trace option settings:

Tab	Trace Options
ISDN	Layer 1, Layer 3, Layer 1 Send, Layer 1 Receive, Layer 3 Send and Layer 3 Receive
Call	Line Send, Line Receive, Extension Send, Extension Receive, Extension RxP, Extension TxP, Short Code Msgs, Call Delta, Targetting and Call Logging
System	Error, Print and Resource Status Prints

Analogue Line

Enable the following trace option settings:

Tab	Trace Options
ATM	Channel, I-O and CM Line
Call	Line Send, Line Receive, Extension Send, Extension Receive, Extension RxP, Extension TxP, Short Code Msgs, Call Delta, Targetting and Call Logging
System	Error, Print and Resource Status Prints

VoIP Line

Enable the following System Monitor settings:

Tab	Trace Options
ISDN[1]	Layer 3 Send[1] and Layer 3 Receive.
ATM[2]	Channel[2] , I-O2 and CM Line.
T1[3]	Line, Channel, Dialler, DSP and CAS.
H.323	H.323, H.323 Send, H.323 Receive, H.323 Fast Start[4], H.245 Send, H.245 Receive and View Whole Packet.
Call	Line Send, Line Receive, Extension Send, Extension Receive, Extension RxP, Extension TxP, Short Code Msgs, Call Delta, Targetting and Call Logging.
System	Error, Print and Resource Status Prints

Notes:

1. If VoIP call traverses a T1 ISDN, E1 ISDN, BRI ISDN or QSig line to get to its final destination.
2. If VoIP call traverses out over an Analogue Line to get to its final destination.
3. If VoIP call traverses out over a Channelized T1 Line to get to its final destination.
4. If in use by VPN Line or VoIP Extension

Channelized T1 Line

Enable the following System Monitor settings:

Tab	Trace Options
T1	Line, Channel, Dialler, DSP and CAS.
Call	Line Send, Line Receive, Extension Send, Extension Receive, Extension RxP, Extension TxP, Short Code Msgs, Call Delta, Targetting and Call Logging.
System	Error, Print and Resource Status Prints

6.10 Problems Involving Non-IP Phones

Enable the following trace option settings:

Tab	Trace Options
Call	Line Send, Line Receive, Extension Send, Extension Receive, Extension RxP, Extension TxP, Short Code Msgs, Call Delta, Targetting and Call Logging.

You should be able to pick up items like Call Setup, Call Proceeding, Alerting, Call Connected, and Call Disconnected. It provides a step by step trace of the process that the call has gone through. It presents all information relating directly to the setup of the call.

6.11 Problems Involving IP Phones

Enable the following trace option settings:

Tab	Trace Options
H.323	H.323, H.323 Send, H.323 Receive, H.323 Fast Start, H.245 Send, H.245 Receive, RAS Send, RAS Receive and View Whole Packet.

You should be able to pick up items like Call Setup, Call Proceeding, Alerting, Call Connected, and Call Disconnected. It provides a step by step trace of the process that the call has gone through. It presents all information relating directly to the setup of the call.

6.12 Locating a Specific PC Making Calls to the Internet

Enable the following trace option settings:

Tab	Trace Options
ISDN	Layer3 Tx and Layer3 Rx.
Interface	Interface Queue
Call	Line Send, Line Receive, Targeting and Call Logging
System	Error, Print and Resource Status Prints.

If NAT is not being used on the connection this produces:

```
Interface Queue: v=UKIP WAN 1 1
            IP Dst=194.217.94.100 Src=212.46.130.32 len=48 id=043e ttl=127 off=4000 pcol=6 sum=017c
             TCP Dst=80 (0050) Src=4105 (1009) Seq=338648156 Ack=0 Code=02 (SYN )
             Off=112 Window=8192 Sum=6aae Urg=0
              0000 02 04 05 b4 01 01 04 02
```

The source (Src) of this packet is 212.46.130.32, the destination (IP Dst) is 194.217.94.100, the protocol is TCP (pcol=6), the destination socket is 80 (80=World Wide Web HTTP i.e. a PC is trying to access a web page), the source socket is 4105 (unassigned - ie. free to be used by any program), the packet is a TCP SYN. All you need to do is locate the PC with address 212.46.130.32. To find out where on the web it was accessing type the IP Dst in the address bar of your browser and it takes you to that page.

