



# **IP Office**

## **IP Office System Monitor**

#### Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

#### Documentation Disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya.

#### Link Disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this Documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

#### License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT <http://support.avaya.com/LicenseInfo/> ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. 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 End User. "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. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s): Designated System(s) License (DS).

End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified 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.

#### Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

#### Third-Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya's web site at: <http://support.avaya.com/ThirdPartyLicense/>

#### Avaya 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. Suspected security vulnerabilities with Avaya Products should be reported to Avaya by sending mail to: [securityalerts@avaya.com](mailto:securityalerts@avaya.com). For additional support telephone numbers, see the Avaya Support web site (<http://www.avaya.com/support>).

#### Trademarks

Avaya and the Avaya logo are registered trademarks of Avaya Inc. in the United States of America and other jurisdictions. Unless otherwise provided in this document, marks identified by "®," "TM" and "SM" are registered marks, trademarks and service marks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

#### Documentation information

For the most current versions of documentation, go to the Avaya Support web site (<http://www.avaya.com/support>) or the IP Office Knowledge Base (<http://marketingtools.avaya.com/knowledgebase/>).

#### Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. The support telephone number is 1 800 628 2888 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>.

# Contents

## 1. The System Monitor Application

1.1 Installing Monitor.....	8
1.2 Starting Monitor.....	9
1.3 Status Report.....	10
1.4 Monitor Icons.....	11
1.5 The Alarm Log.....	12
1.6 Menus .....	13
1.7 File Logging.....	16
1.8 Miscellaneous.....	18

## 2. Trace Options

2.1 ATM .....	21
2.2 Call .....	22
2.3 DTE .....	23
2.4 EConf .....	24
2.5 Frame Relay.....	25
2.6 GOD .....	26
2.7 H.323 .....	27
2.8 Interface .....	28
2.9 ISDN .....	29
2.10 Key/Lamp.....	31
2.11 LDAP .....	32
2.12 Media .....	33
2.13 PPP .....	34
2.14 R2 .....	35
2.15 Routing .....	36
2.16 SCN .....	37
2.17 Services .....	38
2.18 SIP .....	39
2.19 System .....	40
2.20 T1 .....	41
2.21 VPN .....	42
2.22 WAN .....	43

## 3. Status Screens

3.1 US PRI Trunks.....	47
3.2 RTP Sessions.....	48
3.3 Voicemail Sessions.....	49
3.4 Small Community Networking.....	50
3.5 Partner Sessions.....	51
3.6 Alarms .....	52
3.7 Map Status.....	53
3.8 IP Phone Status.....	54

## 4. Example Monitor Settings

4.1 Analog Trunk Caller ID.....	57
4.2 ISDN Trunk Caller ID.....	58
4.3 ISDN Calls Disconnecting.....	59
4.4 System Rebooting.....	61
4.5 ISDN Problems (T1 or E1 PRI connections).....	62
4.6 ISP & Dial-Up Data Connection Problems.....	63
4.7 Remote Site Data Connection Problems over Leased (WAN) Lines.....	64
4.8 Frame Relay Links.....	65
4.9 Speech Calls Dropping.....	66
4.10 Problems Involving Non-IP Phones.....	69

4.11 Problems Involving IP Phones.....	69
4.12 Locating a Specific PC Making Calls to the Internet .....	70
4.13 Firewall Not Working Correctly.....	71
4.14 Remote Site Data Connection over Leased (WAN) Lines .....	71
4.15 Calls Answered/Generated by IP Office Applications .....	72
4.16 Message Waiting Indication.....	72

## 5. Addendum

5.1 IP Office Ports.....	76
5.2 Cause Codes (ISDN).....	79
5.3 Decoding FEC Errors.....	82
Index .....	85



# **Chapter 1.**

# **The System Monitor Application**



# 1. The System Monitor Application

The IP Office System Monitor application is used to assist in the diagnosis of problems. Through configuration of its settings it is able to display information on a specific area of an IP Office's operation. It can capture that information to log files for later analysis.

```

***** 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 intended primarily for use and interpretation by Avaya support staff. The settings within System Monitor and the information shown in the monitor trace frequently change between IP Office software releases.
- Analysis of the information shown in monitor traces requires detailed data and telecommunications knowledge plus IP Office knowledge and is not intended for the general user.
- Despite the above facts, all persons maintaining IP Office systems must be able to run System Monitor in order to capture trace for submission with escalated fault reports even if they cannot interpret the trace themselves.

---

## 1.1 Installing Monitor

System Monitor is supplied on the IP Office Administrator Applications CD. It is normally installed by default along with the IP Office Manager application. However, if necessary it can be installed separately.

- Note  
Two versions of System Monitor are provided on the IP Office Administrator Application CD, one for IP Office 4.0+ systems and one for pre-IP Office 4.0 systems. The former is installed by default.

### Installing System Monitor

1. Inserting the CD into the PC's CD drive. This should start the Installation Wizard.
2. Select the required language.
3. Select Modify and click Next.
4. From the list of available applications ensure that System Monitor is selected. Be careful about de-selecting any other highlighted options as this will trigger their removal if already installed.
  - The item labeled Previous System Monitor is a version of System Monitor for pre-IP Office 4.0 systems.
5. Click Next.



## 1.2 Starting Monitor

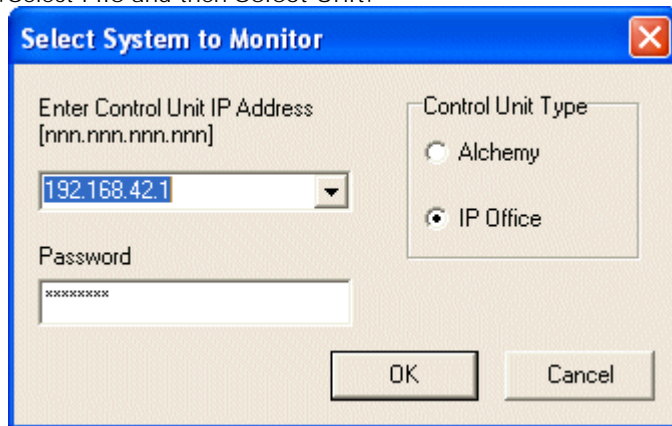
System Monitor can be run from a PC on the same local IP subnet as the targeted IP Office or it can run on a PC on a remote subnet.

If the PC running the System Monitor and the targeted IP Office are on the same subnet then you can either use the IP Office's unique IP address (eg. 192.168.42.1) or the local subnet's broadcast address (eg. 192.168.42.255). If there is more than one IP Office on the local subnet then the IP Office's unique IP address MUST be used.

If the PC running the System Monitor and the targeted IP Office are on the different subnets (these can be different local subnets or from a remote subnet) then the PBX's unique IP address MUST be used. 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 been run before it will attempt to connect with the system which it monitored previously. If otherwise or you want to monitor a different system use the steps below.
3. Select File and then Select Unit.



4. Enter the IP Address and Password (see below) of the IP Office Control Unit you want to monitor.
  - Using IP Office Manager it is possible to set a specific System Monitor Password for System Monitor access to an IP Office system. If the IP Office doesn't have a System Monitor Password set, System Monitor uses the IP Office's System Password. The System Monitor Password and System Password are both set within the IP Office system security configuration settings.
5. For an IP Office system, ensure that the Control Unit Type is set to *IP Office*.
6. Click OK.
7. Once System Monitor has connected with a system, the [status report information](#)<sup>10</sup> for the system is displayed.

## 1.3 Status Report

The status report is output whenever System Monitor connects to an IP Office system.

When first connected to an IP Office, the monitor trace displays some basic information about the IP Office system to which it has connected. The information will vary depending on the type of IP Office control unit and the equipment installed with that control unit. The example below is a typical output for an IP Office IP500 system.

The first few lines include the time, date and IP address of the system being monitored and the up time of that system. A key value for maintainers is the indication of how long the system has been running since it was last rebooted.

```
***** 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: 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 IP Office system. This line is output at regular intervals, set through the [file logging preferences](#) <sup>16</sup>.















```
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 =	<i>Not Used.</i>
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 IP Office reboot.

In addition, when System Monitor is started, the initial output may include the IP Office's alarm log, see [The Alarm Log](#) <sup>12</sup>.

## 1.4 Monitor Icons

The System Monitor window contains a number of icons:

-  Open File  
Open a previous logged monitor file.
-  Save Trace  
Save the current monitor trace to a text file.
-  Rollover Log  
Force the current log file to rollover. A date and time stamp will be added to the log file and a new log started. This button is greyed out when the monitor trace is not being logged to a file.
-  Stop Logging  
Stop logging the monitor trace to a file.
-  Start Logging  
Start logging the monitor trace to a file.
-  Text Log File  
This icon indicates that System Monitor is currently set to text file logging. Clicking the icon changes the mode to binary file logging (forcing a rollover of any current log file).
-  Binary Log File  
This icon indicates that System Monitor is currently set to binary file logging. Clicking the icon changes the mode to text file logging (forcing a rollover of any current log file).
-  Clear Screen Display  
Clear the current trace shown in the display.
-  Run Screen Display  
Show the monitor trace in the display.
-  Freeze Screen Display  
Stop the monitor trace in the display. This does not stop the monitor trace from being logged to file.
-  Reconnect  
Connect to the IP Office specified in the Select Unit options.
-  Filter Trace Options  
Set the filter options for what should be included in the monitor trace.
-  Log Preferences  
Set the format and destination for the monitor log file.
-  Select Unit  
Set the details of the IP Office unit to monitor.

---

## 1.5 The Alarm Log

When started, the System Monitor trace can include an Alarm Log Dump similar to the following:

