IP Office

Monitor (SysMon)

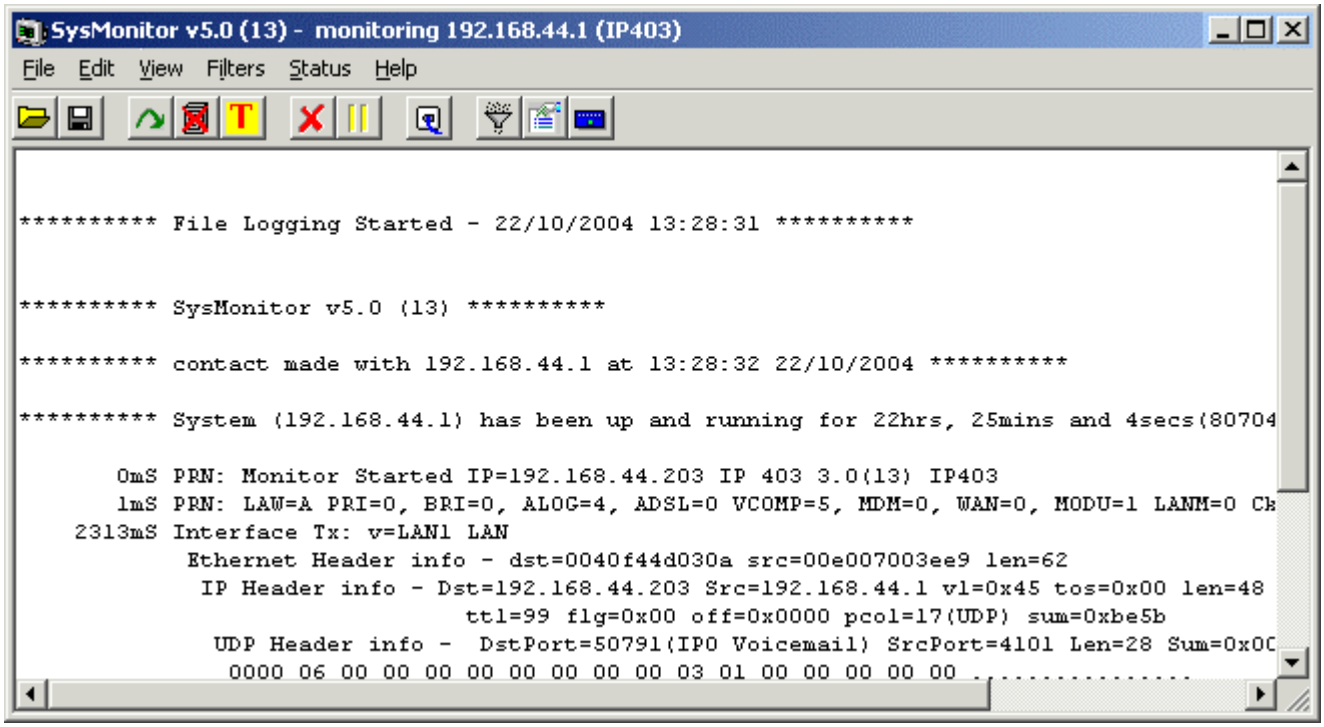
Issue 1e (13th October 2005)

Table of Contents

Monitor

The Monitor Application

The IP Office 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, eg. calls, ISDN, PPP, etc.



- Monitor is intended primarily for use and interpretation by Avaya support staff. The settings within 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 data and telecommunications experience and is not intended for the general user.
- **IMPORTANT**
  Running Monitor can place a high traffic load on the network and so should only be done when specifically necessary to diagnose a fault.

Installing Monitor

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

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.
5. Click **Next**.

Starting Monitor

To start Monitor:

1. Select **Start | Programs | IP Office | Monitor**.
2. If Monitor has been run before it will attempt to connect will the system which is monitored previously. If 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.
    - Within the System form of Manager it is possible to set a specific **Monitor Password** for Monitor access to an IP Office system.
    - If the IP Office doesn't have a **Monitor Password** set, Monitor uses the IP Office's **System Password**.
5. For an IP Office system, ensure that IP400 is selected.
6. Click **OK**.

