IP Office

Maintenance Manual

Issue 1a (16th March 2005)

Table Of Contents

About this Book

Target Audience

The intended audience for this book is field maintenance and support engineers performing or managing fault finding activities on IP Office. Appropriate product training should also be undertaken by individuals performing these tasks.

For a listing of IP Office training courses, schedules and certification programs, see www.avaya-learning.com.

Intended Use

The troubleshooting scenarios in this book are intended to guide and help maintenance and support engineers who are fault finding on the IP Office. The scenarios in this manual have been developed from the knowledge and experience gained by Avaya supporting Business Partners with problems on IP Office. The most common customer issues have been documented in this manual.

If you encounter a scenario that has not been documented in this manual, please email this information (along with steps taken to resolve the case if available) to **maintmanual@avaya.com**.

Escalation

IP Office Technical Escalation Process

If you are unable to solve the customer issue. Refer to Information for Escalating a Case for details of the information required by support organizations to help resolve the issue. Providing this information will facilitate the support organizations diagnosing the issue more simply.

Information for Escalating a Case

The following information may be useful when resolving the customers' issues. If the following information is available when the case is escalated, it can help to reduce the time required to resolve the customer issue.

1. Problem Description
    - A detailed description of the customer issues including what services are being affected, which user actions, user numbers, user types etc.
    - Include a description of what behavior is expected from the operation of the problematic feature. For example when 'Divert No Answer to VM should route calls to VM after x rings if the time is set to y.'
2. IP Office Essential Information
    - A Copy of the IP Office(s) configuration file(s).
    - Confirmation of what version of Manager / Wizard is being used.
    - Any trace codes or log files generated by the System Monitor application (if available).
    - Notes relating to the result of each troubleshooting step performed.
3. IP Office VoIP Issues
    - Network topology diagram.
    - Detailed network connectivity information including connection types and bandwidth.
    - IP addressing scheme with IP addresses and masks of main switches and routers in the network.
        i. List of devices including make and model number.
        ii. What QoS settings have been configured?
        iii. Configuration of devices in non proprietary format.
    - Make and model of IP soft and hard phones connected to the IP Office including software / firmware version.
    - Number of IP Phones connected to the IP Office.
    - How these phones are connected (static / DHCP)?
    - A network sniffer trace of the problem area.
4. IP Office Applications – required for all PC based applications
    - What is the specification of the PC running the IP Office applications (CPU type and speed, memory installed, etc)?
    - What operating system is the PC running?
    - What service pack is installed on the PC?

Voicemail

- Which variant of Voicemail is being used?
- Is Voicemail Pro running as a service or application (provide details of the account and permissions if running as a service)?
- If Voicemail Pro, which version of VM Server is installed?
- What Voicemail functions (applications) are installed and being used (e.g. IMS, IVR, Campaigns)?
- Have a copy of the problem call flow in .mdb format (export call flow from VM pro).

User Applications

- Version numbers of the user applications connected to the PC that is experiencing the issues.
- Version numbers of all Avaya applications running other PCs on the network.

Compact Contact Center

- List the version numbers of all CCC applications installed (Delta Server, CCV, Wallboard Server, etc.).
- What version of MSDE or MS SQL is installed?
- What MSDE and SQL service pack level is running?

Conference Center

- What version of IIS is installed on the PC?
- If MAPI / SMTP client is installed which version?
- What version of internet explorer is installed?

Remote Access

Remote Access can help the process of investigating or fault finding on IP Office. Please refer to Remote Access Options within this manual for information on remote access options.

Remote Access

Remote Access Options

When you escalate a troubleshooting ticket, Avaya T3 may require remote access into the customer's IP Office system for diagnosing and troubleshooting. Avaya advises that remote access is set up on each application server installed; this will help with troubleshooting and trace collection.

The following are the Avaya recommended remote access options.

- **Remote Manager:** Default RAS connection to the IP Office.
- **Dameware:** 3rd party application supplied with each IP Office application CD and is a free install. This software needs to be installed on any PC on which the application requiring support is running. For example, if Voicemail Pro is installed on a separate PC from that of Manager, then Dameware needs to be installed on both PCs for access to both applications.
- **PC Anywhere:** Third party application that is licensed to the host and client. PC Anywhere is NOT provided by or licensed through Avaya. This software needs to be installed on any PC on which the application requiring support is running. For example, if Voicemail Pro is installed on a separate PC from that of Manager, then PC Anywhere needs to be installed on both PCs for access to both applications. Avaya Technical Support will use PC Anywhere to aid in the troubleshooting of certain issues, but the business partner must provide connectivity to the site and username and password information.
- **Webex:** This third party application is a client service and requires customer interaction. This application is NOT provided by or licensed through Avaya. Avaya Technical Support can also use Webex as a remote desktop client for troubleshooting and data collection. With this application, the Avaya Tier 3 engineer assigned to the trouble ticket will provide access information to an Avaya qualified BP engineer. Internet Explorer 6.0 or newer must be available to use Webex.

Remote Manager Setup

IP Office has default settings for remote access. This section walks you through those settings and setup for the remote dialup PC. Once connected, the remote PC is part of the IP Office network and can run many of the IP Office applications.

Procedure - Step I

A remote user must exist on the Manager PC as an initial step to setting up remote access. A remote user (**Remote Manager**) is available by default on Manager. This default user can be used for remote access or another user created if necessary.

To make use of the Remote Manager user, do the following to change the user password.

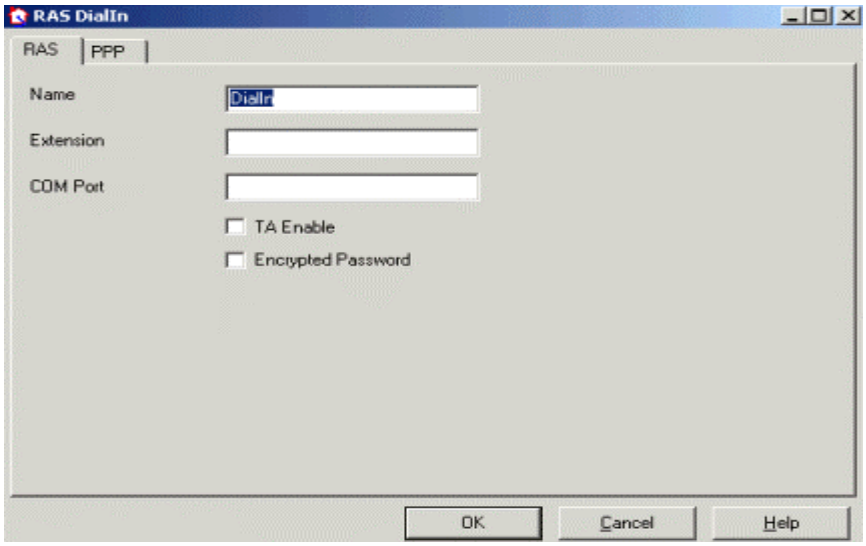
1. Log onto Manager and open the IP Office configuration.
2. Click **User** from the Configuration Tree. A list of users are displayed.
3. Double-click the **Remote Manager** user (default user for dial-in access).
4. On the **User** tab:
    - **Extension:** Leave blank
    - **Password/Confirm Password:** A default password is displayed, for security purposes, enter a new password. Make note of this password in a secure location as this is a remote access link into the customer's network.
5. On the **Dial In** tab, ensure that the **Dial In On** option is enabled/checked.
6. Click **OK** and then  to save the changes.

To create a new remote user:

1. Log onto Manager and open the IP Office configuration.
2. Click the **User** form within the Configuration Tree to display the list of existing users.
3. Right-click on the list area and select **New**.
4. On the **User** tab, enter a **Name** and **Password**. IP Office is case sensitive. Make note of this password in a secure location as this is a remote access link into the customer's network.
5. In the **Dial In** tab, ensure that **Dial In On** is checked.
6. Click **OK** and then  to save the changes.

Procedure - Step II

A RAS (Remote Access Service) is also required to enable remote access. Within Manager, a RAS entry called **DialIn** is available by default. There is no need to create a new **RAS** entry. The existence of this RAS entry can be verified by clicking the **RAS** form on the Manager Configuration Tree. A sample RAS configuration is provided below:

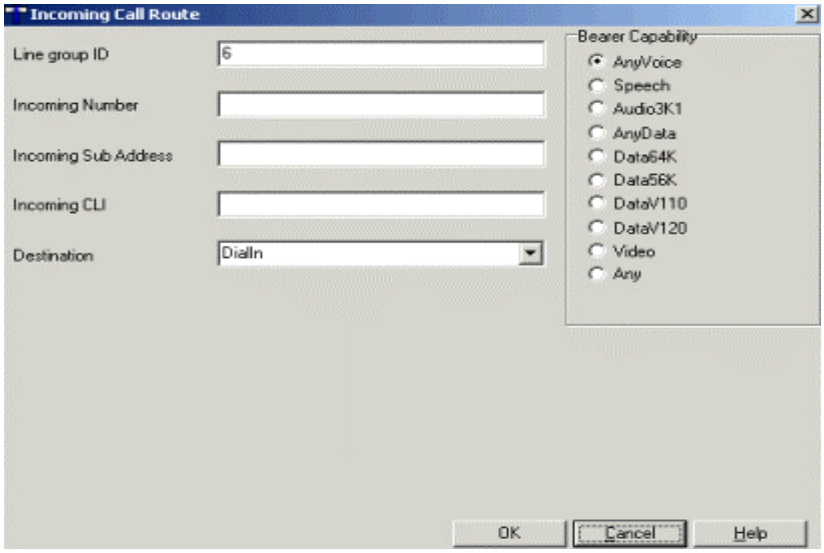


Procedure III

A incoming call route for dial-in access (labelled **DialIn**) is available by default. Additional configuration (Bearer Capability setting) is available if necessary.

To view or configure the incoming call route:

1. Log onto Manager and open the IP Office configuration.
2. Click the **Incoming Call Route** form within the Configuration Tree to display the list of existing call routes. One is labelled **DialIn** under the Destination heading. Double-click on the **DialIn** option. A window similar to the following appears:



3. If using an analog modem, set the **Bearer Capability** to **AnyVoice**. If using Digital TA for any digital dial up (BRI, PRI or T1), set to **AnyData**. If using **AnyVoice** ensure that you don't have another 'Blank' incoming number with a different destination in the LCR table. It is recommended the use of a specific DDI/DID with bearer set to **Any.** This is so all types of **DialIn** can be used. This requires a spare DDI/DID number.
4. In the **Destination** drop-down box, leave as the default, **DialIn**.

5. The values entered for any of the other fields depend on whether the remote user will be calling in on a particular line, phone number or from a set CLID.
6. Click **OK** and then  to save the changes.

Procedure IV

The steps above are sufficient for an incoming digital data connection. However, if the remote user has an IP address that is not in the same domain as the IP Office, then an IP Route is needed for outgoing return data.

If the remote user has an IP Address on the same subnet as the IP Office that was statically assigned you will need an IP Route within a 32bit mask configured with a destination of the RAS. Otherwise the IP Office will look to it's local LAN for the local IP Range.

- This is not necessary if the remote user has an IP address on same domain as the IP Office.
- This is not necessary if the remote user's dial-up connection method is set to 'Obtain an IP Address Automatically' and the IP Office's DHCP mode is set to Server or DialIn.

To create an IP Route:

1. Log onto Manager and open the IP Office configuration.
2. Click **IP Route** from the Configuration Tree.
3. Right-click on the list area and select **New** to enter the routing information.
4. In the **IP Address** and **IP Mask** fields, enter the information of the remote system.
5. In the **Destination** drop-down list, select the appropriate remote user (default is **Remote Manager**).
6. Click **OK** and then  to save the changes.

Call Quality

Analog Calls Cutting Off

Issue

Users experiencing their calls getting cut off.

Action

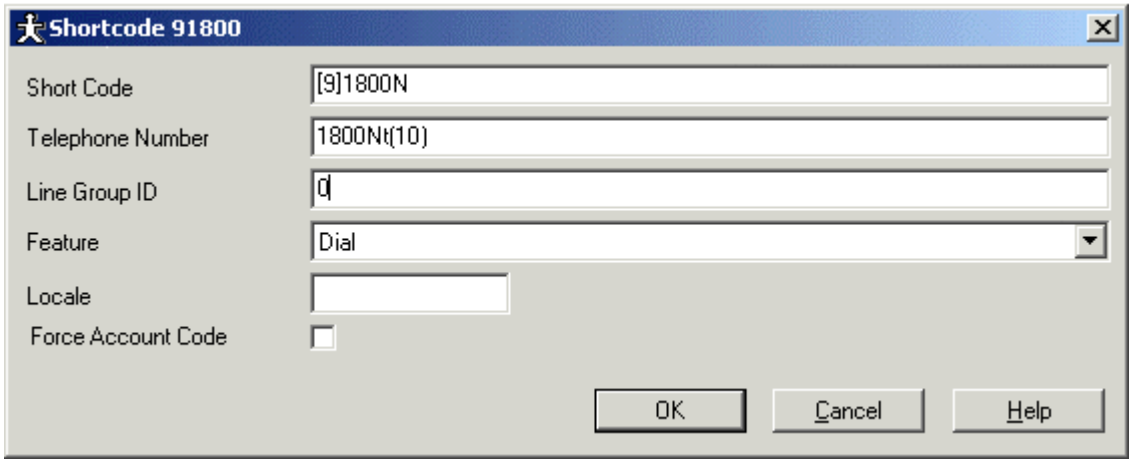
I. Check trunk cross connect for termination problems.

II. Check user and system short codes for **t** configuration. This type of short codes sets the maximum duration for a call (+/-1 minute). Follow the **Telephone Number** entry of short codes using a dial feature with **t(*x*)** where ***x*** is the number of minutes.

PROCEDURE

If only one user is experiencing the problem, check the user-specific short code for the user in question.

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **User** and double-click the user in question.
3. On the **ShortCodes** tab, if there is a short code with a **t** under the **Telephone Number** field, double-click it to access the short code settings. Below is a short code using the **t** in its Telephone Number field:



The short code above means the user on which this short code is set can dial 1800 numbers, but the connection is limited to 10 minutes (plus or minus a minute).

4. The duration setting can be adjusted if necessary by changing the number in the parenthesis or can be removed.

III. The same short code as the above can be set for the system, so check for a short code with **t** in its **Telephone Number** field. Follow steps 1-4 above.

IV. Confirm that the settings with Manager for the analog trunk/line is consistent with those settings provided by the Central Office/Network Provider.

PROCEDURE

To look at the settings within Manager:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Line** and double-click the trunk in question.
    - If it is an analog trunk, then check that the following configurations within the **Analog** tab match those provided by the Central Office/Network Provider:
        - **Trunk Type**
        - **Signaling Type**
        - **Direction**
3. Click **OK**.
4. If any updates have been made that need to be saved, click  and accept the selected reboot mode by clicking **OK**.

V. Verify with users in question to see if they have had intermittent resets on their telephones.

VI. Check Central Office/Network Provider lines for intermittent disconnect problems.

PROCEDURE

1. Ask the service provider if there are any problems on the line in question.
2. Check the System Monitor traces for invalid disconnect cause code in the line messaging.

To use the System Monitor application:

i. On the PC running Manager, click the Windows **Start** icon and select **Programs|IP Office|Monitor**.

ii. On the SysMonitor application, click  **Trace Options** to select the trace settings. Select Default options first, to ensure defaults are enabled.

iii. On the **Call** tab, make sure the **Line Receive** check box is checked. Also select **ATM** options.

iv. Click **OK**.

v. On the SysMonitor window, look for the following trace codes:

```
CMLineRx: v=5

CMReleaseComp

Line: type=Q931Line 5 Call: lid=0 id=29517 in=0

Cause=34, NoChannel
```

vi. If the Cause code is anything other than **16** (normal call clearing), it means there is an error condition on the line.

VII. If the calls are going over an IP line, confirm that the Codec selections are consistent between the two IP-based systems.

PROCEDURE

To look at the settings within Manager:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Line** and double-click the trunk in question.
3. Within the **VoIP** tab, verify that all the configuration selections are consistent with those set at the other end.

- **Compression Mode:** Needs to be hard coded (have a selection OTHER THAN **Automatic**) and the setting must be the same at both the IP Office sites. This is necessary to make use of the most suitable bandwidth available.
- **H450 Support:** This field selects the supplementary service signaling method for use across H.323 connections. The selected method must be supported by the remote end. For IP Office to IP Office connections, H450 is preferred.

4. Click **OK**.
5. If any updates have been made that need to be saved, click  and accept the selected reboot mode by clicking **OK**.

VIII. Check the CSU for intermittent resets. CSU is only available in North and South America.

IX. Using the System Monitor application, check the ATM 16 module for intermittent resets.

PROCEDURE

To use the System Monitor application:

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 **System** tab, make sure the **Error** and **Print** check boxes are checked.
4. Click **OK**.
5. On the SysMonitor window, look for the following trace codes:

```
69516mS ERR: DTExtn Line Down 7
85598mS ERR: DTExtn Line Up 7
85605mS PRN: TDMLink 7 Offline - WARNING!
85615mS PRN: TDMLink 7 Online
85684mS ERR: DTExtn Line Up 7
```

6. The presence of the above trace codes means the module is resetting.

X. Check with the users in question that the people they are speaking with when they experience calls cutting off are not on a cell phone.

XI. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Have the users in questions make the calls again and verify that calls are no longer cutting off.

Calls Clearing Down Without Audible or Visual Evidence of Dialing

Issue

When an internal or external call is made from either a telephone handset or an IP Office application/soft-phone, the call clears down without audible or visual evidence of dialing.

Actions

When **Off Hook Operation**/**Station** is enabled and a user initiates a call, if the other extension is busy or the line/trunk is not available, the call is cleared down immediately without audible (busy tone) or visual (on a soft phone) evidence. This feature is useful for call center agents because it eliminates the need to clear down a busy call or unavailable line before being allowed to make another call. This saves time and effort for the agent.

I. If this is not the desired operation for a particular user, the **Off Hook Operation/Station** function can be disabled via Manager or Phone Manager (Lite or Pro).