```
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 0095e200
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 0095e200
3004mS PRN: +++ END OF ALARM LOG DUMP +++
```







The presence of alarms is not necessarily critical as the IP Office keeps a record of the first 8 alarms received since the alarm log was last cleared. However once the alarm log is full additional alarms are ignored.

You can view the current entries in the alarm log at any time by running System Monitor and selecting Status and then [Alarms](#)<sup>[52]</sup>. This will display the alarms and allows you to clear them by clicking Clear Alarms.


The alarms themselves cannot be easily interpreted. However on a site that is having repeated significant problems you may be asked to provide a record of the alarms for interpretation by Avaya.

## 1.6 Menus


### File Menu

-  Select Unit  
Shows the Select Unit form to specify the IP Office to be monitored.
-  Reconnect  
Re-establish connection with the IP Office set in the Select Unit form.
-  Open File  
Allows a previous monitor log file to be opened. This is useful for opening binary log files that cannot otherwise be opened in plain text editor applications.
-  Save Screen Log As...  
Save the current display contents to a text file (.txt).
-  Rollover Log  
Used in conjunction with logging to end the current log file and start a new log file. The date and time is added to the file name of the log file just ended.
-  Log Preferences  
Allows you to specify the logging of the monitor trace to a file..
- Exit  
Close the System Monitor program.

### Edit Menu

-  Clear Display  
Clear the monitor display.
- Copy  
Copies any currently selected content in the System Monitor display to the Windows clipboard.
- Select All  
Selects all the content in the System Monitor display.
- Find  
Display a search menu for use with the contents of the System Monitor display.
- Filter  
Select an item of text in the current displayed trace and then select Edit | Filter. All matching lines with the same item in the trace are displayed in a separate filtered log window.
- IP Calculate (Selected Hex)  
Converts hexadecimal strings into decimal. Highlight the number to convert in the System Monitor display and then select Edit | IP Calculate.

### View Menu

-  Freeze Screen Logging  
Freeze/unfreeze the display. Any traffic whilst the display is frozen is lost unless logged to a log file.
- Font  
Allows selection of the default font, including font color and size, used in the System Monitor display.
- Background Color  
Allows selection of the background color used in the System Monitor display.

---

## Filters Menu

This menu provides options to select which traffic and events on the IP Office are displayed by System Monitor.

- [Trace Options](#)<sup>[20]</sup>  
Allows you to select and filter trace captured by System Monitor based on a range of categories:
  - [ATM](#)<sup>[21]</sup>  
System Monitor analog trunk traffic and events.
  - [Call](#)<sup>[22]</sup>  
Monitoring of extensions and calls.
  - [DTE](#)<sup>[23]</sup>  
Monitoring of the Control Unit's DTE port.
  - [EConf](#)<sup>[24]</sup>  
System Monitor conference and conferencing server events.
  - [Frame Relay](#)<sup>[25]</sup>  
Monitoring of Frame Relay traffic and events.
  - [GOD](#)<sup>[26]</sup>  
For use by Avaya development engineers only.
  - [H.323](#)<sup>[27]</sup>  
Monitoring of H.323 traffic and events.
  - [Interface](#)<sup>[28]</sup>  
Monitoring IP interfaces such as NAT and the Firewall.
  - [ISDN](#)<sup>[29]</sup>  
System Monitor ISDN traffic and events.
  - [Key/Lamp](#)<sup>[31]</sup>  
System Monitor appearance functions
  - [LDAP](#)<sup>[32]</sup>  
System Monitor LDAP traffic and events.
  - [Media](#)<sup>[33]</sup>
  - [PPP](#)<sup>[34]</sup>  
System Monitor PPP traffic and events.
  - [R2](#)<sup>[35]</sup>  
System Monitor R2 trunk traffic and events.
  - [Routing](#)<sup>[36]</sup>  
System Monitor IP traffic and events.
  - [SCN](#)<sup>[37]</sup>  
System Monitor Small Community Network traffic and information.
  - [Services](#)<sup>[38]</sup>  
System Monitor SNMP alarms events.
  - [SIP](#)<sup>[39]</sup>  
System Monitor SIP trunks and connections.
  - [System](#)<sup>[40]</sup>  
System Monitor internal events.
  - [T1](#)<sup>[41]</sup>  
System Monitor T1 traffic and events.
  - [VPN](#)<sup>[42]</sup>  
System Monitor VPN events.
  - [WAN](#)<sup>[43]</sup>  
System Monitor WAN traffic and events.

### Status Menu

- [US PRI Trunks...](#)<sup>[47]</sup>  
Displays a menu showing the B channel status of US PRI lines installed in the IP Office.
- [RTP Sessions](#)<sup>[48]</sup>
- [Voicemail Sessions](#)<sup>[49]</sup>
- [Small Community Networking](#)<sup>[50]</sup>
- [Partner Sessions](#)<sup>[51]</sup>
- [Alarms](#)<sup>[52]</sup>  
Display and clear the IP Office alarm log. See [The Alarm Log](#)<sup>[12]</sup>.
- [Map Status](#)<sup>[53]</sup>
- [IP Phone Status](#)<sup>[54]</sup>

### Help Menu

- About  
Shows information about the version of the System Monitor program.









---

## 1.7 File Logging

As well as displaying the System Monitor trace, System Monitor can record the trace to a log file. These two activities are separate, ie. the trace can be logged even when the screen display is frozen (paused).

A logged trace can be examined later and, if requested, be sent to Avaya for analysis.

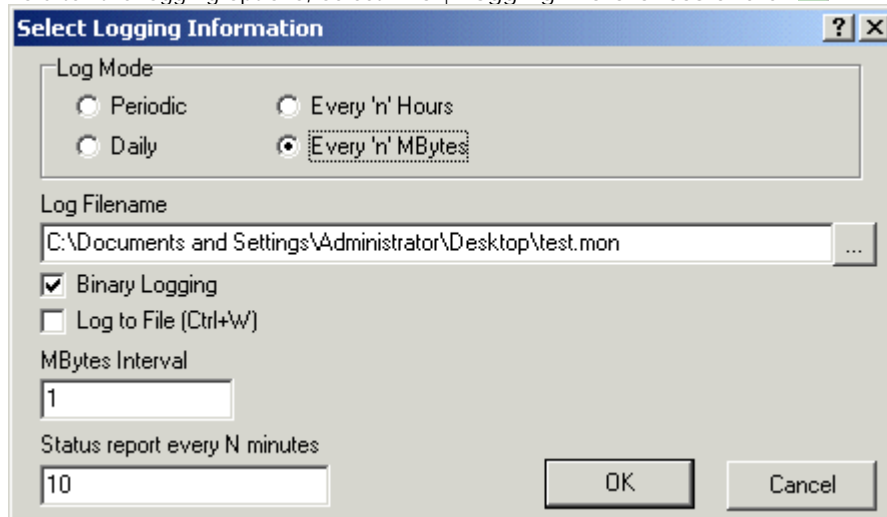
Several of the buttons on the System Monitor toolbar are specifically for control of logging

-  Rollover log  
Add the time and date to the current log files file name and then start a new log file.
  -  Start logging
  -  Logging currently set to text mode  
This icon indicates that System Monitor is currently set to text file logging. Clicking the icon changes the mode to binary file logging (forcing a rollover of any current log file).
  -  Logging currently set to binary mode  
This icon indicates that System Monitor is currently set to text binary logging. Clicking the icon changes the mode to binary text logging (forcing a rollover of any current log file).
  -  Stop logging
-  Log Preferences  
Setup the type, location and rollover frequency for log files.
-  Open File  
Loads a previously captured log file in the System Monitor display area. This automatically freezes and replace any current trace being displayed but does affect any current logging in progress. Both text and binary log files can be opened.
-  Save Screen Log  
Though different from the log options above, this option can be used to save the current displayed trace to a text file similar to a log file.





## Setting the Logging Preferences

1. To alter the logging options, select File | Logging Preferences or click .



2. Set the log file preferences are required:

- **Log Mode**  
Set how often the log file should be automatically rolled over when running. Selecting any of the automatic rollover modes does not stop the log being rolled over manually when required.
  - **Periodic**  
Rollover the log only when  is clicked.
  - **Daily**  
Rollover the log automatically at the end of each day.
  - **Every 'n' Hours**  
Rollover the log automatically every n hours. When selected, an Hours Interval box is displayed to set the number of hours between rollovers.
  - **Every 'n' MBytes**  
Rollover the log automatically every n MB of file size. When selected, a MBytes Interval box is displayed to set the number of MB between rollovers.
- **Log Filename**  
Sets the location and file name of the log files. The default location is the System Monitor application program folder (C:\Program Files\Avaya\IP Office\System Monitor).
- **Binary Logging**  
The log file trace displayed by System Monitor and logged in a text log file has been 'interpreted'. That is read by the System Monitor application and had additional information added. A binary log file is the raw output from the IP Office.
  - When running System Monitor and logging or displaying the trace as text, it is possible for some data packets to be lost due to the high number of packets that require interpretation. Running a binary log and freezing the System Monitor display reduces the chance of such lost packets.
- **Log to File**  
If checked, this box starts file logging once OK is clicked.
- **Status Report every N minutes**  
Sets how often System Monitor should added a [status report](#)  line to the log outputs.

---

## 1.8 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 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](#)<sup>[82]</sup>.

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 IP Office configuration.

### Placing a Marker in the System Monitor Trace

Being able to place a marker line in the System Monitor trace when the problem occurs may be useful. If the only Call setting selected is Call Logging (this is the default) then a simple way to do this is to dial another extension and hangup immediately.

You can then search for a line such as shown below in the System Monitor trace (in this example case Extension 203 dialing 201 and then hanging up):