If NAT is being used - you can tell this from the trace by observing System Monitor Traces like :-

```
PRN: ~NATranslator d40190dc 00000000
PRN: ~UDPNATSession in=c0a84d01 out=d40190dc rem=d401809c in_port=0035 out_port=1000 rem_port=0035
PRN: ~TCPNATSession in=c0a84d02 out=d40190dc rem=c2ed6d49 in_port=0423 out_port=1005 rem_port=0050
```

The above mentioned Interface Queue trace is preceded by the following System Monitor output :-

```
PRN: TCPNATSession in=c0a84d02 out=d40190dc rem=c2ed6d49 in_port=0423 out_port=1005 rem_port=0050
```

Where :-

- "in=" is the IP address (in hex format) of the device on the LAN that is initiating the request;
- "out=" is the IP address of the PBX (i.e. the local IP address of the link) as allocated by the ISP/Remote Routing device;
- "rem=" is the requested destination IP address;
- "in_port=" is the port (socket) number used by the initiating device on the LAN; "out_port=" is the outgoing port we use on the link (due to the NAT), and "rem_port=" is the requested destination port (socket) number.

6.13 Firewall Not Working Correctly

Enable the following trace option settings:

Tab	Trace Options
Interface	Interface Queue, Firewall Fail In and Firewall Fail Out.
System	Error, Print and Resource Status Prints.

When monitoring starts, if you do not see any specified ‘failing’ in the trace, then enable the following additional settings:

Tab	Trace Options
Interface	Interface Queue, Firewall Fail In and Firewall Fail Out.
System	Error, Print and Resource Status Prints.

This traces those packets that are Allowed In and Out of the PBX via the Firewall.

Note: The Interface trace option settings menu includes an **Interface Name** field. You can use this to enter the name of a particular service that you want to monitor.

6.14 Remote Site Data Connection over Leased (WAN) Lines

Enable the following trace option settings:

Tab	Trace Options
WAN	WAN Tx, WAN Rx and Events.
PPP	LCP Tx, LCP Rx, Security Tx, Security Rx, IPCP Tx, IPCP Rx, IP Tx and IP Rx.
System	Error, Print and Resource Status Prints.

- If the line is connected via the WAN port on the system's control unit, System Monitor should be configured to monitor the IP address of the system.
- If the line is connected via a WAN port on a WAN3 module, System Monitor should be configured to monitor the IP address of the WAN3 unit.

If the Leased Line problem is to a specific destination then System Monitor can record information pertinent to that connection only. This is done by entering the appropriate service name in the PPP trace option settings **Interface Name** field. A blank entry means all data connections (Services) are monitored.

You should also look for things like PAP/CHAP password failure. This indicates that the "Service" configuration is not correct.

Note that the WAN Tx and WAN Rx information is in raw hex format only. An in-depth knowledge of the IP Packet make-up is required to manually decode these messages – it is not done automatically.

6.15 Calls Answered/Generated by IP Office Applications

IP Office applications include Call Status, eBLF, eConsole, SoftConsole and Phone Manager (all variants).

Enable the following trace option settings:

Tab	Trace Options
Call	Line Send, Line Receive, Extension Send, Extension Receive, Extension TxP, Extension RxP, Short Code Msgs, Call Delta, Targetting and Call Logging.
System	Error, Print and Resource Status Prints.

6.16 Message Waiting Indication

To determine if Voicemail Pro is transmitting message waiting indication (MWI) information.