The Monitor application 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 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 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.

Please note that increased output is produced when you configure Monitor to trace events/packets on the interface that is used to connect the PC running the Monitor to the IP Office, e.g. Interface packets on LAN1 if tracing locally, IP Tx & IP Rx on the Service/RAS connecting the IP Office to the remote subnet, etc.

Monitor Icons

The 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 button has no action but indicates that the current selected log file format is a text file.
- **Binary Log File**
  This button has no action but indicates that the current selected log file format is a binary 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.

System Information

When first connected to an IP Office, the monitor trace displays some basic information about the IP Office system to which it has connected.

```
********** SysMonitor 4.1 (11) **********
********** contact made with 192.168.42.1 at 14:23 23/4/2004 **********
********** System (192.168.42.1) has been up and running for 22secs(22649mS)
**********
1mS PRN: Monitor Started IP=192.168.42.1 IP 412 2.1(11)
1mS PRN: LAW=A PRI=3, BRI=0, ALOG=0, ADSL=0 VCOMP=30, MDM=0, WAN=1, MODU=6 LANM=1
CkSRC=5 VMAIL=1(VER=2 TYP=1) CALLS=16(TOT=1328)
46mS RES: Fri 23/4/2004 15:08:12 FreeMem=18743616(25) CMMsg=9 (9) Buff=200 835 999
1658 Links=6158
```

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

```
********** SysMonitor 4.1 (11) **********
********** contact made with 192.168.42.1 at 14:23 23/4/2004 **********
********** System (192.168.42.1) has been up and running for 22secs(22649mS)
**********
1mS PRN: Monitor Started IP=192.168.42.1 IP 412 2.1(11)
```

The following lines begin with a time stamp showing the number of milliseconds since the monitor connection was started. The first of these lines gives the IP address of the PC running Monitor, the type of IP Office Control Unit and the software level (.bin file) installed on the Control Unit. For example:

```
1mS PRN: Monitor Started IP=192.168.42.1 IP 412 2.1(11)
```

The next line gives information about various aspects of the IP Office system. For example:

```
1ms PRN: LAW=A, PRI=0, BRI=4, ALOG=4, ADSL=0 VCOMP=5, MDM=2, WAN=1, MODU=0 LANM=1
CkSRC=8 VMAIL=1(VER=2) CALLS=0(TOT=8)
```

- **LAW = A or U law system.**
-
-
- **PRI = Number of PRI channels**
-
-
- **BRI = Number of BRI channels (4=1 card, 8=2 cards).**
-
-
- **ALOG = Number of Analog Trunk Channels**
-
-
- **VCOMP = Number of VCM channels installed.**
-
-
- **MDM = Size of Modem Card Fitted**
-
-

- **WAN = Number of WAN Ports configured.**
- **MODU = Number of TDM modules attached (i.e. POT Phone, DS modules etc.)**
- **LANM = Number of LAN Modules attached (i.e. WAN3s)**
- **CkSRC = Current Clock Source (ISDN port number - 0 = Internal Clock Source)**
- **VMAIL = 1 if connected, 0 if not connected.**
- **VER = the s/w version of the voicemail server if obtainable.**
- **TYP = Type of Voicemail Server (0, 1, 2, … corresponding to the radio button options**
- **on the System Voicemail tab.).**
- **CALLS = Number of current calls**
- **TOT = total number of calls made to date since last IP Office reboot.**

The Alarm Log

When started, the 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 00a13250 00a13638 00a0cb3c
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 0095e278 008b0570 008b0734 008b07b8
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 0095e278 00000001 01e757f8
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 20 alarms received since the alarm log was last cleared. 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 Monitor and selecting **Status** and then **Alarms**. 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.

