# IP Office

## IP Office System Monitor

15-601019 Issue 02b - (28 November 2008)

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.
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 "®," "™" 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



## 2. Trace Options



## 3. Status Screens



## 4. Example Monitor Settings



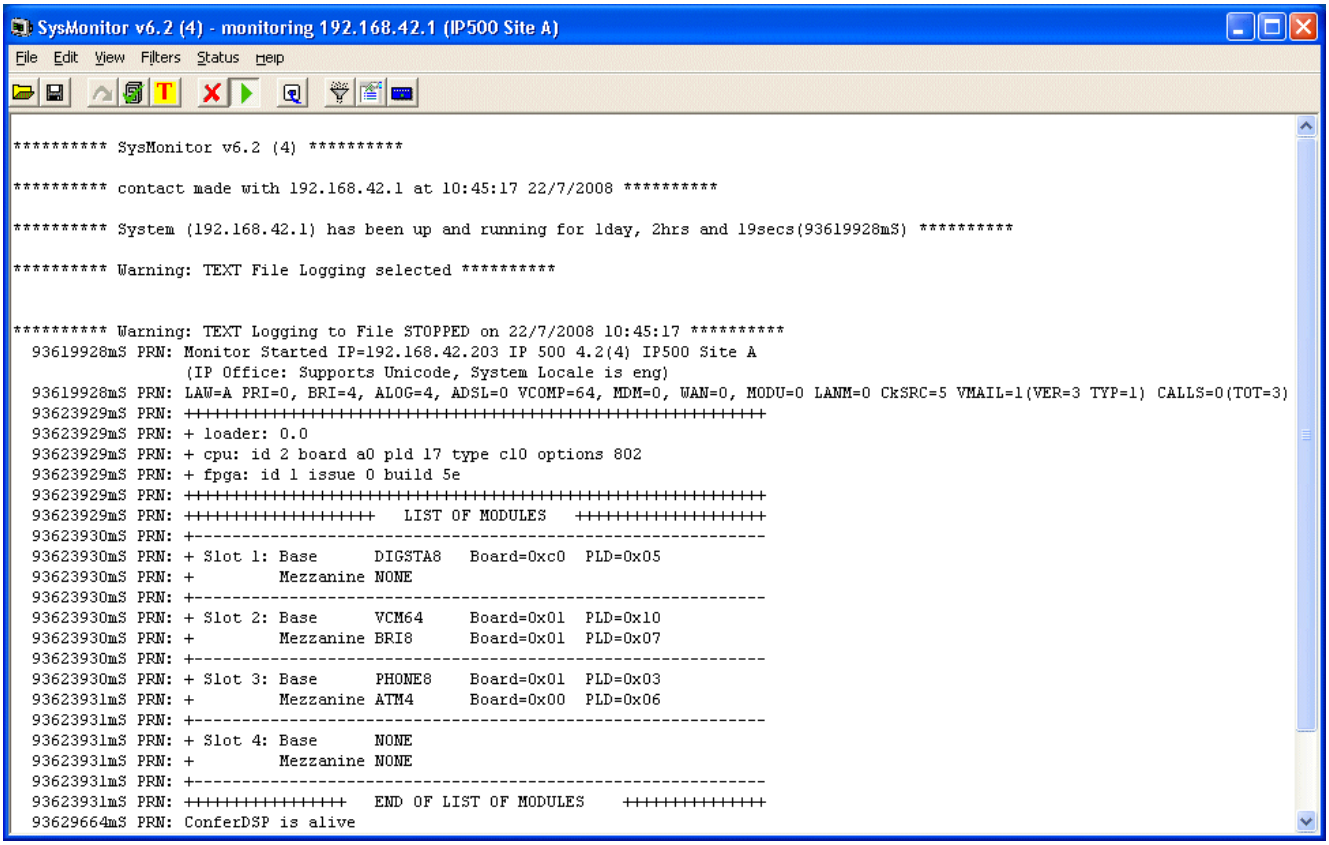
## 5. Addendum

# 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.




- 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

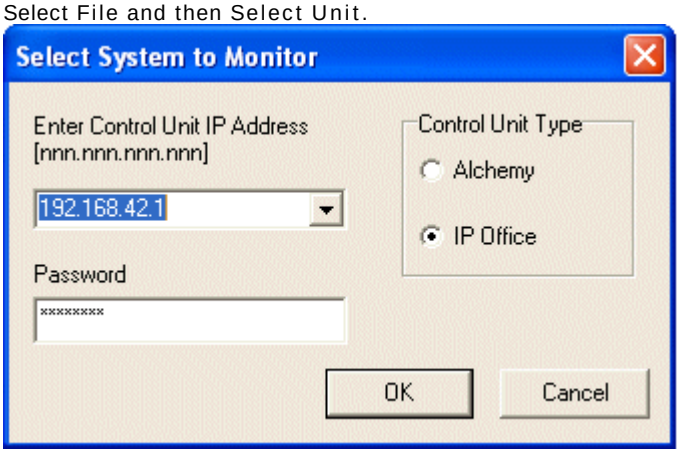
System Monitor can be run from a PC on the same local IP subnet as the targeted IP Office or it can run on a PC on a remote subnet.

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 10 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 16.

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

| | |
|---|---|
| LAW = | A-Law or U-law system. |
| PRI = | Number of PRI channels |
| BRI = | Number of BRI channels. |
| ALOG = | Number of Analog Trunk Channels |
| ADSL = | *Not Used.* |
| VCOMP = | Number of voice compression channels installed. |
| MDM = | Size of Modem Card Fitted |
| WAN = | Number of WAN Ports configured. |
| MODU = | Number of external expansion modules (excluding WAN3 modules) attached. |
| LANM = | Number of WAN3 external expansion modules attached. |
| CkSRC = | The current clock source being used for PRI/BRI trunks (0 = Internal Clock Source). |
| VMAIL = | Indicates whether the voicemail server is connected. 1 if connected, 0 if not connected. |
| VER = | The software version of the voicemail server if obtainable. |
| TYP = | The type of Voicemail Server:<br>0 = None.<br>1 = Voicemail Lite/Pro.<br>2 = Centralized Voicemail Pro.<br>3 = Embedded Voicemail.<br>4 = Group (3rd party) voicemail.<br>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 12.

## 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 0094d78
3019mS PRN: ALARM: 22/04/2004 07:26:44 IP 412 2.1(11) <Program Exception> CRIT RAISED addr=00000000 d=5 pc=00000000 0095dfe0 0095e2
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 0095e2
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 52. 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 20
  Allows you to select and filter trace captured by System Monitor based on a range of categories:
  - ATM 21
    System Monitor analog trunk traffic and events.
  - Call 22
    Monitoring of extensions and calls.
  - DTE 23
    Monitoring of the Control Unit's DTE port.
  - EConf 24
    System Monitor conference and conferencing server events.
  - Frame Relay 25
    Monitoring of Frame Relay traffic and events.
  - GOD 26
    For use by Avaya development engineers only.
  - H.323 27
    Monitoring of H.323 traffic and events.
  - Interface 28
    Monitoring IP interfaces such as NAT and the Firewall.
  - ISDN 29
    System Monitor ISDN traffic and events.
  - Key/Lamp 31
    System Monitor appearance functions
  - LDAP 32
    System Monitor LDAP traffic and events.
  - Media 33
  - PPP 34
    System Monitor PPP traffic and events.
  - R2 35
    System Monitor R2 trunk traffic and events.
  - Routing 36
    System Monitor IP traffic and events.
  - SCN 37
    System Monitor Small Community Network traffic and information.
  - Services 38
    System Monitor SNMP alarms events.
  - SIP 39
    System Monitor SIP trunks and connections.
  - System 40
    System Monitor internal events.
  - T1 41
    System Monitor T1 traffic and events.
  - VPN 42
    System Monitor VPN events.
  - WAN 43
    System Monitor WAN traffic and events.

## Status Menu

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

## 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).

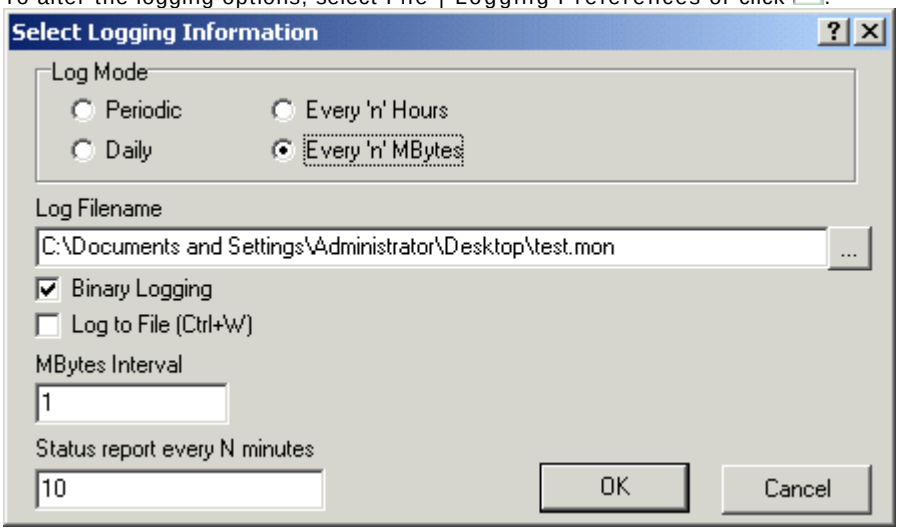
A logged trace can be examined later and, if requested, be sent to Avaya for analysis.

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 10 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 is does not normally indicate a problem and is nothing to worry about unless the error's are streaming in the trace. See Decoding FEC Errors 82.

### 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.

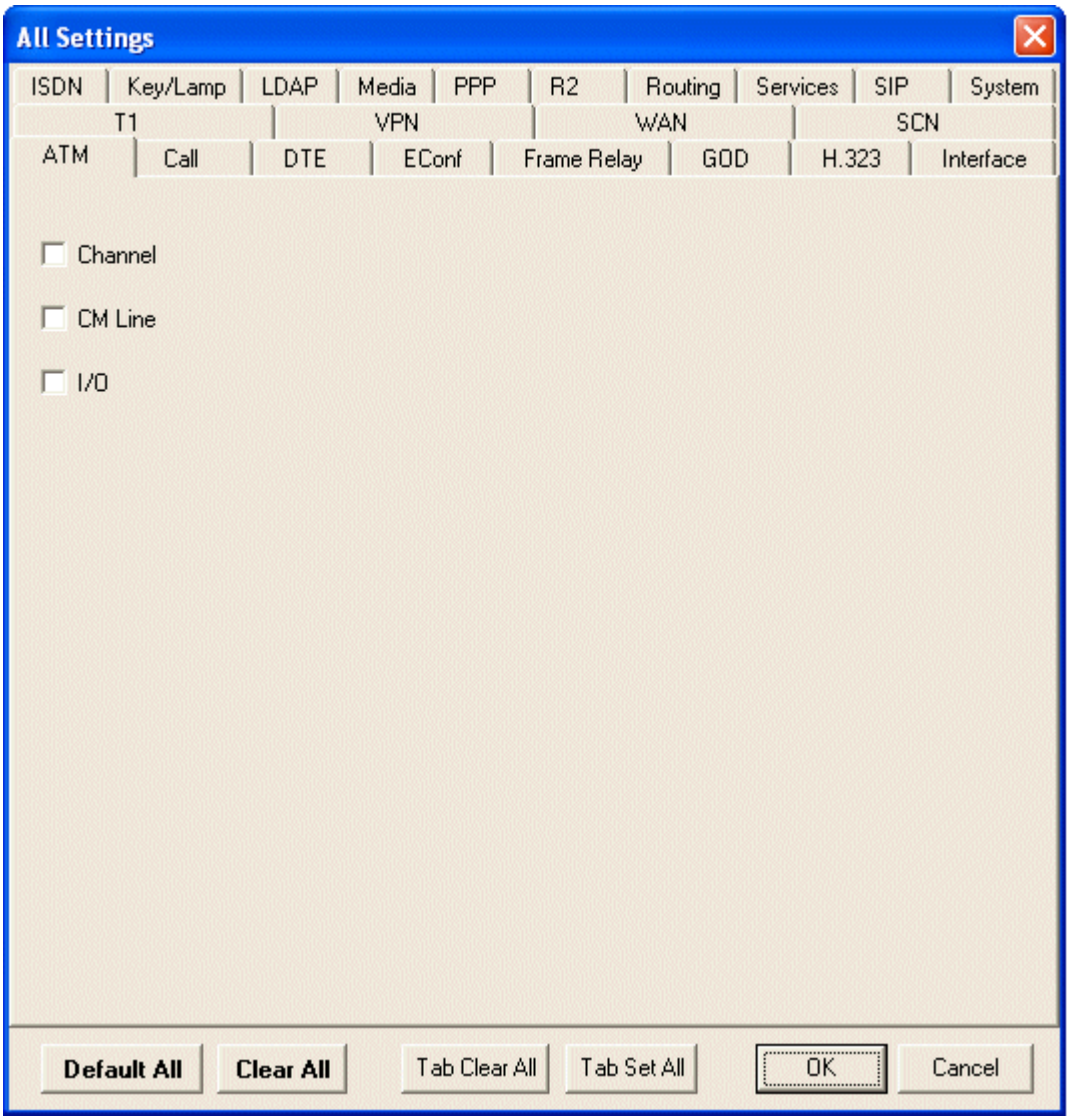
You can then search for a line such as shown below in the System Monitor trace (in this example case Extension 203 dialing 201 and then hanging up):