PROCEDURE

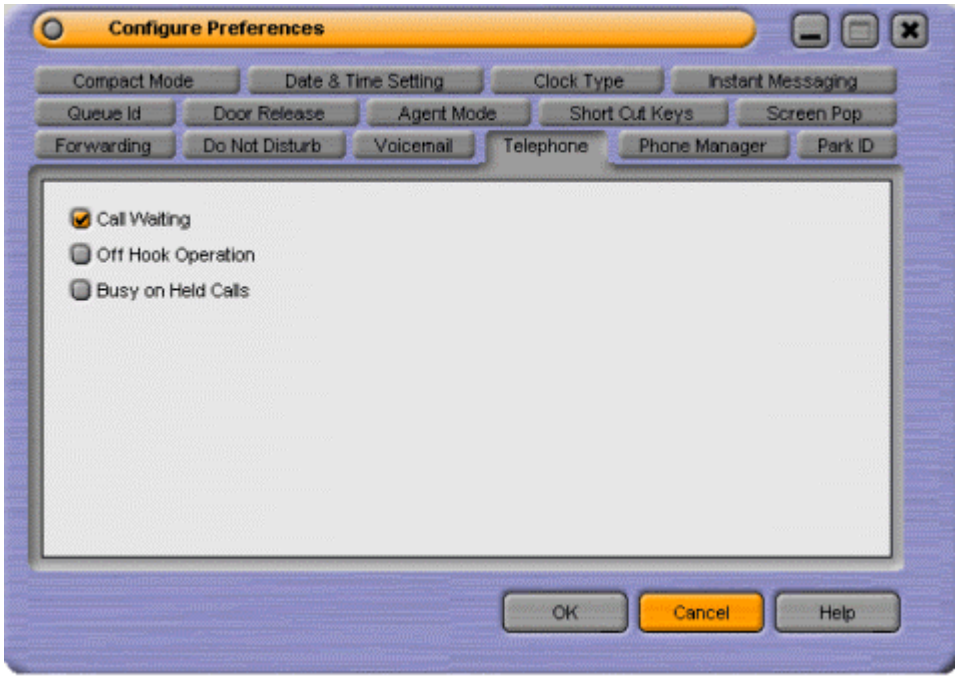
To change the setting via Manager:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **User** and double-click the user in question.
3. On the **Telephony** tab, make sure the **Off Hook Operation/Station** is disabled/unchecked.
4. Click **OK**.
5. Repeat the above steps for all users in question.
6. If any updates have been made and needs to be saved, click  and accept the selected reboot mode by clicking **OK**.

PROCEDURE

To change the setting via Phone Manager:

1. Have the user open Phone Manager and log on.
2. Click the  or select **Configure|Preferences** to open the Configure Preferences window.



3. On the **Telephone** tab, make sure the **Off Hook Operation/Station** is disabled/unchecked.

Note: Off Hook operation is always on if user is set to use iPhone Manager Pro

4. Click **OK**.
5. Have all other users in question perform the same tasks.

II. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Have the users in question make a call and verify that the call is not clearing down on its own.

Calls Over IP Trunk Disconnect Without Busy Tone

Issue

Calls over IP trunk to a remote IP Office site (Small Community Networking) disconnect without busy tone.

Action

VCM resources is only required when there is a non-IP device at one end of the IP call.

I. IP Office software version 2.0 and older will not return a busy tone when all VCM resources are in use. If the customer has IP Office software version 2.0 or older, it is highly recommended that the site is upgraded to the latest software release. See the System Upgrade section for upgrading procedures.

WARNING: If upgrading an IP Office 403 from a version older than 2.0 to one that is 2.0 or newer, you **MUST** follow the instructions closely to ensure a successful upgrade. For USA/CALA refer to IP Office Technical Bulletin 16 - General Availability of IP Office 2.0 software. For EMEA/APAC refer to IP Office Technical Bulletin 18 - General Availability of IP Office 2.0 software.

II. Via the System Monitor software, check the amount of VCM channels on the IP Office. Each time the System Monitor is started up, the number of VCM channels is displayed.

PROCEDURE

To use the System Monitor application:

1. On the PC running Manager, click the Windows **Start** icon and select **Programs|IP Office|Monitor**.
2. About a second after it starts up, click  to pause the trace information. Look for the **VCOMP** information within the following string of information:

```
lmS PRN: Monitor Started IP=192.168.42.2 IP 406 3.0(13) IP406
lmS PRN: LAW=A PRI=0, BRI=4, ALOG=0, ADSL=0 VCOMP=5, MDM=0, WAN=0, MODU=1 LANM=0 CkSRC=0 VMAIL=1(VER=2 TYP=1)
```

From the trace information above, **VCOMP=5**, it means there are 5 VCM channels on the IP Office system.

III. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Incoming Calls to IP Phones Do Not Have Complete Transmission

Issue

Incoming calls to IP phones have one way transmission or no transmission at all.

Actions

I. Check the incoming call route to make sure the call is routed to the correct destination.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Incoming Call Route** and double-click the incoming call route used by the caller when the problem was experienced.
3. If the call route's destination is to a Hunt Group, do the following:
    i. Check that the user experiencing the problem is part of the Hunt Group by doing the following:
        a. From the Configuration Tree, click **Hunt Group** and double-click the corresponding Hunt Group.
        b. On the **HuntGroup** tab, check that the user is listed within the **Extension List**.
    ii. If the user is part of the Hunt Group, check that the user does not have Forward Huntgroup calls enabled by doing the following:
        a. From the Configuration Tree, click **Users** and double-click the user in question.
        b. On the Forwarding tab, verify that **Forward Huntgroup Calls** is not enabled.
    i. Check that all the VoIP users in the Hunt Group have the same Codec type setting.
        a. From the Configuration Tree, click **Extension** and double-click the VoIP extension in question.
        b. On the **VoIP** tab, check that the **Compression Mode** field is set to a specific codec rather than for Automatic Selection. The hard coded codec should match for all users.
4. If the call route's destination is to a voicemail call flow, check that the call flow is directing the call appropriately. If the voicemail call flow is directing calls to an invalid condition or action, this may be the cause of the problem.

Note: An associated topic for this problem is VoIP Calls Not Tagged with Priority over Data Packets. The procedure could help to resolve the problem.

II. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

After the necessary changes have been made, reboot the IP Office and check with users to confirm that the issue has been resolved.

ISDN Calls Cutting Off

Issue

Calls on ISDN lines/trunks cutting off.

Actions

I. Confirm that the ISDN settings within Manager are consistent with the those provided by the Central Office/Network Provider.

PROCEDURE

To look at the settings within Manager:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Line** and double-click then PRI trunk in question.
3. On the **Line** tab, check the following:
   - The **Line SubType** matches that provided by the Central Office/Network Provider.
   - The **Number of Channels** setting matches that provided by the Central Office/Network Provider.
4. On the **Advanced** tab, check the following:
   - The **Clock Quality** is correctly set.
     - If there is only one PRI line/trunk, set the **Clock Quality** to **Network**.
     - If there are more than one PRI lines/trunks, set one of the lines/trunks to **Network** and the others to **Fallback**.
   - The line **Signaling** field should be set to **CPE**.
   - If CRC is enabled at the Central Office/Network Provider, then the **CRC Checking** field on this window should also be checked/enable.
5. Click **OK**.
6. If any updates have been made and needs to be saved, click  and accept the selected reboot mode by clicking **OK**.

II. Check Central Office/Network Provider lines for intermittent disconnect problems.

PROCEDURE

1. Ask the service provider if there are any problems on the line in question.
2. Check the System Monitor traces for invalid disconnect cause code in the line messaging.

   To use the System Monitor application:

   i. On the PC running Manager, click the Windows **Start** icon and select **Programs|IP Office|Monitor**.

   ii. On the SysMonitor application, click  **Trace Options** to select the trace settings.

   iii. On the **ISDN** tab, make sure the following fields (under the **Events** heading) are checked:
   - **Layer 1**
   - **Layer 2**
   - **Layer 3**

   iv. Click **OK**.

v. Trace codes start appearing on the 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:

1072151mS ISDNL1Evt: v=0 peb=5,F2 F1

The PRI in Slot A i.e. Line 5 (peb=5) has gone from the F1 state (normal Operational state) to the F2 state (Fault condition 1 state i.e. receiving RAI or receiving CRC errors).

1072651mS ISDNL1Evt: v=0 peb=5,PHDI ?

Line 5 (peb=5) is now in the Disconnected state (PHDI – Physical Deactivate Indication).

1072651mS ISDNL3Evt: v=0 p1=0,p2=1001,p3=5,p4=127,s1=

ISDN Layer 3 event which gives current status of line 5 (p3=5)

P1=0 -> ISDN Stacknum = 0.

P2=1001 ->Line Disconnecting

P3=5 -> Internal reference number

P4=127 ->TEI = 127

S1= ->not used

1072651mS ISDNL3Evt: v=0 stacknum=0 State, new=NullState, old=Active id=4

ISDN Layer 3 event which indicates that call with id 4 (id=4) on the first ISDN stack (stacknum=0) has changed from being Active (old=Active) to No Call exists (new=NullState).

1072652mS ISDNL3Evt: v=0 stacknum=0 State, new=NullState, old=Active id=24

ISDN Layer 3 event which indicates that call with id 24 (id=24) on the first ISDN stack (stacknum=0) has changed from being Active (old=Active) to No Call exists (new=NullState).

1072653mS ISDNL3Evt: v=0 p1=0,p2=1001,p3=5,p4=0,s1=

ISDN Layer 3 event which gives current status of line 5 (p3=5)

P1=0 -> ISDN Stack number = 0.

P2=1001 ->Line Disconnecting

P3=5 ->Internal reference number

P4=0 ->TEI = 0

S1= ->not used

1072656mS CMLineRx: v=5

CMReleaseComp

Line: type=Q931Line 5 Call: lid=5 id=4 in=1

Cause=38, NetworkOOO

The 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).

Note- There is no ISDNL3RX trace information as the call is dropped by the PBX NOT by the local exchange (due to the fact that we are no longer in communication with the Local Exchange!).

```
1072658mS
CALL:2000/11/2408:40,00:00:17,033,01732464420,I,300,027624,,,,0
```

The Incoming call from 01732464420 to [02083]027624 (Extn300) has been disconnected.

```
1072682mS CMLineRx: v=5

  CMReleaseComp

  Line: type=Q931Line 5 Call: lid=5 id=24 in=1

  Cause=38, NetworkOOO
```

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).

Note- 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).

III. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Have the users in questions make the calls again and verify that calls are no longer cutting off.

VoIP Calls Echo or Have Poor Speech Quality

Issue

Calls over VoIP trunks echo or have poor speech quality.

Actions

I. Check that when the problem is experienced that the call is not terminating on an analog Central Office/Network Provider endpoint. If there is an analog endpoint at the end of an IP connection, delays or echoes are likely and no action is necessary.

PROCEDURE

To verify if the external call is terminating on an analog endpoint, address the following questions to the user experiencing the problem:

1. Was the external call made to a home number or a home office?
   - If the answer is YES, it most likely means the call terminates on an analog endpoint.
   - If the answer is NO, ask question 2.
2. If the external call was made to an office, how many employees are in the company?
   - If the number is small, it most likely means the call terminates on an analog endpoint.
   - If the number is large, it may mean that the endpoint is not analog, so continue with the rest of the troubleshooting actions.

Actions within a Small Community Network (SCN)

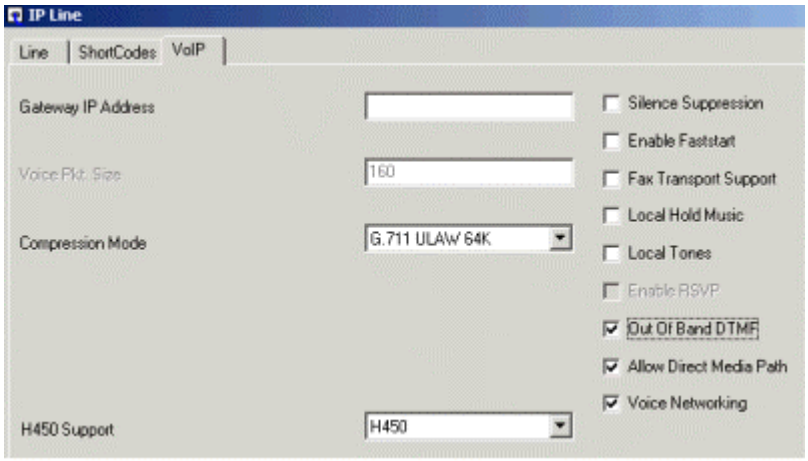
If you have determined that the call terminates on an IP endpoint (for example, the problem is experienced during calls between remote IP Office sites/within a Small Community Network), perform the following actions.

II. Verify the following configuration settings on the IP trunk:

PROCEDURE

To look at the settings within Manager:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Line** and double-click the IP trunk in question.



3. Within the **VoIP** tab:
   i. Confirm that the Codec selections are consistent between the IP-based systems.

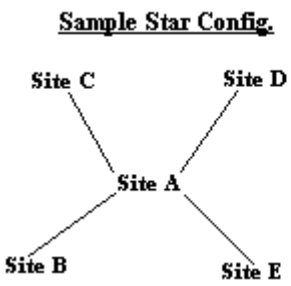
- **Compression Mode:** Needs to be hard coded (have a selection OTHER THAN **Automatic**) and the setting must be the same at both the IP Office sites. This is necessary to make use of the most suitable bandwidth available.
- **H450 Support:** This field selects the supplementary service signaling method for use across H.323 connections. The selected method must be supported by the remote end. For IP Office to IP Office connections, **H450** is preferred.

ii. Confirm the following settings at all the IP-based systems:

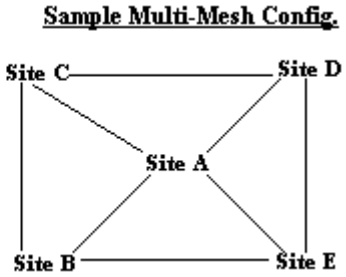
- **Enable Faststart:** Needs to be **UN-CHECKED (DISABLED)**. Having Faststart enabled can effect line quality because certain verifications/handshakes are skipped.
- **Allow Direct Media Path:** Needs to be **CHECKED (ENABLED)**. Enabling Direct Media Path allows the system to make use of the most direct connection between the two IP endpoints. Providing both systems support it.
- **Out-Of-Band DTMF:** Needs to be **ENABLED**.
- **Voice Networking:** Needs to be **ENABLED**. This will enable Small Community Networking.

4. Click **OK**.
5. If any updates have been made and needs to be saved, click and accept the selected reboot mode by clicking **OK**.

III. Check that the VoIP lines between networked sites are set up via a star configuration and NOT multi mesh. Depending if SCN is enabled or disabled.



Correct only when SCN is enabled



Correct only if SCN is disabled

A star configuration generates less SCN traffic on the IP trunks. Hence, it is the preferred configuration to help increase speech quality

PROCEDURE

To see which VoIP line configuration exists on the network, look at the number of IP trunks configured on each IP Office system.

1. Log onto Manager and open a remote site's IP Office configuration.
2. From the Configuration Tree, click **Line**. How many configured IP trunks do you see?
3. Now open the central site's IP Office configuration and open the **Line** configuration, how many IP trunks do you see?
4. From this information, you can work out how the VoIP lines are configured.

IV. Check with the Central Office/Network Provider that the Committed Information Rate (CIR) on Frame Relay is set for an acceptable level, as per the frame size. The setting should never be zero.

V. Verify the following with the System Administrator or the local IT Administrator:

1. Check that VLAN is enabled on all links to separate Voice and Data where available.
2. Check that Diffserve is enabled on supported routers and systems. Also check that the Diffserv Code Point (DSCP) is consistent throughout.
3. Check to see how voice calls are being routed. To do this you can use the Call Status application.
    - Frame Relay
    - Point-to-Point
    - ADSL link

VI. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Retry the voice call to verify that the speech quality is better.

Call Routing

Attempts to Dial Out Locally Get Routed Over VoIP Trunks

Issue

User is trying to dial out locally and the call gets routed over a VoIP trunk.

Actions

Check that the dial string used is routed through the appropriate line group on the User Short Code, User Restriction Short Code, System Short Code and Least Cost Route (LCR) Short Code. These short codes can effect which trunks outgoing calls are routed through, especially because IP Office has an order of priority in place for situations where short code settings conflict. For example, even though a dialing string may be associated with a system short code for dialling 800 numbers through a defined PRI trunk, but if a user uses a dialing string defined within the user short code that specifies routing 800 numbers through an IP trunk, then the user short code over-rides the system short code and the 800 call gets routed through the defined IP trunk.

A brief overview of short code matching:

- **User Short Codes**
  Takes priority over short codes set for user restrictions, the system as a whole and least cost routing. The individual user short codes are matched against dialing by a particular user.
- **User Restriction Short Codes**
  Takes priority over short codes set for the system as whole and least cost routing. The user restriction short codes are matched against dialing by all users linked to the User Restrictions set. They are overridden by individual user short codes.
- **System Short Codes**
  Takes priority over short codes set for least cost routing. System short codes are matched against any dialing by any user. They are overridden by individual user short codes and user restriction short codes.
- **Least Cost Routing Short Codes**
  Least cost routing short codes are matched against any dialing that results in a number to be dialed i.e. the output of a shortcode.

I. Look at the user short codes to check for the dialing string that defines the dialled number or a general short code for dialling out. The short code needs to be configured appropriately and directed to the right trunk/Line Group ID.

PROCEDURE

To check the user short codes:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Users**.
3. Double-click the user in question.
4. Click the **ShortCodes** tab. If there is a short code defining the dial string for 800 numbers, double-click the short code to view its configuration. The short code example below enables the 800 numbers to be dialed and routed through Line Group ID 0.

A sample user short code:

- **Short Code:** 9N;
- **Telephone Number:** 1800N
- **Line Group ID:** 0
- **Feature:** Dial

To see what trunk type Line Group 0 is associated with, click **Line** from the Configuration Tree and double-click the line.

5. If there is no short code associated with this user, continue to the next troubleshooting procedure.

II. Check to see if there is a User Restriction defined for this particular user because there may be one defined that directs the user's calls over an IP trunk.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Users**.
3. Double-click the user in question.
4. On the **User** tab, look at the **Restrictions** field to see if there is a restriction defined for the user. If it is blank, continue to the next troubleshooting step.
5. If there is a restriction defined:
   ii. Close the **User** configuration form and click **User Restriction** to view the configured restrictions. In the **Group Name** field, look for the name that matches the one listed within the **Restrictions** field for the user in question. Double-click on this user restriction to see its configuration.
   i. Click the **Short Code List** tab to see what short code is associated with this user restriction.
   iii. If there is a short code that defines the dial string in question, then make sure that the short code is defined similarly to the sample short code above.
   - If the short code is defined similarly to the above sample short code, check what trunk type the Line Group ID number is associated with by clicking **Line** from the Configuration Tree and double-clicking the line.
   - If the short code prevents the user from dialing out or contradicts with the sample short code above, remove this restriction from the user's **Restriction** field.
6. When all necessary configuration changes have been made, click  to save the changes.