Monitor 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. Doing this freezes the current monitor display.
- **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 Monitor program.

Edit Menu

- **Clear Display**
  Clear the monitor display.
- **Copy**
  Copies any currently selected content in the Monitor display to the Windows clipboard.
- **Select All**
  Selects all the content in the Monitor display.
- **Find**
  Display a search menu for use with the contents of the Monitor display.
- **Filter**
  Switches filter usage on/off. See Settings Menu.
- **IP Calculate (Selected Hex)**
  Converts hexadecimal strings into decimal. Highlight the number to convert in the Monitor display and then select **Edit | IP Calculate**.

View Menu

- **Freeze Screen Logging**
  Freeze/unfreeze the monitor 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 Monitor display.
- **Background Color**
  Allows selection of the background color used in the Monitor display.

Filters Menu

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

- **Trace Options:**
  Allows you to select and filter trace captured by Monitor based on a range of categories:
  - **ATM:** Monitor analog trunk traffic and events.
  - **Call:** Monitoring of extensions and calls.
  - **DTE:** Monitoring of the Control Unit's DTE port.
  - **EConf:** Monitor conference and conferencing server events.
  - **Frame Relay:** Monitoring of Frame Relay traffic and events.
  - **GOD:** For use by Avaya development engineers only.
  - **H.323:** Monitoring of H.323 traffic and events.
  - **Interface:** Monitoring IP interfaces such as NAT and the Firewall.
  - **ISDN:** Monitor ISDN traffic and events.
  - **Key/Lamp:** Monitor appearance functions
  - **LDAP:** Monitor LDAP traffic and events.
  - **PPP:** Monitor PPP traffic and events.
  - **R2:** Monitor R2 trunk traffic and events.
  - **Routing:** Monitor IP traffic and events.
  - **SNMP:** Monitor SNMP events.
  - **System:** Monitor internal events.
  - **T1:** Monitor T1 traffic and events.
  - **VPN:** Monitor VPN events.
  - **WAN:** Monitor WAN traffic and events.

Status Menu

- **US PRI Trunks…**
  Displays a menu showing the B channel status of US PRI lines installed in the IP Office.
- **Alarms**
  Display and clear the IP Office alarm log. See The Alarm Log.

Help Menu

- **About**
  Shows information about the version of the Monitor program. This document is based around **SysMonitor 5.0(13)**.

File Logging

As well as displaying the Monitor trace, 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).

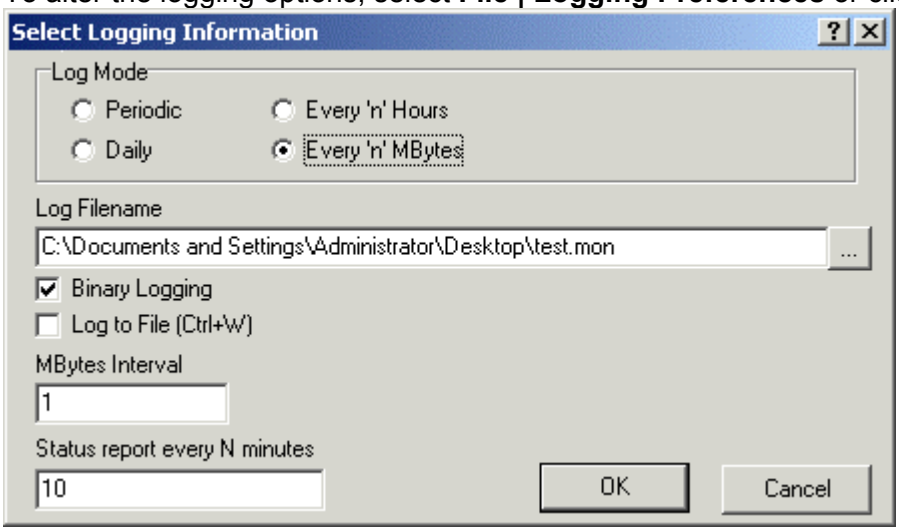
A logged trace can be examined later and, if requested, be sent to Avaya for analysis.