Enable the following trace option settings:

Tab	Trace Options
Call	Extension Send, MonIVR and Targetting
System	Print

Whenever voicemail is accessed for a mailbox (message leaving\retrieval); Voicemail sends a voicemail status update for that mailbox to the PBX. This is traced out within System Monitor with the MonIVR option and is an IVR Event type message.

The following is a trace example received with leaving a message to mailbox 206, note the following:

IVR Events indicate the number of new, read, saved messages. If the new message count is zero then the PBX should extinguish the message waiting light, otherwise the message waiting light should be activated.

When the MWL indication is sent to the phone, the CMExtnTx event should indicate the transmission of the message CMVoiceMailStatus with the number of new messages being in the display field (may also be in the calling party field). The UUI field may also contain the information format (length of UUI, number of messages, unread messages, extension state).

```
7201633mS CMExtnTx: v=203, p1=1
           CMVoiceMailStatus
           Line: type=DigitalExtn 3 Call: lid=0 id=-1 in=0
           Calling[00000001] Type=Default (100)
           UUI type=Local [....] [0x03 0x01 0x01 0x00 ]
           Display [Extn203 Msgs=1]
           Timed: 06/05/05 12:26
 7201634mS IVR Event: Voicemail message update for [Extn203]:- New=1,Read=1,Saved=0
```

Chapter 7.
Addendum

7. Addendum

7.1 Ports

The port being used by a data packet is shown as ***src=*** followed by a port number (http://www.iana.org/assignments/port-numbers).

For the following ports, System Monitor automatically adds the protocol name after the number when the log is displayed. For example ***src=23*** is displayed as ***src=23 (Telnet)***.

Number	Protocol
20	File Transfer [Default Data]
21	File Transfer [Control]
23	Telnet
25	Simple Mail Transfer
37	Time
43	Who Is
53	Domain Name Server
67	Bootstrap Protocol Server
68	Bootstrap Protocol Client
69	Trivial File Transfer
70	Gopher
79	Finger
80	World Wide Web-HTTP
115	Simple File Transfer Protocol
123	Network Time Protocol
137	NETBIOS Name Service
138	NETBIOS Datagram Service
139	NETBIOS Session Service
156	SQL Service
161	SNMP
162	SNMPTRAP
179	Border Gateway Protocol
1719	H.323Ras
1720	H.323/H.245
1764	NA Monitor
1765	NA PCPartner
1766	NA BLF/TAPI
1775	NA Who-Is response
3851	NA Voicemail
3852	NA Network DTE
3867	NA SoloMail
50791	IPO Voicemail
50792	IPO Network DTE
50793	IPO Solo Voicemail
50794	IPO Monitor
50795	IPO Voice Networking
50796	IPO PCPartner
50797	IPO TAPI
50798	IPO Who-Is response
50799	IPO BLF
50800	IPO License Dongle
54050	BT Fusion

7.2 Protocols

The protocol being used by a data packet is shown as ***pcol=*** followed by a protocol number (http://www.iana.org/assignments/protocol-numbers).

For the following common protocols, System Monitor automatically adds the protocol name after the number when the log is displayed. For example ***pcol=1*** is displayed as ***pcol=1 (ICMP)***.

Number	Protocol	Monitor shows...
1	Internet Control Message	ICMP
2	Internet Group Management	IGMP
6	Transmission Control	TCP
8	Exterior Gateway Protocol	EGP
9	Interior Gateway Protocol	IGP
17	User Datagram	UDP
41	Ipv6	IPV6
46	Reservation Protocol	RSVP
47	General Routing Encapsulation	GRE
58	ICMP for IPv6	IPv6-ICMP
111	IPX in IP	IPX-In-IP
115	Layer Two Tunneling Protocol	L2TP
121	Simple Message Protocol	SMP

7.3 IP Office Ports

As mentioned, a number of different ports are used for access to systems. The following table lists some of the ports on which the system control unit listens for different types of access.⬅ Indicates a listening port on the system control unit. ➡ indicates a port to which the IP Office sends, for example to a PC running an IP Office application.