III. Check the System short codes for one that defines the dial string in question. Make sure it is configured correctly.

PROCEDURE

To look at the system short codes:

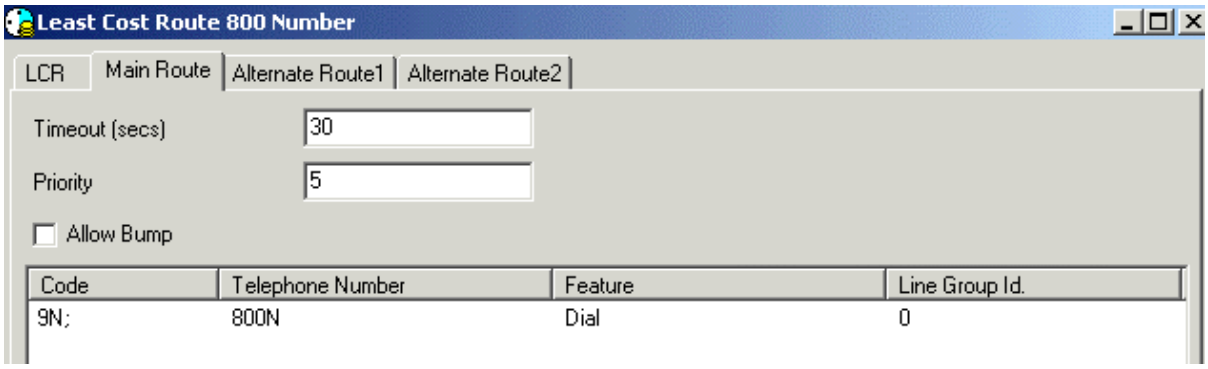
1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Shortcodes**. The list of system short codes are listed on the right hand side. If a short code exists for the dial string in question (a short code similar to the sample short code above), check what trunk type the Line Group ID number is associated with by clicking **Line** from the Configuration Tree and double-clicking the line.
3. If there is no such short code, continue to the next troubleshooting step.

IV. Check the least cost route (LCR) short codes to see if the dialling string has LCR rules set against it. LCR allows the administrator to route outgoing calls through specific carriers at specified times for cost saving purposes.

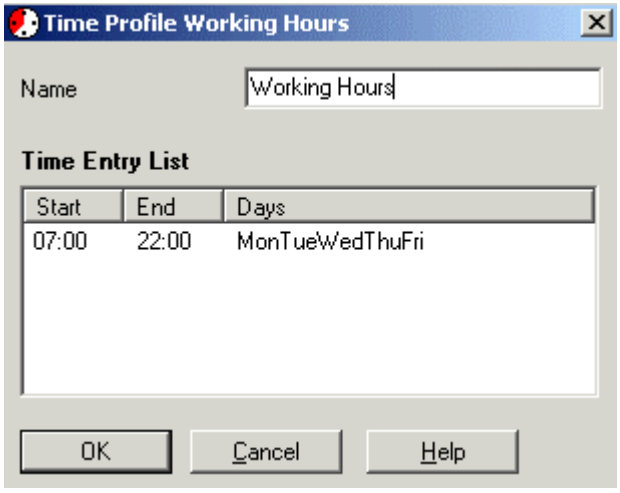
PROCEDURE

To look at LCR settings:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Least Cost Route**. If there is a LCR configured, double-click with the corresponding LCR name. A **Least Cost Route** window appears.



   i. In the **Time Profile** field, if there is a time profile set, make sure the dialed number was attempted within the configured time slot. To view the defined time for that profile, open the **Time Profile** configuration form and open the corresponding profile. A Time Profile window similar to the following displays:



   ii. On the **MainRoute**, **Alternate Route 1** and **Alternate Route 2**, verify that there are no short codes configured that routes the dialling string through an IP trunk.

   iii. Check that there are no overlapping short codes. For example, if the following short code is added to the **MainRoute** configuration in the above screenshot, the LCR feature would be compromised because one short code defines 800 calls through Line Group ID 0 while another short code defines the same outgoing 800 calls to go through Line Group ID 2:

   - **Short Code:** 9N;
   - **Telephone Number:** 1800N
   - **Feature:** Dial
   - **Line Group ID:** 2

iv. If there is a LCR short code with the dial string in question, verify the following:

- The user in question has waited for at least the **Timeout** period. This value sets how long the system waits before trying short codes configured on the Alternate Route 1 and 2 when a call goes to a line group where all lines are busy.
- The user has the priority level to make the call. For example, if the LCR **Priority** field is set to 5 (highest), then the user's priority (configured with the **User** configuration field) is also set to 5.

v. Look at the Alternate Routes to verify that any short codes configured for them are equally as valid as the ones configured for the **Main Route**.

V. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Confirm that the call is connecting via the desired trunk.

Delay Between Incoming Analog Line Ringing and Call Presented to Extensions

Issue

Incoming analog line rings several times before the call is presented to the extension. In other words, the caller hears several rings before the actual extension being contacted begins ringing.

Actions

If the analog trunk is configured to wait for caller ID (CLI/ICLID) information from the Central Office/ Network Provider but the Central Office/ Network Provider is not providing CLI/ICLID information, then there will be a delay between the time the line/trunk rings and the call being presented to the extensions.

I. It is good practice to confirm that the settings with Manager for the analog trunk/line is consistent with the trunk type provided by the Central Office/ Network Provider. At the same time, if the Central Office/ Network Provider is not providing CLI/ICLID information, the **Trunk Type** is set to **Loop Start**.

PROCEDURE

To look at and update the settings within Manager:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Line** and double-click the trunk in question.
    - Check that the following configurations within the **Analog** tab match those provided by the Central Office/ Network Provider:
        - **Signaling Type**
        - **Direction**
    - If the **Trunk Type** is set to **Loop Start ICLID**, set it to **Loop Start** so that the analog trunk/line will not wait for CLI/ICLID information.
3. Click **OK**.
4. If any updates have been made and needs to be saved, click  and accept the selected reboot mode by clicking **OK**.

II. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Verify that incoming calls ring extensions without delay.

Enabling Fax Machines to Dial Out Without Dialing 9

Issue

The customer's fax machines currently require that 9 is dialed to enable an outgoing fax. They want the fax system configured so that a 9 is NOT required.

Actions

I. If there are more than one fax machines that require this setup, it is more efficient to create a user restriction which defines a short code access without the 9. If there is just one fax machine, the same short code can be created just for the specific user.

Below is a sample short code to enable fax dialing without the 9:

- **Short Code:** ?
- **Telephone Number:** .
- **Line Group ID:** 0 (analog trunk/line)
- **Feature:** Dial

Procedure

To create the above short code as a User Restriction and apply it to the user which has a fax machine against it:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **User Restriction**.
3. Right-click within the Manager window and select **New**.
    - In the **Name** field, enter a name for this user restriction, i.e. **fax dialling**.
4. On the **Short Code List** tab, right-click and select **Add**.
    - Configure a short code similar to the above short code.
    - Click **OK**.
5. Click **OK** on the User Restrictions window.

To apply the fax dialling user restriction to a user:

1. From the Configuration Tree, select **User** and double-click the user which has a fax machine against it.
2. On the **Restrictions** field, click the drop down list and select the User Restriction previously created. Based on our example above, the user restriction is called **fax dialling**.
3. Click **OK**.
4. Repeat steps 1-3 to apply the user restriction to all users that have a fax machine against it.
5. When you are ready, click  to save the changes.

II. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Verify that the fax in question no longer requires dialing 9.

Incoming Calls Connected Together

Issue

Incoming calls are connected together.

Actions

To resolve this issue, call routing related settings and the key presses performed by users while transferring the incoming calls should be checked.

I. Check with the users transferring the incoming calls that they are transferring the calls to the right extension number and performing the hold properly.

II. If the problem occurs in relation to an incoming call without any transfers being performed, check the incoming call route for the number being dialed.

PROCEDURE

To check the incoming call route:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Incoming Call Route** and double-click the call route in question.
3. On the configuration window for that incoming call route, check the **Destination** field to verify that the call is being routed to the correct destination. Make sure the call is NOT being routed to a conference short code or Voicemail Pro conference module.
4. Click **OK**.
5. If any configuration changes have been made, click **OK** and then  to save the changes.

III. If the problem occurs after a transfer has been performed via a 4450 DSS console, it is most likely caused by the first transfer not being completed (the transfer destination is busy or has not answered the call) and the user of the 4450 DSS console transfers a second call. In this scenario, the two transferred calls are connected together.

IV. Also check with the Central Office/Network Provider that they are not experiencing any issues on the lines.

V. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Monitor to ensure that the problem is resolved.

LCR for Routing Calls Over IP Lines Not Working

Issue

Least Cost Routing (LCR) is configured to route external calls over the VoIP lines when the local ISDN lines are busy or fail, but the LCR is not working when the local lines fail.

Actions for Line Failures

Calls will not follow LCR on ISDN line failures. LCR is only supported when ISDN lines are busy.

Actions for Busy Lines

For busy ISDN lines, check the following to troubleshoot LCR for VoIP lines.

I. Verify that LCR is configured correctly on Manager.

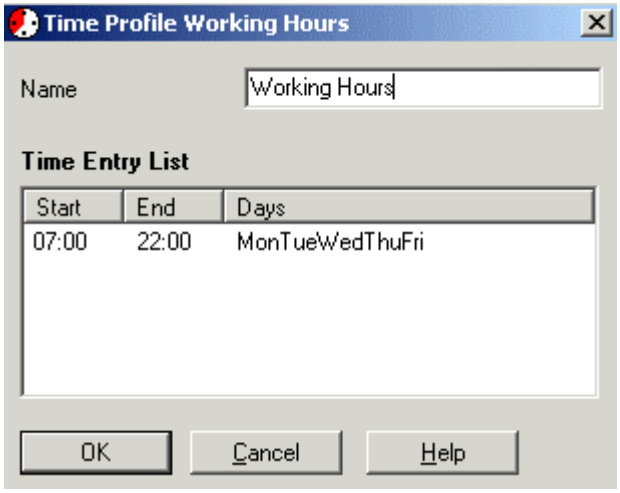
PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Least Cost Route**.
3. Double-click the LCR in question.
4. On the **LCR** tab, check that the **Time Profile** selected is set correctly for the working hours (the time period in which the customer wants external calls routed over the VoIP lines when local lines are busy or fails). If no profile is selected, the LCR settings apply at all times.

If there is a Time Profile selected, you can view that profile setting by doing the following:

i. From the Configuration Tree, click **Time Profile**.

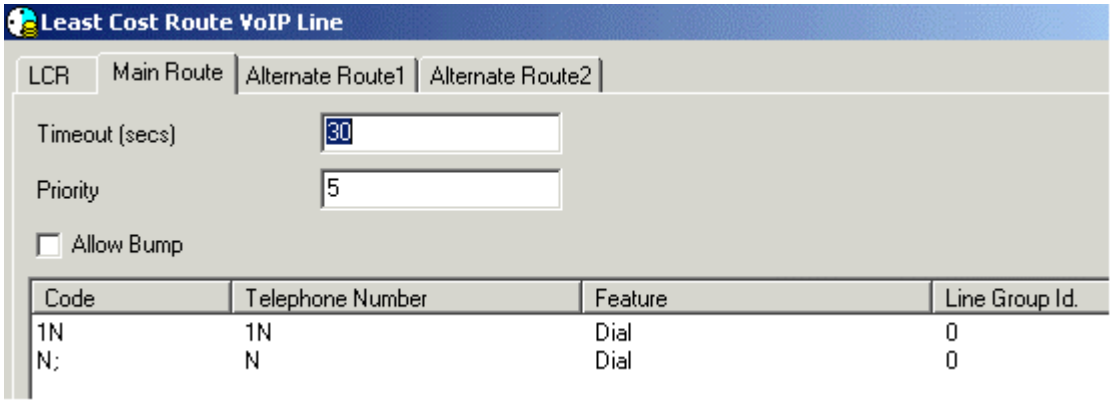
ii. Double-click the name of the time profile that was listed in the LCR configuration. A window opens which displays time settings for that time profile.



iii. Within the **Time Entry List**, check that the **Start/End** times and **Days** are set appropriately for the customer's working hours.

iv. If the entries need to be edited or deleted, right-click on it and make the necessary selection.

5. On the **Main Route** tab, check the following:



- 0 is the ISDN Group Id.
- The **Timeout value** is set appropriately. This value sets how long the system waits before trying short codes configured on the Alternate Route1 when a call goes to a line group where all lines are busy.
- The **Priority** setting for this route is within the priority setting for the User profile making the call. Priority of 0 is the lowest and 5 is the highest. If the User profile is assigned a priority of 5 and this route has the priority 3, then when the user makes a call but the call goes to a line group where all lines are busy, the system routes the call via the Alternate Route1 without waiting for the timeout value to expire. The default priority setting for User profiles is 5.
- Short codes for dialling out through the local ISDN lines are entered correctly and matches the system default short codes or user short codes. Check that there are no overlapping of short codes.

For example, the LCR feature would be compromised if a short code similar to the following is added to the above 2 LCR short codes:

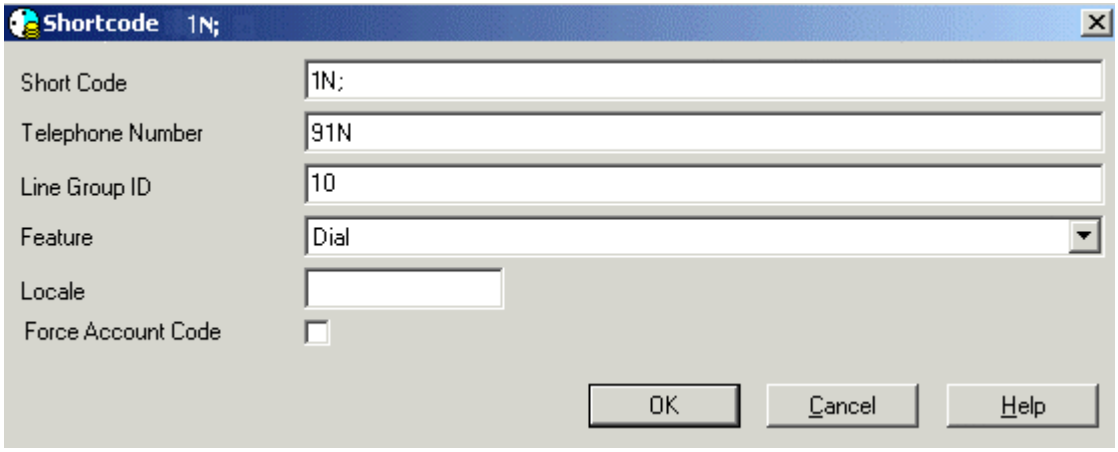
Short code: N;

Telephone Number: N

Feature: Dial

Line Group ID: 2

6. On the **Alternate Route 1** tab, check the following:
   - The **Timeout value** is set appropriately. This value sets how long the system waits before trying short codes configured for the Alternate Route2 when a call goes to a line group where all lines are busy.
   - The **Priority** setting for this LCR is within the priority setting for the User profile making the call. Priority of 0 is the lowest and 5 is the highest. If the User profile is assigned a priority of 5 and this route has the priority 3, then when the user makes a call but the call goes to a line group where all lines are busy, the system routes the call via the Alternate Route1 without waiting for the timeout value to expire. The default priority setting for User profiles is 5.
   - The short code is configured appropriately for routing calls over the VoIP lines. The short code should look similar to the following:



- Check that there are no overlapping of short codes. For example, the LCR feature would be compromised if a short code similar to the following is added to the list of LCR short codes that already contains the above short code because the short code below requires that the caller enters a number starting with 1234 before the call is routed through. So if the caller does not meet this requirement, the call will not be routed through, even though the above short code defines that any number is acceptable.
    - **Short code:** 1N;
    - **Telephone Number:** 1234N
    - **Feature:** Dial
    - **Line Group ID:** 10

II. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

After making the necessary changes to the configuration, test that external calls are routed over the VoIP lines when the local ISDN lines are busy.

Not Able to Set the Outgoing Caller ID Information

Issue

Can not set the outgoing caller ID (ICLID/CLI) information to a specified number.

Actions

I. Check with the Central Office/Network Provider that they will accept outgoing caller ID information being sent to them and that they will pass it on to the network. In some countries, the caller ID feature must be purchased from the Central Office/Network Provider before it is activated.

II. Verify that the outgoing caller ID number being sent is part of the DID/DDI range for that customer. Check with the IT/System Administrator or the Central Office/Network Provider for this information.

III. In order to view caller ID information, the caller ID feature may also need to be purchased at the other end (depending on locale). Check that the person expecting the caller ID information is capable of receiving the information.

Actions Specific to Short Code Configuration

Verify that the dialing string used to access the outside line has the ICLID/CLI information defined. The dialing string can be configured via the User Short Code, a User Restriction Short Code, a System Short Code or a Least Cost Route Short Code. These short codes can effect what outgoing ICLID/CLI information is sent on which PRI circuit, especially because IP Office has an order of priority in place for situations where short code settings conflict. For example, even though the dialing string may be associated with a system short code for sending out a specified ICLID/CLI, but if a user uses a dialing string defined within the user short code that specifies another ICLID/CLI information, then the user short code over-rides the system short code and the ICLID information defined within the user short code is presented. If there are no specific ICLID/CLI information defined, the user's incoming call route is used as the outgoing caller ID.

A brief overview of short code matching:

- **User Short Codes**
  Takes priority over short codes set for user restrictions, the system as a whole and least cost routing. The individual user short codes are matched against dialing by a particular user.
- **User Restriction Short Codes**
  Takes priority over short codes set for the system as whole and least cost routing. The user restriction short codes are matched against dialing by all users linked to the User Restrictions set. They are overridden by individual user short codes.
- **System Short Codes**
  Takes priority over short codes set for least cost routing. System short codes are matched against any dialing by any user. They are overridden by individual user short codes and user restriction short codes.
- **Least Cost Routing Short Codes**
  Least cost routing short codes are matched against any dialing that results in a number to be dialed i.e. the output of a shortcode.

I. Look at the user short codes to check for the dialing string that defines the outgoing ICLID/CLI information sent. If there is a user short code that defines the ICLID/CLI information, have the user apply the short code.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Users**.
3. Double-click the user in question.