Several of the buttons on the 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.
  - Logging currently set to binary mode.
- **Stop logging**
- **Log Preferences**
  Setup the type, location and rollover frequency for log files.
- **Open File**
  Loads a previously captured log file in the 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 Monitor application program folder (*C:\Program Files\Avaya\IP Office\Monitor*).
- **Binary Logging**
  The log file trace displayed by Monitor and logged in a text log file has been 'interpreted'. That is read by the Monitor application and had additional information added. A binary log file is the raw output from the IP Office.
  - When running 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 Monitor display reduces the chance of such lost packets.
- **Log to File**
  If checked, this box starts file logging once **OK** is clicked.

Miscellaneous

Why Does Monitor Give Information for Options Not Selected?

This probably means another PC is also running Monitor and monitoring the same IP Office. When two Monitors are running simultaneously monitoring the same IP Office, the options selected in one Monitor will also affect the trace seen by the other Monitor.

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.

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 Monitor Trace

Being able to place a marker line in the 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 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,,""
```

Examples

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:

- System Rebooting
- ISDN Problems (T1 or E1 PRI connections)
- ISP & Dial-Up Data Connection Problems
- Remote Site Data Connection Problems over Leased (WAN) Lines
- Frame Relay Links
- Speech Calls Dropping
- Problems Involving Non-IP Phones
- Problems Involving IP Phones
- Locating a Specific PC Making Calls to the Internet
- Problem with Calls Answered/Generated by IP Office Applications
- Firewall Not Working Correctly

System Rebooting

Enable the following 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 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 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].

ISDN Problems (T1 or E1 PRI Connections)

Enable the following 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 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.

ISP & Dial-Up Data Connection Problems

Enable the following 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 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.

Remote Site Data Connection Problems over Leased (WAN) Lines

Enable the following 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, 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, Monitor should be configured to monitor the IP address of the WAN3 unit.

If the Leased Line problem is to a specific destination then 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 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 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.

Frame Relay Links

Enable the following 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**

Speech Calls Dropping

ISDN or QSIG Line

Enable the following 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 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 Monitor settings:

- **ISDN/Packets/Layer 3 Send**[1]
- **ISDN/Packets/Layer 3 Receive**[1]
- **ATM/Channel**[2]
- **ATM/I-O**[2]
- **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 Start**[4]
- **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 Channelised 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 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**

Problems Involving Non-IP Phones

Enable the following 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.

Problems Involving IP Phones

Enable the following 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.

Locating a Specific PC Making Calls to the Internet

Enable the following 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 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 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.

Problem with Calls Answered/Generated by IP Office Applications

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

Firewall Not Working Correctly

Enable the following 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 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.

Remote Site Data Connection Problems over Leased (WAN) Lines

Enable the following 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, 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, Monitor should be configured to monitor the IP address of the WAN3 unit.

If the Leased Line problem is to a specific destination then 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 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 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.

Problem with Calls Answered/Generated by IP Office Applications

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

Message Waiting Indication

To determine if Voicemail Pro is transmitting message waiting indication (MWI) information, the following trace options should be used in 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 MWL, otherwise the MWL 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
```

Addendum

IP Office Ports

The list below details many of the IP ports used by IP Office control units and IP Office applications. Many of these are standard ports for different IP traffic protocols.

- ⬅ Indicates a port on the IP Office.
- ➡ indicates a port on a PC running an IP Office service or application.
- The names in brackets are those shown in the IP Office Monitor application after the port number.