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

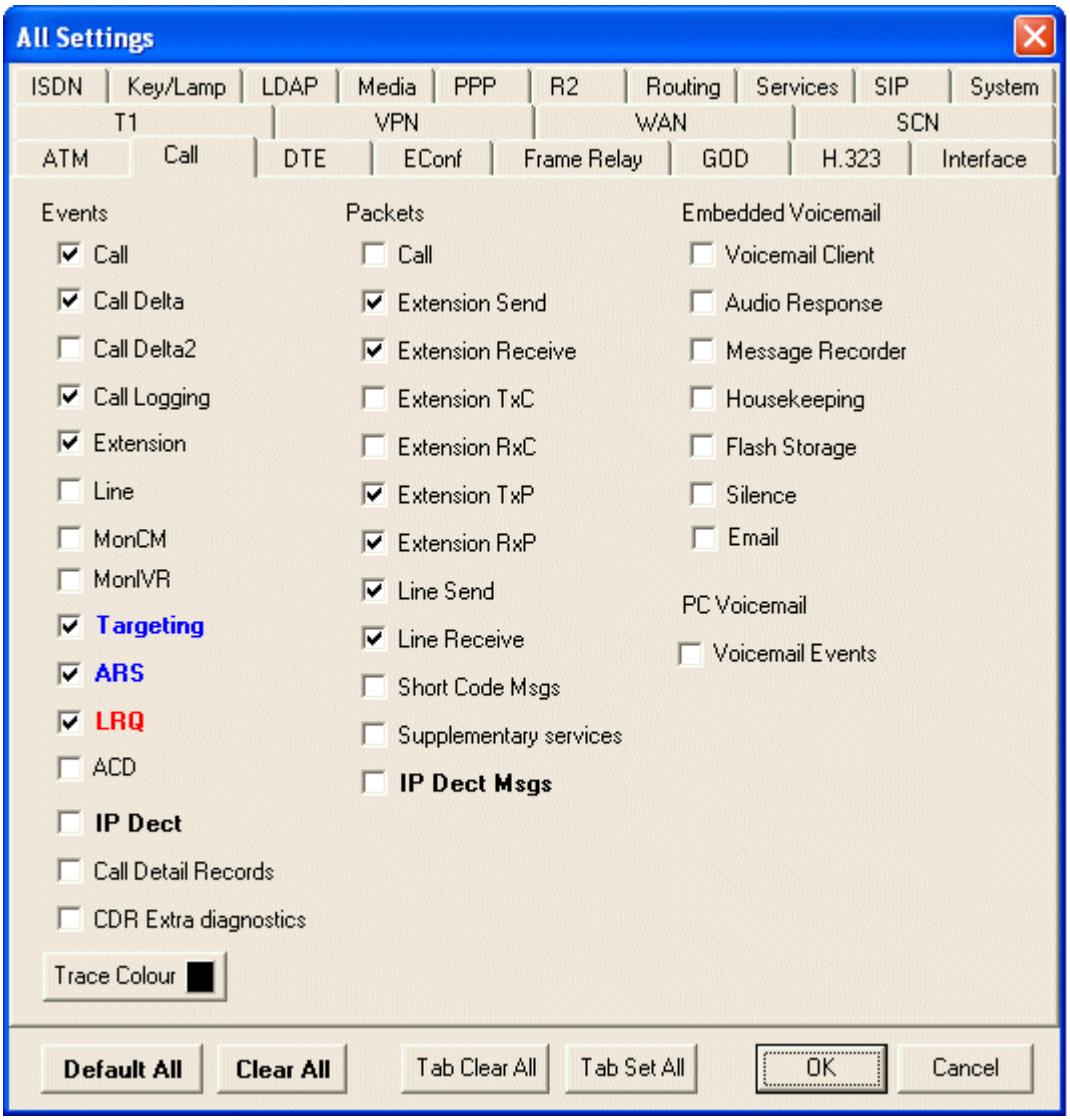
# Chapter 2.
# Trace Options

# 2. Trace Options

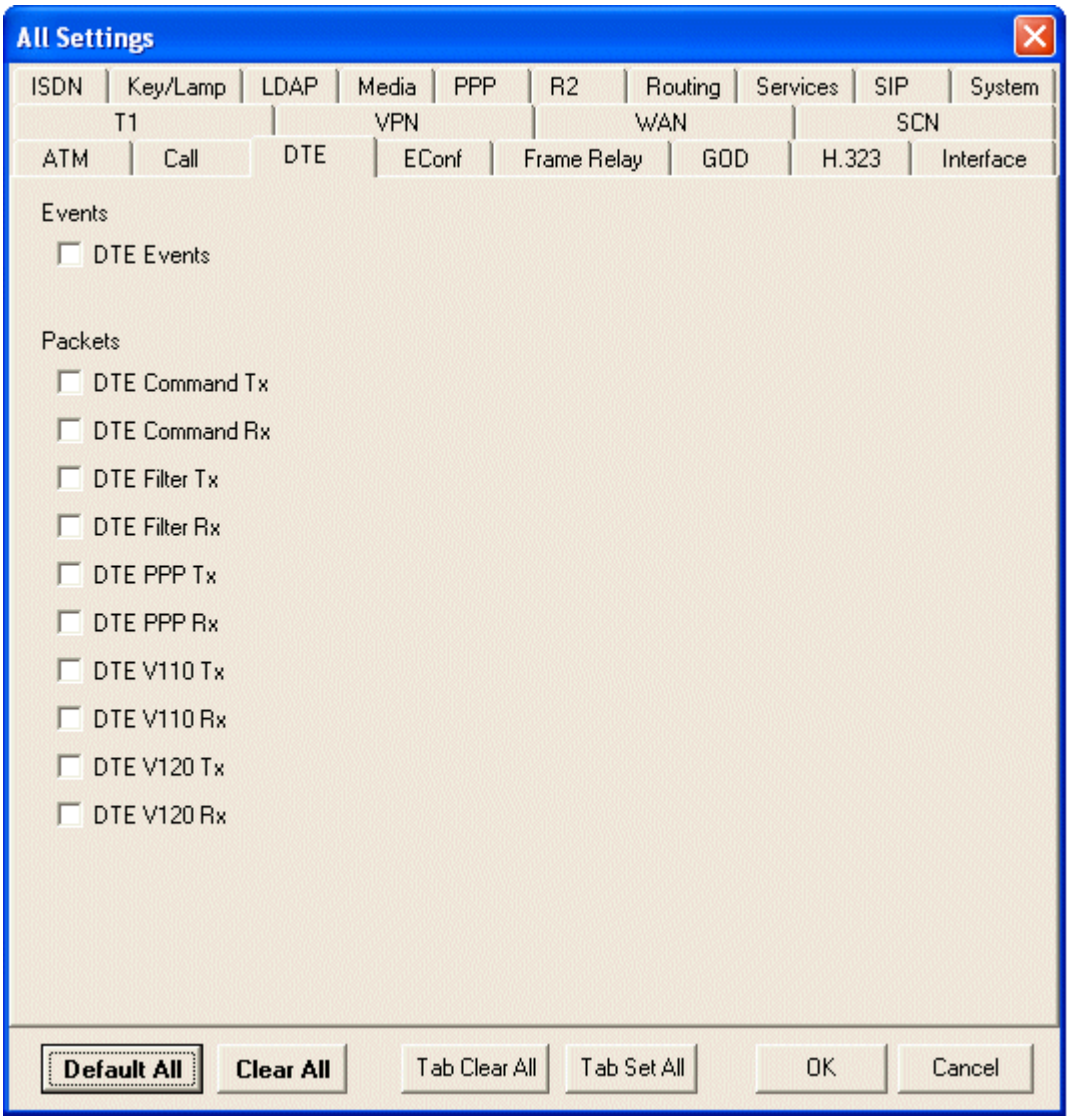
## 2.1 ATM


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
Channel
CM Line
I/O
Default All
Clear All
Tab Clear All
Tab Set All
OK
Cancel

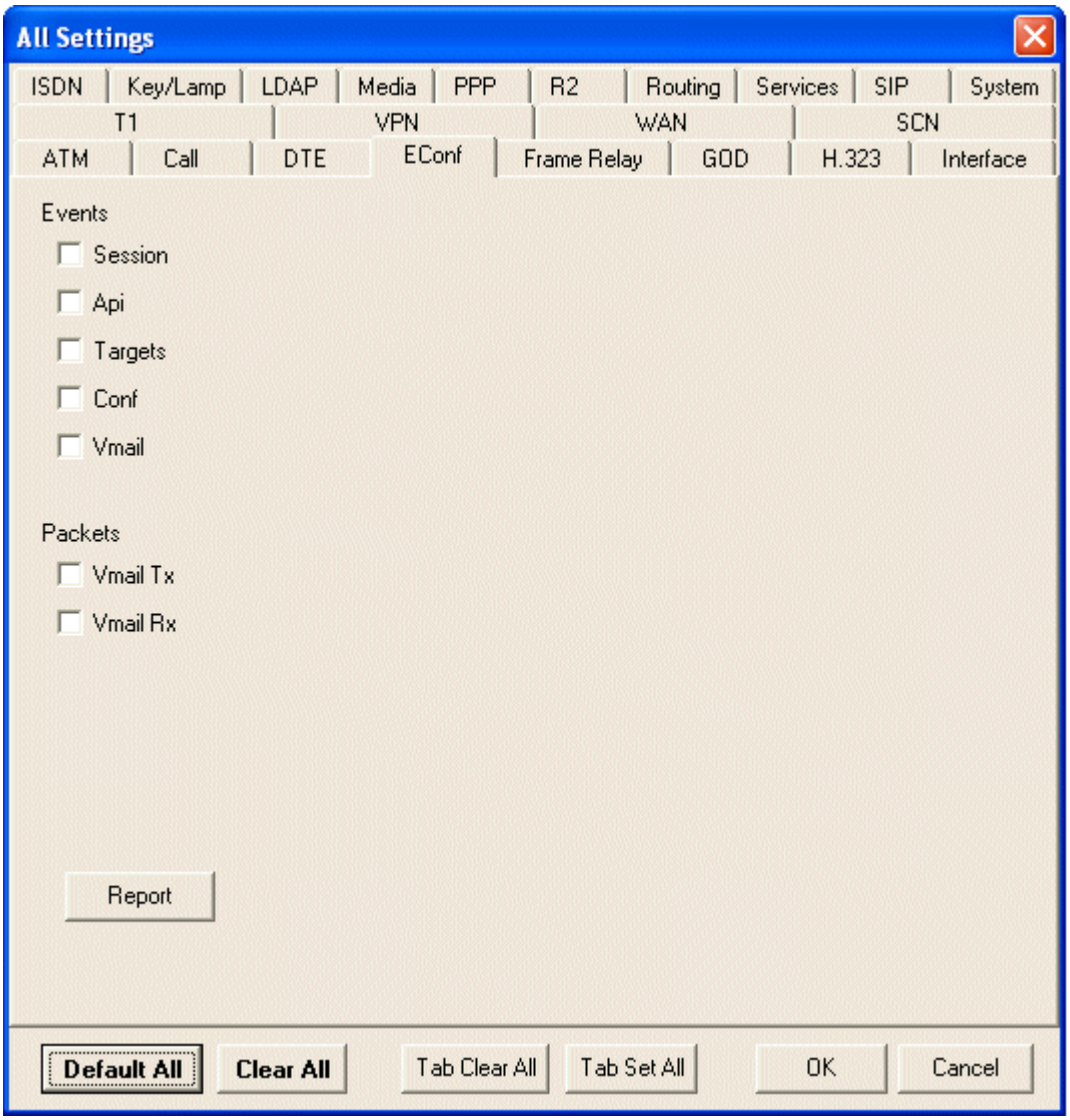
## 2.2 Call


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
Call
Call Delta
Call Delta2
Call Logging
Extension
Line
MonCM
MonIVR
Targeting
ARS
LRQ
ACD
IP Dect
Call Detail Records
CDR Extra diagnostics
Trace Colour
Packets
Call
Extension Send
Extension Receive
Extension TxC
Extension RxC
Extension TxP
Extension RxP
Line Send
Line Receive
Short Code Msgs
Supplementary services
IP Dect Msgs
Embedded Voicemail
Voicemail Client
Audio Response
Message Recorder
Housekeeping
Flash Storage
Silence
Email
PC Voicemail
Voicemail Events
Default All
Clear All
Tab Clear All
Tab Set All
OK
Cancel