4. Click the **ShortCodes** tab. If there is a short code with an "**s**" in its **Telephone Number** field, double-click on the short code to display the configuration. If the short code configuration looks similar to the sample below, then the string of numbers immediately following the **s** is the outgoing ICLID/CLI information displayed when the user dials using this short code.

A sample user short code:

- **Short Code:** 9N;
- **Telephone Number:** Ns4085551234
- **Line Group ID:** 5
- **Feature:** Dial

If there is a short code similar to the above associated with this user, have the user apply the short code.

5. If there is no short code associated with this user, continue to the next troubleshooting procedure.

II. Check to see if there is a User Restriction defined for this particular user because there may be one defined that prevents the user from sending out caller ID information.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Users**.
3. Double-click the user in question.
4. On the **User** tab, look at the **Restrictions** field to see if there is a restriction defined for the user. If it is blank, continue to the next troubleshooting step.
5. If there is a restriction defined:

ii. Close the **User** configuration form and click **User Restriction** to view the configured restrictions. In the **Group Name** field, look for the name that matches the one listed within the **Restrictions** field for the user in question. Double-click on this user restriction to see its configuration.

i. Click the **Short Code List** tab to see what short code is associated with this user restriction.

iii. If there is a short code that defines an outgoing ICLID/CLI number, then make sure that the short code is defined similarly to the sample short code above.

- If the short code is defined similarly to the sample short code, have the user apply this short code.
- If the short code prevents the user from dialing out or contradicts with the sample short code above, remove this restriction from the user's **Restriction** field.

6. When all necessary configuration changes have been made, click  to save the changes.

III. Check the system short codes for one that defines the required outgoing ICLID/CLI information to be sent. If the dialed number matches a system short code, apply the short code.

PROCEDURE

To look at the system short codes:

1. Log onto Manager and open the IP Office configuration.

2. From the Configuration Tree, select **Shortcodes**. The list of system short codes are listed on the right hand side. If a short code exists for the outgoing ICLID/CLI information (a short code similar to the sample short code above), apply the short code.
3. If there is no such short code, continue to the next troubleshooting step.

IV. Check to see if a least cost route (LCR) has been defined for sending out the specified caller ID. If a LCR is configured for sending out caller ID information and there is a **Time Profile** defined for it, then when users dial the dial string, the caller ID information will only be sent out within the time specified.

PROCEDURE

To look at the LCR settings:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Least Cost Route**. If there is a LCR configured, double-click with the corresponding LCR name. A **Least Cost Route** window appears:
3. Click the **MainRoute** tab and look for short codes that define the use of ICLID/CLI information. A sample short code is displayed below:
    - **Short Code:** 9N;
    - **Telephone Number:** Ns4085551234
    - **Line Group ID:** 5
    - **Feature:** Dial
2. When all necessary configuration changes have been made, click  to save the changes.

V. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Make an external call and check that the required caller ID information is being sent.

User Cannot Make External Calls and Phone Displays "No User"

Issue

A user cannot make external calls and the telephone display shows "No User".

Actions

I. Check the user's configuration for Hot Desk settings. Hot desking allows several users to use the same extension, but each user logs in to access their user settings and Voicemail. Any phone can be used to hot desk. Hot desking is useful for people who are not at their desks throughout long periods of the day. Each user can be defined as a Hot Desk user by assigning a Login Code for use on any phone.

PROCEDURE

To check this user's Hot Desk settings:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **User** and double-click the user in question.
3. On the **Telephony** tab, check to see if there is any information in the **Login Code** field.
    - If there is a code entered, it means the user in question can make use of the hot desk feature. If the user can remember the assigned login code, have the user dial the default extension login short code (***35*N#**), where **N** represents the login code.
    - If there is a login code entered but the user cannot remember the code:
        i. Enter a new code (minimum of 4 characters).
        ii. Click **OK** and then  to save the changes.
        iii. Have the user dial the default extension login short code (***35*N#**), where **N** represents the new login code. Someone may have used the phone is question for hot desking, so this procedure will log the user back on with all its corresponding settings and configurations.
        iv. "No User" should no longer be displayed.
    - If there is no login code:
        i. Enter a code (minimum of 4 characters).
        ii. Click **OK** and then  to save the changes.
        iii. Have the user dial the default extension login short code (***35*N#**), where **N** represents the login code. Someone may have used the phone is question for hot desking, so this procedure will log the user back on with all its corresponding settings and configurations.
        iv. "No User" should no longer be displayed.

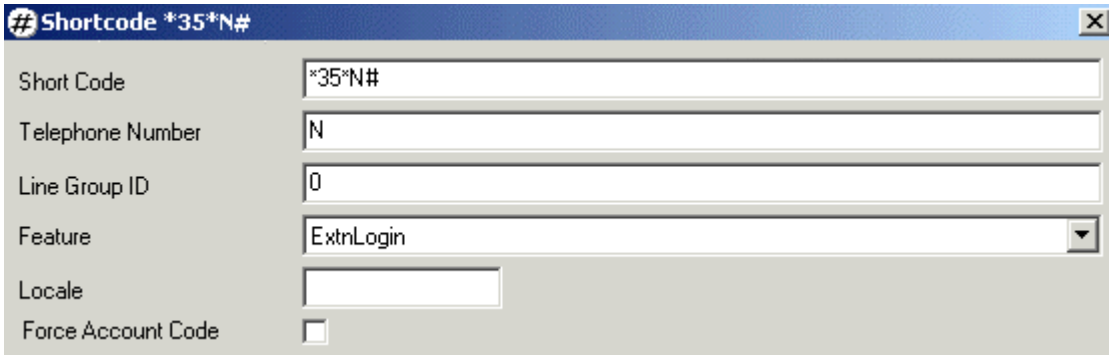
II. If the default extension login short code (*35*N#) does not allow the user to log onto the phone, it may be because the default short code has been amended.

PROCEDURE

To check the list of system short codes for the extension login short code:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Shortcode**. The list of system short codes are displayed.

3. Under the **Feature** heading, look for **ExtnLogin**. If displayed, double-click it to display the short code configuration. The short code configuration should look similar to the following (with the only difference being the short code number).



4. Have the user apply this short code to log onto the phone.

III. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

After using the **ExtnLogin** short code to log in, the user should now be logged onto the phone and able to make external calls.

User is Unable to Make Internal or External Calls

Issue

User is unable to make internal or external calls.

Actions

I. Check the handset is working by off hook /on hook tests. Verify if there is dial tone. Check all connections and remove and replace connections as necessary.

II. Replace with a similar handset.

A system user may or may not have an extension number that physically exists. Not having a physical extension is useful for users who are not physically located in the office (for example), but need to use system features, i.e. voicemail, forwarding, etc.

I. Confirm that the number the user is dialling can be completed by other users - at that site as well as offsite (cell/mobile for example). This step will rule out the dialled number as the cause of the problem.

II. Confirm that the user is logged on.

PROCEDURE

If the user is using Phone Manager, this is the quickest way to confirm the user's log on status. To check log on status via Phone Manager:

1. Have the user in question open the Phone Manager application. The user's name should be displayed in the Phone Manager title bar. If it is not, have the user log on by doing the following:
    i. Click **Configure|PBX**. A **PBX Configuration Information** window appears.
    ii. In the **UserName** drop-down menu, select the user's name.
    iii. If a password has been set for this user on Manager within the **User** tab, then enter this password here. This password is NOT the **Login Code** within the **Telephony** tab that makes the user a hot desking user (if hot desking is configured for this user).
    iv. Make sure the **PBX Address** is that of the IP Office control unit.
    v. Click **OK**. The user is now logged on.

PROCEDURE

If the user in question does not have Phone Manager, manually log the user onto the phone via the default system short code (***35*N#**), where **N** is the extension number. For example, dialing *35*202# logs on extension 202. If the user associated with extension 202 is logged onto another phone, this logs the user out on that other phone and logs the user onto the existing phone.

III. Confirm that **Outgoing Call Bar** is not configured for the user in question.

PROCEDURE

To check the user's Outgoing Call Bar setting:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Users** and double-click the user in question.
3. From the **Telephony** tab, check that the **Outgoing Call Bar** check box is unchecked.
4. Click **OK**.

5. If any configuration changes have been made, click **OK** and then to save the changes.

IV. After confirming the above three actions, check the dialed number against the following options. These options check to see if the dialed number has been associated with a User Short Code, a User Restriction Short Code, a System Short Code or a Least Cost Route Short Code. These short codes may effect how calls are routed, especially because IP Office has an order of priority in place for situations where short code settings conflict. For example, even though the number may be associated with a system short code for dial out, but if a user short code has been created that prevents the number from being dialed out, then the user short code over-rides the system short code and the number cannot be dialed out.

A brief overview of short code matching:

- **User Short Codes**
  Takes priority over short codes set for user restrictions, the system as a whole and least cost routing. The individual user short codes are matched against dialing by a particular user.
- **User Restriction Short Codes**
  Takes priority over short codes set for the system as whole and least cost routing. The user restriction short codes are matched against dialing by all users linked to the User Restrictions set. They are overridden by individual user short codes.
- **System Short Codes**
  Takes priority over short codes set for least cost routing. System short codes are matched against any dialing by any user. They are overridden by individual user short codes and user restriction short codes.
- **Least Cost Routing Short Codes**
  Least cost routing short codes are matched against any dialing that results in a number to be dialed.

OPTIONS

1. Look at the user short codes to confirm that there are no short codes to prevent the number from being dialed. If the dialed number matches a User Short Code, apply the shortcode.

   PROCEDURE

   To check if there is a user short code assigned to the dialed number:

   i. Log onto Manager and open the IP Office configuration.

   ii. From the Configuration Tree, select **Users**.

   iii. Double-click the user in question.

   iv. Click the **ShortCodes** tab. If a user short code is set against the dialed number, apply the short code.

   A sample user short code is:

   - **Short Code:** [9]1800N;
   - **Telephone Number:** 1800N
   - **Line Group ID:** 0
   - **Feature:** Dial

   In this example, the user on which this short code is set can dial numbers starting with 1800 after dialling 9 to get an external line.

2. Check to see if the number matches a short code in the user restriction set associated with the user. **User Restriction** short codes are useful when applied to the **Restriction** field for

each user. When applied to a user, these short codes can be used by those specific users and eliminate the need to recreate the short codes for each user.

PROCEDURE

To see if there is a User Restriction short code set against the dialed number:

i. Log onto Manager and open the IP Office configuration.

ii. From the Configuration Tree, select **User Restrictions**. If there is a User Restriction:

   a. Double-click the restriction. A **User Restrictions** window opens.

   b. Click the **Short Code List** tab to see what short code is associated with this user restriction.

   c. If the short code makes use of the dialed number, then check to see if this user restriction is associated with the user in question.

iii. If there is no User Restrictions set, move on to Option 3.

To see if the user in question has an associated short code restriction:

i. Log onto Manager and open the IP Office configuration.

ii. From the Configuration Tree, select **Users**.

iii. Double-click the user in question.

iv. On the **User** tab, look at the **Restriction** field to see if there is a restriction applied. If a restriction exists and that restriction contains a short code which allows the user to make the call in question, then apply that short code. If no restriction exists for the user, then continue to Option 3.

3. Check the system short codes to see if the dialed number is assigned a special dialing method. If the dialed number matches a system short code, apply the short code.

PROCEDURE

To look at the system short codes:

i. Log onto Manager and open the IP Office configuration.

ii. From the Configuration Tree, select **Shortcodes**. The list of system short codes are listed on the right hand side. If a short code exists for the dialed number and it enables users to dial out (a short code similar to the sample short code above), apply the short code.

iii. If there is no system short code for dialing out, create one.

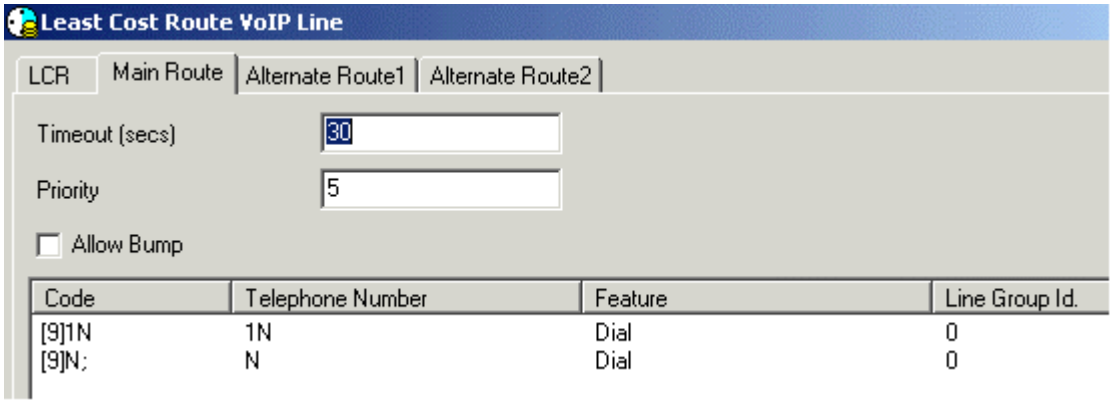
4. Check the least cost route (LCR) short codes to see if the dialed number has LCR rules set against it. LCR allows the administrator to route outgoing calls through specific carriers at specified times for cost saving purposes.

PROCEDURE

To look at LCR settings:

i. Log onto Manager and open the IP Office configuration.

ii. From the Configuration Tree, select **Least Cost Route**. If there is a LCR configured, double-click with the corresponding LCR name. A **Least Cost Route** window appears:



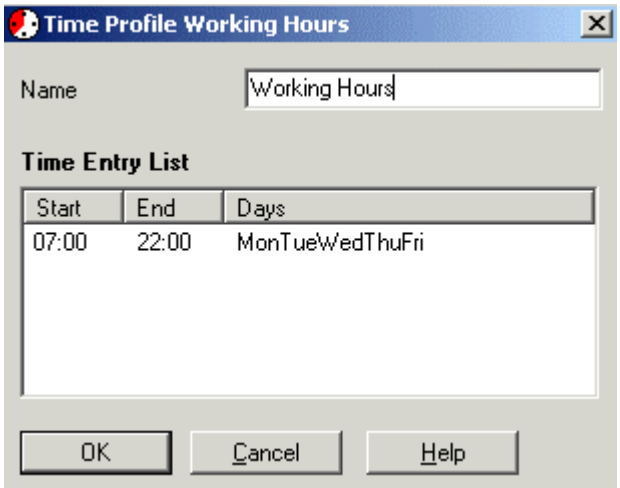
a. On the **MainRoute**, **Alternate Route 1** and **Alternate Route 2**, verify that there are no short codes configured to prevent the dialed number from being dialed.

b. Check that there are no overlapping short codes. For example, if the following short code is added to the **MainRoute** configuration in the above screenshot, the LCR feature would be compromised because one short code defines all outgoing calls through Line Group ID 0 while another short code defines the same outgoing calls to go through Line Group ID 2:

   - **Short Code:** [9]N;
   - **Telephone Number:** N
   - **Feature:** Dial
   - **Line Group ID:** 2

c. If there is a LCR short code with the number in question configured for dialing, verify the following:

   - The user in question has waited for at least the **Timeout** period. This value sets how long the system waits before trying short codes configured on the Alternate Route 1 and 2 when a call goes to a line group where all lines are busy.
   - The user has the priority level to make the call. For example, if the LCR **Priority** field is set to 5 (highest), then the user's priority (configured with the **User** configuration field) is also set to 5.
   - In the **Time Profile** field, if there is a time profile set, make sure the dialed number was attempted within the configured time slot. To view the defined time for that profile, open the **Time Profile** configuration form and open the corresponding profile. A Time Profile window similar to the following displays:



iii. Look at the Alternate Routes to verify that any short codes configured for them are equally as valid as the ones configured for the **Main Route**.

iv. Click **OK** and then  to save the changes..

V. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Have the user in question dial the internal or external telephone number.

User is Unable to Receive Calls

Issue

User can not receive incoming or internal calls.

Action

I. Confirm that the number being dialed is the number displayed on the telephone display window.

II. Confirm the user has a system dial tone.

III. Confirm the user in question is logged in on the phone in which incoming calls are expected.

IV. Check the Forwarding options for the user via Manager or Phone Manager.

PROCEDURE

If the user is using Phone Manager, this is the quickest way to confirm the user's log on status. To check log on status via Phone Manager:

1. Have the user in question open the Phone Manager application. The user's name should be displayed in the Phone Manager title bar. If it is not, have the user log on by doing the following:
    i. Click **Configure|PBX**. A **PBX Configuration Information** window appears.
    ii. In the **UserName** drop-down menu, select the user's name.
    iii. If a password has been set for this user on Manager within the **User** tab, then enter this password here. This password is NOT the **Login Code** within the **Telephony** tab that makes the user a hot desking user (if hot desking is configured for this user).
    iv. Make sure the **PBX Address** is that of the IP Office control unit.
    v. Click **OK**. The user is now logged on.

PROCEDURE

If the user in question does not have Phone Manager, manually log the user onto the phone via the default system short code (***35*N#**), where **N** is the extension number. For example, dialing *35*202# logs on extension 202. If the user associated with extension 202 is logged onto another phone, this logs the user out on that other phone and logs the user onto the existing phone.

IV. Check that the user does not have **Do Not Disturb** configured. Having DND configured will send all incoming calls to voicemail or the defined divert number.

PROCEDURE

1. If the user's telephone has a display, look on the display for a **N**, **DND** or **NoCalls** setting (display varies depending on the type of phone). If the user has Phone Manager (Lite or Pro), check to see if there is a **DND** label next to the user's name on the Phone Manager application. DND settings can also be verified on Manager for the user in question.
2. If there is a DND configured, disable the feature via Manager by doing the following:
    a. Log onto Manager and open the IP Office configuration.
    b. From the Configuration Tree, select **User** and double-click the user in question.
    c. On the **DND** tab, make sure that the **Do Not Disturb** check box is not checked.
    d. If any configuration changes have been made, click **OK** and then  to save the changes.
3. DND can also be configured/disabled on Phone Manager by doing the following:
    a. Have the user in question open the Phone Manager application and log on.

b. Click **Configure|Preferences**.

c. On the **Do Not Disturb** tab, make sure the **Do Not Disturb** check box is unchecked.

d. Click **OK**.