```
2816496ms CALL:2002/11/0610:03,00:00:00,000,203,0,201,201,Extn202,,,1,, "
```

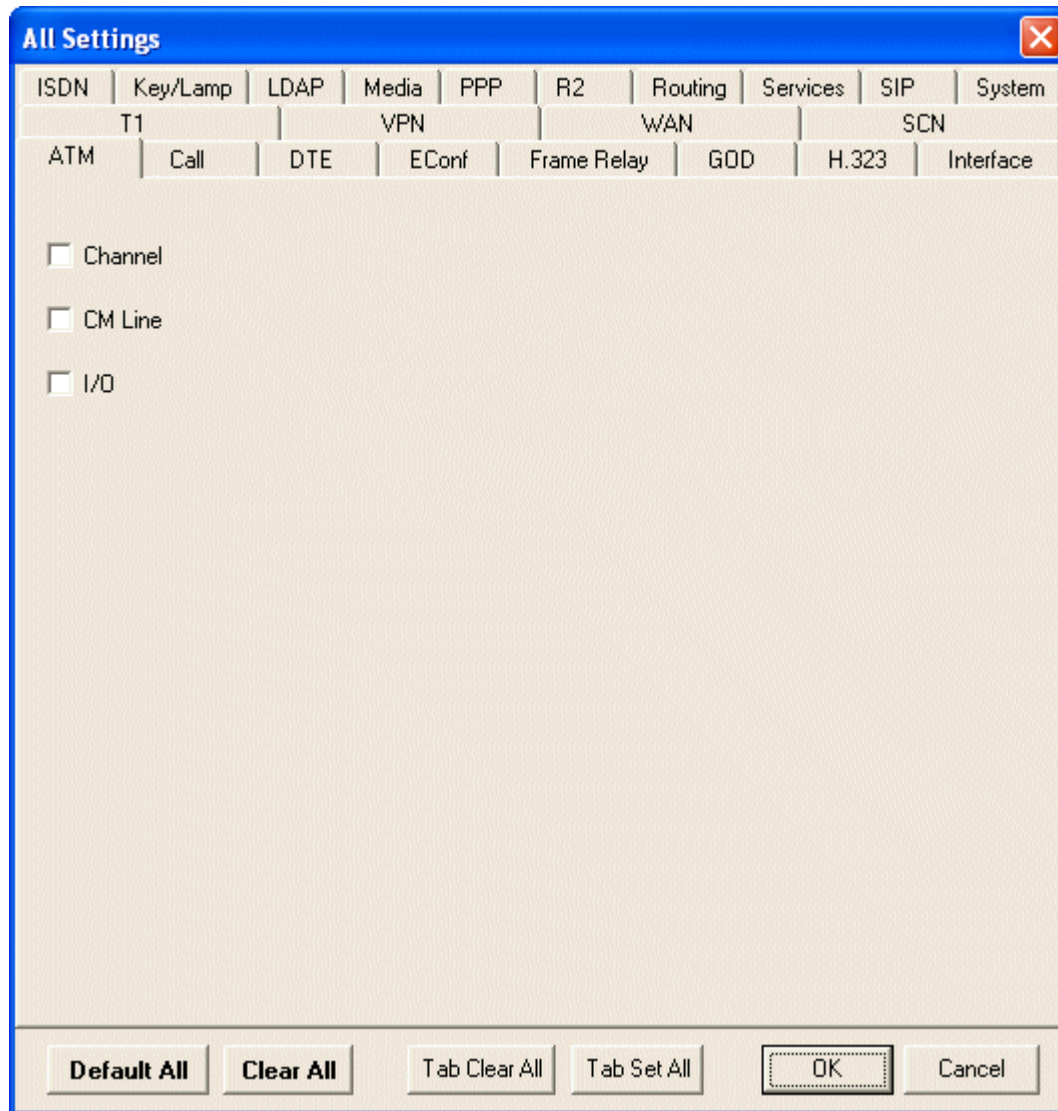
# Chapter 2.

# Trace Options

---

## 2. Trace Options

## 2.1 ATM



## 2.2 Call

**All Settings** [X]

ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System
T1		VPN			WAN			SCN	
ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface		

Events

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

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

Trace Colour █

**Default All** **Clear All** Tab Clear All Tab Set All **OK** Cancel

## 2.3 DTE

**All Settings** ✖

ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System
T1		VPN			WAN		SCN		
ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface		

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

**Default All**   **Clear All**   Tab Clear All   Tab Set All   OK   Cancel

## 2.4 EConf

The screenshot shows the 'All Settings' dialog box with the 'EConf' tab selected. The dialog has a blue title bar and a close button in the top right corner. The main area is divided into several sections:

- Events:** Contains five checkboxes: Session, Api, Targets, Conf, and Vmail. All are currently unchecked.
- Packets:** Contains two checkboxes: Vmail Tx and Vmail Rx. Both are currently unchecked.
- Buttons:** A 'Report' button is located below the packet settings.
- Footer:** A row of control buttons: 'Default All' (highlighted with a dotted border), 'Clear All', 'Tab Clear All', 'Tab Set All', 'OK', and 'Cancel'.

ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System
T1		VPN			WAN		SCN		
ATM	Call	DTE	EConf	Frame Relay	GDD	H.323	Interface		



## 2.5 Frame Relay

**All Settings** ✖

ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System
T1		VPN			WAN		SCN		
ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface		

Events

- Frame Relay Events
- Management Events

Packets

- Tx Data
- Rx Data

**Default All**   **Clear All**   Tab Clear All   Tab Set All   OK   Cancel

## 2.6 GOD

**All Settings** ✖

ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System
T1		VPN			WAN		SCN		
ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface		

Client Tx  
 Client Rx  
  
 Server Tx  
 Server Rx

**Default All**   **Clear All**   Tab Clear All   Tab Set All   OK   Cancel

## 2.7 H.323

**All Settings** ✖

ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System
T1		VPN			WAN		SCN		
ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface		

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

Trace Colour

**Default All**   **Clear All**   Tab Clear All   Tab Set All   OK   Cancel

## 2.8 Interface

**All Settings** [X]

ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System
T1		VPN			WAN		SCN		
ATM	Call	DTE	EConf	Frame Relay	GDD	H.323	Interface		

**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

**Filter Options**

IP Address 1 (nnn.nnn.nnn.nnn)  
[ ]

IP Address 2 (nnn.nnn.nnn.nnn)  
[ ]

MAC Address 1 (abcdefabcdef)  
[ ]

MAC Address 2 (abcdefabcdef)  
[ ]

Broadcast

WAN3 chat

ARP

MultiCast

Interface Name  
[ ]

Payload Display Size (0-1500)  
32

**Default All**   **Clear All**   Tab Clear All   Tab Set All   **OK**   **Cancel**

## 2.9 ISDN

**All Settings** ✖

ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface		
T1		VPN		WAN		SCN			
ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System

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

Trunk Packets (IP401 only)

- Trunk 1 Tx
- Trunk 1 Rx
- Trunk 2 Tx
- Trunk 2 Rx

**Default All**   **Clear All**   Tab Clear All   Tab Set All   OK   Cancel

---

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
TxEr	A Transmit error has occurred
UnLocked	The IP Office is not able to lock its clock to this line
Locked	The IP Office and the clock extracted from this line are locked together.

## 2.10 Key/Lamp

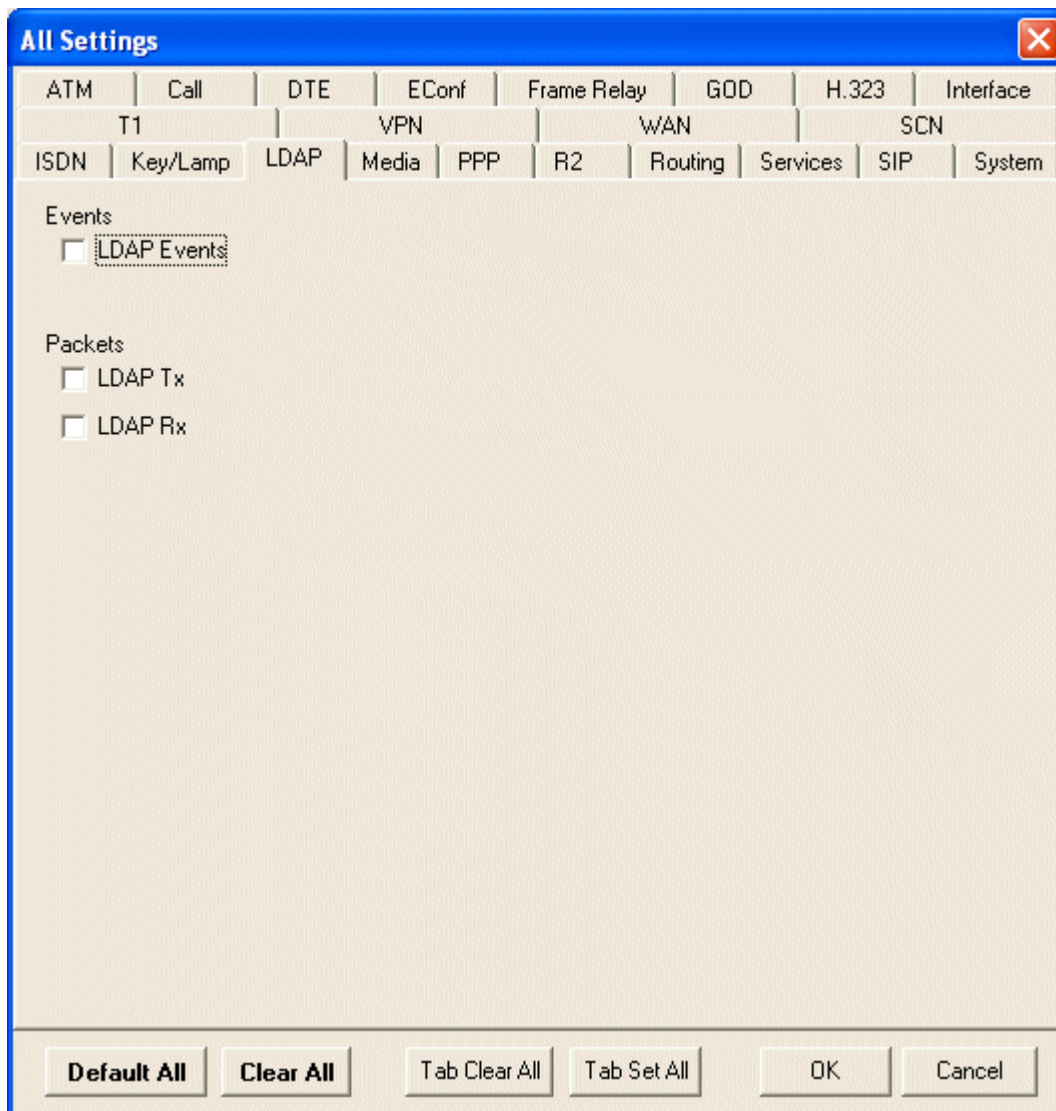
**All Settings** ✖

ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface
T1		VPN		WAN		SCN	
ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services
				SIP	System		

<p><b>Events</b></p> <p><input type="checkbox"/> Appearance</p> <p><input type="checkbox"/> Appearance Group</p> <p><input type="checkbox"/> Call</p> <p><input type="checkbox"/> Facility</p> <p><input type="checkbox"/> Local Appearance</p> <p><input type="checkbox"/> Phone State Change</p> <p><input type="checkbox"/> Switch Hook</p> <p><input type="checkbox"/> User Config</p> <p><b>Messages</b></p> <p><input type="checkbox"/> Call Interface - Level 1</p> <p><input type="checkbox"/> Call Interface - Level 2</p> <p><input type="checkbox"/> Key Resolver Interface - Level 1</p> <p><input type="checkbox"/> Key Resolver Interface - Level 2</p>	<p><b>Exclude Classes</b></p> <p><input type="checkbox"/> Adapter</p> <p><input type="checkbox"/> Phone</p> <p><input type="checkbox"/> Appearance</p> <p><input type="checkbox"/> Appearance Group</p> <p><input type="checkbox"/> Appearance Selector</p> <p><input type="checkbox"/> Ringer</p> <p><input type="checkbox"/> Switch Hook</p> <p><input type="checkbox"/> Call</p> <p><input type="checkbox"/> Line</p> <p><input type="checkbox"/> Primary Coverage Facility</p> <p><b>T3</b></p> <p><input type="checkbox"/> API Events</p> <p><input type="checkbox"/> API Messages</p> <p><input type="checkbox"/> Phone Model</p>
--	--

## 2.11 LDAP





## 2.12 Media

**All Settings** [X]

ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface		
T1		VPN		WAN		SCN			
ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System

**Media Events**

- Extension Cut
- Media handlers
- Connection handler
- Map

**VoIP Events**

- VoIP High
- Primitives High

**VoIP Packets**

- Fast Start Info
- Primitives

**Default All** **Clear All** Tab Clear All Tab Set All OK Cancel

## 2.13 PPP

**All Settings** ✖

ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface		
T1		VPN		WAN		SCN			
ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System

Events

Err Msg       Include LCP Echo

Stack

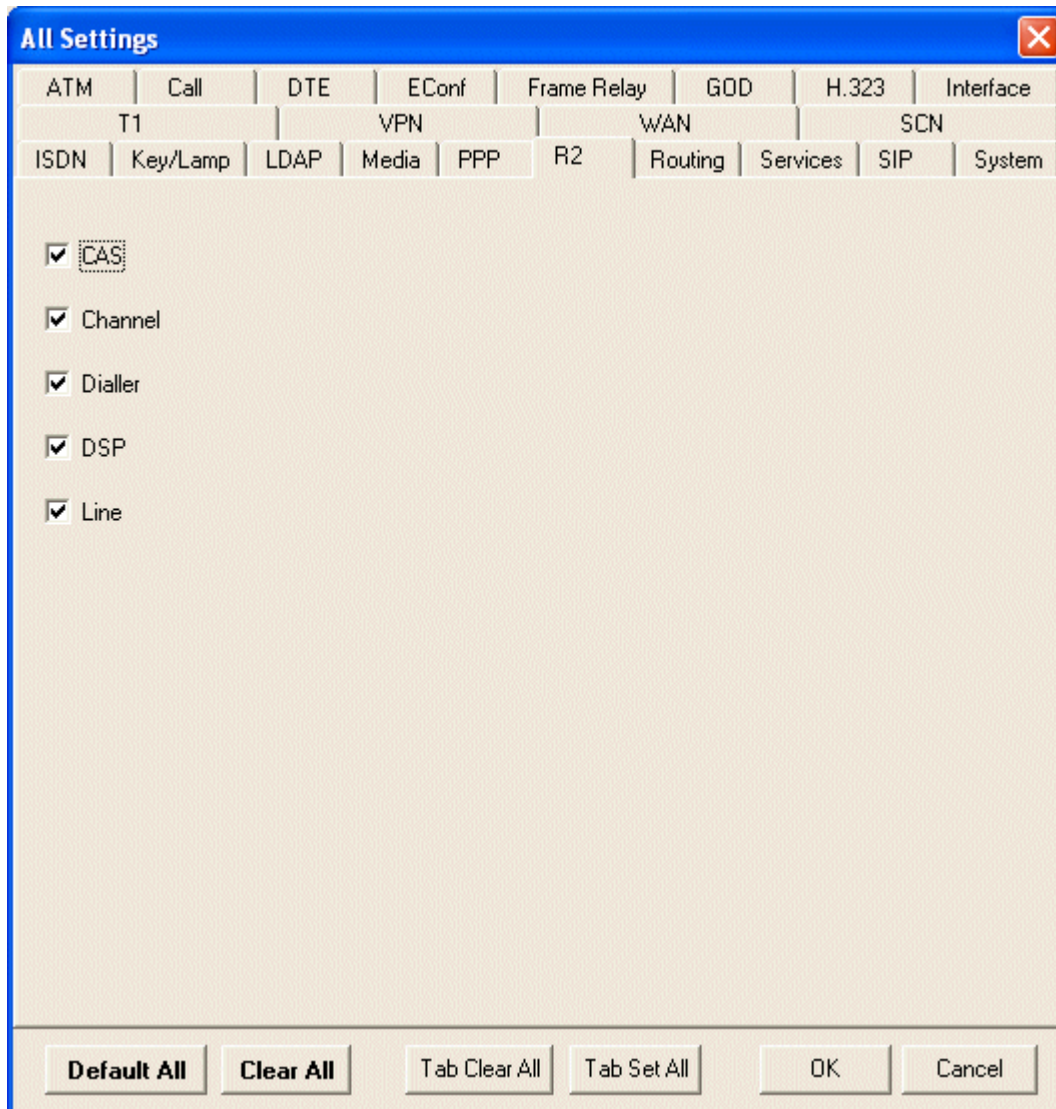
Packets

<input type="checkbox"/> LCP Tx	<input type="checkbox"/> CCP Tx
<input type="checkbox"/> LCP Rx	<input type="checkbox"/> CCP Rx
<input type="checkbox"/> Security Tx	<input type="checkbox"/> CRTP Tx
<input type="checkbox"/> Security Rx	<input type="checkbox"/> CRTP Rx
<input type="checkbox"/> M LCP Tx	<input type="checkbox"/> IPHC Tx
<input type="checkbox"/> M LCP Rx	<input type="checkbox"/> IPHC Rx
<input type="checkbox"/> IPCP Tx	<input type="checkbox"/> IP Tx
<input type="checkbox"/> IPCP Rx	<input type="checkbox"/> IP Rx
<input type="checkbox"/> BACP Tx	<input type="checkbox"/> Link Tx
<input type="checkbox"/> BACP Rx	<input type="checkbox"/> Link Rx

Interface Name

**Default All**   **Clear All**   Tab Clear All   Tab Set All   OK   Cancel

## 2.14 R2



## 2.15 Routing

**All Settings** [X]

ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface		
T1		VPN		WAN		SCN			
ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System

**Data**

Events

<input type="checkbox"/> Route Cache Events	<input type="checkbox"/> RIP In
<input type="checkbox"/> Routing Table	<input type="checkbox"/> RIP Out
<input checked="" type="checkbox"/> Routing Table Changes	<input type="checkbox"/> IGMP

**Voice**

Messages	Packet Contents
<input type="checkbox"/> Received AVRIP	<input type="checkbox"/> AVRIP Tx
<input type="checkbox"/> Inter Node	<input type="checkbox"/> AVRIP Rx
<input type="checkbox"/> Remote Node	<input type="checkbox"/> VPNNTFTP Tx
<input type="checkbox"/> Node forwarding	<input type="checkbox"/> VPNNTFTP Rx

Default All   Clear All   Tab Clear All   Tab Set All   OK   Cancel

## 2.16 SCN

**All Settings** ✖

ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System
ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface		
T1		VPN		WAN		SCN			

Events

- DHG Call Routing
- DHG Membership
- DHG Longest Idle Info
- DHG Service Change
- DHG Config Change
- SCN User Events
- SCN Dump

Messages

- Control Stream Tx
- Control Stream Rx

**Default All**   **Clear All**   Tab Clear All   Tab Set All   OK   Cancel

## 2.17 Services

**All Settings** [Close]

ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface		
T1		VPN		WAN		SCN			
ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System

SNMP Events

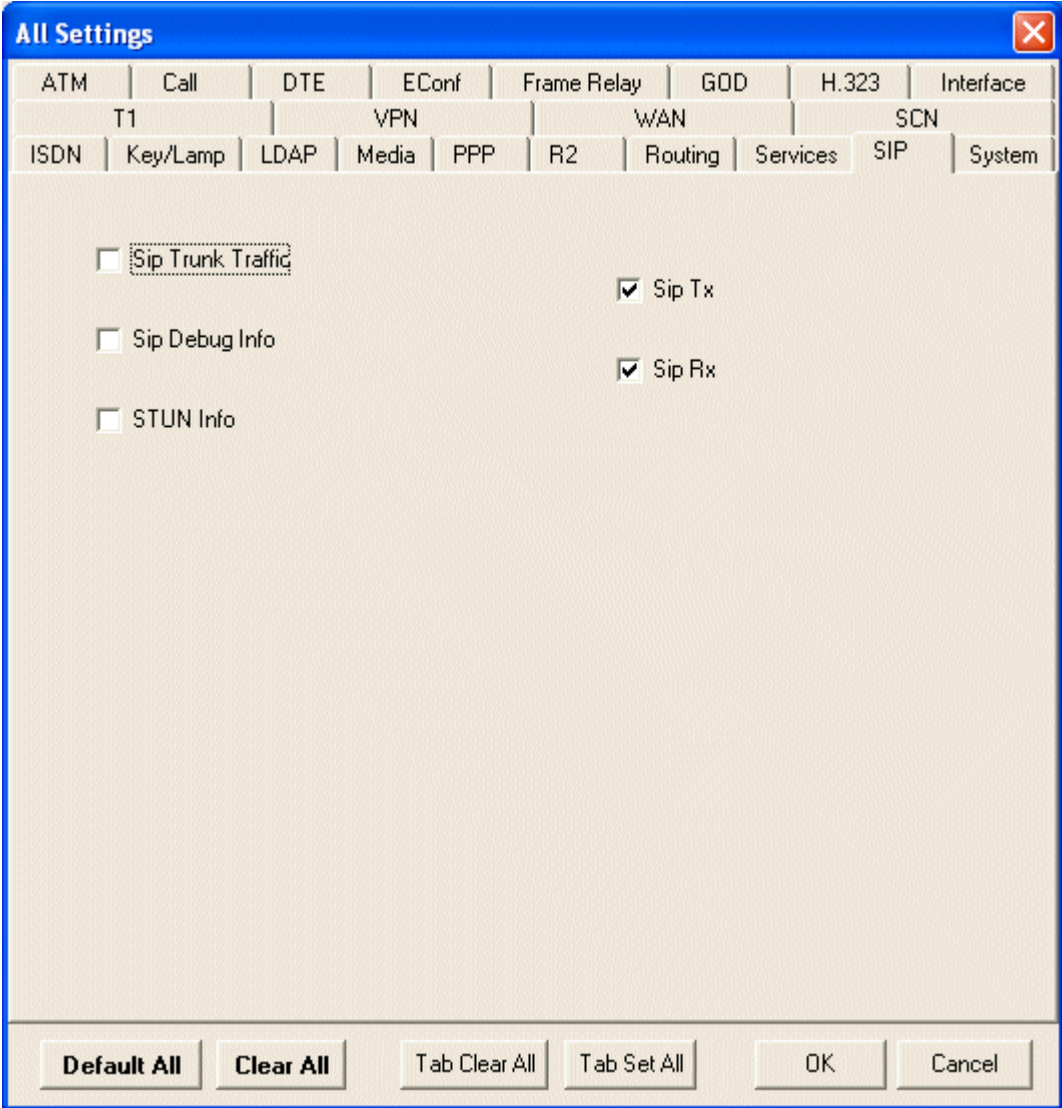
- Received Message Processing
- Trap Generation

Service Events

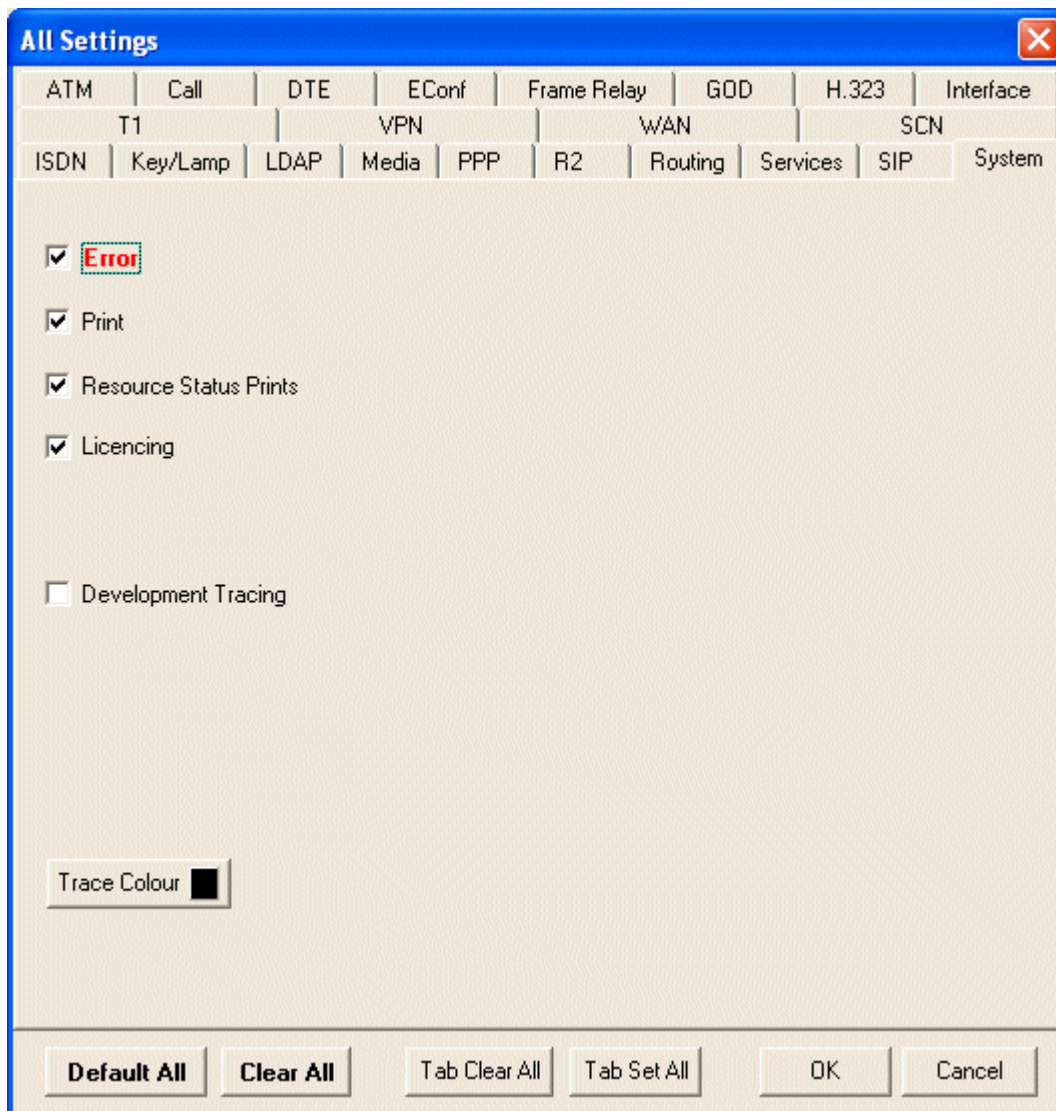
- TFTP
  - (TFTP Warnings)
  - (TFTP Download)
- DNS
- DHCP
- Telnet
- CSTA
- TAPI
- HTTP

Default All   Clear All   Tab Clear All   Tab Set All   OK   Cancel

## 2.18 SIP



## 2.19 System





## 2.20 T1

**All Settings** ✖

ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System
ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface		
T1		VPN			WAN		SCN		

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

## 2.21 VPN

**All Settings** ✖

ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System
ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface		
T1		VPN			WAN		SCN		

**IPSec**

Events

IPSec Events     Decode     IPO-SNet

Packets

Rx Data     Data Events

Tx Data     Warnings

Debug

**L2TP**

Events

L2TP Events

Packets

Rx Data

Tx Data

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

## 2.22 WAN

**All Settings** ✖

ISDN	Key/Lamp	LDAP	Media	PPP	R2	Routing	Services	SIP	System
ATM	Call	DTE	EConf	Frame Relay	GOD	H.323	Interface		
T1		VPN		WAN		SCN			

Events

WAN Events

Packets

WAN Tx

WAN Rx

**Default All**   **Clear All**   Tab Clear All   Tab Set All   OK   Cancel



# **Chapter 3.**

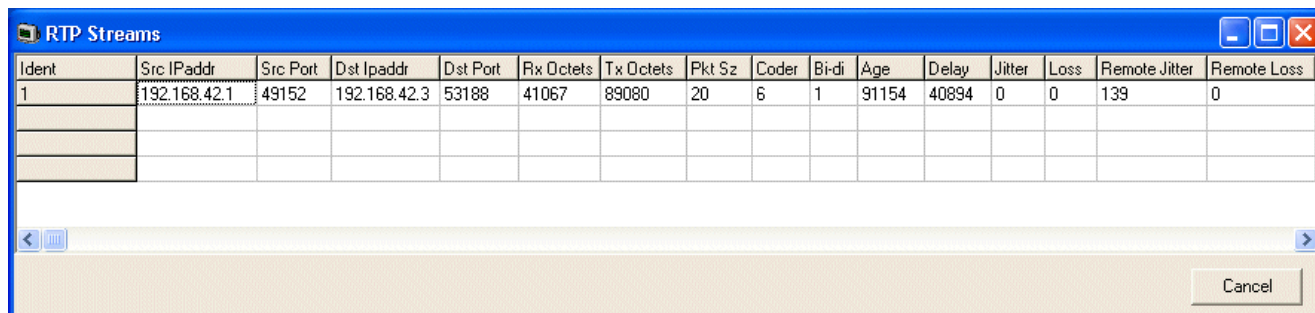
# **Status Screens**

---

### 3. Status Screens

## 3.1 US PRI Trunks

### 3.2 RTP Sessions



The screenshot shows a window titled "RTP Streams" with a table of data. The table has 15 columns: Ident, Src IPAddr, Src Port, Dst IPaddr, Dst Port, Rx Octets, Tx Octets, Pkt Sz, Coder, Bi-di, Age, Delay, Jitter, Loss, Remote Jitter, and Remote Loss. The first row contains the following values: 1, 192.168.42.1, 49152, 192.168.42.3, 53188, 41067, 89080, 20, 6, 1, 91154, 40894, 0, 0, 139, 0. There are three empty rows below the first row. At the bottom right of the window is a "Cancel" button.

Ident	Src IPAddr	Src Port	Dst IPaddr	Dst Port	Rx Octets	Tx Octets	Pkt Sz	Coder	Bi-di	Age	Delay	Jitter	Loss	Remote Jitter	Remote Loss
1	192.168.42.1	49152	192.168.42.3	53188	41067	89080	20	6	1	91154	40894	0	0	139	0



### 3.3 Voicemail Sessions

**Voicemail Status**
\_ □ ×

**Status**

Voicemail Source    **192.168.42.203**

Operational        **1**

Version             **3**

Record Supported   **1**

Max Sessions       **4**

Current Sessions   **2**

**Licences**

VM Pro             **1**

VPIM               **0**

IMS                **0**

Recordings        **0**

SQL                **0**

VB Script         **0**

Outlook            **0**

Scansoft TTS      **0**

Generic TTS       **0**

Ident	State	Access	Mailbox	Calling Party	TxBuf	RxBuf	RxErr	TxDiscards	TxEmpty	TxPurge
100	2	2	Extn203	203	224	84	0	0	0	0
101	2	2	Extn207	207	175	84	0	0	0	0

---

## 3.4 Small Community Networking

### 3.5 Partner Sessions

The screenshot shows a window titled "PCPartnerStatus" with a blue title bar. Below the title bar, it displays "Num Sessions: 1". A table with 7 columns is shown, containing one row of data. Below the table is a scrollable area with a "Cancel" button at the bottom right.

IPAddress	User Name	Extn Num	SendQ	SendCnt	Pro	IP
192.168.42.203	Extn201	201	0	0	1	0

---

## 3.6 Alarms

## 3.7 Map Status

### 3.8 IP Phone Status

The screenshot shows the IPPhoneStatus application window. At the top, it displays 'Total Configured: 6' and 'Total Registered: 1'. A progress bar for 'Registered Status' shows 1 out of 6 phones registered. Below this is a table with columns: Extn Num, Phone Type, IP Address, Mac Address, Version Id, EP identifier, and Status. The table lists 6 phones, with 5 unregistered and 1 registered. At the bottom, there are 'Display Options' (Show All, Registered, UnRegistered), and buttons for 'Print', 'Reset Phones', and 'Cancel'.

Total Configured: 6  
Total Registered: 1  
Registered Status: [Progress Bar]

Extn Num	Phone Type	IP Address	Mac Address	Version Id	EP identifier	Status
308	Unknown	0.0.0.0	00-00-00-00-00-00	V?	EP?	RAS: UnRegistered
301	Unknown	0.0.0.0	00-00-00-00-00-00	V?	EP?	RAS: UnRegistered
299	Unknown	0.0.0.0	00-00-00-00-00-00	V?	EP?	RAS: UnRegistered
304	Unknown	0.0.0.0	00-00-00-00-00-00	V?	EP?	RAS: UnRegistered
307	Unknown	0.0.0.0	00-00-00-00-00-00	V?	EP?	RAS: UnRegistered
305	1608	192.168.42.3	00-07-3b-bc-a3-8b	1.010	IP500 Site A_488050b4140f79a5	RAS: Registered, DHCP: Returned

Display Options:  Show All  Registered  UnRegistered

Buttons: Print, Reset Phones, Cancel

# **Chapter 4.**

# **Example Monitor Settings**

---

## 4. 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:

- [Analog Trunk Caller ID](#) <sup>[57]</sup>
- [ISDN Trunk Caller ID](#) <sup>[58]</sup>
- [ISDN Calls Disconnecting](#) <sup>[59]</sup>
- [System Rebooting](#) <sup>[61]</sup>
- [ISDN Problems \(T1 or E1 PRI connections\)](#) <sup>[62]</sup>
- [ISP & Dial-Up Data Connection Problems](#) <sup>[63]</sup>
- [Remote Site Data Connection Problems over Leased \(WAN\) Lines](#) <sup>[64]</sup>
- [Frame Relay Links](#) <sup>[65]</sup>
- [Speech Calls Dropping](#) <sup>[66]</sup>
- [Problems Involving Non-IP Phones](#) <sup>[69]</sup>
- [Problems Involving IP Phones](#) <sup>[69]</sup>
- [Locating a Specific PC Making Calls to the Internet](#) <sup>[70]</sup>
- [Firewall Not Working Correctly](#) <sup>[71]</sup>
- [Remote Site Data Connection over Leased \(WAN\) Lines](#) <sup>[71]</sup>
- [Call Answered/Generated by IP Office Application](#) <sup>[72]</sup>
- [Message Waiting Indication](#) <sup>[72]</sup>



## 4.1 Analog Trunk Caller ID


Elements of a typical trace taken from an Analogue Trunk that supports ICLID/CLI terminated on an IP Office is shown below.

System Monitor Trace	Explanation
108691mS PRN: AtmTrunk1: StateChange CLIPossibleIncoming->Idle	AtmTrunk1 = Line Number 1. 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	<ul style="list-style-type: none"> <li>Month: 30 (hex) = 0 (ASCII), 31 (hex) = 1 (ASCII) &gt; 01 (January)</li> <li>Day: 31 (hex) = 1 (ASCII), 34 (hex) = 4 (ASCII) &gt; 14th.</li> <li>Hours: 31 (hex) = 1 (ASCII), 36 (hex) = 6 (ASCII) &gt; 16:00.</li> <li>Minutes: 30 (hex) = 0 (ASCII), 35 (hex) = 5 (ASCII) &gt; 00:05.</li> </ul> The call date and time is 16:05 on 14th January.
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	<ul style="list-style-type: none"> <li>30 (hex) = 0 (ASCII), 31 (hex) = 1 (ASCII) &gt; 01</li> <li>37 (hex) = 7 (ASCII), 30 (hex) = 0 (ASCII) &gt; 70</li> <li>37 (hex) = 7 (ASCII), 2d (hex) = - (ASCII) &gt; 7-</li> <li>33 (hex) = 3 (ASCII), 39 (hex) = 9 (ASCII) &gt; 39</li> <li>30 (hex) = 0 (ASCII), 33 (hex) = 3 (ASCII) &gt; 03</li> <li>39 (hex) = 9 (ASCII), 31 (hex) = 1 (ASCII) &gt; 91</li> </ul> The Calling Party Number is 01707-390391
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 detection 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.

Targeting tracing intimates the ICLID/CLI received as [calling =]. In this case 01707-390391  
 CMTARGET: LOOKUP CALL ROUTE:3 type=100 called\_party= sub= calling=01707-390391 in=1 complete=1  
 CMTARGET: LOOKUP INCOMING CALL ROUTE:3, calling party is 01707-390391. Using destination 326

---

## 4.2 ISDN Trunk Caller ID

1. On the PC running Manager, click the Windows Start icon and select Programs|IP Office|Monitor.
2. On the SysMonitor application, 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. On the SysMonitor 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  1.!.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]

## 4.3 ISDN Calls Disconnecting

### Issue

Calls on ISDN lines/trunks cutting off.

### Actions

1. On the PC running Manager, click the Windows Start icon and select Programs|IP Office|Monitor.
2. On the SysMonitor application, click  Trace Options to select the trace settings.
3. On the ISDN tab, make sure the following fields under the Events heading are ticked:
  - Layer 1.
  - Layer 2.
  - Layer 3.
4. Click OK.
5. Trace codes start appearing on the SysMonitor window. In the example below, the actual trace codes are in bold and the explanation are in regular type. This is a sample trace of an PRI line going down, cutting off the calls in progress and then the line coming back up:

System Monitor Trace	Explanation
<b>1072151mS ISDNL1Evt: v=0 peb=5,F2 F1</b>	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).
<b>1072651mS ISDNL1Evt: v=0 peb=5,PHDI ?</b>	Line 5 (peb=5) is now in the Disconnected state (PHDI – Physical Deactivate Indication).
<b>1072651mS ISDNL3Evt: v=0 p1=0,p2=1001,p3=5,p4=127,s1=</b>	ISDN Layer 3 event which gives current status of line 5 (p3=5) <ul style="list-style-type: none"> <li>• P1=0 -&gt; ISDN Stacknum = 0.</li> <li>• P2=1001 -&gt;Line Disconnecting</li> <li>• P3=5 -&gt; Internal reference number</li> <li>• P4=127 -&gt;TEI = 127</li> <li>• S1= -&gt;not used</li> </ul>
<b>1072651mS ISDNL3Evt: v=0 stacknum=0 State, new=NULLState, old=Active id=4</b>	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).
<b>1072652mS ISDNL3Evt: v=0 stacknum=0 State, new=NULLState, old=Active id=24</b>	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).