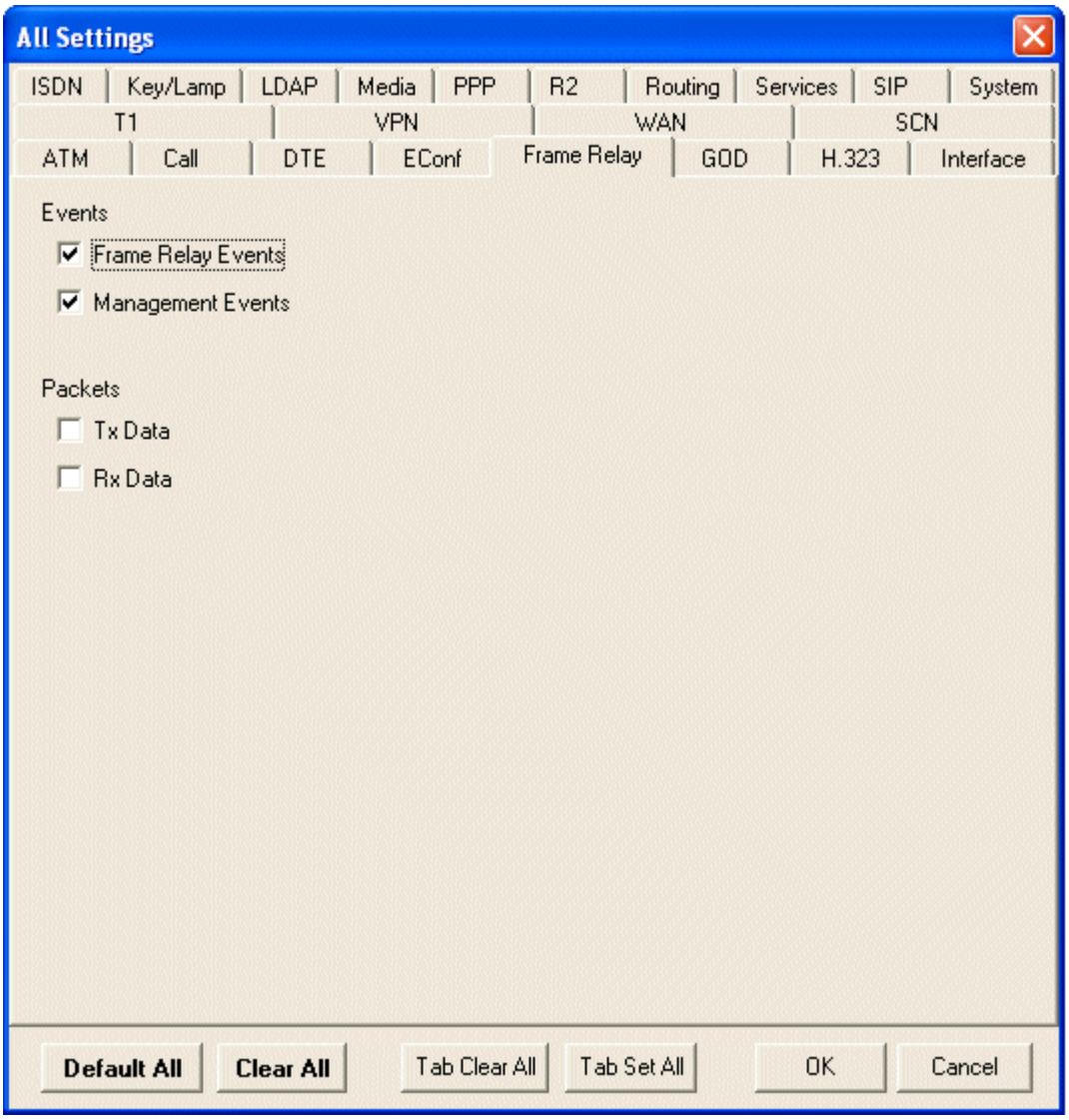
## 2.3 DTE


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

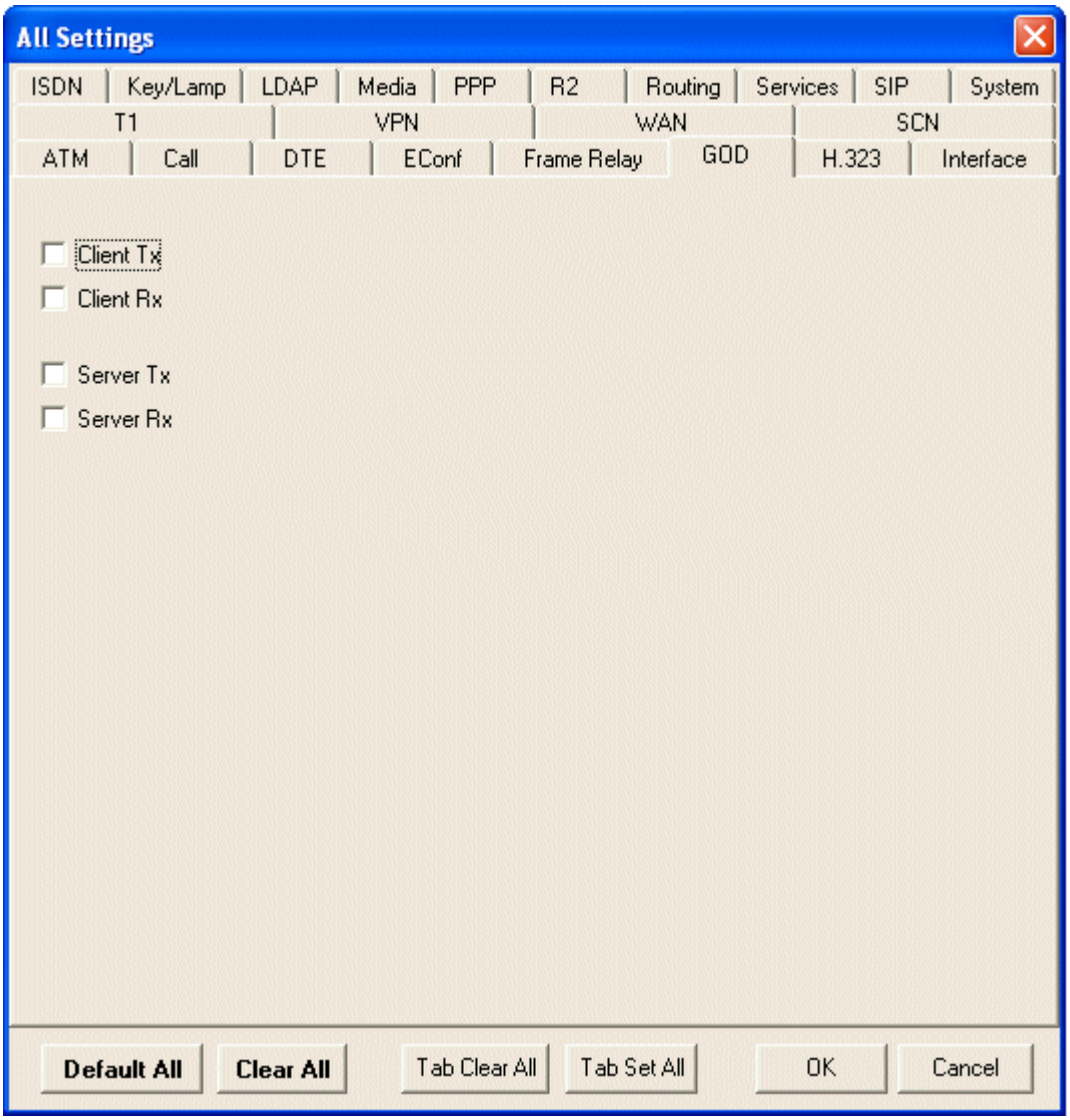
## 2.4 EConf


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
Session
Api
Targets
Conf
Vmail
Packets
Vmail Tx
Vmail Rx
Report
Default All
Clear All
Tab Clear All
Tab Set All
OK
Cancel