V. Check that the user does not have divert/forward options enabled.

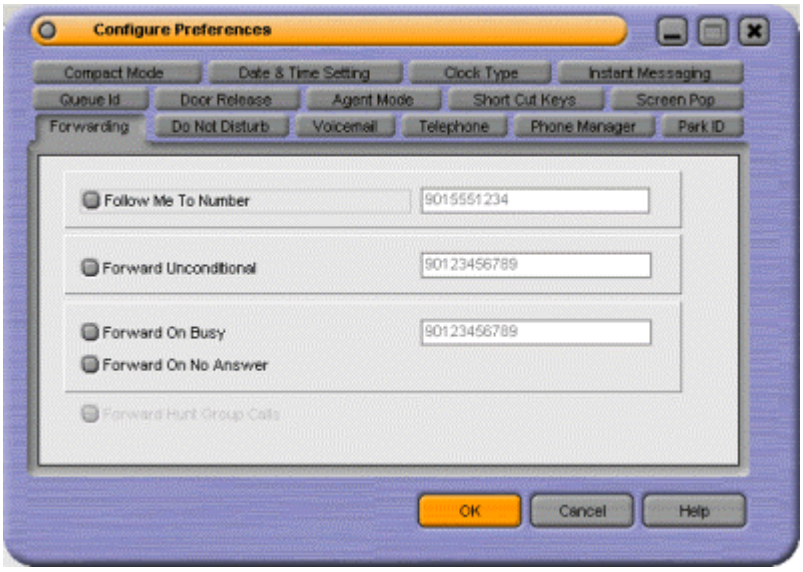
PROCEDURE

1. If the user's telephone has a display, look on the display for a **D** or **Divert** setting (display varies depending on the type of phone). If the user has Phone Manager (Lite or Pro), check to see if there is a **Fwd unconditional** label next to user's name on the Phone Manager application. Divert/forward settings can also be verified on Manager for the user in question.
2. If there is a divert/forward configured, disable the feature via Manager by doing the following:
    a. Log onto Manager and open the IP Office configuration.
    b. From the Configuration Tree, select **User** and double-click the user in question.
    c. On the **Forwarding** tab, make sure that the **Forward Unconditional** check box is unchecked.
    d. If any configuration changes have been made, click **OK** and then  to save the changes.
3. Divert/Forwarding can also be configured/disabled on Phone Manager by doing the following:
    a. Have the user in question open the Phone Manager application and log on.
    b. Click **Configure|Preferences**.
    c. On the **Forwarding** tab, make sure the **Forward Unconditional** check box is unchecked.
    d. Click **OK**.

VI. Check that the user does not have Follow Me options enabled. The Follow Me feature is similar to forwarding or diverting a call.

PROCEDURE

1. If the user has Phone Manager (Lite or Pro), check to see if there is a **Follow to** label next to user's name on the Phone Manager application. If the user in question does not have Phone Manager, check for the Follow Me setting on Manager by doing the following:
    a. Log onto Manager and open the IP Office configuration.
    b. From the Configuration Tree, select **User** and double-click the user in question.
    c. On the **Forwarding** tab, make sure that in the text box corresponding to the **Follow Me Number** field there are no numbers selected.
    d. If any configuration changes have been made, click **OK** and then  to save the changes.
2. Follow Me can also be configured/disabled on Phone Manager by doing the following:
    a. Have the user in question open the Phone Manager application and log on.
    b. Click **Configure|Preferences**.



c. On the **Forwarding** tab, make sure the **Follow Me To** check box is unchecked.

d. Click **OK**.

VII. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Make a call to the user in question and verify that the call goes through.

VoIP Calls Not Tagged with Priority over Data Packets

Issue

VoIP calls are not tagged with priority over data packets on the LAN network.

Actions

For VoIP calls to be routed and treated appropriately on the LAN network, they need to be tagged with the appropriate Quality of Service/DiffServe values and the same values need to be set on the network.

I. Check the tagging values IP Office is assigning to VoIP calls.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. Click **System** and double-click the system you are configuring.
3. On the **Gatekeeper** tab, check the following fields:
    - **DSCP(Hex):** The value entered here defines the Quality of Service/DiffServe setting applied to the VoIP calls. The default value is **0xB8** which equates to a DSCP (DiffServ Code Point) of **46** in decimal format.
    - **DSCP Mask(Hex):** The value entered here defines the mask to be applied to the packets for the DSCP value. The default value is **0xFC** with **63** as the equivalent value in decimal format.
4. Check that all routers and switches on the LAN network are set to use the same values to allow for proper routing of VoIP calls.

II. Using a Protocol Analyzer such as Ethereal, Observer or Sniffer. Check that the IP Office is sending data with the appropriate priority header settings as defined above.

III. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

If the priority is set appropriately and the Protocol Analyzer trace shows the priority value and the problem still persists, then the customer's network needs investigating.

DTE Port Maintenance

DTE Port Maintenance

The DTE port on the back of an IP Office Control Unit is not normally used when configuring an IP Office system. However the DTE port can be used to erase the system's operational software and/or configuration if necessary.

Instances where the system configuration may need to be cleared are:

- Forgotten IP Office system password: In this instance, erasing the system configuration from the control unit allows you to access the control unit via a default configuration and then load the backup copy of the old configuration (with all the system settings, user settings, etc.)

Due to the drastic nature of these actions, they should only be performed if absolutely necessary to return a system back to working order.

Before using the DTE port to erase the system software and/or configuration, a backup copy of the system configuration MUST be available.

Save a backup copy of the system configuration

Make a copy of the current configuration file by saving it offline before clearing the system software and/or configuration. Having this backup configuration will save time and effort once the box is erased and ready to have a configuration loaded.

PROCEDURE

To save an existing configuration file offline:

1. With the configuration file opened on Manager, click **File | Save As**.
2. On the **Save As** window, browse to the folder directory in which you want to save the configuration file.
3. Click **Save**.

Configuring the DTE port settings

Access to the DTE port requires a serial cable wired as shown below using D-type plugs. The DTE port on the IP Office Control Unit may be either 25-pin or 9-pin.

IP Office 25-pin	IP Office 9-pin	Signal	PC 9-pin
2	3	Receive Data	3
3	2	Transmit Data	2
4	7	RTS	7
5	8	CTS	8
6	6	DSR	6
7	5	Ground	5
8	1	DCD	1
20	4	DTR	4
22	9	RI	9

An asynchronous terminal program such as HyperTerminal is also required. Configure this for operation via a PC serial port, as follows:

- **Bits per second:** 38,400.
- **Data bits:** 8.
- **Parity:** None.
- **Stop Bits:** 1.
- **Flow Control:** None.
- **Settings | Emulation:** TTY or VT100.

Check the loader version

It may sometimes be necessary to find out the version of Loader software on the IP Office Control Unit.

PROCEDURE

Do the following to view the Loader software version:

1. Switch off power to the IP Office Control Unit.
2. Attach the serial cable between the PC and the DTE port on the IP Office Control Unit.
3. Start the terminal program on your PC. Ensure that it has been setup as listed in "Configuring the DTE Port Settings" above.
    - Within a HyperTerminal session the current settings are summarized across the base of the screen.
4. Power on the IP Office Control Unit and press the escape key every second until you get a ***Loader*** message. Below is an example.

    ```
    P2 Loader 0.7 (4MB-2xLV160 Flash-120nS SDRAM-10)
    CPU Revision 0x0501
    ```

5. To return the IP Office Control Unit to normal operation, switch power to it off and then back on.
6. Close the terminal program session.

Erasing the flash configuration

This process erases the configuration held in the IP Office Control Unit's Flash memory. Following this action, all aspects of the configuration will return to their factory defaults.

Ensure that you have a backup copy of the IP Office's configuration before performing this action.

This procedure should ONLY be performed on IP Office control units and NOT IP Office modules.

PROCEDURE

To erase the configuration:

1. Switch off power to the IP Office Control Unit.
2. Attach the serial cable between the PC and the DTE port on the IP Office Control Unit.
3. Start the terminal program on your PC. Ensure that it has been setup as listed in "Configuring the DTE Port Settings".
    - Within a HyperTerminal session, the current settings are summarized across the base of the screen.
4. Power on the Control Unit and press the escape key every second until you get a ***Loader*** message. Below is an example.

    ```
    P2 Loader 0.7 (4MB-2xLV160 Flash-120nS SDRAM-10)
    CPU Revision 0x0501
    ```

5. Enter **AT** (note upper case). The Control Unit should respond ***OK***.

6. Enter **AT-X2**. The Control Unit should respond ***0x0200C000H Erase***.
7. Enter **AT-X3**. The Control Unit should respond ***0x02001000H Erase.***
8. ***IP Office 403 only:*** If running an IP Office 403 control unit, enter **AT-X4**.
9. Switch power to the Control Unit off and then back on. Within the terminal program you should see various messages as the Control Unit performs various start up tasks. See DTE Port Trace of Defaulted Unit Reboot for an example.
10. Close the terminal program session.
11. Manager can now be used to alter and then upload an old configuration file or receive and edit the Control Unit's now defaulted configuration.

Erasing the Operational Software

Do not perform this process unless absolutely necessary. If you want to upgrade the software, this can be done via the Upgrade tool in the Manager application (**File | Advanced | Upgrade**).

This process erases the operational software and system configuration. Before attempting this process you **must know** the MAC and IP addresses of the system, plus have a backup copy of its configuration and the correct .bin file for the Control Unit type and level of software.

1. Run Manager. In the **BOOTP** entries check that there is an entry that matches the MAC Address, IP Address and .bin file used by the system (the first two details can be found in the **Unit** settings in the system's configuration file).
2. If an entry isn't present, create a new entry. Then close and restart Manager.
3. Under **File | Preferences** ensure that Manager is set to 255.255.255.255.
4. Select **View | TFTPLog**.
5. Check that the required .bin file is present in Manager's working directory.
6. If you do not have the above information. **DO NOT** continue or you may end up with a non working system.
7. Attach the serial cable between the PC and the DTE port on the IP Office Control Unit.
8. Start the terminal program on your PC. Ensure that it has been setup as listed in "DTE Port Settings".
9. Arrange the program windows so that the Terminal program and Manager TFTP Log are visible at the same time.
10. Switch off power to the IP Office Control Unit.
11. Power on the Control Unit and press the escape key every second until you get a ***Loader*** message.
12. Enter **AT** (note upper case). The Control Unit should respond ***OK***.
13. Enter **AT-X**. The Control Unit should respond ***Multi-Sector Erase***.
14. The Control Unit will now request the .bin file it requires from Manager. This process appears in the TFTPLog.
15. When completed the system will reboot.

Sample TFTPLog of a successful transfer:

If you see the following in the TFTPLog, it means the transfer was performed successfully:

```
: Received BOOTP request for 00e007000123 192.168.42.1 ip403.bin
: Sending BOOTP response for 00e007000123 192.168.42.1 ip403.bin
: Sending ip403.bin length 1757520 bytes to 192.168.42.1
: Sent 10% of ip403.bin
: Sent 20% of ip403.bin
: Sent 30% of ip403.bin
: Sent 40% of ip403.bin
: Sent 50% of ip403.bin
: Sent 60% of ip403.bin
: Sent 70% of ip403.bin
: Sent 80% of ip403.bin
: Sent 90% of ip403.bin
: Sent 100% of ip403.bin
: Sent ip403.bin length 1757520 bytes
```

The following in the TFTPLog indicates that the required .bin file is not in Manager's Working Directory. A set of .bin files is available on the IP Office Administration Applications CD in the \bin folder.

```
: Received BOOTP request for 00e007000123 192.168.42.1 ip403.bin
: Sending BOOTP response for 00e007000123 192.168.42.1 ip403.bin
: Unable to send ip403.bin length 0 bytes
```

The following in the TFTPLog indicates that a matching BOOTP entry was not found. If this occurs, use Manager to add or edit the required BOOTP entry.

```
: Received BOOTP request for 00e007000123 192.168.42.1 ip403.bin, unable to
process
```

Hunt Groups

Hunt Group Forwarding Not Working

Issue

Call forwarding from a Hunt Group not working as programmed.

Possible Cause

Forwarding Hunt Group calls is configured on a per Hunt Group member basis. Each Hunt Group member can be configured to have Hunt Group targeted calls redirected to a different number if desired. For Hunt Group calls to be forwarded, the following needs to be in place:

- Forwarding for the Hunt Group member in question must be properly configured.
- The proper Hunt Group ring mode must be defined and the Hunt Group must be **In Service**.

These verification steps are specified below.

Action

I. For the Hunt Group member in question, verify that forwarding options are properly configured.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **User** and double-click the user in question.
3. On the **Forwarding** tab:
   i. Make sure the **Forward Unconditional** check box is checked.
   ii. Check that there is a valid phone number or extension in the **Forward Number** field corresponding to the **Forward Unconditional** check box. If it is an external telephone number, make sure the entire number is entered - including any digits necessary for dialing out (i.e. 9) and area codes if necessary.
   iii. Make sure the **Forward Huntgroup Calls** check box is checked.
4. If any updates have been made and needs to be saved, click  and accept the selected reboot mode by clicking **OK**.

II. For the Hunt Group in question, verify that the Hunt Group specific settings are properly configured.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Hunt Group** and double-click the Hunt Group in question.
3. On the **HuntGroup** tab, check that the **Ring Mode** is set to either **Hunt/Linear** or **Rotary/Circular** mode. The forwarding of Hunt Group calls only work when the Hunt Group ring mode is set to one of these modes.
4. On the **Fallback** tab, check that the **Service Mode** is set to **In Service** because calls will only be forwarded when the Hunt Group is in service.
5. If any updates have been made and needs to be saved, click  and accept the selected reboot mode by clicking **OK**.

III. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Make sure that the user in question is the next Hunt Group member to receive a Hunt Group call and make a call to that group. The call should follow the forwarding number of the user.

Message Waiting Lights Not Displayed When Message is Left for a Hunt Group

Issue

Message waiting light is not displayed when a message is left on a Hunt Group's mailbox.

Possible Cause

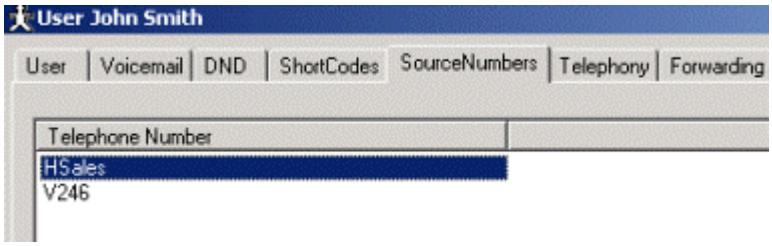
Hunt Group message waiting light is configured for each user individually and will only display when that Hunt Group is configured within the user's source number settings. Specific instructions are outlined below.

Action

I. Each Hunt Group member must be individually configured to receive message waiting indication for Hunt Group messages.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **User** and double-click the user for whom you want to configure message waiting indication for Hunt Group messages.



3. On the **SourceNumbers** tab, there needs to be source number in the form of an **H** followed by a Huntgroup name, i.e. **HSales**, where **Sales** is the name of a Huntgroup. With this configuration setting, the user in question will receive message waiting indication when a message is left in the Sales Hunt Group's mailbox.
    - If no such source number is configured for the user, create one for the Hunt Group in which the user wants message waiting indication for by doing the following:
        i. Right-click within the **SourceNumbers** window and select **Add**.
        ii. In the **Telephone Number** field, enter **H** followed by the name of the hunt group, i.e. **HSales**.
4. Steps 2 & 3 must be repeated for each user requiring message waiting indication for Hunt Group messages.
5. If any configuration changes have been made, click **OK** and then  to save the changes.

II. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Leave a message on the Hunt Group's mailbox and verify that the users in question receive message waiting indication.

Overflowed Calls do not Follow Overflow Group Settings

Issue

When a Hunt Group call goes to the defined Overflow Hunt Group, it does not follow the settings of the Overflow Hunt Group.

Actions

No action is required because the call goes to the Overflow Hunt Group, it is still constrained by the settings of the original Hunt Group. For example, if the Allocated Answer Time/No Answer Time is set to 10 seconds on the original Hunt Group and a call overflows to an Overflow Hunt Group, the call is still constrained by the 10 seconds answer time, regardless of the setting within the Overflow Hunt Group.

Overflow Hunt Group Not Being Activated

Issue

Calls to a Hunt Group with an overflow group configured does not get sent to the overflow Hunt Group.

Possible Cause

If a call cannot be answered by a member of the originating Hunt Group, it can be passed to another Hunt Group called an Overflow Group. The Overflow Group acts as a single extension in the Hunt Group. In order for the overflow group to be activated, an Overflow Group must be defined and at least one member of the overflow group is available to take calls. If queuing is enabled for the originating Hunt Group, then the Voicemail Pro **Queued** and **Still Queued** call flows must not direct the call elsewhere. For calls to the originating Hunt Group to be directed to an Overflow Hunt Group, the following configurations must be in place:

- The overflow settings within the originating Hunt Group must be configured appropriately, including the **Overflow Time**.
- The Overflow Hunt Group members are enabled to take Hunt Group calls.
- If queuing is enabled and a specific start point for the Hunt Group in question is defined within Voicemail Pro, then **Queued** and **Still Queued** call flows must not direct the call elsewhere.
- If queuing is enabled for the default start point within Voicemail Pro, then **Queued** and **Still Queued** call flows must not direct the call elsewhere.
- If queuing is enabled the overflow time must be configured.

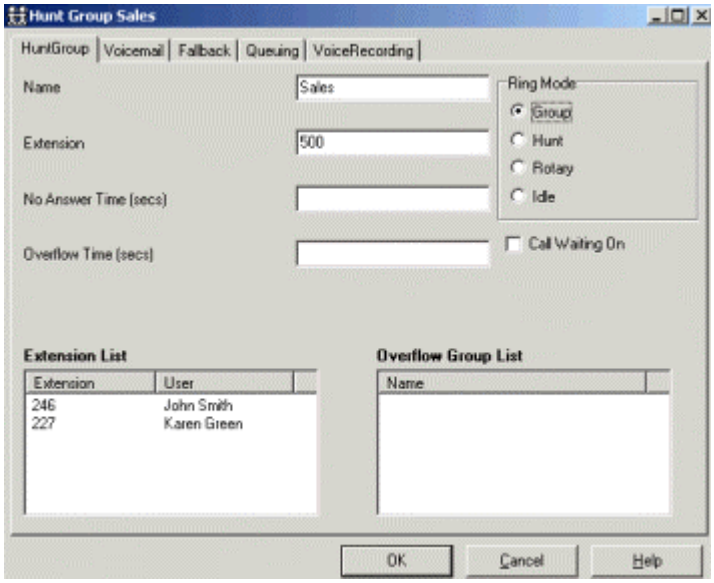
Each configuration is discussed in detail below.

Action

I. Check overflow settings in the originating Hunt Group.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Hunt Group** and double-click the originating Hunt Group.