<b>1072653mS ISDNL3Evt: v=0 p1=0,p2=1001,p3=5,p4=0,s1=</b>	ISDN Layer 3 event which gives current status of line 5 (p3=5) <ul style="list-style-type: none"> <li>• P1=0 -&gt; ISDN Stack number = 0.</li> <li>• P2=1001 -&gt;Line Disconnecting</li> <li>• P3=5 -&gt;Internal reference number</li> <li>• P4=0 -&gt;TEI = 0</li> <li>• S1= -&gt;not used</li> </ul>
<b>1072656mS CMLineRx: v=5 CMReleaseComp Line: type=Q931Line 5 Call: lid=5 id=4 in=1 Cause=38, Network000</b>	The in coming 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!).
<b>1072658mS CALL:2000/11/2408:40,00:00:17,033,01732464420,I,300,027624,,,,0</b>	The Incoming call from 01732464420 to [02083]027624 (Extn300) has been disconnected.

System Monitor Trace	Explanation
1072682mS CMLineRx: v=5 CMReleaseComp Line: type=Q931Line 5 Call: lid=5 id=24 in=1 Cause=38, Network000	The in coming 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).

## 4.4 System Rebooting

Enable the following System Monitor settings:

- Call/Packets/Line Send
- Call/Packets/Line Receive
- Call/Packets/Extension Send
- Call/Packets/Extension Receive
- Call/Packets/Extension RxP
- Call/Packets/Extension TxP
- Call/Events/Call Delta
- Call/Events/Map
- Call/Events/Targetting
- Call/Events/Call Logging
- System/Error
- System/Print
- System/Resource Status Prints

You should also capture the data that is output on the DTE port on the back of the IP Office Control Unit. Refer to the IP Office Job Aid "DTE Port Maintenance" for details of doing this. 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].

---

## 4.5 ISDN Problems (T1 or E1 PRI connections)

Enable the following System Monitor settings:

- ISDN/Events/Layer 1
- ISDN/Events/Layer 2
- ISDN/Events/Layer 3
- ISDN/Packets/Layer 1 Send
- ISDN/Packets/Layer 1 Receive
- ISDN/Packets/Layer 2 Send
- ISDN/Packets/Layer 2 Receive
- ISDN/Packets/Layer 3 Send
- ISDN/Packets/Layer 3 Receive
- Call/ Packets/Extension Send
- Call/ Packets/Extension Receive
- Call/ Packets/Extension TxP
- Call/ Packets/Extension RxP
- Call/Packets/Line Send
- Call/Packets/Line Receive
- Call/Events/Targetting
- Call/Events/Call Logging
- System/Error
- System/Print
- System/Resource Status Prints

This will provide information about the ISDN line itself and any calls in progress. It will tell us things like the line is going down.

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.

## 4.6 ISP & Dial-Up Data Connection Problems

Enable the following System Monitor settings:

- ISDN/Packets/Layer3 Tx
- ISDN/Packets/Layer3 Rx
- Call/Packets/Line Send
- Call/Packets/Line Receive
- Call/Events/Targetting
- Call/Events/Call Logging
- Interface/Interface Queue
- PPP/LCP Tx
- PPP/LCP Rx
- PPP/Security Tx
- PPP/Security Rx
- PPP/IPCP Tx
- PPP/IPCP Rx
- System/Error
- System/Print
- System/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 Monitor's PPP settings. It must be entered in the same way as it appears in the Service configuration form associated with unit being monitored. A blank entry means all data connections (Services) will be monitored.

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

---

## 4.7 Remote Site Data Connection Problems over Leased (WAN) Lines

Enable the following System Monitor settings:

- WAN/WAN Tx
  - WAN/WAN Rx
  - WAN/WAN/Events
  - PPP/LCP Tx
  - PPP/LCP Rx
  - PPP/Security Tx
  - PPP/Security Rx
  - PPP/IPCP Tx
  - PPP/IPCP Rx
  - PPP/IP Tx
  - PPP/IP Rx
  - System/Error
  - System/Print
  - System/Resource Status Prints
- 
- If the line is connected via the WAN port on the IP Office Control Unit, System Monitor should be configured to monitor the IP address of the IP Office Control Unit.
  - 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 "Interface Name" field in Monitor's PPP settings. It must be entered in the same way as it appears in the Service configuration form associated with unit being Monitored. 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.

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 "Port Number" in the "Interface Name" field in the System Monitor WAN form. It must be entered in the same way as it appears in the WAN port configuration form associated with unit being Monitored. An entry of [0] means all ports on the WAN3 unit are monitored.

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



## **4.8 Frame Relay Links**

Enable the following System Monitor settings:

- Frame Relay/Events
- Frame Relay/Tx Data
- Frame Relay/Tx Data Decode
- Frame Relay/Rx Data
- Frame Relay/Rx Data Decode
- Frame Relay/Tx Data
- Frame Relay/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 :-

- PPP/LCP Tx
- PPP/LCP Rx
- PPP/Security Tx
- PPP/Security Rx
- PPP/IPCP Tx
- PPP/IPCP Rx
- PPP/IP Tx
- PPP/IP Rx

---

## 4.9 Speech Calls Dropping

### ISDN or QSIG Line

Enable the following System Monitor settings:

- ISDN/Events/Layer 1
- ISDN/Events/Layer 3
- ISDN/Packets/Layer 1 Send
- ISDN/Packets/Layer 1 Receive
- ISDN/Packets/Layer 3 Send
- ISDN/Packets/Layer 3 Receive
- Call/Packets/Line Send
- Call/ Packets/Line Receive
- Call/ Packets/Extension Send
- Call/ Packets/Extension Receive
- Call/ Packets/Extension RxP
- Call/ Packets/Extension TxP
- Call/ Packets/Short Code Msgs
- Call/Events/Call Delta
- Call/Events/Targetting
- Call/Events/Call Logging
- System/Error
- System/Print
- System/Resource Status Prints

### Analogue Line

Enable the following System Monitor settings:

- ATM/Channel
- ATM/I-O
- ATM/CM Line
- Call/Packets/Line Send
- Call/ Packets/Line Receive
- Call/ Packets/Extension Send
- Call/ Packets/Extension Receive
- Call/ Packets/Extension RxP
- Call/ Packets/Extension TxP
- Call/ Packets/Short Code Msgs
- Call/Events/Call Delta
- Call/Events/Targetting
- Call/Events/Call Logging
- System/Error
- System/Print
- System/Resource Status Prints

## VoIP Line

Enable the following System Monitor settings:

- ISDN/Packets/Layer 3 Send<sup>[1]</sup>
- ISDN/Packets/Layer 3 Receive<sup>[1]</sup>
- ATM/Channel<sup>[2]</sup>
- ATM/I-O2
- ATM/CM Line<sup>[2]</sup>
- T1/Line<sup>[3]</sup>
- T1/Channel<sup>[3]</sup>
- T1/Dialler<sup>[3]</sup>
- T1/DSP<sup>[3]</sup>
- T1/CAS<sup>[3]</sup>
- H.323/Events/H.323
- H.323/Packets/H.323 Send
- H.323/Packets/H.323 Receive
- H.323/Packets/H.323 Fast Start4
- H.323/Packets/H.245 Send
- H.323/Packets/H.245 Receive
- H.323/Packets/View Whole Packet
- Call/Packets/Line Send
- Call/ Packets/Line Receive
- Call/ Packets/Extension Send
- Call/ Packets/Extension Receive
- Call/ Packets/Extension RxP
- Call/ Packets/Extension TxP
- Call/ Packets/Short Code Msgs
- Call/Events/Call Delta
- Call/Events/Targetting
- Call/Events/Call Logging
- System/Error
- System/Print
- System/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

In all the above scenarios you should be able to pick up items like Call Setup, Call Proceeding, Alerting, Call Connected, and Call Disconnected. It will provide a step by step process of what the call has gone through. It presents all information relating directly to the setup of the call.

---

## Channelized T1 Line

Enable the following System Monitor settings:

- T1/Line
- T1/Channel
- T1/Dialler
- T1/DSP
- T1/CAS
- Call/Packets/Line Send
- Call/ Packets/Line Receive
- Call/ Packets/Extension Send
- Call/ Packets/Extension Receive
- Call/ Packets/Extension RxP
- Call/ Packets/Extension TxP
- Call/ Packets/Short Code Msgs
- Call/Events/Call Delta
- Call/Events/Targetting
- Call/Events/Call Logging
- System/Error
- System/Print
- System/Resource Status Prints

## 4.10 Problems Involving Non-IP Phones

Enable the following System Monitor settings:

- Call/Packets/Line Send
- Call/ Packets/Line Receive
- Call/ Packets/Extension Send
- Call/ Packets/Extension Receive
- Call/ Packets/Extension RxP
- Call/ Packets/Extension TxP
- Call/ Packets/Short Code Msgs
- Call/Events/Call Delta
- Call/Events/Targetting
- Call/Events/Call Logging

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

## 4.11 Problems Involving IP Phones

Enable the following System Monitor settings:

- H.323/Events/H.323
- H.323/Packets/H.323 Send
- H.323/Packets/H.323 Receive
- H.323/Packets/H.323 Fast Start
- H.323/Packets/H.245 Send
- H.323/Packets/H.245 Receive
- H.323/Packets/RAS Send
- H.323/Packets/RAS Receive
- H.323/Packets/View Whole Packet

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

---

## 4.12 Locating a Specific PC Making Calls to the Internet

Enable the following System Monitor settings:

- ISDN/Packets/Layer3 Tx
- ISDN/Packets/Layer3 Rx
- Interface/Interface Queue
- Call/Packets/Line Send
- Call/ Packets/Line Receive
- Call/Events/Targeting
- Call/Events/Call Logging
- System/Error
- System/Print
- System/Resource Status Prints

If NAT is not being used on the connection this will produce:

```
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 - i.e. 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 will take 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.

## 4.13 Firewall Not Working Correctly

Enable the following System Monitor settings:

- Interface/Interface Queue
- Interface/Firewall Fail In
- Interface/Firewall Fail Out
- System/Error
- System/Print
- System/Resource Status Prints

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

- Interface/Firewall Allowed In
- Interface/Firewall Allowed Out
- System/Error
- System/Print
- System/Resource Status Prints

This will then trace those packets that are Allowed In and Out of the PBX via the Firewall.

Note: The Firewall settings menu in System Monitor includes an Interface Name field. You can use this to enter the name of the "Service" that you wish to monitor. It must be entered in the same way as it appears in the configuration file of the unit.

## 4.14 Remote Site Data Connection over Leased (WAN) Lines

Enable the following System Monitor settings:

- WAN/WAN Tx
- WAN/WAN Rx
- WAN/WAN/Events
- PPP/LCP Tx
- PPP/LCP Rx
- PPP/Security Tx
- PPP/Security Rx
- PPP/IPCP Tx
- PPP/IPCP Rx
- PPP/IP Tx
- PPP/IP Rx
- System/Error
- System/Print
- System/Resource Status Prints

- If the line is connected via the WAN port on the IP Office Control Unit, System Monitor should be configured to monitor the IP address of the IP Office Control Unit.
- 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 "Interface Name" field in Monitor's PPP settings. It must be entered in the same way as it appears in the Service configuration form associated with unit being Monitored. 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.

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 "Port Number" in the "Interface Name" field in the System Monitor WAN form. It must be entered in the same way as it appears in the WAN port configuration form associated with unit being Monitored. An entry of [0] means all ports on the WAN3 unit are monitored.

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

## 4.15 Calls Answered/Generated by IP Office Applications

IP Office applications include Call Status, eBLF, eConsole, SoftConsole and Phone Manager (all variants). Enable the following System Monitor settings:

- Call/Packets/Line Send
- Call/Packets/Line Receive
- Call/Packets/Extension Send
- Call/Packets/Extension Receive
- Call/Packets/Extension TxP
- Call/Packets/Extension RxP
- Call/Packets/Short Code Msgs
- Call/Events/Call Delta
- Call/Events/Targetting
- Call/Call Logging
- System/Error
- System/Print
- System/Resource Status Prints

The Extension TxP & RxP options monitor the "conversations" between the PBX and the IP Office applications. With the "Line" and "Extension" options enabled we can see what extensions/lines are involved and use this information to try to re-create the problem.

## 4.16 Message Waiting Indication

To determine if Voicemail Pro is transmitting message waiting indication (MWI) information, the following trace options should be used in System Monitor:

- Filters, Trace Options (Ctrl+T)
- Select the option to CLEAR ALL FIELDS.
- For Call events enable Extension Send, MonIVR and Targetting.
- For System events enable Print.

Whenever voicemail is accessed for a mailbox (message leaving\retrieval); Voicemail will send a voicemail status update for that mailbox to the PBX. This is traced out within SYSMON 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
```



## Example Monitor Settings: Message Waiting Indication

---

```
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 5.

# Addendum

## 5. Addendum

### 5.1 IP Office Ports

As mentioned, a number of different ports are used for access to IP Office systems. The following table lists some of the ports on which the IP Office control unit listens for different types of access. ← Indicates a listening port on the IP Office 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 IP Office to SMTP server. For IP Office 4.2 also used for Voicemail Email on Embedded Voicemail.
37	→	Time	UDP	Time requests from the IP Office 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 IP Office.
69	→	TFTP	UDP	File requests by the IP Office.
161*	←	SNMP	UDP	From SNMP applications.
162*	→	SNMP Trap	UDP	To addresses set in the IP Office configuration.
500	←	IKE	UDP	Key exchange for IPSec protocol.
389*	→	LDAP	TCP	Lightweight Directory Access Protocol.
520	→	RIP	UDP	To and from the IP Office 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 IP Office.
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 IP Office 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 IP Office 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 Monitor	UDP	From the IP Office 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 IP Office application (for example Phone Manager or SoftConsole). Used to initiate a session between the IP Office and the application.
50797	←	IPO TAPI	UDP	From an IP Office TAPI user PC.
50798	→	(UDP)	UDP	<i>BT Fusion variant. No longer used.</i>
50799	→	IPO BLF	UDP	Broadcast to the IP Office 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 IP Office configuration.
50801	←	EConf	UDP	Conference Center Service to IP Office.
50802	←	Discovery	TCP	IP Office discovery from Manager.
50804 *	←	Service Access Protocol	TCP	IP Office configuration settings access.

Port	Protocol	Function
50805 *	←	TCP " TLS Secure.
50808 *	←	TCP IP Office system status access.
50812 *	←	TCP IP Office security settings access.
50813 *	←	TCP " TLS Secure.

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

## Ports

IP Office 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), IP Office System Monitor also displays the names of more commonly used ports including IP Office specific ports.