* Indicates that the port and or protocol can be changed.

Port		Protocol		Function
25*	➡	SMTP	TCP	Email system alarms from the system to SMTP server.
37	➡	Time	UDP	Time requests from the system to a Time Server (RFC868).
53	⬅	DNS	UDP	Domain Name Service responses.
67	⬅	BOOTP/DHCP	UDP	DHCP server operation.
68	➡	BOOTP/DHCP	UDP	DHCP client operation.
69	⬅	TFTP	UDP	File requests to the system.
69	➡	TFTP	UDP	File requests by the system.
161*	⬅	SNMP	UDP	From SNMP applications.
162*	➡	SNMP Trap	UDP	To addresses set in the system configuration.
500	⬅	IKE	UDP	Key exchange for IPSec protocol.
389*	➡	LDAP	TCP	Lightweight Directory Access Protocol.
520	➡	RIP	UDP	To and from the system to other RIP devices. For RIP1 and RIP2 (RIP1 compatible) the destination address is a subnet broadcast, eg. 192.168.42.255. For RIP2 Multicast the destination address is 224.0.0.9.
520	⬅	RIP	UDP	
1701	⬅	L2TP	UDP	Layer 2 tunneling protocol.
1718	⬅	H.323	UDP	H.323 Discovery
1719	⬅	H.323 RAS	UDP	H.323 Status. VoIP device registering with the system.
1720	➡	H.323/H.245	UDP	H.323 Signalling. Data to a registered VoIP device.
2127	➡	(UDP)	UDP	PC Wallboard to CCC Wallboard Server.
3478	➡	SIP	UDP	Port used for STUN requests from the system to the SIP provider.
5060	⬅ ➡	SIP	UDP/ TCP*	SIP Line Signalling
8080	➡	HTTP	TCP	Browser access to the Delta Server application.
8089	➡	Enconf	UDP	From the system to the Conferencing Center Server Service. User access to the conference center is direct via HTTP sessions.
8888	➡	HTTP	TCP	Browser access to the IP Office ContactStore (VRL) application.
49152 to 53247 *	⬅ ➡	RTP/RTCP	UDP	Dynamically allocated ports used during VoIP calls for RTP and RTCP traffic. The port range can be adjusted through the System | Gatekeeper tab.
50791	➡	IPO Voicemail	UDP	To voicemail server address.
50793	⬅	IPO Solo Voicemail	UDP	From IP Office TAPI PC with Wave drive user support.
50794	⬅	IPO System Monitor	UDP	From System Monitor application.
50795	⬅	IPO Voice Networking	UDP	Small Community Network signalling (AVRIP) and BLF updates. Each system does a broadcast every 30 seconds. BLF updates are sent required up a maximum of every 0.5 seconds.
50796	⬅	IPO PCPartner	UDP	From an system application (for example Phone Manager or SoftConsole). Used to initiate a session between the system and the application.
50797	⬅	IPO TAPI	UDP	From an system TAPI user PC.
50798	➡	(UDP)	UDP	*BT Fusion variant. No longer used.*
50799	➡	IPO BLF	UDP	Broadcast to the system LAN and the first 10 IP addresses registered from other subnets.
50800	➡	IPO License Dongle	UDP	To the License Server IP Address set in the system configuration.
50801	⬅	EConf	UDP	Conference Center Service to system.
50802	⬅	Discovery	TCP	IP Office discovery from IP Office Manager.
50804 *	⬅	Service Access Protocol	TCP	IP Office configuration settings access.
50805 *	⬅		TCP	" TLS Secure.

Port		Protocol		Function
50808 *	←		TCP	system status access.
50812 *	←		TCP	IP Office security settings access.
50813 *	←		TCP	" TLS Secure.