3. On the **Hunt Group** tab:
   i. Check that there is a Hunt Group name in the **Overflow Group List** and that this is the Hunt Group the customer wants calls to overflow to.

- If there are no Hunt Groups in the list, right-click and select **Add** to add an overflow group.

ii. Check the **Overflow Time** is set appropriately. This setting defines the amount of time (in seconds) a call will ring round the Extension List before being passed to the overflow group. If queuing is enabled for this group, the **Overflow Time** defines the amount of time a caller is held in the group queue before being passed to the overflow group.

iii. Check that Hunt Group members are enabled to take calls. In the **Extension List**, if there is a user with an asterisk (*) next to the extension number, right-click that user and select **Enable**. A Hunt Group member's ability to take calls can be enabled/disabled via this method.

4. On the **Fallback** tab, check that the Service Mode is set to **In Service**.

II. Make sure that callers have waited for the length of time set in the **Overflow Time**.

III. Check the status of the members of the Overflow Hunt Group.

PROCEDURE

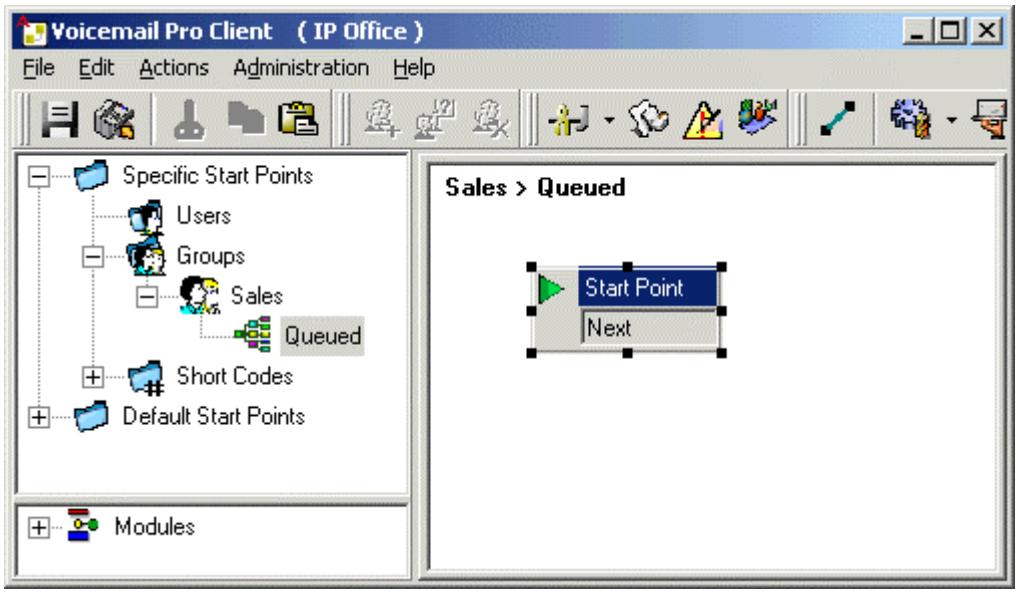
1. Verify that members of the overflow Hunt Group are logged onto their phones.
2. Check that the overflow Hunt Group members are enabled to take calls. In the **Extension List** of the Hunt Group acting as the overflow, if there is a user with an asterisk (*) next to the extension number, right-click that user and select **Enable**.

IV. If queuing is enabled for the Hunt Group in question, check that the **Queued** and **Still Queued** call flows for the Hunt Group in question within the specific and default start points are not directing the call elsewhere. Specific start point for a specific user or group takes preference over a default start point.

PROCEDURE

To check the **Specific Start Points**:

1. Open the system's Voicemail Pro.
2. Double-click **Specific Start Points**.
3. Click the **Queued** call flow. Make sure the call flow is not directing the call elsewhere. The call flow example below is for a Sales Hunt Group. If you have configured a specific start point for a Hunt Group and want should look similar to the following:

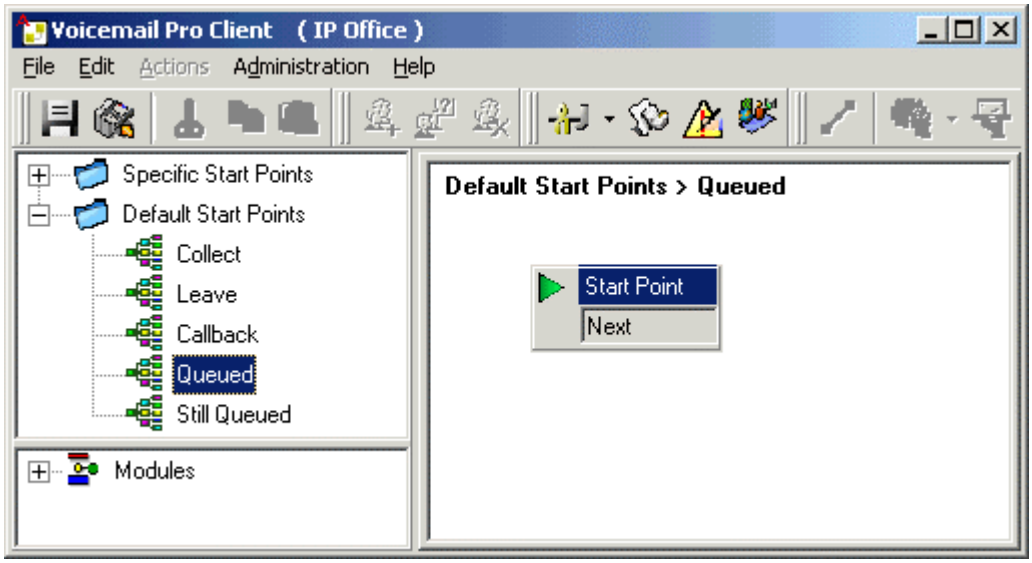


4. Click the **Still Queued** call flow. Make sure the call flow is not directing the call elsewhere.

PROCEDURE

To check the **Default Start Points**:

1. Open the system's Voicemail Pro.
2. Double-click **Default Start Points**.
3. Click the **Queued** call flow. Make sure the call flow is not directing the call elsewhere. The call flow should look similar to the following:



4. Click the **Still Queued** call flow. Make sure the call flow is not directing the call elsewhere.

V. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Make sure all members of the originating Hunt Group are in busy status and make a call to the group. Let the call overflow to the designated overflow Hunt Group.

SCN Users Can Not Contact Hunt Groups at Other Sites

Issue

Users in a Small Community Network (SCN) can not contact Hunt Groups at the remote IP Office sites.

Actions

I. Check that user to user calls between remote IP Office sites can be made to verify VoIP dialing and trunks are working properly.

II. Verify that the remote IP Office site experiencing the problem have short codes configured for the correct IP trunk line numbers with the Hunt Group directory number or prefix included in the Short Code dial string. For example, if Site A has Hunt Group extensions 301, 302 and 303 and an IP trunk with Line Group 10 connecting to Site B in which all calls between the two sites are to be routed, then Site B should have a short code with the following configuration in order to contact those Hunt Groups:

- **Short Code:** 3N
- **Telephone Number:** 3N
- **Line Group ID:** 10
- **Feature:** Dial

With the above short code example, users at Site B can contact all Hunt Groups at Site A with extension numbers starting with 3.

III. Check that there are no duplicate User or Hunt Group extension numbers on and across any of the remote IP Office sites. Duplicate extension numbers cause routing confusion among the networked IP Office sites and should be avoided.

PROCEDURE

To view the list of extensions on an IP Office system:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Extensions**. The list of extensions are displayed on the right hand side of the Manager window.
3. Check this list against the extension list on all IP Office systems on the network.

IV. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Verify that users can dial the Hunt Groups in question.

Voicemail Queuing not Working for Hunt Group

Issue

Calls are ringing at the hunt group, but voicemail queuing will not pick up the call.

Possible Cause

Queuing allows callers to a Hunt Group to be held in a queue when all members of the Hunt Group are busy. Queuing is only supported with a local Voicemail Pro setup and must be properly configured for each Hunt Group. For Hunt Group queuing to function, the following must be in place:

- Voicemail Pro is locally installed i.e. on the same IP Office that the Hunt Group is configured on.
- Queuing is enabled and the ring time is properly configured for the Hunt Group in question.
- The proper user expectations have been set for queuing.

Each verification steps are explained in detail below.

Action

I. Check that Voicemail Pro/Lite is installed and working. Queuing is NOT supported on Embedded Voicemail. To verify that Voicemail Pro/Lite is working, dial the Voicemail access code (***17** is the default access short code).

II. Queuing is only supported for IP Office systems with a local Voicemail Pro/Lite installed. For example, in order for Hunt Groups at site A to have queuing, Voicemail Pro/Lite must also be installed at site A.

III. Check the queue settings for the Hunt Group in question.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Hunt Group** and double-click the Hunt Group in question.
3. On the **Queuing** tab:
   i. Check that the **Queuing On** check box is checked, which means queuing is enabled for this Hunt Group.
   ii. Check that the **Queue Ring Time** is set within the customer's expected time to answer. This setting defines the time (in seconds) before the caller is placed in the queue.
   iii. Check the **Queue Limit** option is set appropriately, i.e. not set to 0, because this field defines the number of calls that is held in the queue at any one time. If this number is exceeded, the caller will hear a busy tone or be passed to Voicemail (if operational). If left blank, it means there is no limit to the number of calls that can be in the queue.
4. If any updates have been made and needs to be saved, click  and accept the selected reboot mode by clicking **OK**.

IV. Verify with the customer that during the time of the incident, there are no available agents in the Hunt Group. Queuing will only take effect if all agents are in a busy state or logged off.

V. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Make sure that all agents belonging to the Hunt Group in question are either in busy status or logged off, then place a call to the Hunt Group and after the allocated Queue Ring Time, call queuing messages should be heard.

IP Routes

Adding IP Route Breaks Connection Between IP Office and Manager

Issue

I have added an IP route to the IP Office configuration and the IP Office no longer communicates with the Manager.

Actions

I. Open the configuration sent to the IP Office offline and review the changes made to verify their accuracy. Offline files are useful for making changes and updates without actually affecting the live system. This means you can save your IP Office configuration file offline, then open it within Manager but still offline, make any necessary changes and when ready, send the configuration to the live system.

PROCEDURE

To open the configuration file offline:

1. Log onto Manager, click the **File** menu and select **Offline|Open File**.
2. Browse to the folder directory where the configuration file is saved and double click the file. The offline configuration file opens within Manager.
3. Verify that all changes you have made to the configuration file including the following:
    - From the Configuration Tree, click **IP Route** and double-click the IP route with the destination defined for LAN 1 or LAN 2. On the IP Route configuration window:
        i. Check with the Network Administrator that the **Metric/HOP Count** defined for the IP route is correct. The Metric/HOP Count defines which route the IP route will use.
        ii. Check that the subnet mask for the IP route is correct based on the IP address for the IP route.
        iii. Check that the gateway IP address is within the same IP subnet as the local IP Office system.
4. Check that there are no duplicate IP routes configured for the IP Office system.
5. Click **OK**.
6. If any updates have been made and needs to be saved, click or choose **File | Save**.

II. When you are ready to send the offline configuration back to the live system via a system Reboot, follow the instructions below. Sending an offline configuration file to the live system will replace your existing live configuration with the new configuration. Make sure that this is what you want to do because you will not be able to revert back to your old configuration unless you have saved a copy offline.

PROCEDURE

To send the offline configuration to the live system:

i. Check the IP addresses on the P.C. against the offline config.

ii. With the offline configuration file opened via Manager, click or choose **File | Save**.

iii. Go to **File** menu, select **Offline | Send Config**. The Manager program scans the LAN for all Control Units.

iv. If only one Control Unit is detected, the **Sending Config To** dialogue box appears - go to step 5 otherwise Manager then offers a list of the Control Units found.

v. Select the Control Unit you wish to send the configuration to.

vi. Enter the System password in the **Sending Config To** dialogue box and select the **Reboot** mode.

vii. Select **OK**. This sends the configuration to the flash memory and reboots the Control Unit to transfer the configuration from the Flash memory to the RAM.

III. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Check that you can open the IP Office configuration on Manager.

Newly Created IP Route Does Not Work

Issue

The newly created IP Route does not work as expected.

Actions

I. Check that the IP Route was configured correctly.

II. Check if RIP is being used or not.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **IP Route** and double-click the IP route in question. On the IP Route configuration window:
    i. Check with the Network Administrator that the **Metric/HOP Count** defined for the IP route is correct. The Metric/HOP Count defines which route the IP route will use.
    ii. Check that the subnet mask for the IP route is correct based on the IP address for the IP route.
    iii. Check that the gateway assigned to the IP routed is valid and online.
2. Check that there are no duplicate IP routes configured for the IP Office system.
3. Click **OK**.
4. If any updates have been made and needs to be saved, click or choose **File | Save**.
5. Reboot the IP Office system to make the changes active. A merge to the system will NOT make the changes active.

II. Via Manager, check that RIP routes is not favoured over Static routes.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **System** and double-click the IP Office system you are configuring.
3. On the System tab, ensure that the **Favour RIP Routes over static routes** field is NOT checked. We want the static route to take preference over any RIP routes.

III. With the assistance of the Network Administrator, check the network topology to ensure routing is correct.

IV. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

After making the changes, ensure that you can now ping to the required destination.

Licenses

Backup License Key

Issue

Customer requires a backup of the license keys for disaster recovery.

Action

Before backing up the license keys, it is good practice to verify that the licenses are valid by doing the following:

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **License**. The list of license keys are displayed on the right-hand-side of the Manager window. The status should all show Valid.
3. If any are invalid, see Licenses Show Invalid or Unknown.

II. After verifying the validity of all license keys, export them by doing the following:

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. Click the **File** menu and select **Import/Export|Export Configuration Entities**.
3. A **Enter export details** window displays. Select **License** from the list of configuration forms.
4. The default file directory for saving the backup license is within the Manager folder. If you want to save backup elsewhere, click the Browse button to navigate to the desired file directory.
5. The default file name is config.exp. The file name can be amended, but the file extension must remain **.exp** in order for the system to recognize it when the file is imported.
6. Click **OK** to complete the export procedure.

III. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Navigate to the location where the backup license keys are stored and verify that it is there.

Existing Licenses are Invalid Upon Opening or Merging System Configuration

Issue

Existing license keys are shown as invalid upon opening or merging the system configuration.

Possible Causes

License keys are unique and tied to the serial number of the Feature Key (also known as a license key or dongle) plugged into a Feature Key Server PC on the network. The address of the Feature Key Server PC (also known as License Key Server) is set through the **System** form.

New and altered license keys are not validated against the Server PC's Feature Key until after a Control Unit reboot. Following a Feature Key Server PC reboot, it will only communicate with the first IP Office Control Unit that contacts it.

For license keys to continue functioning, the following must be kept in mind:

- IP Office - Small Office Edition and the IP Office 412 control unit also support a direct plug-in of serial license keys.
- Feature key must be properly installed on the PC supporting the feature key and the PC must be running.
- The PC supporting the feature key must be able to communicate with the IP Office control unit.

Each of these verification issues are discussed in detail below.

Action

I. Check that the PC supporting the feature key is running then proceed to the third action item. If the customer has an IP Office - Small Office Edition or an IP Office 412 control unit, see the second action item below.

II. If the customer has an IP Office - Small Office Edition or an IP Office 412 control unit, a serial license key can be plugged directly into these control units. If this is the case, check that the serial license dongle is plugged snugly into the correct serial port and the license server IP address is defined properly.

III. Check that if using an a PC that either the parallel or USB dongle is connected correctly.

III. On the PC supporting the feature key, verify the following:

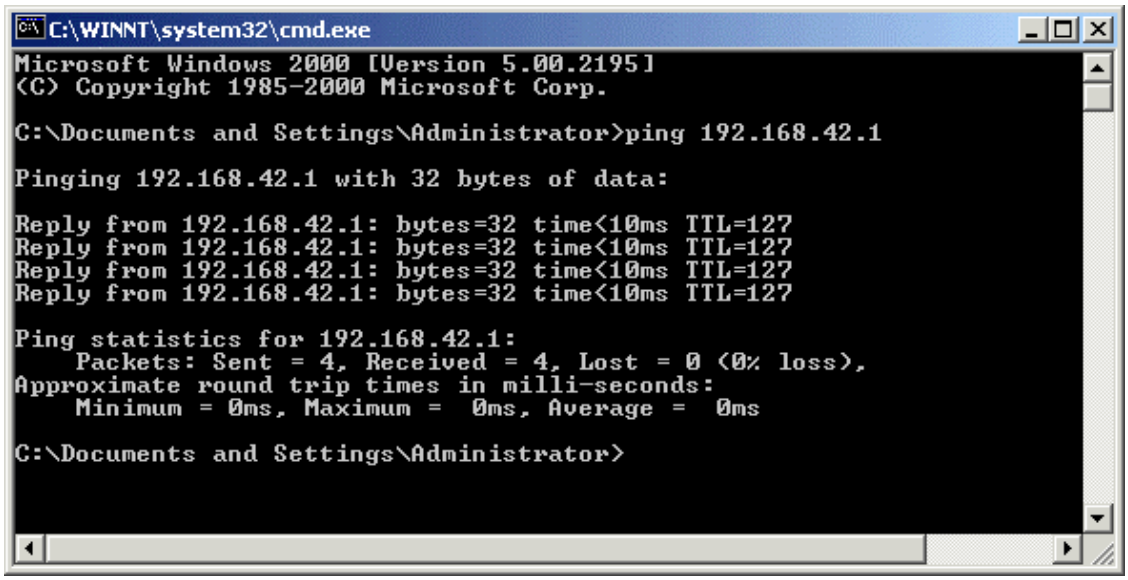
PROCEDURE

Check that the feature key is validated in the tool tray on the PC's task bar. The tool tray typically resides to the left of the clock on your PC monitor. An example is provided below:

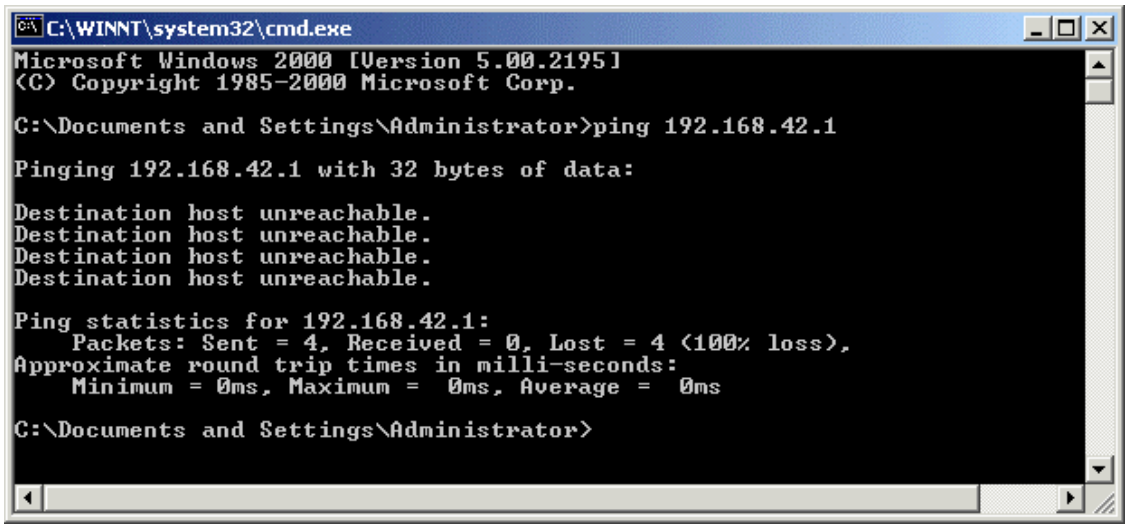
- If there is a  (red feature key icon) is displayed, it means the feature key (dongle) is connected properly in the back of the PC and is working.
- If the icon is white with a red cross through it  , it means the feature key (dongle) is not connected properly or not working. Check that the feature key is connected properly to the back of the PC before continuing with the troubleshooting procedures.