- ⬅ **Port 69 (Trivial File Transfer):** File requests to the IP Office.
- ➡ **Port 69 (Trivial File Transfer):** File requests by the IP Office.
- ⬅ **Port 161 (SNMP):** From SNMP applications.
- ➡ **Port 162 (SNMP Trap):**
  To addresses set in the IP Office configuration. Both SNMP Port numbers can be changed through the IP Office configuration.
- ➡ **Port 520 RIP:**
  From 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.
- ⬅ **Port 520 RIP:** To the IP Office from RIP devices.
- ➡ **Port 1719 (H.323 RAS):** Response to a VoIP device registering with IP Office.
- ➡ **Port 1720 (H.323/H.245):** Data to a registered VoIP device.
- ➡ **Port 2127:** PC Wallboard to CCC Wallboard Server.
- ➡ **Port 8080:** Browser access to the Delta Server application.
- ➡ **Port 8089:** Conferencing Center Server Service.
- ➡ **Port 8888:** Browser access to the IP Office ContactStore (VRL) application.
- ➡ **Ports 49152 to 53247:** Dynamically allocated ports used during VoIP calls for RTP and RTCP traffic. The port range can be adjusted through the System | Gatekeeper tab.
- ➡ **Port 50791 (IPO Voicemail):** To voicemail server address.
- ⬅ **Port 50793 (IPO Solo Voicemail):** From IP Office TAPI PC with Wave drive user support.
- ⬅ **Port 50794 (IPO Monitor):** From the IP Office Monitor application.
- ⬅ **Port 50795 (IPO Voice Networking):** Small Community Network signalling (AVRIP) and BLF updates.
- ⬅ **Port 50796 (IPO PCPartner):**
  From an IP Office application (for example Phone Manager or SoftConsole). Used to initiate a session between the IP Office and the application.
- ⬅ **Port 50797 (IPO TAPI):** From an IP Office TAPI user PC.
- ➡ **Port 50799 (IPO BLF):** Broadcast to the IP Office LAN, eg. 255.255.255.255.
- ➡ **Port 50800 (IPO License Dongle):** To the License Server IP Address set in the IP Office config.
- ⬅ **Port 50801 (EConf):** Used by the Conference Center service.

Ports

IP Office 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 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 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 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 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 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]

Cause Codes (ISDN)

When a call is ended, a cause code may be shown in the 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 **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.

- 0 Unknown.
- 1 Unallocated (unassigned) number.
- 2 No route to specific transit network/(5ESS)Calling party off hold.
- 3 No route to destination / (5ESS) Calling party dropped while on hold.
- 4 Send special information tone / (NI-2) Vacant Code.
- 5 Misdialed trunk prefix.
- 6 Channel unacceptable.
- 7 Call awarded and being delivered.
- 8 Preemption/(NI-2)Prefix 0 dialed in error.
- 9 Preemption, cct reserved / (NI-2) Prefix 1 dialed in error.
- 10 (NI-2) Prefix 1 not dialed.
- 11 (NI-2) Excessive digits received call proceeding.
- 16 Normal call clearing.
- 17 User busy.
- 18 No user responding / No response from remote device.
- 19 No answer from user.
- 20 Subscriber absent (wireless networks).
- 21 Call rejected.
- 22 Number changed.
- 23 Redirection to new destination.
- 25 Exchange routing error.
- 26 Non-selected user clearing.
- 27 Destination Out Of Order.
- 28 Invalid number format.
- 29 Facility rejected.
- 30 Response to STATUS ENQUIRY.

- 31 Normal, unspecified.
- 34 No cct / channel available.
- 38 Network out of order.
- 39 Permanent frame mode connection out of service.
- 40 Permanent frame mode connection is operational.
- 41 Temporary failure.
- 42 Switching equipment congestion.
- 43 Access information discarded.
- 44 Requested cct / channel not available.
- 45 Pre-empted.
- 46 Precedence blocked call.
- 47 Resources unavailable/(5ESS)New destination.
- 49 Quality of service unavailable.
- 50 Requested facility not subscribed.
- 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.
- 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)+.
- 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)+.

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:*** = Indicated that message was output as the result of having the System | Print option enabled.
- ***PLATFORM_*** = Indicate 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

Avaya
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