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

The list below details the ports currently decoded by IP Office System Monitor. For a full list of assigned non-IP Office 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

IP Office 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 IP Office 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]

## 5.2 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 IP Office specific codes.

To display cause codes, ensure that the System Monitor | Call | Extension Send option is enabled. The cause code is then shown as 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.

Cause Code	Definition
49	Quality of service unavailable.
50	Requested facility not subscribed.
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.
<b>IP Office Specific Cause Codes</b>	
103	Parameter not implemented.
110	Message with unrecognised parameter.
111	Protocol error, unspecified.
117	Parked (Internal IP Office code).
118	UnParked (Internal IP Office code).
119	Pickup (Internal IP Office code).
120	Reminder (Internal IP Office code).
121	Redirect (Internal IP Office code).
122	Call Barred (Internal IP Office code).
123	Forward To Voicemail (Internal IP Office code).
124	Answered By Other (Internal IP Office code).
125	No Account Code (Internal IP Office code).
126	Transfer (Internal IP Office code).
129	Held Call (Internal IP Office code).*
130	Ring Back Check (Internal IP Office code).*
131	Appearance Call Steal (Internal IP Office code).*
132	Appearance Bridge Into (Internal IP Office code).*
133	Bumped Call (Internal IP Office code).*
134	Line Appearance Call (Internal IP Office code).+
135	Unheld Call (Internal IP Office code).+
136	Replace Current Call (Internal IP Office code).+



Cause Code	Definition
137	Glare (Internal IP Office code). +
138	R21 Compatible Conf Move (Internal IP Office code). +
139	RingBack Answered (Internal IP Office code). +
140	Transfer Request Failed (Internal IP Office code). +
141	HuntGroup Drop (Internal IP Office code). +

## 5.3 Decoding FEC Errors

This section details how to decoding the FEC Receiver Error “PRN” statements that appear in the SysMonitor 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\_ = Indicatse the type of IP Office 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 decod 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 (RxB D)”. The table below shows the bits within the RxB D 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 on SysMonitor 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 RxB D is set) – note that the first byte (A) is missing so it is equal to 0, resulting in a 3 byte error code.



# Index

## A

Access 9, 70, 79  
     Delta Server application 76  
     IP Office ContactStore 76  
 Ack 70  
 Address 9, 18, 70, 76  
 ADSL  
     Number 10  
 ALARM 12  
 Alarm Log 12, 13  
 Alarm Log Dump  
     include 12  
 Alarms 12, 13  
 Alerting 66, 69  
 Allowed In 71  
 ALOG 10  
 Analog Trunk Channels  
     Number 10  
 Analogue Line 66  
 ATM 13  
 ATM/Channel 66  
 ATM/Channel2 66  
 ATM/CM Line 66  
 ATM/CM Line2 66  
 ATM/I-O 66  
 ATM/I-O2 66  
 Avaya 7, 12, 13, 16  
 AVRIP 76

## B

B 13, 82  
 B4 01 01 04 02 70  
 Back  
     IP Office Control Unit 61  
 Background Color 13  
 BCD 82  
 Bi-directional 9  
 Bi-directional routing 9  
 Binary Log File 11, 16  
 Binary Logging 16  
 BLF 76  
 Bootstrap Protocol Client 76  
 Bootstrap Protocol Server 76  
 Border Gateway Protocol 76  
 Both SNMP Port 76  
 BRI 66  
     Number 10  
 BRI ISDN 66  
 Broadcast 9  
     IP Office LAN 76  
 Byte B 82  
 Byte C 82  
 Byte D 82

## C

Call 7, 10, 13, 18, 62, 66, 69, 70, 72, 76, 79  
 Call Connected 66, 69  
 Call Disconnected 66, 69  
 Call having 79  
 Call Logging 18  
 Call Proceeding 66, 69  
 Call Rejected 79  
 Call Setup 66, 69  
 Call state 79  
 Call Status 72

Call/ Packets/Extension Receive 62, 66, 69  
 Call/ Packets/Extension RxP 62, 66, 69  
 Call/ Packets/Extension Send 62, 66, 69  
 Call/ Packets/Extension TxP 62, 66, 69  
 Call/ Packets/Line Receive 66, 69, 70  
 Call/ Packets/Short Code Msgs 66, 69  
 Call/Call Logging 72  
 Call/Events/Call Delta 61, 66, 69, 72  
 Call/Events/Call Logging 61, 62, 63, 66, 69, 70  
 Call/Events/Map 61  
 Call/Events/Targeting 70  
 Call/Events/Targeting 61, 62, 63, 66, 69, 72  
 Call/Packets/Extension Receive 61, 72  
 Call/Packets/Extension RxP 61, 72  
 Call/Packets/Extension Send 61, 72  
 Call/Packets/Extension TxP 61, 72  
 Call/Packets/Line Receive 61, 62, 63, 72  
 Call/Packets/Line Send 61, 62, 63, 66, 69, 70, 72  
 Call/Packets/Short Code Msgs 72  
 CALLS 10  
 Calls Answered/Generated 72  
 Cause Codes 79  
 CCC Wallboard Server  
     PC Wallboard 76  
 CD  
     Inserting 8  
 Channel Unacceptable 79  
 Channelised T1 Line 66  
 Channelized T1 Line 66  
 Circuit/channel 79  
 CkSRC 10  
 CL 82  
 Clear 11, 12, 79, 82  
     IP Office 13  
 Clear Alarms  
     clicking 12  
 Clear Display 13  
 Clear Screen Display 11  
 Clicking  
     Clear Alarms 12  
 Clock Source 10  
 Close  
     Monitor 13  
 CMMsg 10  
 Code 70, 79, 82  
 Conference Center 76  
 Conferencing 13  
 Conferencing Center Server Service 76  
 Configuration Lines List 62  
 Connect 10, 64, 66, 69, 71  
     IP Office 11  
     PC 9  
 Contains 11  
     CRC 82  
 Control Unit 10, 13  
 Control Unit's DTE  
     Monitoring 13  
 Conversations" 72  
 CR  
     set 82  
 CRC  
     contains 82  
 CRC Error 82  
 CRIT RAISED addr 12  
 Current Clock Source 10

---

## D

Decoding  
  FEC Errors 82  
  FEC Receiver Error 82  
Default Data 76  
Delta Server application  
  access 76  
Dial-Up Data Connection Problems 63  
Displaying  
  Monitor 16  
  Protocol 76  
Domain Name Server 76  
DS 10  
DT 10  
DTE 13, 61  
DTE Port Maintenance 61  
During  
  VoIP 76

## E

E1 ISDN 66  
E1 PRI Connections 62  
EBLF 72  
EConf 13, 76  
EConsole 72  
Edit 13  
Edit Menu 13  
Eg 7, 9, 76  
EGP 76  
END OF ALARM LOG DUMP 12  
Enter 63, 64, 71  
  IP Address 9  
  ISDN 62  
Error 18, 79  
  IP Office control unit reporting 82  
Ethernet Receive Buffer Descriptor 82  
Events/packets 9  
Every 'n 16  
Example Monitor Settings 56  
Exceeding  
  2047 82  
Exit 13  
Expiry 79  
Extension 203 18  
Extension 203 dialing 201 18  
Extension TxP 72  
Extension" 72  
Extensions/lines 72  
Exterior Gateway Protocol 76

## F

Failing' 71  
Fast Ethernet Controller 18  
FEC 18, 82  
FEC Error Decoding 82  
FEC Errors  
  Decoding 82  
FEC Receiver Error  
  decoding 82  
FEC stands 18  
FIFO 82  
File 10, 11, 13, 71, 76  
  Log 16  
  n MB 16  
File Logging 16  
File Menu 13  
File name 13, 16

Filter Trace Options 11  
Filters Menu 13  
Firewall 13, 71  
Firewall Not Working Correctly 71  
Following  
  Monitor 70  
  PPP 65  
Frame Relay 65  
  Monitoring 13  
Frame Relay Links 65  
Frame Relay/Events 65  
Frame Relay/Mgmt Events 65  
Frame Relay/Rx Data 65  
Frame Relay/Rx Data Decode 65  
Frame Relay/Tx Data 65  
Frame Relay/Tx Data Decode 65  
FreeMem 10  
Freeze Screen Display 11  
Freeze Screen Logging 13  
Freeze/unfreeze 13  
Freezing  
  Monitor 16  
Fri 23/4/2004 15 10

## G

General Routing Encapsulation 76  
Give Information  
  Options Not Selected 18  
Gives 18, 56  
  IP 10  
GOD 13  
GRE 76  
Greyed 11

## H

H.323 76  
  Monitoring 13  
H.323 RAS 76  
H.323/Events/H.323 66, 69  
H.323/H.245 76  
H.323/Packets/H.245 Receive 66, 69  
H.323/Packets/H.245 Send 66, 69  
H.323/Packets/H.323 Fast Start 69  
H.323/Packets/H.323 Fast Start4 66  
H.323/Packets/H.323 Receive 66, 69  
H.323/Packets/H.323 Send 66, 69  
H.323/Packets/RAS Receive 69  
H.323/Packets/RAS Send 69  
H.323/Packets/View Whole Packet 66, 69  
H.323Ras 76  
Hangup 18  
Help Menu 13  
Hours 16  
Hours Interval 16

## I

ICMP  
  IPv6 76  
Ie 16, 70, 82  
IGMP 76  
IGP 76  
IMPORTANT 7  
In\_port 70  
Including  
  Alarm Log Dump 12  
  IP Office 76  
Inserting  
  CD 8

- Installation Wizard
    - start 8
  - Installing
    - Monitor 8
  - Interface Name 71
  - Interface Name" 63, 64, 71
  - Interface Name" fieldin 63
  - Interface Name" fieldin Monitor's PPP 63
  - Interface Queue 70
  - Interface/Firewall 71
  - Interface/Firewall Allowed In 71
  - Interface/Firewall Allowed Out 71
  - Interface/Firewall Fail In 71
  - Interface/Firewall Fail Out 71
  - Interface/Interface Queue 63, 70, 71
  - Interior Gateway Protocol 76
  - Internet 70, 76
  - Internet Control Message 76
  - Internet Group Management 76
  - Interworking 79
  - Invalid 79
  - IP 7, 8, 9, 11, 12, 16, 18, 61, 64, 69, 70, 71, 72, 76, 82
    - gives 10
    - Monitoring 13
  - IP 412 2.1 10, 12
  - IP Address 10, 64, 70, 71
    - Enter 9
  - IP Calculate 13
  - IP Dst 70
  - IP Office 7, 8, 10, 12, 16, 18, 61, 64, 71, 72, 82
    - clear 13
    - Connect 11
    - including 76
    - Monitor 9
    - requests 76
    - specify 13
  - IP Office Administrator Applications CD 8
  - IP Office application 72, 76
  - IP Office config 76
  - IP Office ContactStore
    - access 76
  - IP Office Control Unit 9, 64, 71, 82
    - back 61
    - type 10
  - IP Office control unit reporting
    - error 82
  - IP Office Job Aid
    - Refer 61
  - IP Office keeps 12
  - IP Office LAN
    - Broadcast 76
  - IP Office Manager 8
  - IP Office Monitor 7, 9, 76
  - IP Office Monitor application 7, 76
  - IP Office Ports 76
  - IP Office TAPI 76
  - IP Office TAPI PC 76
  - IP Office Voicemail Server
    - looking 18
  - IP Office's
    - use 9
  - IP Office's System Password 9
  - IP Packet 64, 71, 76
  - IP Rx
    - Service/RAS 9
  - IP subnet 9
  - IP Tx 9
  - IP400 9
  - IP401NG 82
  - IP403 82
  - IP403\_FEC 82
  - IP405 82
  - IP406 82
  - IP406V2 82
  - IP412 82
  - IPO BLF 76
  - IPO License Dongle 76
  - IPO Monitor 76
  - IPO Network DTE 76
  - IPO PCPartner 76
  - IPO Solo Voicemail 76
  - IPO TAPI 76
  - IPO Voice Networking 76
  - IPO Voicemail 76
  - IPO Who-Is 76
  - Ipv6
    - ICMP 76
  - IPv6-ICMP 76
  - IPX 76
  - IPX-In-IP 76
  - ISDN 7, 10, 13, 66, 79
    - entering 62
  - ISDN Problems 62
  - ISDN/Events/Layer 62, 66
  - ISDN/Packets/Layer3 Tx 63
  - ISDN/Packets/Layer 62, 66
  - ISDN/Packets/Layer3 Rx 63, 70
  - ISDN/Packets/Layer3 Tx 70
  - ISP 63
  - ISP/Remote Routing 70
- K**
- Kbytes 82
  - Key/Lamp 13
- L**
- L 82
  - L2TP 76
  - LAN 10, 18, 61, 70
  - LAN Modules
    - Number 10
  - LAN1 9
  - LANM 10
  - LAW 10
  - Layer Two Tunneling Protocol 76
  - LDAP 13
  - Leased 64, 71
  - Leased Line 64, 71
  - Len 70
  - Length Error 82
  - LG 82
  - License Server IP Address 76
  - Line 10, 13, 18, 62, 64, 66, 71
  - Line" 72
  - Lines include 10
  - Links 10, 65, 70
  - Locating
    - PC 70
    - Specific 70
    - Specific PC Making Calls 70
  - Log Filename 16
  - Log Mode 16
  - Log Preferences 11, 13