2. Check that there is a network connection light on both the IP Office and the PC's Network Interface Card (NIC).

3. Verify that the PC supporting the feature key can ping the IP Office control unit. (If the PC supporting the feature key is not directly connected to the IP Office LAN ports, seek the advice from the customer's IT department to help test the network.)
   i. From the **Start** menu of the computer running Manager, select **Run**.
   ii. Enter **cmd** in the text box.
   iii. In the Command Prompt window, type **ping xxx.xxx.xxx.xxx** (where x = IP address of the IP Office control unit).
   iv. A message similar to the following should appear:



   v. If a message similar to the following appears and you have performed all the verification checks relating to this issue, then contact T3 support:



4. Check that the **Key Server** service is running.
   i. On the PC supporting the feature key, go to the Windows **Start** menu and select **Settings|Control Panel**.
   ii. Double-click **Administrative Tools**.
   iii. Double-click **Services**.
   iv. Find the **Key Server** service and check that it has a **Started** status.
      - If the service is started, right-click it and select **Stop** and then **Restart**. This will ensure that the service is running.
      - If it is not started, right-click the service and select **Start**.

PROCEDURE

If there are more than one IP Office systems on the network (same subnet) with either a broadcast address of 255.255.255.255 or a direct match to the IP address of the key server PC in the **System | License Server IP Address** field, the key server will assume that there are two IP Office systems attempting to use the same license key. This can cause licenses to go invalid.

To check the license server IP address configuration:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **System** and double-click the system in question.
3. On the **System** tab, verify that the **License Server IP Address** field is blank (if using a serial dongle and a specific IP address if using a license server with parallel or USB dongle)
4. Click **OK**.
5. If any configuration updates have been made, click  and accept the selected reboot mode by clicking **OK**.

PROCEDURE

After performing the above troubleshooting steps, merging the license information back to the system can sometimes trigger the licenses to validate. To trick the system into thinking that new license information has been entered and requiring a merge, do the following:

To check the license server IP address configuration:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **License** and double-click on a license.
3. The License window appears displaying the license string. Click **OK**. This makes the system think that new license information has been entered.
4. Merge the "update" back to the system by clicking  and selecting the **Merge Config** option. Click **OK**.

IV. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Check within the Licenses configuration form that all licenses are valid and the application is working.

IP Office License Issues

License keys are unique and tied to the serial number of the Feature Key plugged into a Feature Key Server PC on the network. The address of the Feature Key Server PC (also known as License Key Server) is set through the **System** form.

New and altered license keys are not validated against the Server PC's Feature Key until after a Control Unit reboot. Following a Feature Key Server PC reboot, it will only communication with the first IP Office Control Unit that contacts it.

Newly Added Licenses Show Invalid or Unknown

Issue

New licenses added show invalid or unknown.

Possible Causes

License keys are unique and tied to the serial number of the Feature Key (also known as a license key or dongle) plugged into a Feature Key Server PC on the network. The address of the Feature Key Server PC (also known as License Key Server) is set through the **System** form. If the customer is running the IP Office - Small Office Edition or the IP Office 412, a serial license key can also be plugged directly into these control units.

New and altered license keys are not validated against the Server PC's Feature Key until after a Control Unit reboot. Following a Feature Key Server PC reboot, it will only communication with the first IP Office Control Unit that contacts it.

The most common cause for this issue is that the wrong license key number was entered. The EXACT license key number must be entered. Because of certain ambiguities, such as the difference between the letter O and the number 0, it is highly recommended that license key number is copied from its original form and pasted into proper field within Manager.

Actions

I. Check the license keys against those on the Excel spreadsheet key generator provided a the time of license purchase.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **License** and double-click the license key in question.
3. A **License** window opens with the license string that was entered for the particular application/feature. Check this license string against the one on the Excel spreadsheet. The two license strings need to match exactly.
4. If there is any doubt that the license string in Manager is incorrect, copy the license string from the Excel spreadsheet and paste it into the **License String** field on Manager.
5. Click **OK**.
6. Click  and accept the selected reboot mode by clicking **OK**. New and altered license keys are not validated against the Server PC's Feature Key until after an IP Office Control Unit reboot.

II. Follow resolution procedures in Existing Licenses are Invalid Upon Opening or Merging System Configuration.

III. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

After the reboot, open the license configuration form again and check for valid licenses.

Restore License Keys

Issue

Customer requires a restore of the license file for disaster recovery.

Action

I. If a backup of the license keys have been made, importing the file into the working Manager configuration can be performed by doing the following:

1. Log onto Manager and open the IP Office configuration.
2. Click the **File** menu and select **Import/Export|Import Configuration Entities**.
3. In the Look in drop down box, navigate to where the backup file is stored.
4. Double-click the .exp file.
5. Click  and accept the selected reboot mode by clicking **OK**.

II. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

After sending the configuration back to the IP Office, log back onto Manager, open the License configuration form and make sure the license keys are valid.

System

Control or Expansion Units Rebooting Constantly

Issue

The main IP Office control unit or expansion modules are rebooting constantly.

Actions

The following troubleshooting steps can be applied to both the control unit and expansion module.

I. Check for power supply failures or a faulty power brick by plugging a multi-meter instrument onto the power supply.

II. For the control unit or expansion module in question, disconnect the power supply for 30 seconds and then reconnect it. This action will eliminate any residual power that may remain on the control unit or expansion module.

III. Replace Power Supply Unit as precaution to the unit rebooting.

Actions

The following troubleshooting steps will verify problems on the expansion module.

I. If the expansion module is not connected properly to the IP Office control unit, this can cause the module to reboot. Therefore, it is a good idea to check that the TDM cable (blue cable) connecting the expansion module to the control unit is connected properly and working. To confirm the connection, check that the LED lamp on the front of the expansion unit is lit.

II. To rule out faulty hardware as the cause, try the expansion module in question in another expansion slot (if a free one is available) by doing the following:

1. With one end of the TDM (blue) cable plugged into the expansion slot of the expansion module, unplug the other end of the cable from its existing expansion slot on the control unit and plug it into another slot.
2. If the module stops rebooting, then it most likely means the faultiness lies with the expansion slot rather than the expansion module itself.

III. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

The main IP Office control unit or expansion modules stop rebooting and the system is functioning as expected.

Manager Application Not Contacting the IP Office System

Issue

The Manager application does not recognize the IP Office System.

Possible Causes

Manager is a Windows application for viewing and editing the configuration file of IP Office Control Units.

The Control Unit holds the configuration as files in the Control Unit's flash memory. Thus the files are not lost when power is removed from the system. Whenever the system is rebooted, the file is loaded from flash memory into the systems RAM memory.

The most likely cause for Manager not contacting the IP Office control unit is network-related configurations and settings. Depending on whether the PC running Manager is directly connected to the IP Office control unit or it is remotely connected, the verification steps vary slightly. Thus, the suggested actions taken to resolve the issue are divided into those two headings below.

Actions for Directly Connected Systems

If the PC running Manager is directly connected to the IP Office, do the following:

I. Verify that the computer running Manager has a static IP address and the address is within the IP range and subnet range that the IP Office control unit is configured with. The two IP addresses need to be on the same network. For example, if the IP and subnet range of the IP Office control unit is **192.168.42.1** and **255.255.255.0** respectively, then the IP address of the computer running Manager should be within the range **192.168.42.2** to **192.168.42.254**.

Procedure

To check and update the IP address of the computer running Manager:

Right-click **My Network Places** and select **Properties**.

Right-click **Local Area Connections** and select **Properties**.

Select **Internet Properties (TCP/IP)** and click **Properties**.

With **Use the following IP address** selected, the fields for IP address and Subnet mask is available for editing. Make the necessary changes based on IP range of the IP Office control unit.

Click **OK**.

II. Check the default gateway programmed on the Manager computer. The default gateway is normally the IP Office. If it is not check with your IT administrator what the Default Gateway on the network should be.

Procedure

To check and update the default gateway of the computer running Manager:

1. Right-click **My Network Places** and select **Properties**.
2. Right-click **Local Area Connections** and select **Properties**.
3. Select **Internet Properties (TCP/IP)** and click **Properties**.
4. With **Use the following IP address** selected, the **Default Gateway** field is available for editing. The default gateway should be the IP Office. Make the necessary updates.
5. Click **OK**.

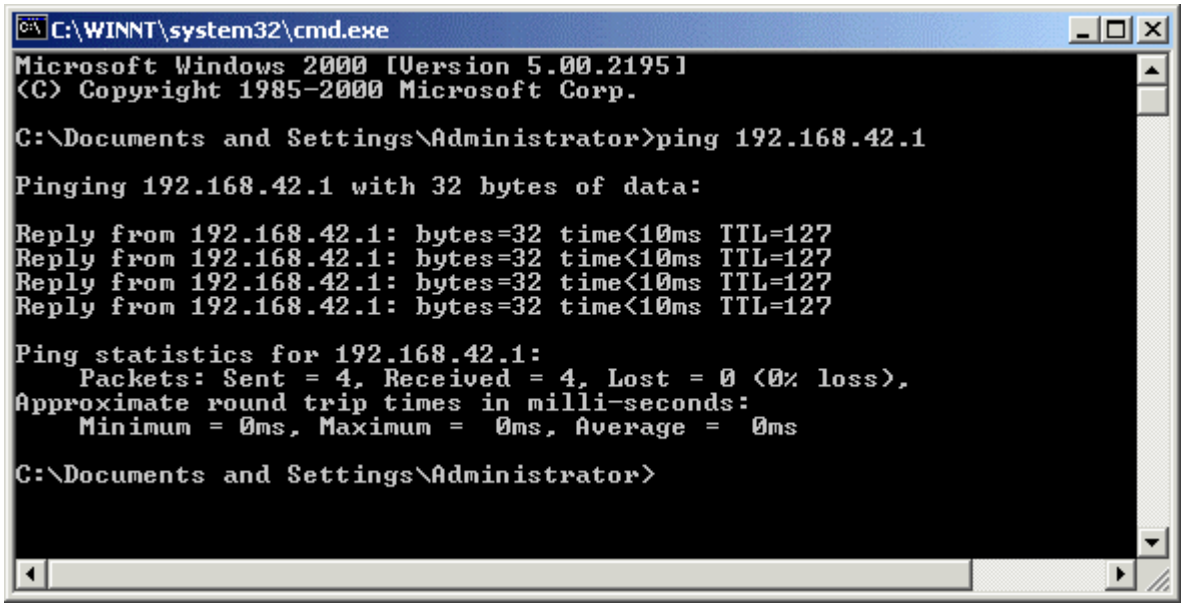
III. Ensure that the PC running Manager is connected directly into the LAN port on the IP Office and remove any other network connections temporarily from the IP Office LAN port to negate conflicts.

IV. Check that there is a network connection light on both the IP Office and the computer's network interface card (NIC).

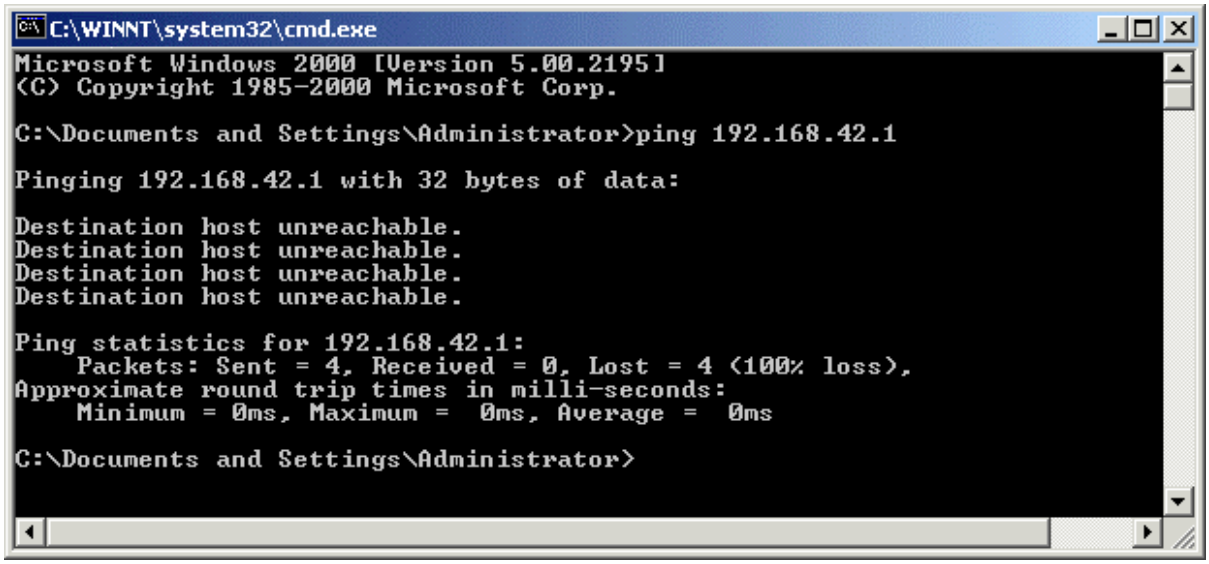
V. Check you can ping the IP Office's IP address.

Procedure

1. From the **Start** menu of the computer running Manager, select **Run**.
2. Enter **cmd** in the text box.
3. In the Command Prompt window, type **ping xxx.xxx.xxx.xxx** (where x = IP address of the IP Office control unit).
4. A message similar to the following should appear:



5. If a message similar to the following appears and you have performed all the verification checks relating to this issue, then contact T3 support:



VI. Check the **Preferences** setting on Manager. There should be one set to 255.255.255.255.

Procedure

1. Log onto Manager.
2. Click **File|Preferences**.
3. There should be a **255.255.255.255** (a broadcast address) setting configured.
4. Select this IP address.

VII. Reboot the Manager PC.

VIII. If the connection to the IP Office still cannot be made, the system will require a DTE configuration clear. See DTE Port Maintenance.

IX. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Actions for Networked Systems

If the PC running Manager is connected to the IP Office over the network (with a router or switch in-between) or is remotely connected, do the following:

I. Check the default gateway programmed on the Manager computer. The default gateway should be the router or the IP Office control unit.

Procedure

To check and update the default gateway of the computer running Manager:

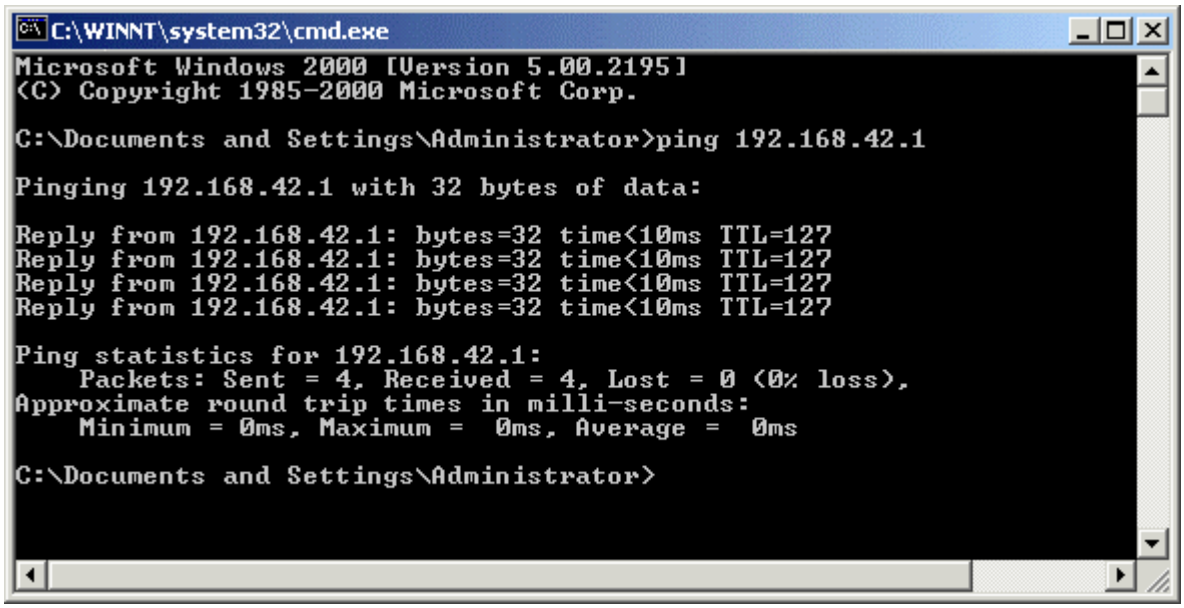
1. Right-click **My Network Places** and select **Properties**.
2. Right-click **Local Area Connections** and select **Properties**.
3. Select **Internet Properties (TCP/IP)** and click **Properties**.
4. With **Use the following IP address** selected, the **Default Gateway** field is available for editing. Make the necessary updates.
5. Click **OK**.

II. Check that there is a network connection light on both the IP Office and the computer's network interface card (NIC).

III. Check you can ping the IP Office's IP address.

Procedure

1. From the **Start** menu of the computer running Manager, select **Run**.
2. Enter **cmd** in the text box.
3. In the Command Prompt window, type **ping xxx.xxx.xxx.xxx** (where x = IP address of the IP Office control unit).
4. A message similar to the following should appear:



5. If you are unable to ping the remote IP Office system, contact the site's IT manager because there could be a firewall preventing you from pinging the system even when you are connected to it.