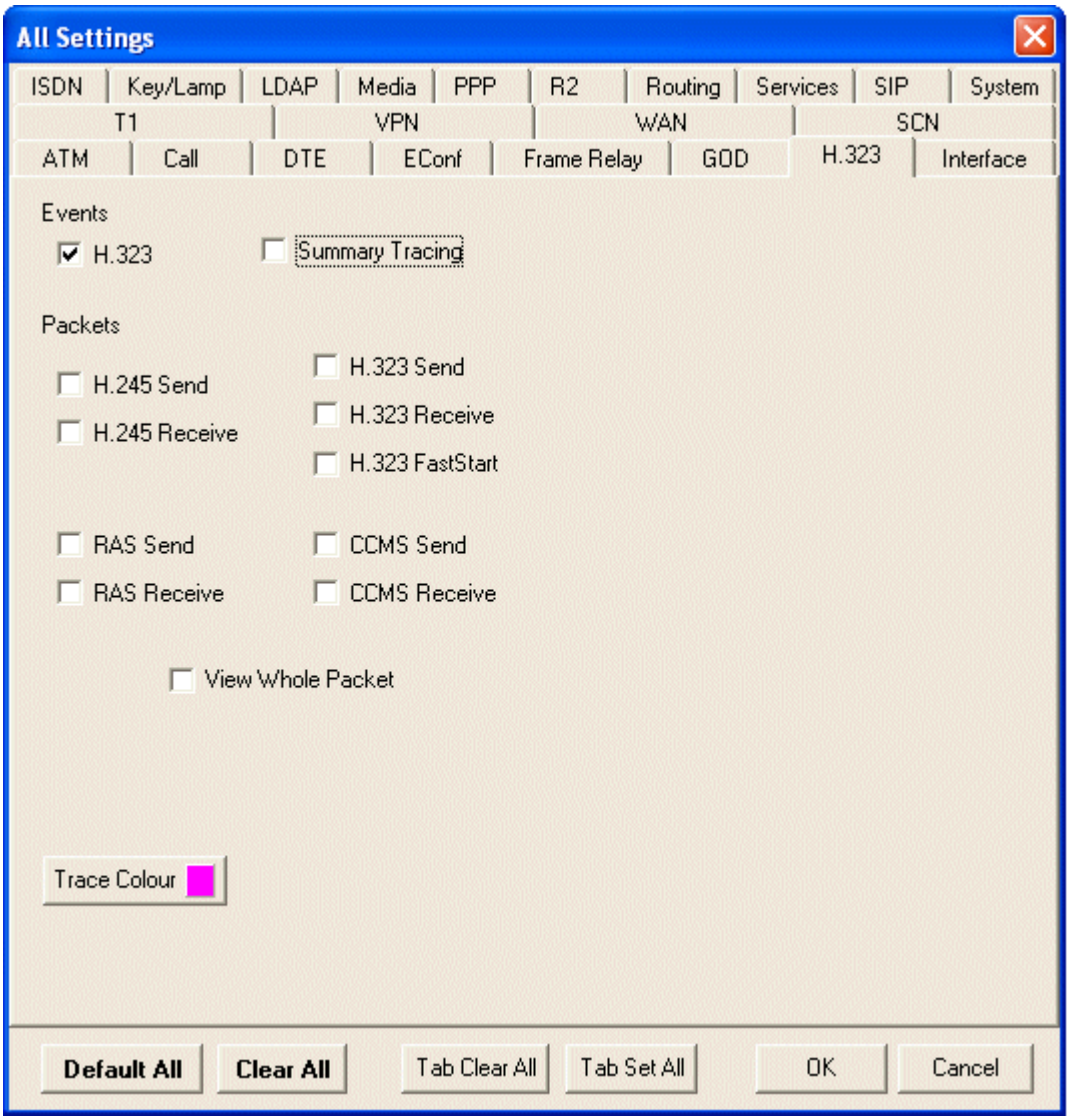
## 2.5 Frame Relay



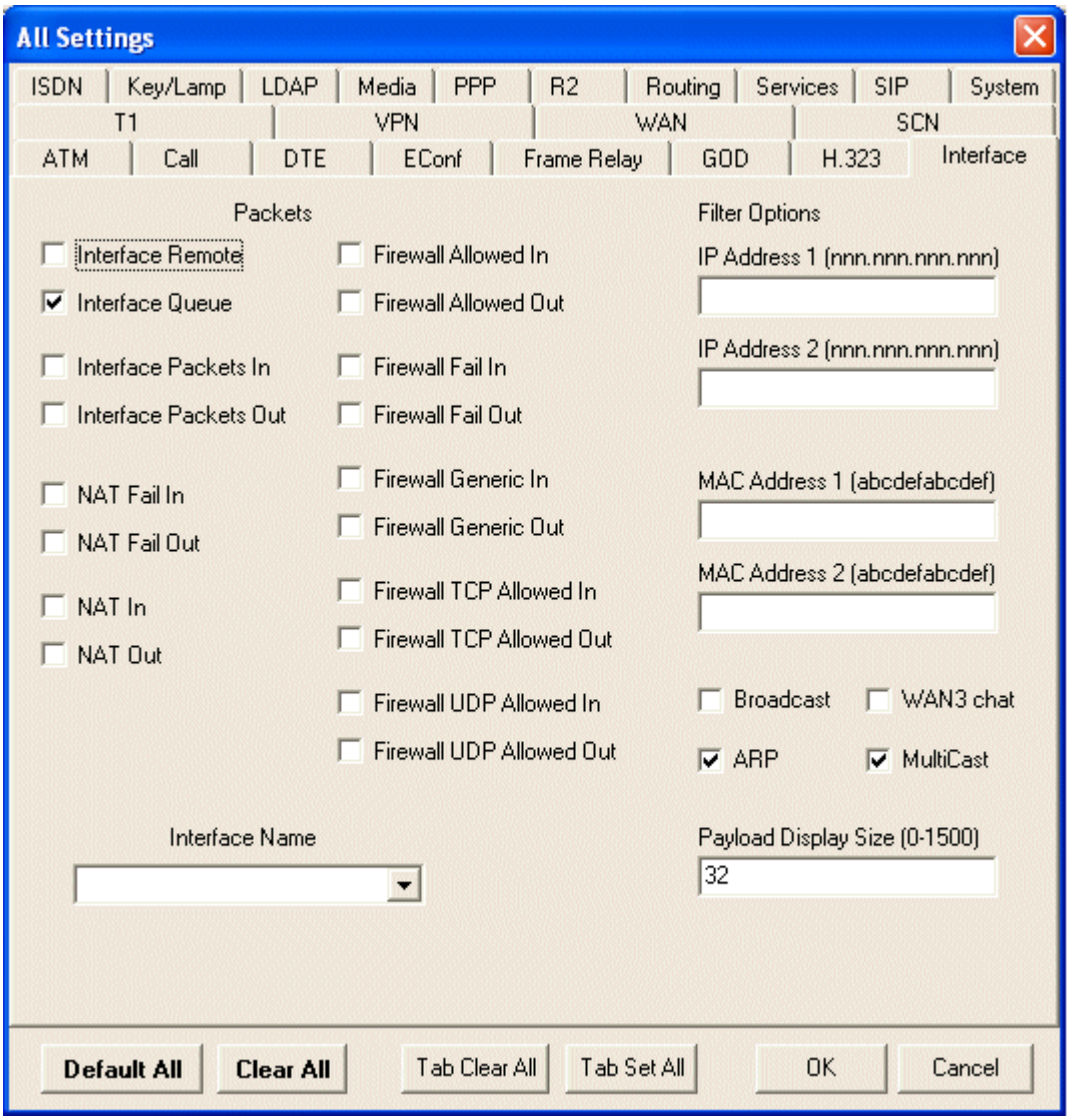
## 2.6 GOD


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

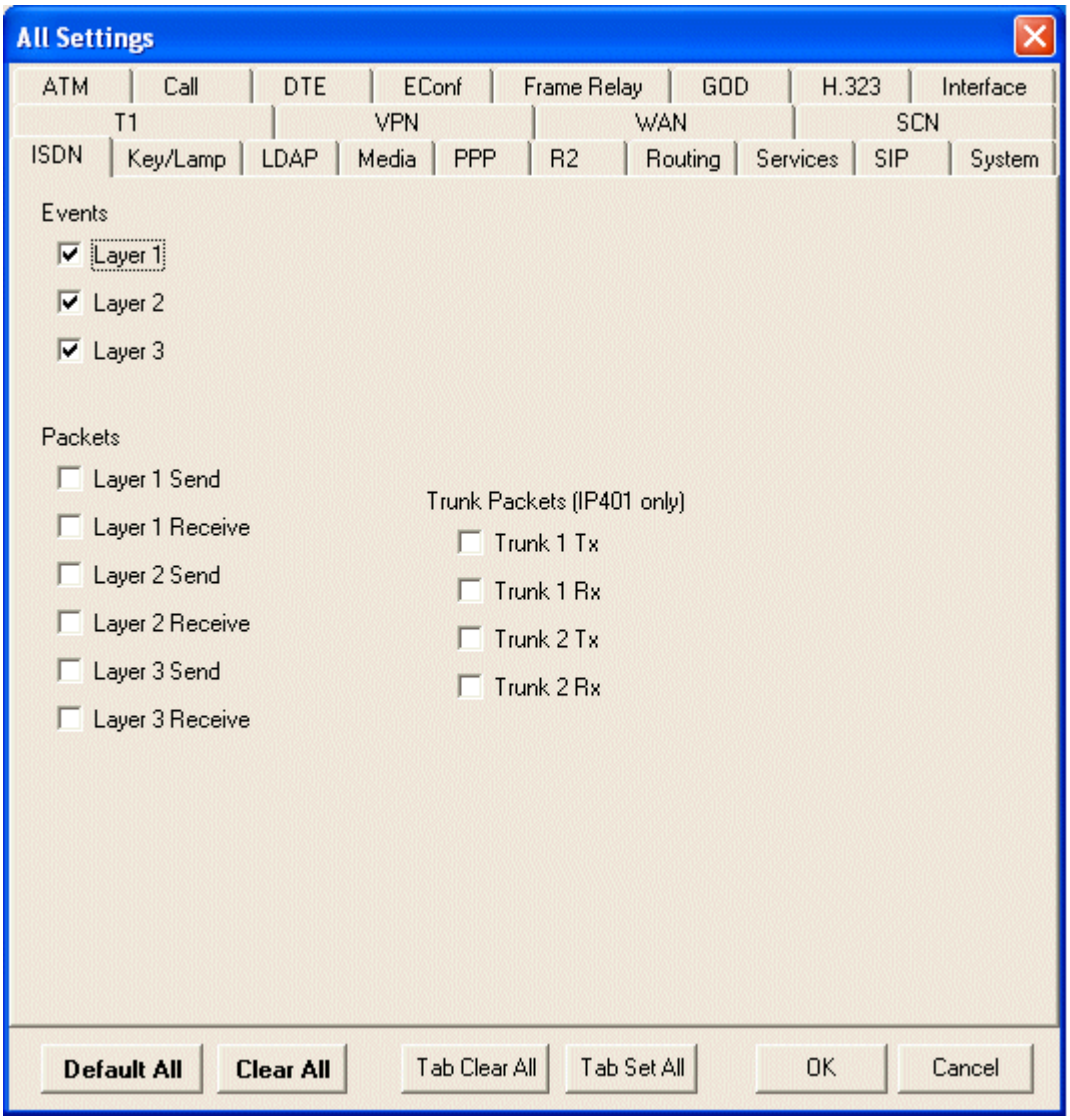
## 2.7 H.323


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.245 Receive
H.323 Send
H.323 Receive
H.323 FastStart
RAS Send
RAS Receive
CCMS Send
CCMS Receive
View Whole Packet
Trace Colour
Default All
Clear All
Tab Clear All
Tab Set All
OK
Cancel

## 2.8 Interface



## 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:

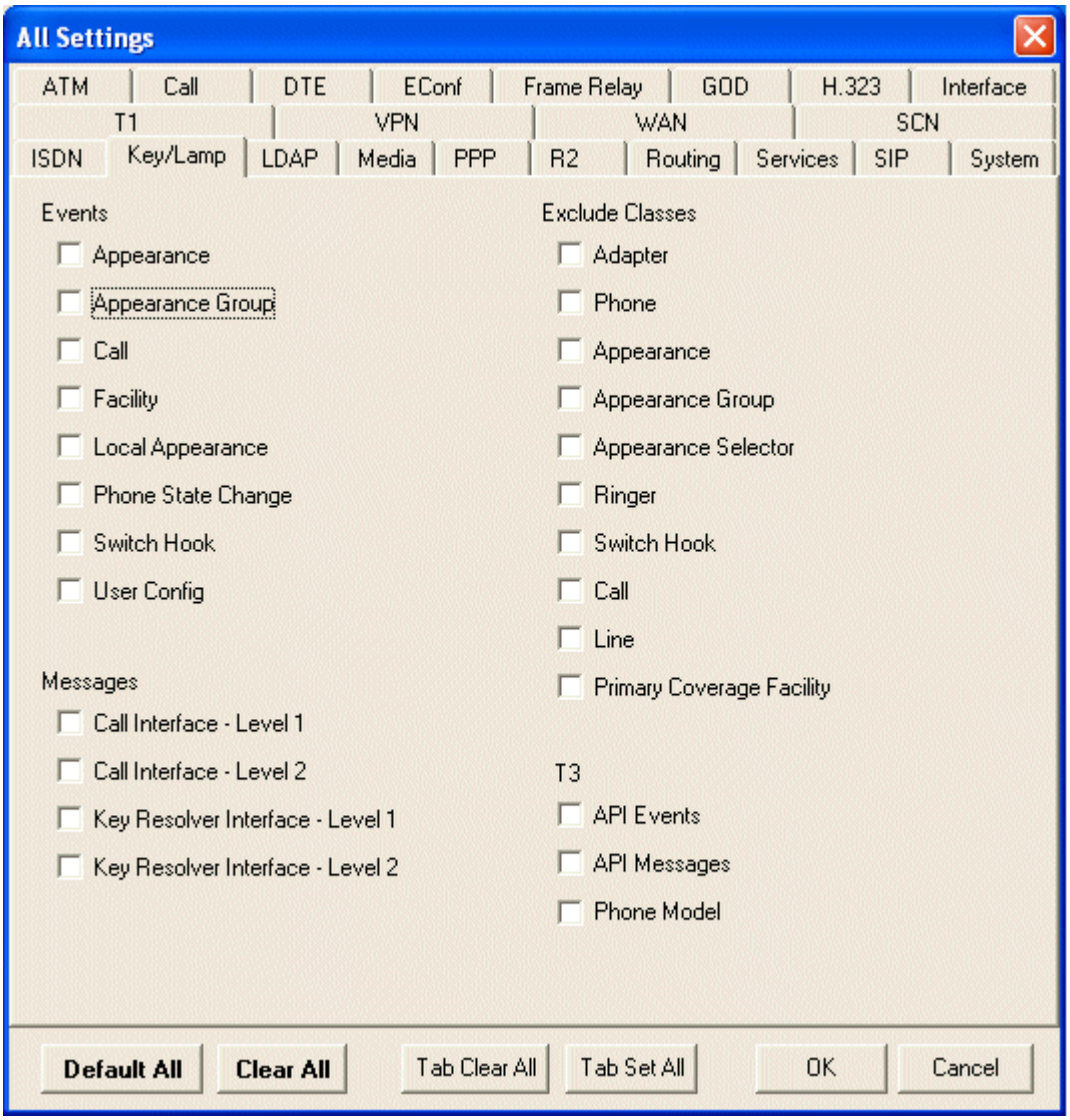
| Value | Definition |
|---|---|
| F1 | Inactive. |
| F2 | Sensing. |
| F3 | Deactivated. |
| F4 | Awaiting signal. |
| F5 | Identifying input. |
| F6 | Synchronised. |
| F7 | Activated. |
| F8 | Lost framing. |

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

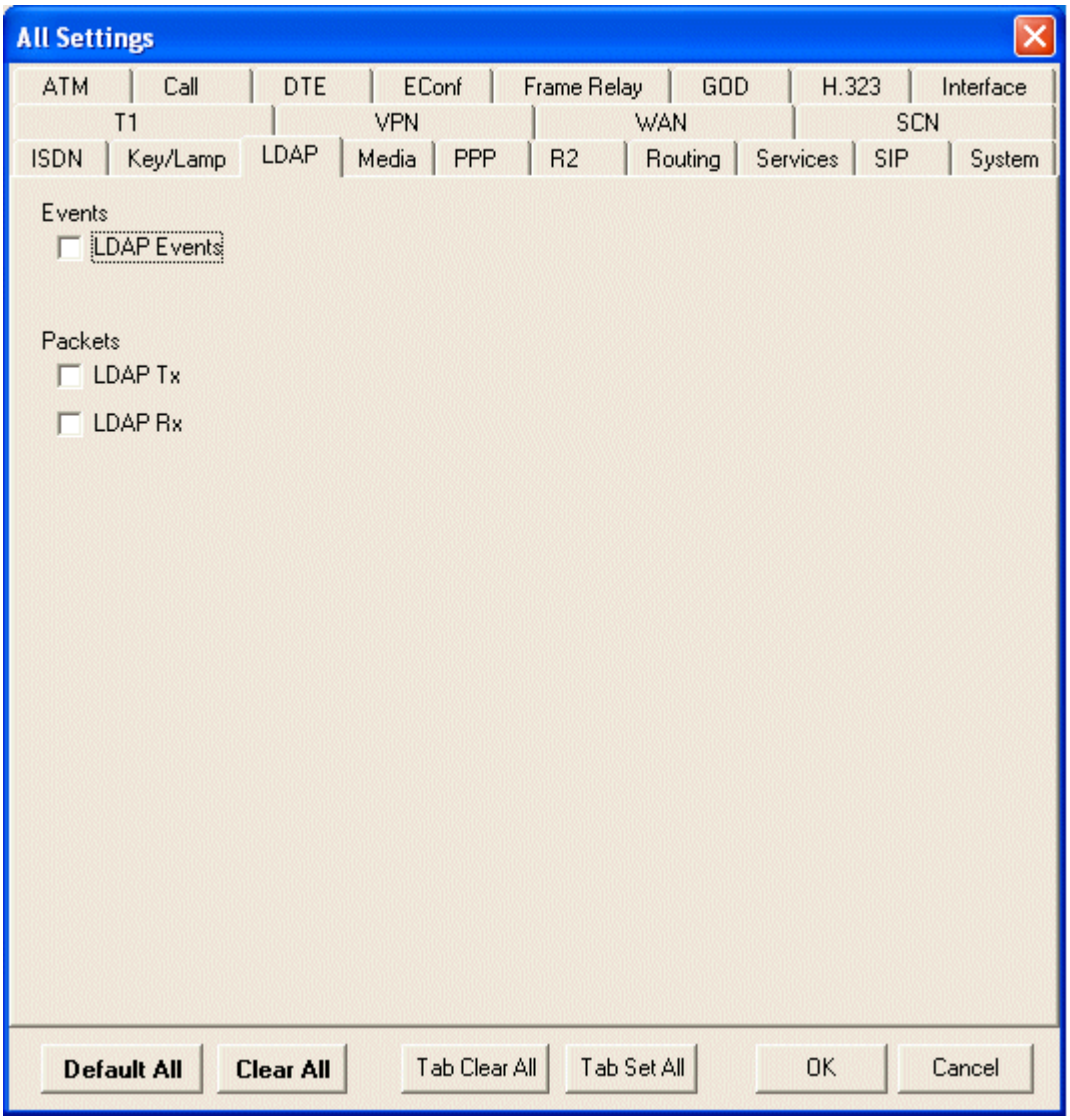
where message value are:

| Value | Definition |
|---|---|
| PHAI | Physical Activate Indication (i.e. Line is UP) |
| PHDI | Physical Deactivate Indication (Line is DOWN) |
| T3TO | T3 timeout has occurred |
| TxErr | 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. |

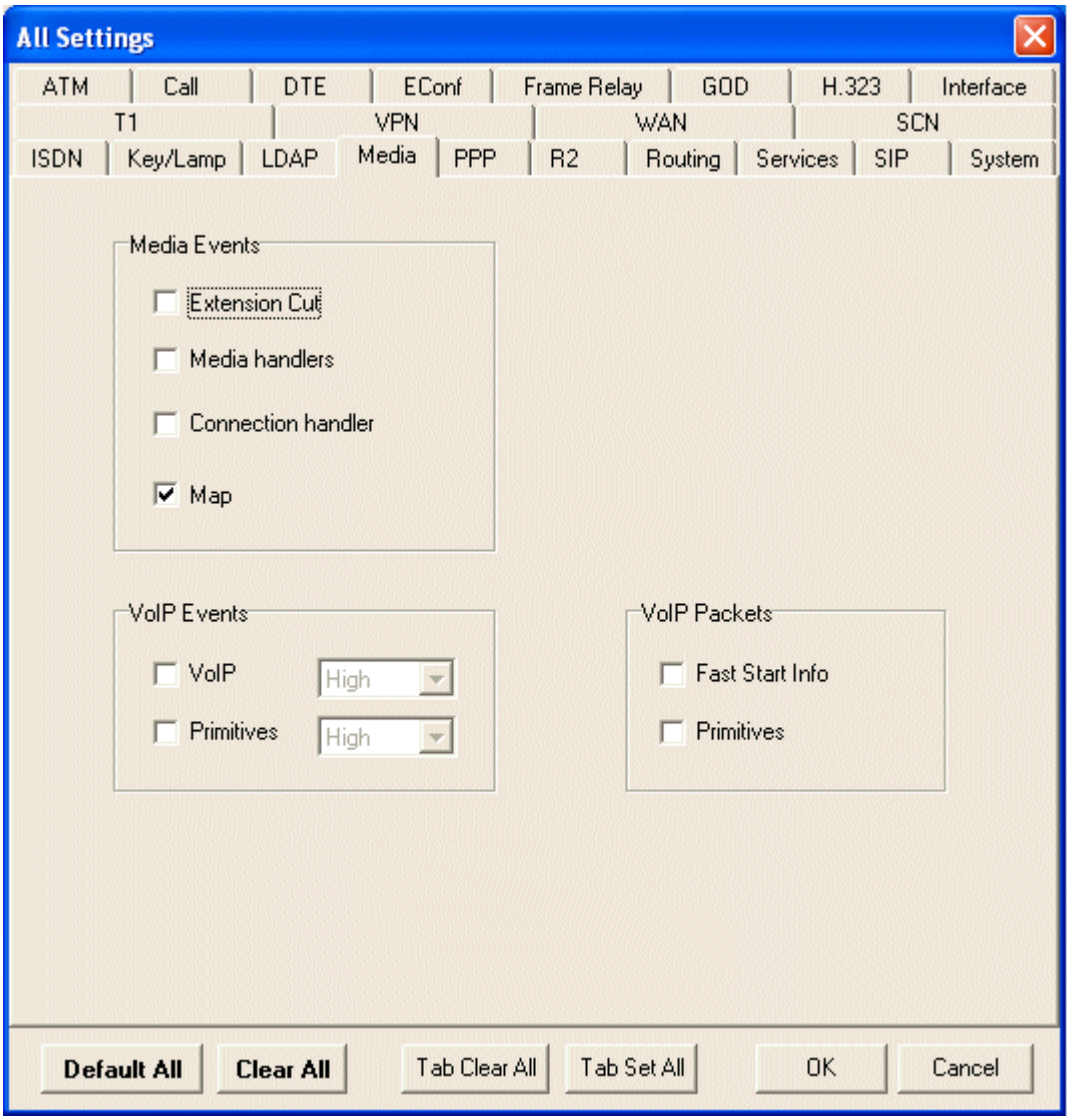
## 2.10 Key/Lamp


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
Events
Appearance
Appearance Group
Call
Facility
Local Appearance
Phone State Change
Switch Hook
User Config
Messages
Call Interface - Level 1
Call Interface - Level 2
Key Resolver Interface - Level 1
Key Resolver Interface - Level 2
Exclude Classes
Adapter
Phone
Appearance
Appearance Group
Appearance Selector
Ringer
Switch Hook
Call
Line
Primary Coverage Facility
T3
API Events
API Messages
Phone Model
Default All
Clear All
Tab Clear All
Tab Set All
OK
Cancel