- CDR/SMDR from the system is sent to the port number and IP address defined during configuration and using either TCP or UDP as selected.

Ports

System Monitor can be used to display IP packet details including the source and destination Port numbers. As well as displaying the port numbers (in decimal), System Monitor also displays the names of more commonly used ports including system specific ports.

For example "src = 23" is interpreted as "src = 23 (Telnet)".

The list below details the ports currently decoded by System Monitor. For a full list of assigned non-system ports see http://www.iana.org/assignments/port-numbers.

- 20 File Transfer [Default Data]
- 21 File Transfer [Control]
- 23 Telnet
- 25 Simple Mail Transfer
- 37 Time
- 43 Who Is
- 53 Domain Name Server
- 67 Bootstrap Protocol Server
- 68 Bootstrap Protocol Client
- 69 Trivial File Transfer
- 70 Gopher
- 79 Finger
- 80 World Wide Web-HTTP
- 115 Simple File Transfer Protocol
- 123 Network Time Protocol
- 137 NETBIOS Name Service
- 138 NETBIOS Datagram Service
- 139 NETBIOS Session Service
- 156 SQL Service
- 161 SNMP
- 162 SNMPTRAP
- 179 Border Gateway Protocol
- 1719 H.323Ras
- 1720 H.323/H.245
- 50791 IPO Voicemail
- 50792 IPO Network DTE
- 50793 IPO Solo Voicemail (i.e. Wave driver for TAPI)
- 50794 IPO System Monitor
- 50795 IPO Voice Networking
- 50796 IPO PCPartner
- 50797 IPO TAPI
- 50798 IPO Who-Is response
- 50799 IPO BLF
- 50800 IPO License Dongle
- 50801 EConf

Protocols

System Monitor, as well as displaying the Protocol number (in decimal) of packets, also displays the names of the more common Protocols. For example "pcol = 1" is decoded as "pcol = 1 (ICMP)".

Protocol numbers currently decoded by System Monitor are:

- 1 - Internet Control Message [ICMP]
- 2 - Internet Group Management [IGMP]
- 6 - Transmission Control [TCP]
- 8 - Exterior Gateway Protocol [EGP]
- 9 - Interior Gateway Protocol [IGP]
- 17 - User Datagram [UDP]
- 41 - Ipv6 [IPV6]
- 46 - Reservation Protocol [RSVP]
- 47 - General Routing Encapsulation [GRE]
- 58 - ICMP for IPv6 [IPv6-ICMP]
- 111 - IPX in IP[IPX-In-IP]
- 115 - Layer Two Tunneling Protocol [L2TP]
- 121 - Simple Message Protocol [SMP]

7.4 Cause Codes (ISDN)

When a call is ended, a cause code may be shown in the System Monitor trace. This cause code is not necessarily an error as cause codes are shown at the end of normal calls. Cause codes 0 to 102 are standard ISDN cause codes. Causes codes 103 upwards are system specific codes.

To display cause codes, ensure that the System Monitor | Call | Extension Send option is enabled. The cause code is then shown are part of ***CMExtnTx:*** events within the monitor trace. For example:

```
10185mS CMExtnTx: v=100, p1=1
        CMReleaseComp
        Line: type=DigitalExtn 3 Call: lid=0 id=-1 in=0
        UUI type=Local [....] [0x03 0x00 0x00 0x00 ]
        Cause=16, Normal call clearing
        Timed: 12/07/05 11:00
```

The cause codes are listed below. Those marked with a * were added in release 3.0.1. Those marked with a + were added in 3.0.40. Note that the Disconnect codes marked with a * or + are not available in 2.1 or 3.0DT releases.