Log Preferences 11, 13  
 Setting 16  
 Logging  
 File 16  
 Looking  
 IP Office Voicemail Server 18  
**M**  
 Making 70  
 Management 65  
 Manager  
 System form 9  
 Marker  
 Placing 18  
 MAX\_FRAME\_LENGTH 82  
 MB 16  
 MBytes 16  
 MBytes Interval 16  
 MDM 10  
 Message 18, 64, 71, 79, 82  
 Miscellaneous 18  
 Modem Card Fitted 10  
 MODU 10  
 Monitor 10, 11, 56, 61, 62, 63, 64, 65, 66, 69, 71, 72, 79  
 Close 13  
 Control Unit's DTE 13  
 displaying 16  
 following 70  
 Frame Relay 13  
 freezing 16  
 H.323 13  
 Installing 8  
 IP 13  
 IP Office 9  
 Monitor Password 9  
 PC running 9  
 running 7, 12, 16, 18  
 Starting 9  
 Monitor application 7, 9, 16, 61  
 Monitor display  
 Windows 13  
 Monitor Icons 11  
 Monitor includes 71  
 Monitor IP 13  
 Monitor ISDN 13  
 Monitor LDAP 13  
 Monitor Menus 13  
 Monitor Password  
 Monitor 9  
 Monitor R2 13  
 Monitor SNMP 13  
 Monitor Started IP 10  
 Monitor T1 13  
 Monitor toolbar 16  
 Monitor Trace 7, 10, 11, 12, 13, 16, 18, 79  
 observing 70  
 Monitor VPN 13  
 Monitor WAN 13, 64, 71  
 Monitor window 11  
 Monitor's PPP 13, 63, 64, 71  
 MUST 9  
**N**  
 N 16  
 N MB  
 file 16  
 N/U 82

N/U" 82  
 NAT 13, 70  
 NATranslator d40190dc 00000000 70  
 NETBIOS Datagram Service 76  
 NETBIOS Name Service 76  
 NETBIOS Session Service 76  
 Network Time Protocol 76  
 Next 8, 10  
 NO 82  
 Non-IP Office 76  
 Non-Octet 82  
 NOT 82  
 Number 11, 13, 16, 18, 62, 70, 76, 79, 82  
 ADSL 10  
 Analog Trunk Channels 10  
 BRI 10  
 LAN Modules 10  
 PRI 10  
 TDM 10  
 VCM 10  
 WAN Ports 10  
**O**  
 Observing  
 Monitor Traces 70  
 OK 9, 16  
 On/off 13  
 Open File 11, 13, 16  
 Options Not Selected  
 Give Information 18  
 Why Does Monitor Give Information 18  
 Out 11, 66, 70, 79  
 PBX 71  
 Out\_port 70  
 OV 82  
 Overrun Error 82  
**P**  
 PAP/CHAP 63, 64, 71  
 Password 9, 63, 64, 71  
 PBX 70, 72  
 Out 71  
 PBX's 9  
 PC 10, 12, 18, 76  
 connect 9  
 locate 70  
 PC running 10, 76  
 Monitor 9  
 PC Wallboard  
 CCC Wallboard Server 76  
 Pcol 70, 76  
 PC's CD 8  
 Phone Manager 72, 76  
 Placing  
 Marker 18  
 PLATFORM 82  
 PLATFORM\_FEC 82  
 Port 10, 13, 18, 61, 62, 64, 70, 71, 76  
 Port 520 RIP 76  
 Port during 61  
 Port Number" 62, 64, 71  
 Ports including 76  
 POT 10  
 PPP 7, 13  
 following 65  
 PPP/IP Rx 64, 65, 71  
 PPP/IP Tx 64, 65, 71



- PPP/IPCP Rx 63, 64, 65, 71
- PPP/IPCP Tx 63, 64, 65, 71
- PPP/LCP Rx 63, 64, 65, 71
- PPP/LCP Tx 63, 64, 65, 71
- PPP/Security Rx 63, 64, 65, 71
- PPP/Security Tx 63, 64, 65, 71
- PRI 62
  - Number 10
- Print 61, 62, 63, 64, 66, 70, 71, 72, 82
- PRN 10, 12, 18, 70, 82
- PRN" 82
- Problem 7, 12, 18, 61, 62, 63, 64, 69, 71, 72
- Problems Involving IP Phones 69
- Problems Involving Non-IP Phones 69
- Program Exception 12
- Program Files/Avaya/IP Office/Monitor 16
- Programs 9, 12, 13, 16, 70
- Protocol 70, 79
  - displaying 76
- Q**
- QSig 66
- QSIG Line 66
- R**
- R2 13
- Receive 12, 18, 62, 66, 82
- Receive CRC 82
- Receive1 66
- ReceiverError 18, 82
- ReceiverError 844 82
- ReceiverError ABCD 82
- ReceiverError Codes 82
- Recovery 79
- Refer
  - IP Office Job Aid 61
- Rem 70
- Rem\_port 70
- Remote Site Data Connection Problems 64, 71
- Requested circuit/channel 79
- Requests 16, 70, 79
  - IP Office 76
- Reselect 61
- Reservation Protocol 76
- RIP 76
- RIP1 76
- RIP2 76
- RIP2 Multicast 76
- Rollover Log 11, 13, 16
- RSVP 76
- Run Screen Display 11
- Running
  - 22secs 10
  - Monitor 7, 12, 16, 18
- Rx 82
- RxBD 82
- RxP 72
- S**
- S/w 10
- Save Screen Log 13, 16
- Save Screen Log As... 13
- Save Trace 11
- Select All 13
- Select File 9, 16
- Select Modify 8
- Select Start 9
- Select Unit 9, 11
  - Shows 13
- Select Unit form
  - specify 13
- Selected Hex 13
- Selecting
  - Status 12
- Send 18, 61, 62, 66
- Send1 66
- Seq 70
- Service 63, 64, 71, 76, 79
- Service Name" 63, 64, 71
- Service/RAS
  - IP Rx 9
- Service" 63, 64, 71
- Set 9, 11, 13, 18, 76
  - CR 82
  - Logging Preferences 16
- Setting menu 13
- SH 82
- Short Frame 82
- Shows 10, 11, 82
  - B 13
  - Select Unit 13
- Simple File Transfer Protocol 76
- Simple Mail Transfer 76
- Simple Message Protocol 76
- Small Community Network 76
- Small Community Network signalling 76
- Small Office Edition 82
- SMP 76
- SNMP 13, 76
- SNMP Trap 76
- SNMPTRAP 76
- SoftConsole 76
- Specific
  - Locating 70
- Specific PC Making Calls
  - Locating 70
- Specify 11, 71, 79
  - IP Office 13
  - Select Unit form 13
- Speech Calls Dropping 66
- SQL Service 76
- Src 70, 76
- Start Logging 11
- START OF ALARM LOG DUMP 12
- Starting
  - Installation Wizard 8
  - Monitor 9
- Status 13, 61, 62, 63, 64, 66, 70, 71, 72, 79, 82
  - selecting 12
- Status Menu 13
- Stop Logging 11
- Subnet 9, 76
- Subnet's 9
- Subnets 9
- Sum 70
- SYN 70
- SysMonitor 10, 13, 82
- SysMonitor 4.1 10
- SysMonitor 5.0 13
- System 8, 9, 10, 13, 18, 61, 82
- System form
  - Manager 9
- System Information 10
- System Monitor 8

---

System Rebooting 61  
System Voicemail 10  
System/Error 61, 62, 63, 64, 66, 70, 71, 72  
System/Print 61, 62, 63, 64, 66, 70, 71, 72, 82  
System/Resource 61, 62, 63, 64, 66, 70, 71, 72  
System/Resource Status Prints 61, 62, 63, 64, 66, 70, 71, 72

## T

T1 13, 62, 66  
T1 ISDN 66  
T1/CAS 66  
T1/CAS3 66  
T1/Channel 66  
T1/Channel3 66  
T1/Dialler 66  
T1/Dialler3 66  
T1/DSP 66  
T1/DSP3 66  
T1/Line 66  
T1/Line3 66  
TAPI 76  
TCP 70, 76  
TCP Dst 70  
TCP SYN 70  
TCPNATSession 70  
TDM  
    Number 10  
Telecommunications 7  
Telecoms 56  
Telnet 76  
Text Log File 11, 16  
These "Fast Ethernet Controller" 82  
TOT 10  
TR 82  
Trace Options 13  
Traces 70  
Transfer 76  
Transmission Control 76  
Trivial File Transfer 76  
Truncate Error 82  
Txt 13  
TYP 10  
Type 16, 70, 79, 82  
    IP Office Control Unit 10  
    Voicemail Server 10

## U

U 10  
UDP 18, 76  
UDPNATSession 70  
UKIP WAN 70  
US PRI 13  
US PRI Trunks... 13  
Use 7, 13, 66, 70, 71, 72, 79  
    IP Office's 9  
User Datagram 76

## V

VCM  
    Number 10  
VCOMP 10  
VER 10  
Version 2.1 82  
View Menu 13  
VMAIL 10  
Voicemail 10, 18, 76  
Voicemail IP Address 18

Voicemail Server 76  
    Type 10  
VoIP 66  
    during 76  
VoIP Extension 66  
VoIP Line 66  
VPN 13, 66  
VPN Line 66  
VRL 76

## W

WAN 10, 13, 64, 71  
WAN Ports 64, 71  
    Number 10  
WAN Rx 64, 71  
WAN Tx 64, 71  
WAN/WAN Rx 64, 71  
WAN/WAN Tx 64, 71  
WAN/WAN/Events 64, 71  
WAN3s 10, 64, 71  
WATCHDOG 12  
Wave 76  
Why Does 18  
Why Does Monitor Give Information  
    Options Not Selected 18  
Windows 70  
    Monitor display 13  
Wizard 8  
World Wide Web HTTP 70  
World Wide Web-HTTP 76  
Www.iana.org/assignments/port-numbers 76



Performance figures and data quoted in this document are typical, and must be specifically confirmed in writing by Avaya before they become applicable to any particular order or contract. The company reserves the right to make alterations or amendments to the detailed specifications at its discretion. The publication of information in this document does not imply freedom from patent or other protective rights of Avaya or others.

Intellectual property related to this product (including trademarks) and registered to Lucent Technologies have been transferred or licensed to Avaya.

All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

This document contains proprietary information of Avaya and is not to be disclosed or used except in accordance with applicable agreements.

Any comments or suggestions regarding this document should be sent to "wgctechpubs@avaya.com".

© 2008 Avaya Inc. All rights reserved.

Avaya  
Unit 1, Sterling Court  
15 - 21 Mundells  
Welwyn Garden City  
Hertfordshire  
AL7 1LZ  
England.

Tel: +44 (0) 1707 392200  
Fax: +44 (0) 1707 376933

Web: <http://www.avaya.com/ipoffice/knowledgebase>