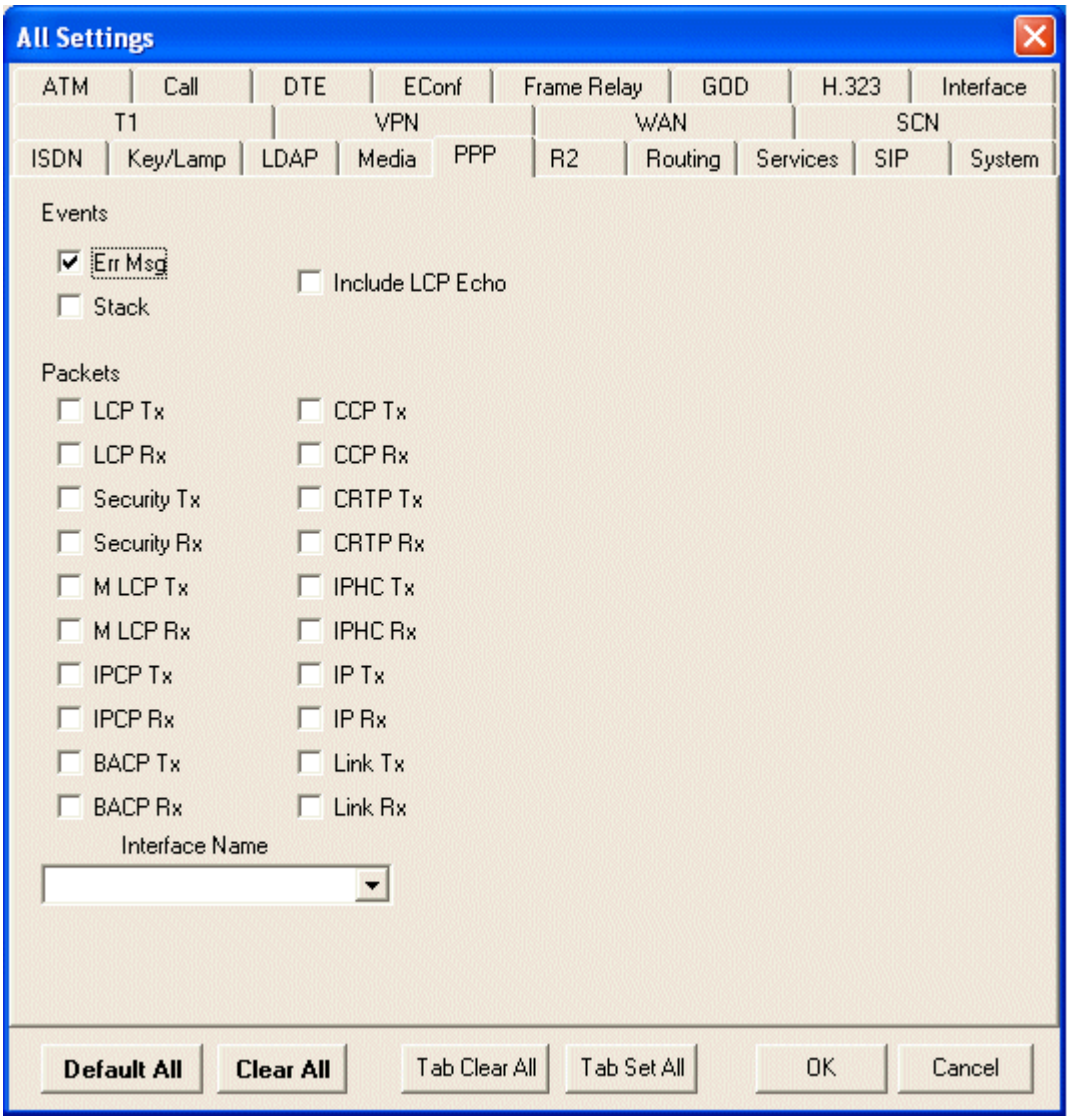
## 2.11 LDAP


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
LDAP Events
Packets
LDAP Tx
LDAP Rx
Default All
Clear All
Tab Clear All
Tab Set All
OK
Cancel

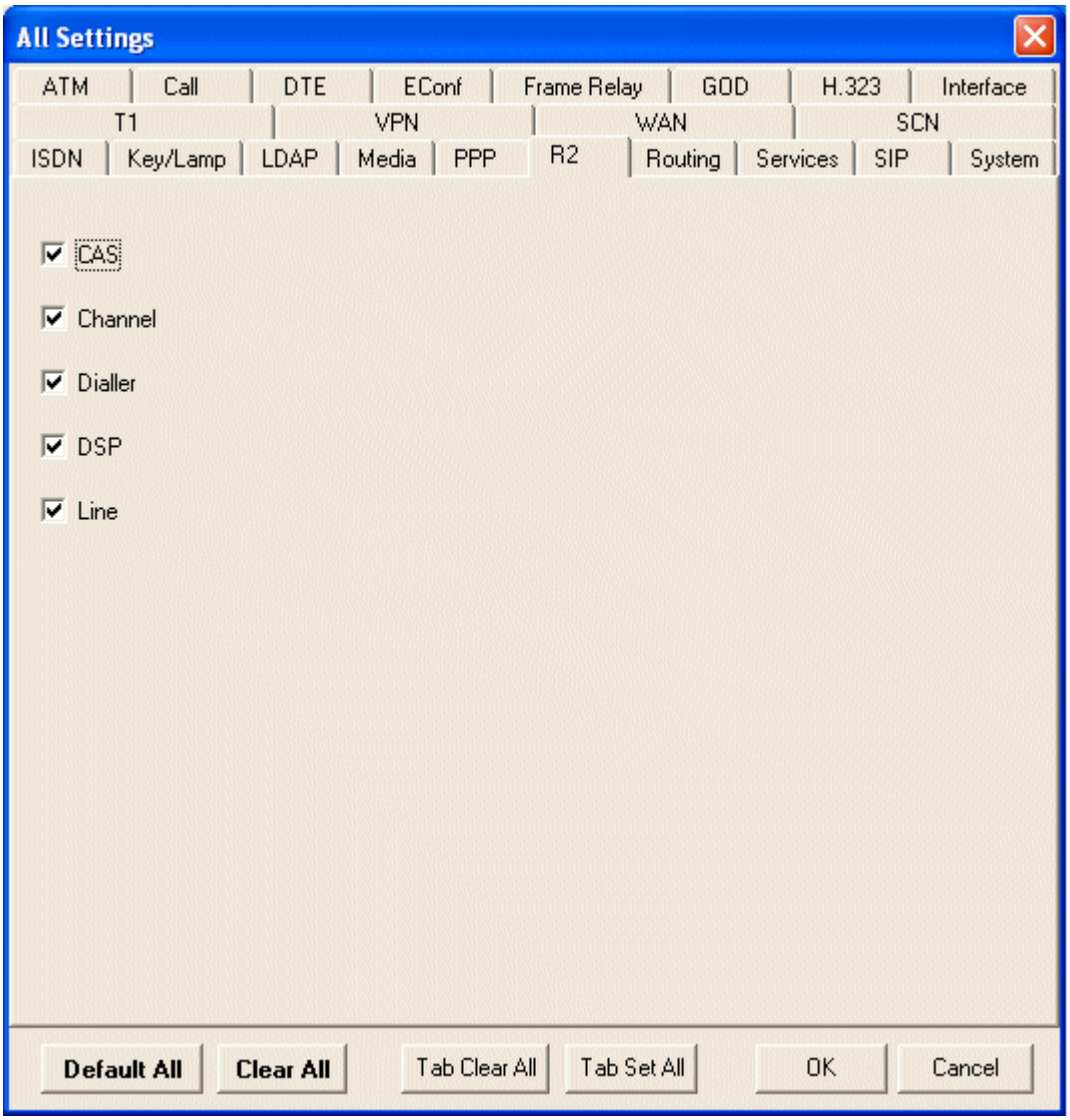
## 2.12 Media


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
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

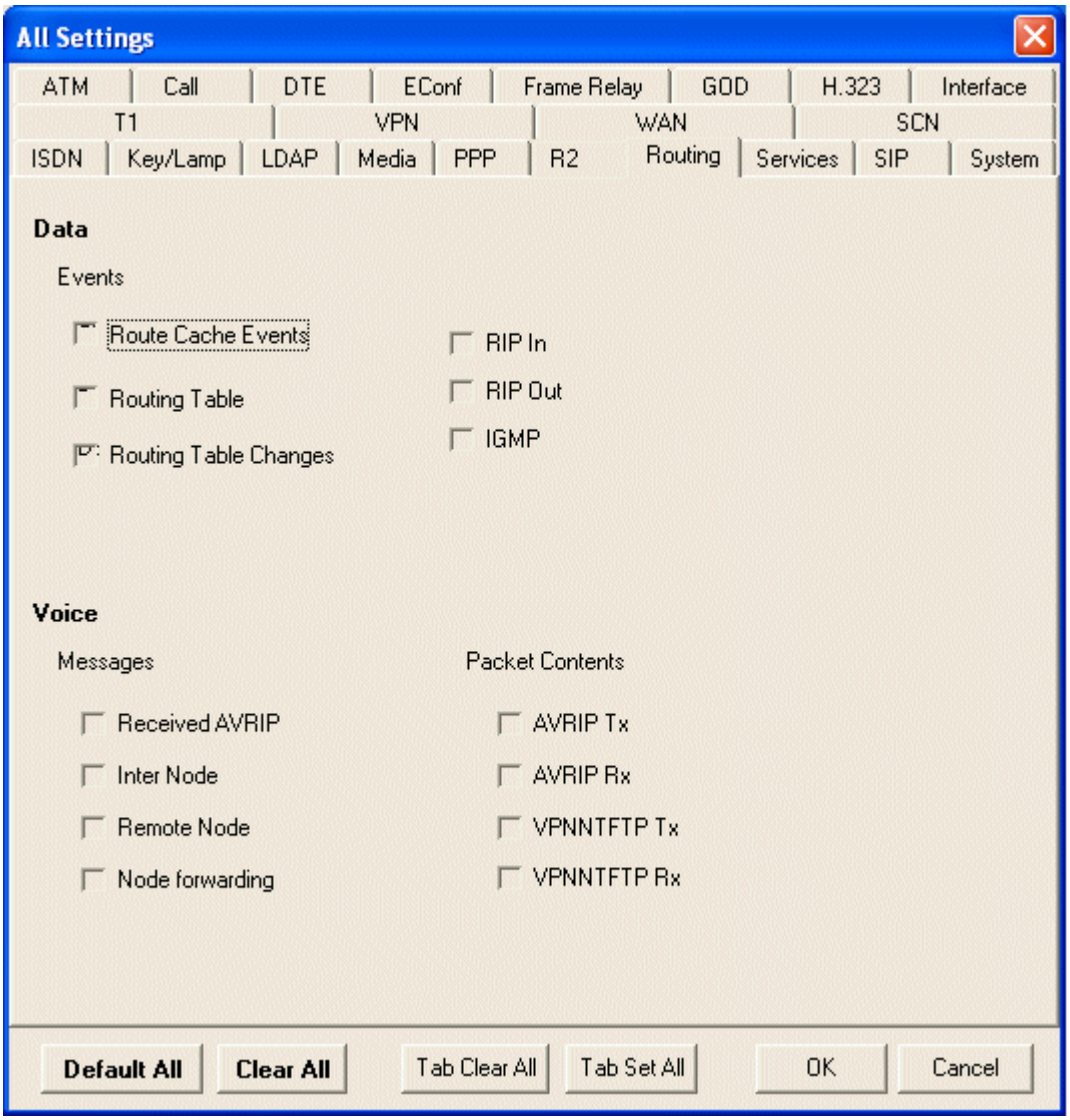
## 2.13 PPP


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
Stack
Include LCP Echo
Packets
LCP Tx
LCP Rx
Security Tx
Security Rx
M LCP Tx
M LCP Rx
IPCP Tx
IPCP Rx
BACP Tx
BACP Rx
CCP Tx
CCP Rx
CRTP Tx
CRTP Rx
IPHC Tx
IPHC Rx
IP Tx
IP Rx
Link Tx
Link Rx
Interface Name
Default All
Clear All
Tab Clear All
Tab Set All
OK
Cancel