Cause Code	Definition
0	Unknown.
1	Unallocated (unassigned) number.
2	No route to specific transit network/(5ESS)Calling party off hold.
3	No route to destination / (5ESS) Calling party dropped while on hold.
4	Send special information tone / (NI-2) Vacant Code.
5	Misdialed trunk prefix.
6	Channel unacceptable.
7	Call awarded and being delivered.
8	Preemption/(NI-2)Prefix 0 dialed in error.
9	Preemption, cct reserved / (NI-2) Prefix 1 dialed in error.
10	(NI-2) Prefix 1 not dialed.
11	(NI-2) Excessive digits received call proceeding.
16	Normal call clearing.
17	User busy.
18	No user responding / No response from remote device.
19	No answer from user.
20	Subscriber absent (wireless networks).
21	Call rejected.
22	Number changed.
23	Redirection to new destination.
25	Exchange routing error.
26	Non-selected user clearing.
27	Destination Out Of Order.
28	Invalid number format.
29	Facility rejected.
30	Response to STATUS ENQUIRY.
31	Normal, unspecified.
34	No cct / channel available.
38	Network out of order.
39	Permanent frame mode connection out of service.
40	Permanent frame mode connection is operational.
41	Temporary failure.
42	Switching equipment congestion.
43	Access information discarded.
44	Requested cct / channel not available.
45	Pre-empted.
46	Precedence blocked call.
47	Resources unavailable/(5ESS)New destination.
49	Quality of service unavailable.
50	Requested facility not subscribed.

Cause Code	Definition
52	Outgoing calls barred.
54	Incoming calls barred.
57	Bearer capability not authorised.
58	Bearer capability not presently available.
63	Service or option not available, unspecified.
65	Bearer capability not implemented.
66	Channel type not implemented.
69	Requested facility not implemented.
70	Only restricted digital bearer capability is available.
79	Service or option not implemented, unspecified.
81	Invalid call reference.
82	Identified channel does not exist.
83	A suspended call exists, but this id does not.
84	Call id in use.
85	No call suspended.
86	Call having the requested id has been cleared.
87	User not a member of Closed User Group.
88	Incompatible destination.
90	Non-existent Closed User Group.
91	Invalid transit network selection.
95	Invalid message, unspecified.
96	Mandatory information element missing.
97	Message type non-existent/not implemented.
98	Message not compatible with call state, non-existent or not implemented.
99	Information element non-existent or not implemented.
100	Invalid information element contents.
101	Message not compatible with call state / (NI-2) Protocol threshold exceeded.
102	Recovery on timer expiry.
IP Office Specific Cause Codes	
103	Parameter not implemented.
110	Message with unrecognised parameter.
111	Protocol error, unspecified.
117	Parked (Internal system code).
118	UnParked (Internal system code).
119	Pickup (Internal system code).
120	Reminder (Internal system code).
121	Redirect (Internal system code).
122	Call Barred (Internal system code).
123	Forward To Voicemail (Internal system code).
124	Answered By Other (Internal system code).
125	No Account Code (Internal system code).
126	Transfer (Internal system code).
129	Held Call (Internal system code).*
130	Ring Back Check (Internal system code).*
131	Appearance Call Steal (Internal system code).*
132	Appearance Bridge Into (Internal system code).*
133	Bumped Call (Internal system code).*
134	Line Appearance Call (Internal system code).+
135	Unheld Call (Internal system code).+
136	Replace Current Call (Internal system code).+
137	Glare (Internal system code).+
138	R21 Compatible Conf Move (Internal system code).+

Cause Code	Definition
139	RingBack Answered (Internal system code).+
140	Transfer Request Failed (Internal system code).+
141	HuntGroup Drop (Internal system code).+

7.5 Decoding FEC Errors

This section details how to decoding the FEC Receiver Error "PRN" statements that appear in the log. These "Fast Ethernet Controller" error messages are shown when the System/Print option is enabled.