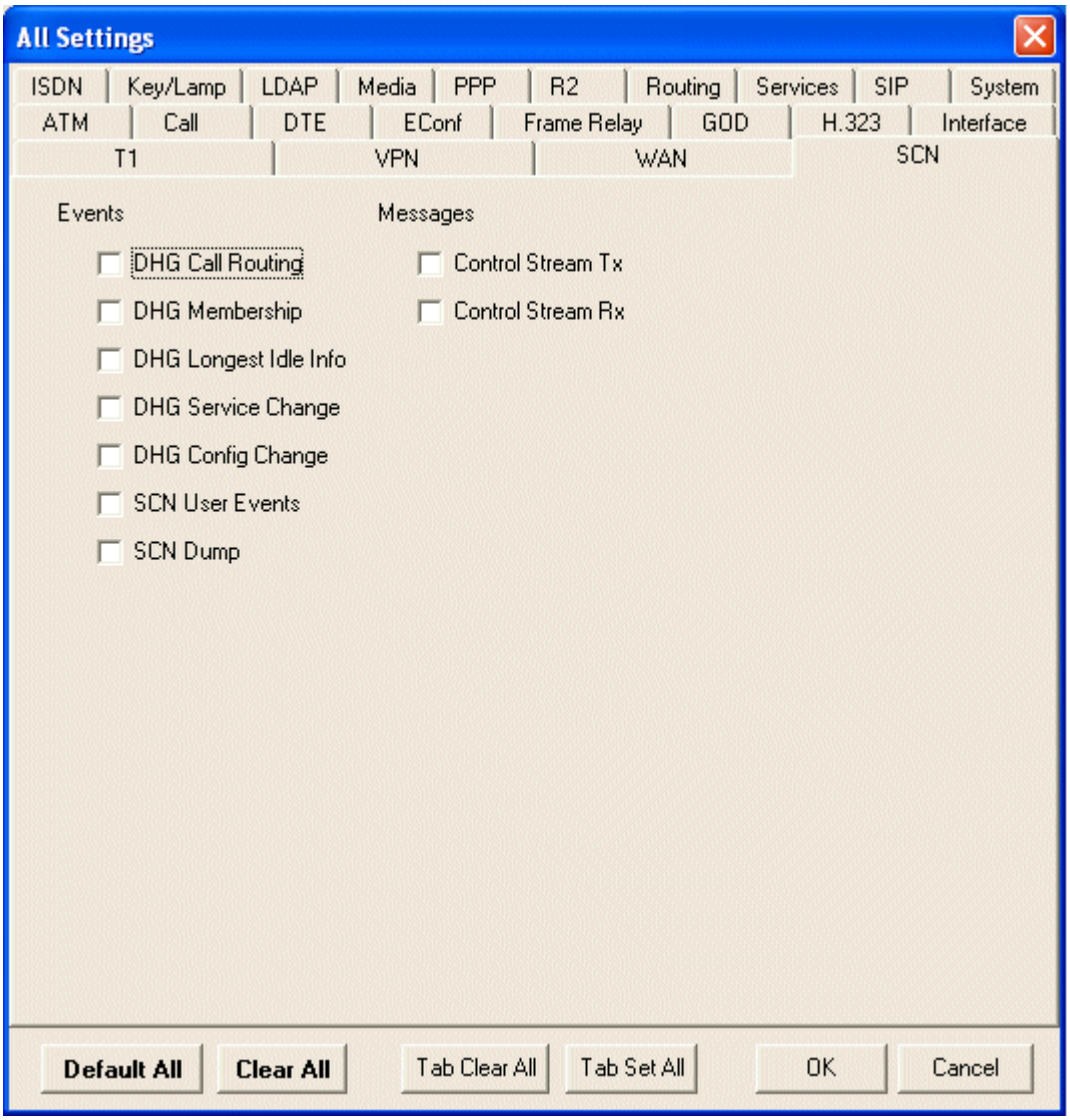
## 2.14 R2


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
CAS
Channel
Dialler
DSP
Line
Default All
Clear All
Tab Clear All
Tab Set All
OK
Cancel

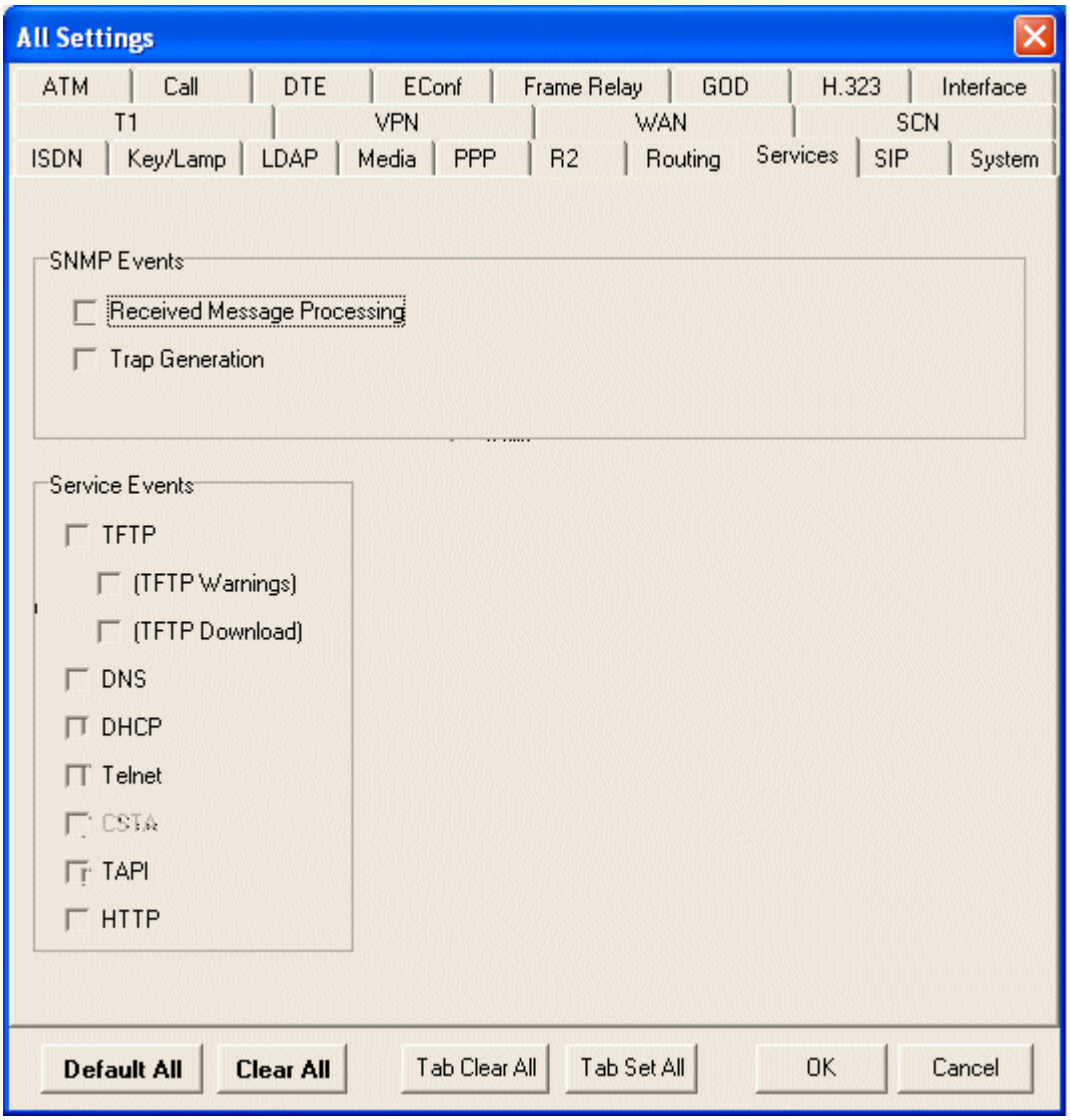
## 2.15 Routing


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
Data
Events
Route Cache Events
Routing Table
Routing Table Changes
RIP In
RIP Out
IGMP
Voice
Messages
Received AVRIP
Inter Node
Remote Node
Node forwarding
Packet Contents
AVRIP Tx
AVRIP Rx
VPNNTFTP Tx
VPNNTFTP Rx
Default All
Clear All
Tab Clear All
Tab Set All
OK
Cancel

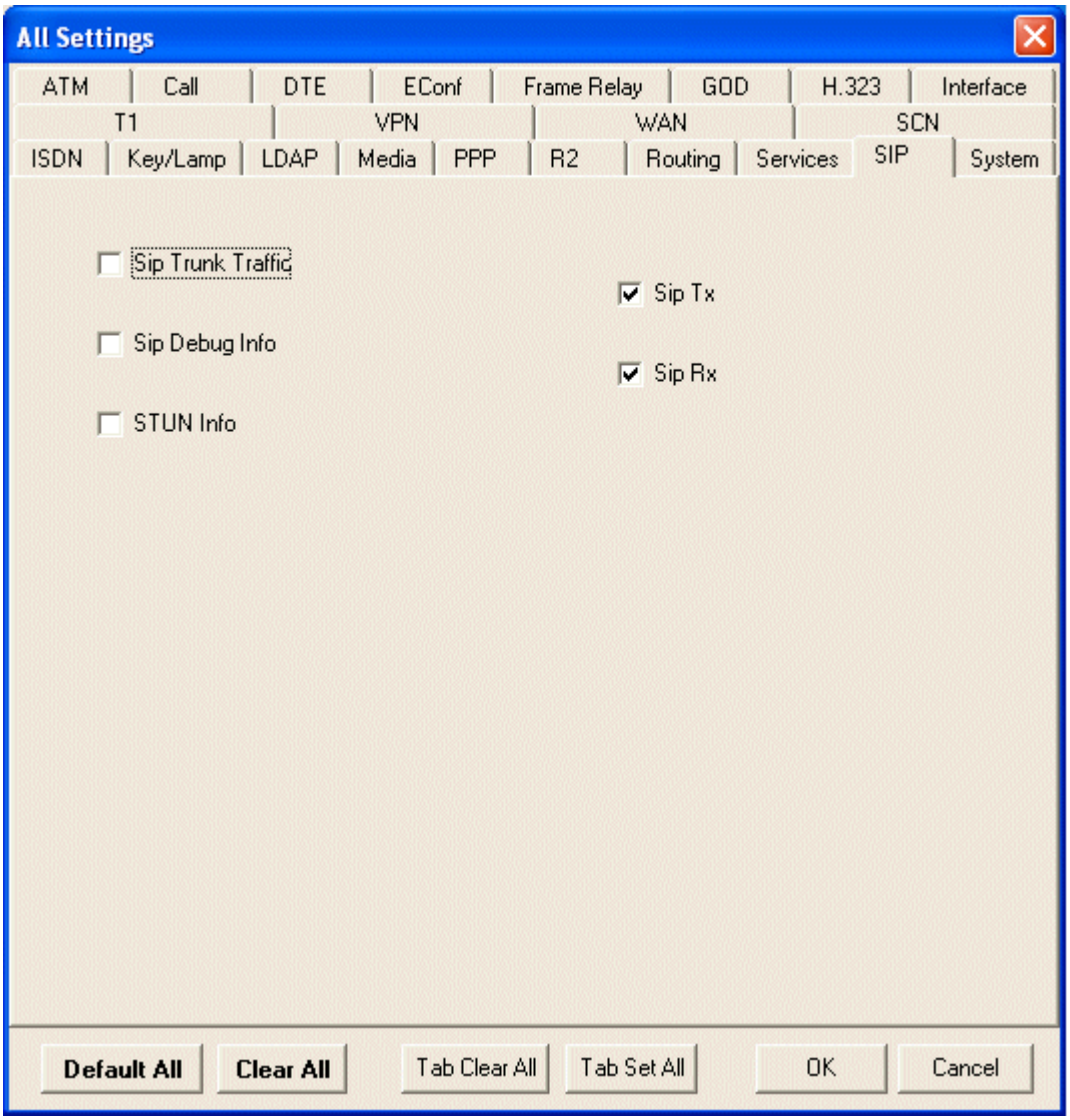
## 2.16 SCN


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

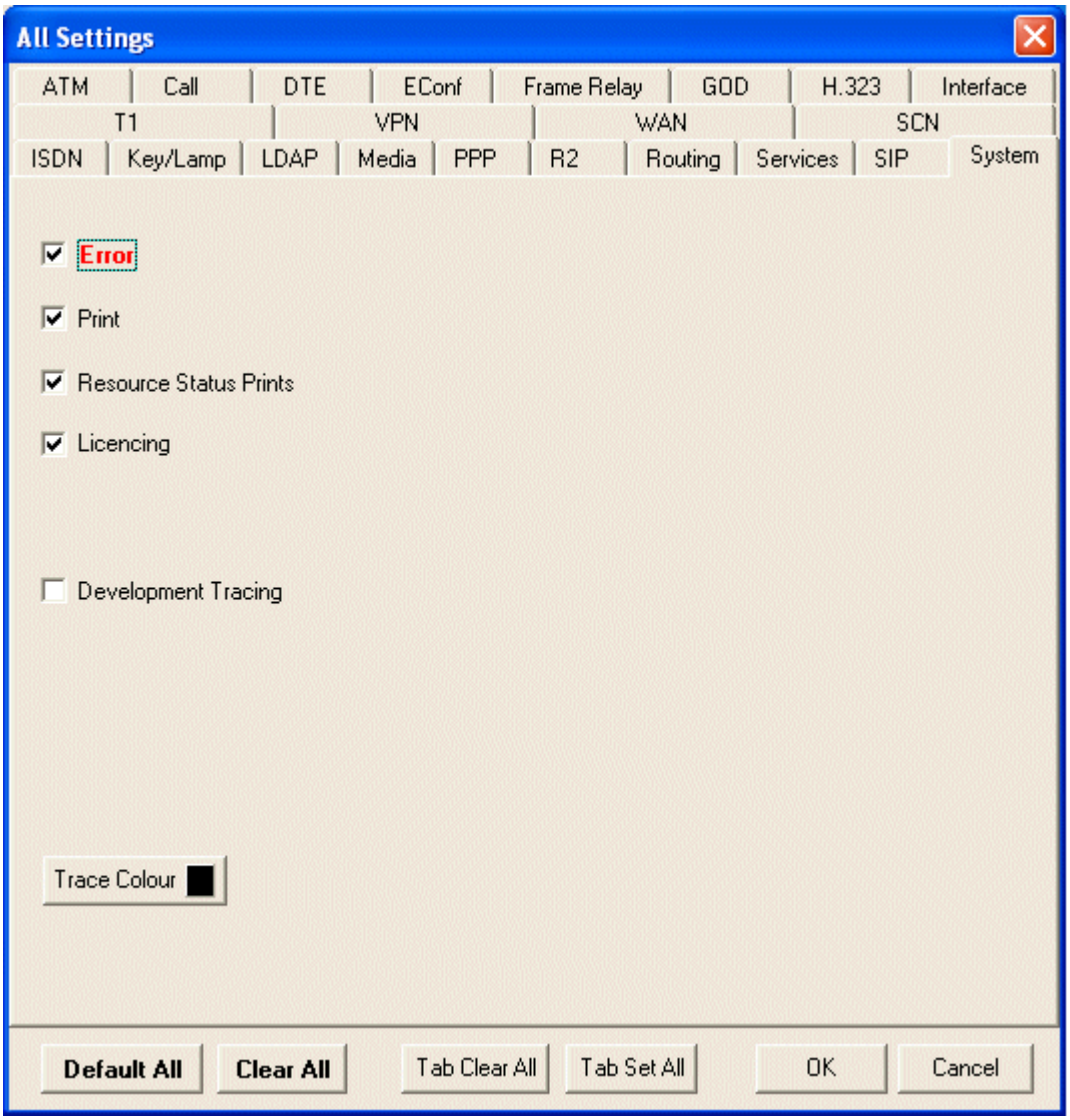
## 2.17 Services



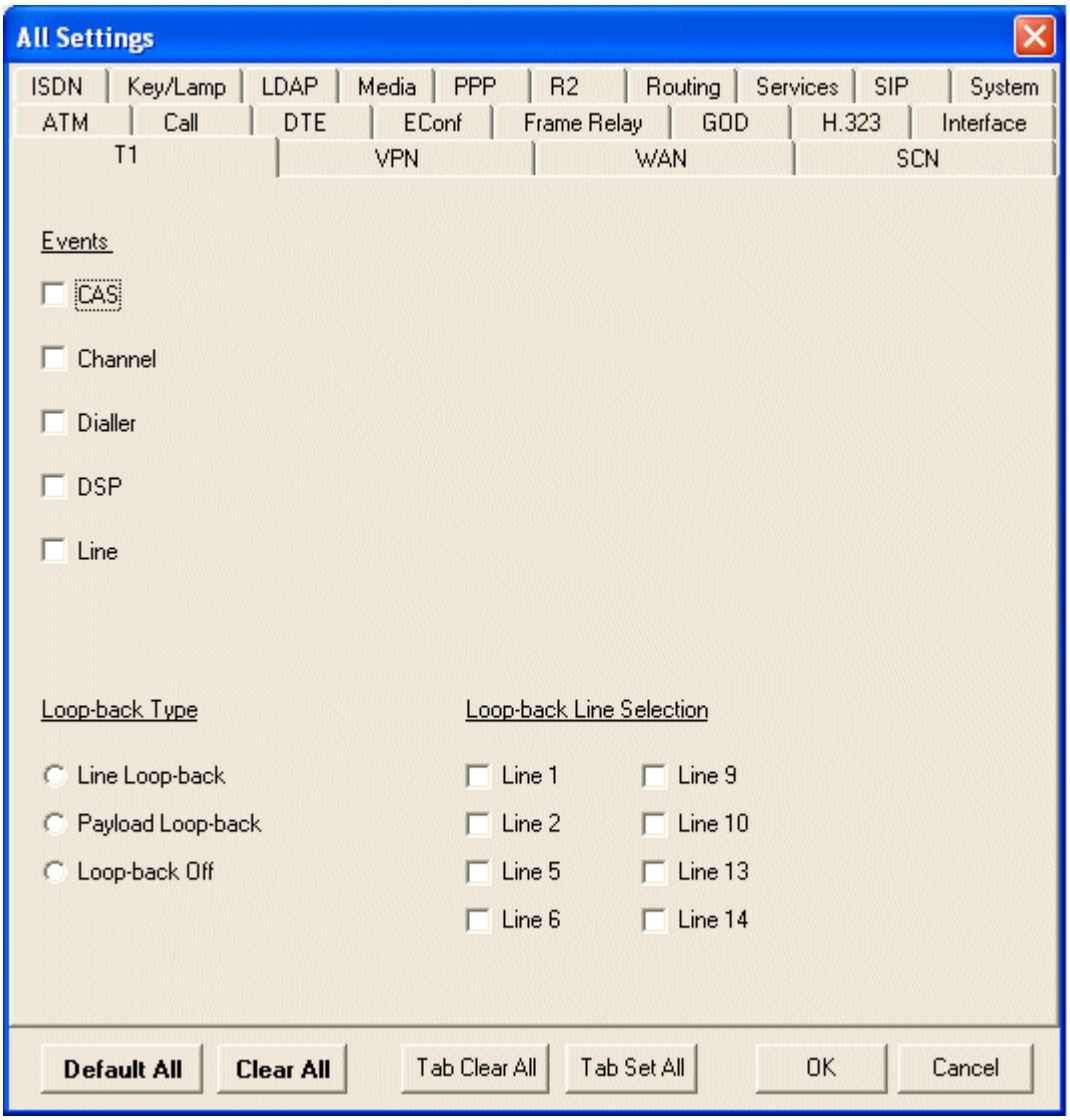
## 2.18 SIP


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
Sip Trunk Traffic
Sip Tx
Sip Debug Info
Sip Rx
STUN Info
Default All
Clear All
Tab Clear All
Tab Set All
OK
Cancel

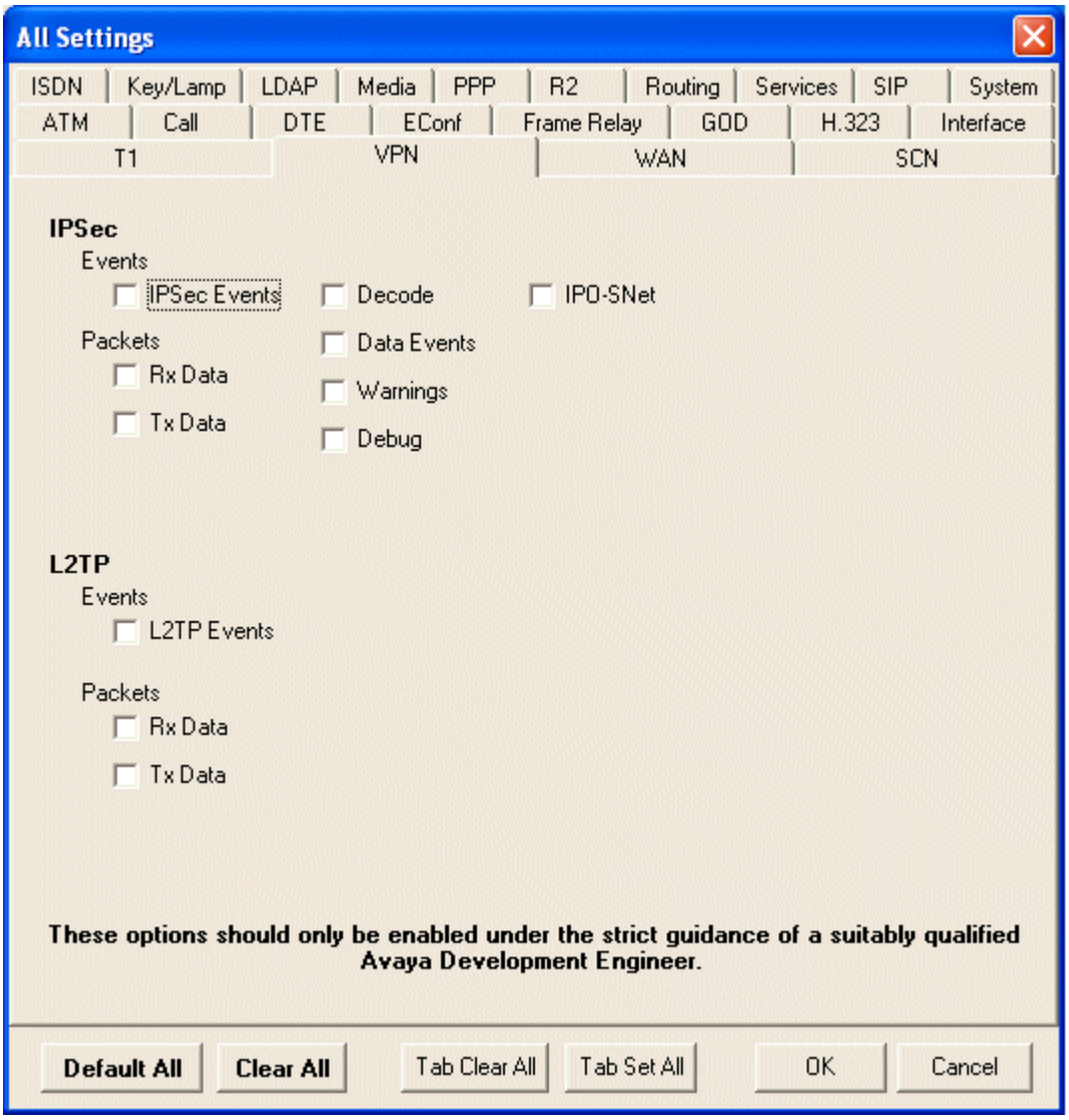
## 2.19 System


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
Error
Print
Resource Status Prints
Licencing
Development Tracing
Trace Colour
Default All
Clear All
Tab Clear All
Tab Set All
OK
Cancel

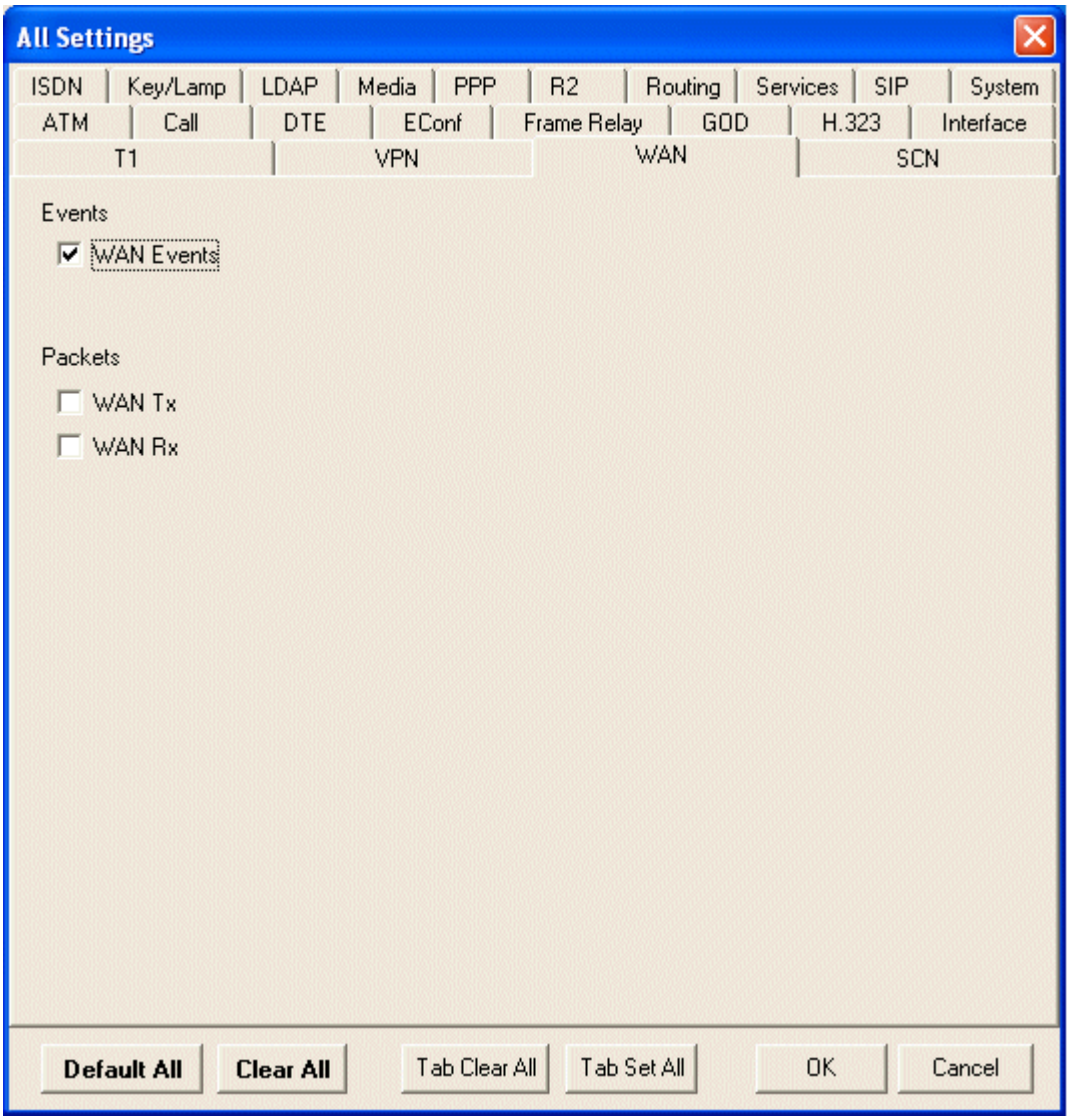
## 2.20 T1


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 2
Line 5
Line 6
Line 9
Line 10
Line 13
Line 14
Default All
Clear All
Tab Clear All
Tab Set All
OK
Cancel

## 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
Data Events
Rx Data
Warnings
Tx Data
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.
Default All
Clear All
Tab Clear All
Tab Set All
OK
Cancel

## 2.22 WAN

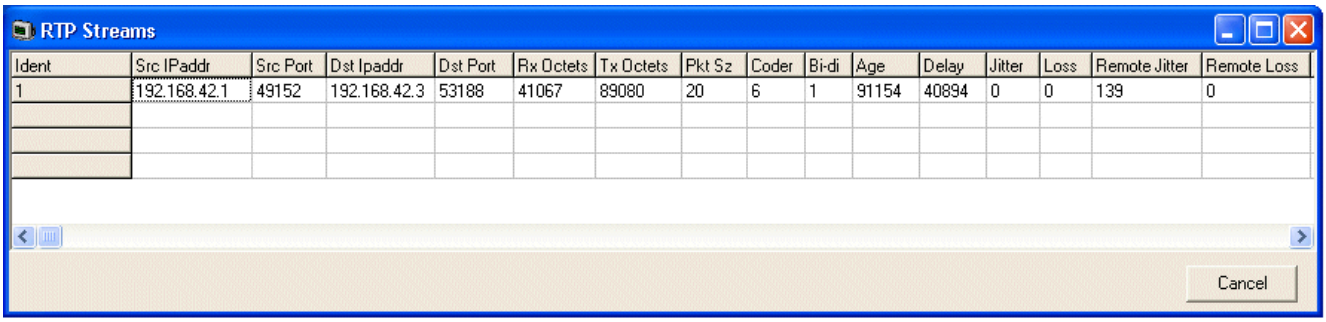

All Settings
ISDN
Key/Lamp
LDAP
Media
PPP
R2
Routing
Services
SIP
System
ATM
Call
DTE
EConf
Frame Relay
GOD
H.323
Interface
T1
VPN
WAN
SCN
Events
WAN Events
Packets
WAN Tx
WAN Rx
Default All
Clear All
Tab Clear All
Tab Set All
OK
Cancel