An example error would be:

```
PRN: IP403_FEC::ReceiverError 844
```

The message format is:-

```
PRN: PLATFORM_FEC::ReceiverError ABCD
```

Where:-

- PRN: = Indicates that message was output as the result of having the **System | Print** option enabled.
- PLATFORM_ = Indicates the type of system control unit reporting the error. Possible values are IP401NG (Small Office Edition), IP403, IP406, IP406V2 (shows as IP405 in Version 2.1(27)) and IP412.
- ABCD = This is the actual error code. It is a decode of the "Ethernet Receive Buffer Descriptor" packet. Note that if the most significant byte (ie. A) is 0 (zero) it is not printed and the error code is only 3 characters long (ie. BCD).

FEC::ReceiverError Codes are derived from the "Ethernet Receive Buffer Descriptor (RxBD)". The table below shows the bits within the RxBD that are used to generate the error codes. Those labeled as "N/U" are NOT used in the FEC Error Decoding mechanism although they may be non zero.

Byte	Bit	Value	Option	Description
A	0	8	N/U	May be non-zero but not used for FEC decode.
	1	4	N/U	May be non-zero but not used for FEC decode.
	2	2	N/U	May be non-zero but not used for FEC decode.
	3	1	N/U	May be non-zero but not used for FEC decode.
B	4	8	L	Last in frame. 0 = The buffer is not the last in the frame. 1 = The buffer is the last in the frame.
	5	4	0	Always zero.
	6	2	0	Always zero.
	7	1	N/U	May be non-zero but not used for FEC decode.
C	8	8	N/U	May be non-zero but not used for FEC decode.
	9	4	N/U	May be non-zero but not used for FEC decode.
	10	2	LG	Length Error: Rx frame length violation. The frame length exceeds the value of MAX_FRAME_LENGTH in the bytes. The hardware truncates frames exceeding 2047 bytes so as not to overflow receive buffers This bit is valid only if the L bit is set to 1.
	11	1	NO	Non-Octet: A frame that contained a number of bits not divisible by 8 was received and the CRC check that occurred at the preceding byte boundary generated an error. NO is valid only if the L bit is set. If this bit is set, the CR bit is not set.
D	12	8	SH	Short Frame: A frame length that was less than the minimum defined for this channel was recognized.
	13	4	CR	CRC Error: This frame contains a CRC error and is an integral number of octets in length. This bit is valid only if the L bit is set.
	14	2	OV	Overrun Error: A receive FIFO overrun occurred during frame reception. If OV = 1, the other status bits, LG, NO, SH, CR, and CL lose their normal meaning and are cleared. This bit is valid only if the L bit is set.
	15	1	TR	Truncate Error: Set if the receive frame is truncated (= 2 Kbytes)

Example
Decode of typical message produced using above information :-

```
PRN: IP403_FEC::ReceiverError 844
```

The Error code in the above example is 844.

- Byte A = 0 and so was not shown.
- Byte B = 8, which is 1000 in binary - so bit 4 (L) is set
- Byte C = 4, which is 0100 in binary – so bit 9 (N/U) is set
- Byte D = 4, which is 0100 in binary – so bit 13 (CR) is set

This is a Receive CRC error (as bit 13 of the RxBD is set) – note that the first byte (A) is missing so it is equal to 0, resulting in a 3 byte error code.

7.6 Miscellaneous

What does the message "PRN: FEC::ReceiverError" mean?

FEC stands for Fast Ethernet Controller (100mb LAN). The "ReceiverError" line is followed by a number that denotes the exact problem.

Basically it is stating that the system received a packet that it considers wrong or corrupt in some way or perhaps there was a collision so it threw it away, the packet would then have been re-sent. This is does not normally indicate a problem and is nothing to worry about unless the error's are streaming in the trace. See Decoding FEC Errors 133.

What does the message "PRN: UDP::Sending from indeterminate address to 0a000003 3851" mean?

The port number 3851 at the end indicates that the system is looking for an IP Office Voicemail Server.

If your system is not using voicemail, remove the entry in the Voicemail IP Address field, found on the Voicemail tab of the System form in the system configuration.

Index