# Chapter 3.
# Status Screens

# 3. Status Screens

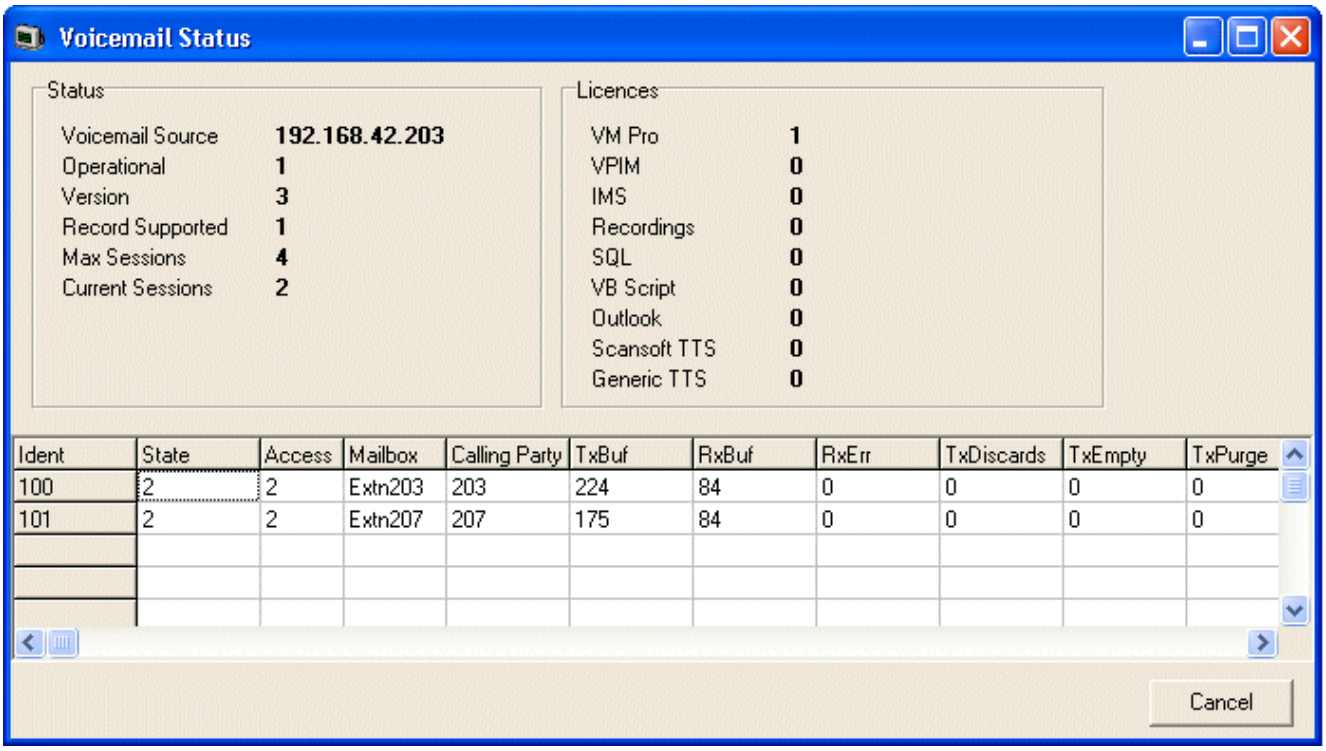
## 3.1 US PRI Trunks

## 3.2 RTP Sessions



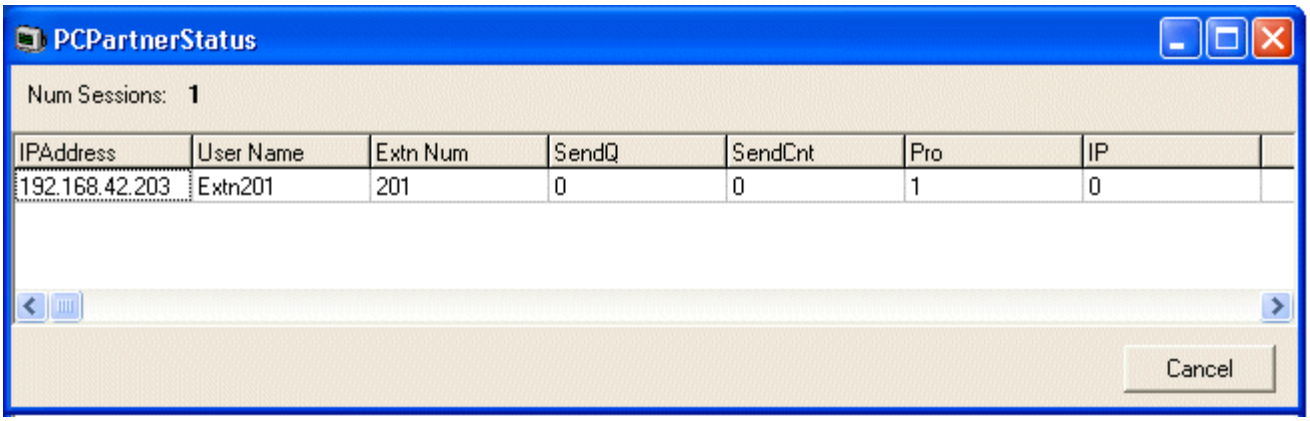

| Ident | Src IPaddr | Src Port | Dst Ipaddr | Dst Port | Rx Octets | Tx Octets | Pkt Sz | Coder | Bi-di | Age | Delay | Jitter | Loss | Remote Jitter | Remote Loss |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 192.168.42.1 | 49152 | 192.168.42.3 | 53188 | 41067 | 89080 |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

## 3.3 Voicemail Sessions



## 3.4 Small Community Networking

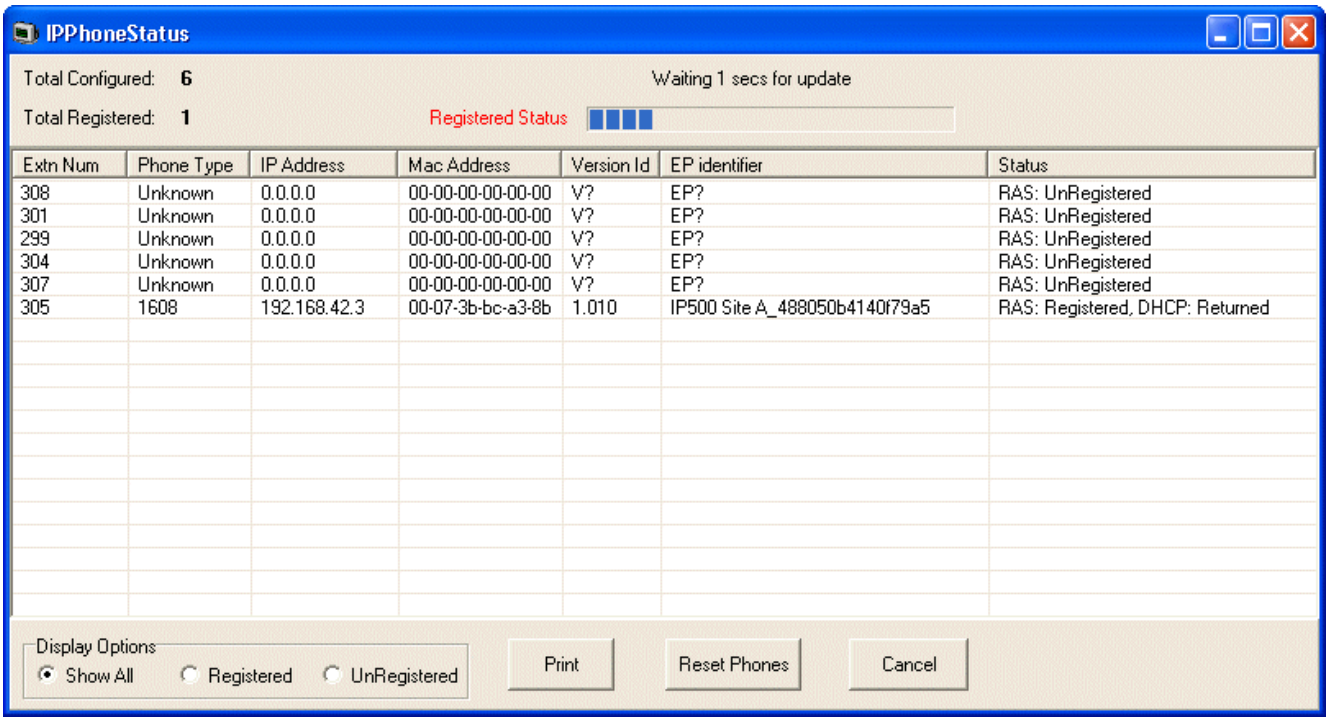
## 3.5 Partner Sessions



## 3.6 Alarms

## 3.7 Map Status

## 3.8 IP Phone Status




| 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 |

# 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:

# 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.<br>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<br>109704mS PRN: 0x3134<br>109704mS PRN: 0x3136<br>109704mS PRN: 0x3035 | • Month: 30 (hex) = 0 (ASCII), 31 (hex) = 1 (ASCII) > 01 (January)<br>• Day: 31 (hex) = 1 (ASCII), 34 (hex) = 4 (ASCII) > 14th.<br>• Hours: 31 (hex) = 1 (ASCII), 36 (hex) = 6 (ASCII) > 16:00.<br>• Minutes: 30 (hex) = 0 (ASCII), 35 (hex) = 5 (ASCII) > 00:05.<br>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<br>109706mS PRN: 0x3730<br>109706mS PRN: 0x372d<br>109706mS PRN: 0x3339<br>109706mS PRN: 0x3033<br>109707mS PRN: 0x3931 | • 30 (hex) = 0 (ASCII), 31 (hex) = 1 (ASCII) > 01<br>• 37 (hex) = 7 (ASCII), 30 (hex) = 0 (ASCII) > 70<br>• 37 (hex) = 7 (ASCII), 2d (hex) = - (ASCII) > 7-<br>• 33 (hex) = 3 (ASCII), 39 (hex) = 9 (ASCII) > 39<br>• 30 (hex) = 0 (ASCII), 33 (hex) = 3 (ASCII) > 03<br>• 39 (hex) = 9 (ASCII), 31 (hex) = 1 (ASCII) > 91<br>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 dectection has been disabled. |
| 109708mS PRN: AtmTrunk1: StateChange CLIAwaitData->CLIDataSettle<br>109911mS PRN: AtmTrunk1: StateChange CLIDataSettle->CLIAwaitSecondRing<br>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       l.!.6187093991
                InformationElement = CalledPartyNumber
             0000 70 08 c1 36 34 36 37 31 33 31                   p..6467131
                InformationElement = HigherLayerCompat
             0000 7d 02 91 81                                     }...
```

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

# 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 |
|---|---|
| `1072151mS ISDNL1Evt: v=0 peb=5,F2 F1` | PRI Line 5 (peb=5) has gone from the F1 state (normal Operational state) to the F2 state (Fault condition 1 state - receiving RAI or receiving CRC errors). |
| `1072651mS ISDNL1Evt: v=0 peb=5,PHDI ?` | Line 5 (peb=5) is now in the Disconnected state (PHDI – Physical Deactivate Indication). |
| `1072651mS ISDNL3Evt: v=0 p1=0,p2=1001,p3=5,p4=127,s1=` | ISDN Layer 3 event which gives current status of line 5 (p3=5)<br>• P1=0 -> ISDN Stacknum = 0.<br>• P2=1001 ->Line Disconnecting<br>• P3=5 -> Internal reference number<br>• P4=127 ->TEI = 127<br>• S1= ->not used |
| `1072651mS ISDNL3Evt: v=0 stacknum=0  State, new=NullState, old=Active id=4` | ISDN Layer 3 event which indicates that call with id 4 (id=4) on the first ISDN stack (stacknum=0) has changed from being Active (old=Active) to No Call exists (new=NullState). |
| `1072652mS ISDNL3Evt: v=0 stacknum=0  State, new=NullState, old=Active id=24` | ISDN Layer 3 event which indicates that call with id 24 (id=24) on the first ISDN stack (stacknum=0) has changed from being Active (old=Active) to No Call exists (new=NullState). |
| `1072653mS ISDNL3Evt: v=0 p1=0,p2=1001,p3=5,p4=0,s1=` | ISDN Layer 3 event which gives current status of line 5 (p3=5)<br>• P1=0 -> ISDN Stack number = 0.<br>• P2=1001 ->Line Disconnecting<br>• P3=5 ->Internal reference number<br>• P4=0 ->TEI = 0<br>• S1= ->not used |
| `1072656mS CMLineRx: v=5`<br>`CMReleaseComp`<br>`Line: type=Q931Line 5 Call: lid=5 id=4 in=1`<br>`Cause=38, NetworkOOO` | 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).<br>There is no ISDNL3RX trace information as the call is dropped by the PBX NOT by the local exchange (due to the fact that we are no longer in communication with the Local Exchange!). |
| `1072658mS CALL:2000/11/2408:40,00:00:17,033,01732464420,I,300,027624,,,,0` | The Incoming call from 01732464420 to [02083]027624 (Extn300) has been disconnected. |

| System Monitor Trace | Explanation |
|---|---|
| 1072682mS CMLineRx: v=5<br>CMReleaseComp<br>Line: type=Q931Line 5 Call: lid=5 id=24 in=1<br>Cause=38, NetworkOOO | 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).<br>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/Later3 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” fieldin 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[1]
- ISDN/Packets/Layer 3 Receive[1]
- ATM/Channel[2]
- ATM/I-O2
- ATM/CM Line[2]
- T1/Line[3]
- T1/Channel[3]
- T1/Dialler[3]
- T1/DSP[3]
- T1/CAS[3]
- 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 - ie. free to be used by any program), the packet is a TCP SYN. All you need to do is locate the PC with address 212.46.130.32. To find out where on the web it was accessing type the IP Dst in the address bar of your browser and it 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 filed. 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
```

```
            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 | *BT Fusion variant. No longer used.* |
| 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 are part of *CMExtnTx:* events within the monitor trace. For example:

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

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

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

| 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. |
| IP Office Specific Cause Codes | |
| 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 (RxBD)”. The table below shows the bits within the RxBD that are used to generate the error codes. Those labeled as “N/U” are NOT used in the FEC Error Decoding mechanism although they may be non zero.

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

Example

Decode of typical message produced 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 RxBD is set) – note that the first byte (A) is missing so it is equal to 0, resulting in a 3 byte error code.

# Index

## K



## L

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



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