IV. Check the **Preferences** setting on Manager. There should be one set to the IP address of the IP Office control unit you are managing.

Procedure

To enter the IP address of the IP Office control unit:

1. Log onto Manager.
2. Click **File|Preferences**.
3. Select the IP address of the IP Office control unit you are managing. Select **File|Close** to close the previous system configuration and click to open the configuration for the newly defined IP Office control unit.
4. If the IP address is not listed, do the following:
   i. Select **Edit** and enter the IP address of the IP Office control unit in question. Leave the other configuration fields at their default.
   ii. Click **OK**.
   iii. Select **File|Close** to close the previous system configuration.
   iv. Click to open the configuration for the newly defined IP Office control unit.

V. If the connection to the IP Office still cannot be made, the system will require a DTE configuration clear. See DTE Port Maintenance.

VI. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Use the following procedure to verify that Manager can contact the IP Office system.

Procedure

1. From the **Start** menu of the computer running Manager, select **Run**.
2. Enter **cmd** in the text box.
3. In the Command Prompt window, type **ping xxx.xxx.xxx.xxx** (where x = IP address of the IP Office control unit).
4. The following message should appear:
5. Go to Manager and open a configuration by clicking and entering the system password.

Remote System Displayed Within My Configuration

Issue

When I open the configuration for the system I'm configuring, the remote IP Office systems are displayed.

Action

No action is required; this is an expected IP Office system interaction. Any IP Office control units on the same LAN/subnet will display in each configuration when accessed via Manager.

Unable to Load Bin Files After DTE Reset

Issue

The IP Office is unable to load the working Bin files after a DTE reset of the system.

Possible Cause

When the operating software has been deleted from the IP Office control unit using the DTE commands, the IP Office will attempt to load a new firmware image over the Ethernet (LAN1) using BOOTP (Bootstrap Protocol) from a suitable system - typically the PC running Manager. For the firmware to load successfully, the first verification step is to ensure that PC running Manager and the IP Office must be directly connected with a valid LAN cable and the link state LED must be on for both the Manager PC and the IP Office. After this is verified in the positive, the following must also be in place:

- A valid BOOTP entry must exist in Manager.
- Manager must be setup with the broadcast IP address.
- Manager's directory setting must be correctly set to where the image/bin file resides.
- The PC running Manager must have a valid IP address that is in the same subnet as the IP Office - a static address is recommended.

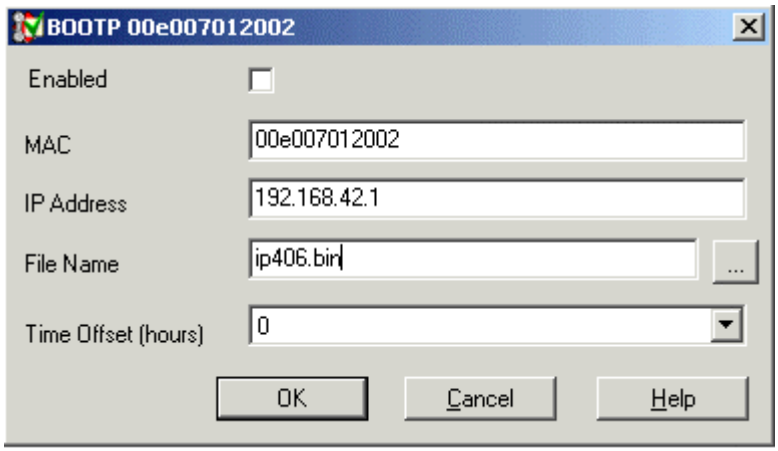
Each of these verifications are discussed in detail below.

Action

Via Manager, check the options in the BOOTP entry.

Procedure

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **BOOTP** and double-click the BOOTP of the system in question. The number of BOOTP displayed is dependent upon the number of IP Office systems the PC running Manager is connected to. A BOOTP window similar to the following is displayed:

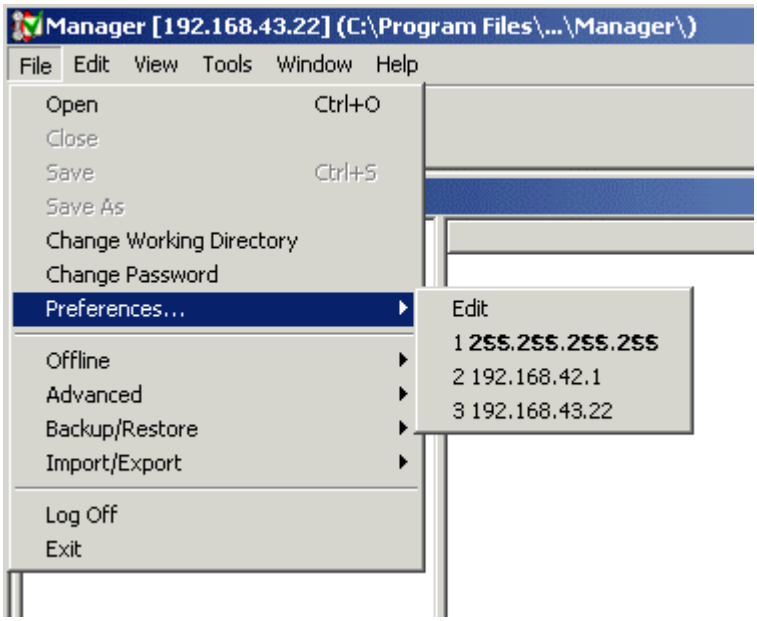


3. Verify that the BOOTP entry is enabled via the **Enabled** check box.
4. Check that the MAC address of the IP Office is accurate. This number is the same as the serial number displayed in the Unit configuration form. Alternatively, the MAC address can be found on Manager by clicking **View|TFTPLog**.
5. Check that the correct IP address for TFTP is entered in the **IP Address** field. In most scenarios, the IP Office control unit is the TFTP server.
6. In the **File Name** field, check that the correct file name for the system bin file is entered. It should be one of the following:
    - ip401ng.bin

- ip403.bin
- ip406.bin
- ip412.bin
- ip406v2.bin

7. Check that the **Time Offset** field is set to **0**. This field defines the offset between the PC time and the time sent to the IP Office system in response to a time request.

II. Check the **Preferences** setting on Manager by clicking **File|Preferences**. If the broadcast address of **255.255.255.255** is not in bold, then select it. This configures Manager with the broadcast IP address. Below is an example of the Preferences selection:



III. Check that the binary directory (bin files) of the Manager program is directed to the location of the IP hard phone bin files. Bin files are stored in the root of the Manager directory, so the binary files' directory needs to point to the Manager directory.

Procedure

To verify the directory location (and update it if necessary):

1. Log onto Manager.
2. Click **File|Change Working Directory**. A **Select Directory** window appears.
3. In the **Binary Directory (.bin files)** field, make sure that it contains the file path of where the Manager application was installed. If it does not, click the Browse icon to the right of the text box to browse to the correct location.
4. Click **OK**.

IV. Verify that the computer running Manager has a static IP address and the address is within the IP range and subnet range that the IP Office control unit is configured with. The two IP addresses need to be on the same network. For example, if the IP and subnet range of the IP Office control unit is **192.168.42.1** and **255.255.255.0** respectively, then the IP address of the computer running Manager should be anywhere between **192.168.42.2** to **192.168.42.254**.

Procedure

To check and update the IP address of the computer running Manager:

1. Right-click **My Network Places** and select **Properties**.
2. Right-click **Local Area Connections** and select **Properties**.
3. Select **Internet Properties (TCP/IP)** and click **Properties**.
4. With **Use the following IP address** selected, the fields for IP address and Subnet mask is available for editing. Make the necessary changes based on IP range of the IP Office control unit.
5. Click **OK**.

VI. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Load the bin files again.

User Account Configurations Have Reverted Back to the Defaults

Issue

The programming changes, such as button programming, user specific short codes, etc., made to a user's account have reverted back to their default settings.

Actions

I. Some telephones have the capability to make certain configuration changes directly. Hence, it is a good idea to check that the user has not made those configuration changes in question.

II. If the changes have been made via Phone Manager, which means those changes have only been saved to IP Office's RAM memory and will not be copied to flash memory until midnight unless you have received and sent a copy of the config. Prior to a power failure before midnight (default time when information in flash memory is copied to RAM), the changes will not have been copied to RAM memory and will be lost because when the IP Office system comes back on, it gets its files from the flash memory. The quickest way to see if the IP Office system has rebooted recently is via the System Monitor application.

PROCEDURE

To use the System Monitor application:

1. On the PC running Manager, click the Windows **Start** icon and select **Programs|IP Office|Monitor**.
2. At the beginning of the System Monitor window, look for a line similar to the following:

   ```
   System (192.168.42.1) has been up and running for 8mins and 27secs(507748mS)
   ```

   This information will give you a good indication of whether or not the system has lost power or rebooted unexpectedly.

III. Check that there is only one instance of the IP Office system being configured at any one time. If there are more than one configuration being performed at the same time, configuration updates will get overridden.

IV. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Reprogram the features, open a new configuration and merge it back to the IP Office.

User Numbers are Not in the Correct Order

Issue

Users' extension numbers are not in the correct order or the expansion module does not seem to work.

Actions

I. When an expansion module is properly connected to an IP Office control unit, the control unit automatically detects the module and creates user numbers accordingly. For example, when the first module is connected to a control unit, the system creates the first set of relevant users with extensions 201 onwards (i.e. the last extension number for a module with 30 extension ports is 231); when the second module is connected, the user numbering continues from 232 onwards.

If an expansion module is already connected and the users configured, then the module is disconnected and re-connected via a different expansion slot on the control unit, the system will not delete the existing user numbers; therefore, it will automatically create the next set of user numbers and the existing users will not have any of the same extensions or user settings as before.

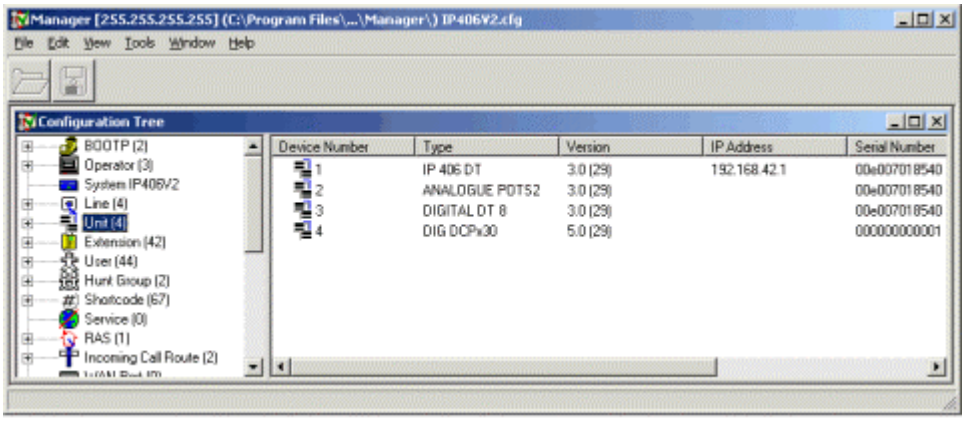
PROCEDURE

If you are replacing one expansion module (i.e. a DS module) with another (i.e. an analog module), the proper procedure for replacing the two must be performed to ensure that the system detects it and the correct user extensions are created. To properly replace an expansion module:

Delete the old module from the list of units.

i. Log onto Manager and open the IP Office configuration.

ii. Click **Units** from the Configuration Tree. A list of modules that have been connected to the control unit is listed. This list includes all modules (even those that have been disconnected or powered down) that have ever been connected to the unit. The system does not automatically update this list when a module is removed. A sample list is provided below.



iii. Right-click the expansion module to be removed and select **Delete**.

2. Click **Extension** from the Configuration Tree. The list of all extensions are listed. Delete all the extensions relating to the old module.
3. Power up the new module and connect this module to the IP Office control unit. A list of new extensions and users are automatically created.
4. Power cycle/reboot the IP Office control unit.

5. Delete the list of new users created because you want to retain the existing users and their settings.
6. Map the existing users to the new extensions.
7. Power cycle/reboot the IP Office control unit.

II. If the IP Office configuration was configured using the Wizard application, the port assignment of the expansion module is defined during the configuration process. If the hardware setup does not mimic the configuration setting, this can cause discrepancies with extension numbering and expansion module settings. The quickest way to resolve the discrepancy is to:

1. Reconnect the modules into the appropriate port based on what was defined in Wizard.
2. Power cycle/reboot the IP Office control unit.

III. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

The user numbering should be as expected and all users are able to make and receive calls.

System Upgrade

IP Office Does Not Reboot or Goes into a Reboot Loop After a System Upgrade

Issue

The IP Office does not reboot or goes into a reboot loop after a system upgrade.

Actions

If you experience this issue, then the upgrade has not been successful. You must perform the upgrade again. Before performing an upgrade, it is critical that you keep the following issues in mind:

- Follow the pre-upgrade checks and upgrade instructions below because certain IP Office control units and software levels require additional steps and procedures.
- It is highly recommended that when the IP Office control unit software is upgraded, the Manager application is upgraded as well.

Pre-Upgrade Checks

I. Check the network connection between the PC running Manager and the IP Office. Are the two on the same LAN segment?

- This verification step is critical if the IP Office system is running software version 2.0 or older because there will be no validation of the existence of a system software before the old software is erased from the system memory. If the IP Office system and/or Manager is running software version 2.0 or older, make sure the Manager PC and the IP Office are on the same LAN segment and the upgrade is not being performed across WAN or RAS links.
- If the customer's site is running Manager 2.1 or newer and IP Office 2.1 or newer, then a **Validated Upgrade** is available. With a validated upgrade, it is not required that the Manager PC and the IP Office are on the same LAN segment.

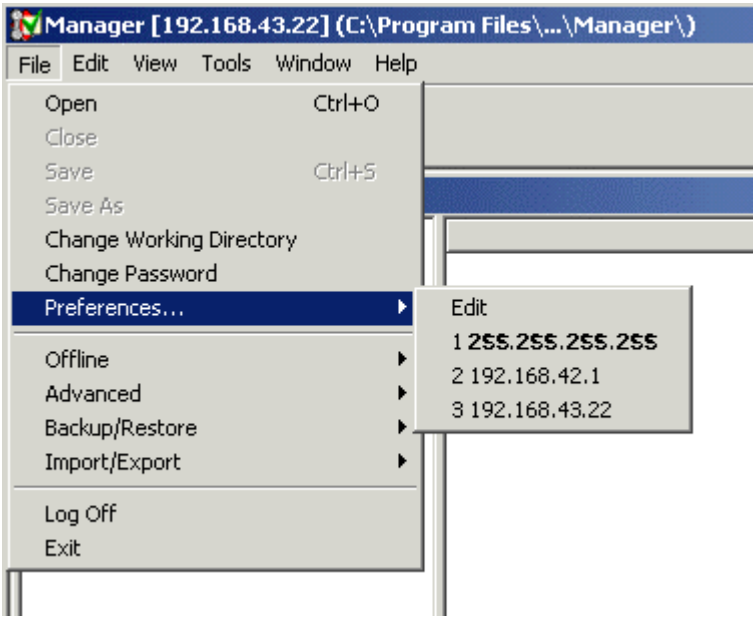
II. Ensure that the Manager PC has a fixed (static) IP address. This address should be on the same subnet as the IP Office control unit with the subnet mask set correctly.

III. Test the broadcast routing between the Manager PC and IP Office by setting the **Preferences** to **255.255.255.255** and check that Manager can receive the configuration from the IP Office being upgraded.

PROCEDURE

To check the Preferences setting:

1. Log onto Manager.
2. Click **File | Preferences** and select **255.255.255.255**.



3. Open the configuration of the IP Office being upgraded. If Manager is successful at receiving the configuration, it means the broadcast routing is working correctly.

IV. Check that the Manager program's binary directory is pointing to the folder containing the bin files. Bin files are stored in the root of the Manager directory, so the binary files' directory needs to point to the Manager directory.

PROCEDURE

The directory is shown in the Manager's title bar and can be set by doing the following:

1. Log onto Manager.
2. Click **File|Change Working Directory**. A **Select Directory** window appears.
3. In the **Binary Directory (.bin files)** field, make sure that it contains the file path of where the Manager application was installed. If it does not, click the Browse icon to the right of the text box to browse to the correct location.
4. Click **OK**.

V. Obtain the .bin files. If the Manager application has already been upgraded, then the appropriate .bin files are already copied to Manager's binary directory (default = c:\program files\avaya\ip office\manager). A set of .bin files can also be found in the \bin folder on the IP Office Administration CD.

VI. Make a copy of the current configuration file by saving it offline before performing the upgrade. If the upgrade fails, the current configuration may be erased so a backup copy is an essential precaution.

PROCEDURE

To save an existing configuration file offline:

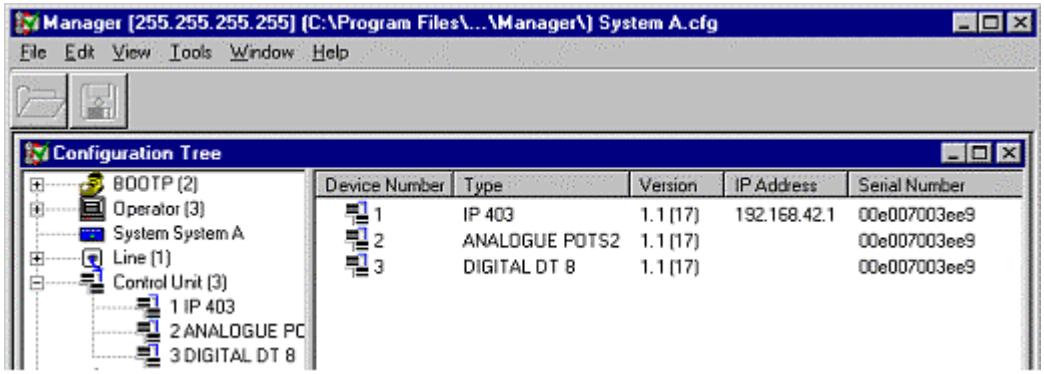
1. With the configuration file opened on Manager, click **File | Save As**.
2. On the **Save As** window, browse to the folder directory in which you want to save the configuration file.
3. Click **Save**.

VII. Where several IP Offices are connected in a voice and/or data network, they should all be running the same level of software.

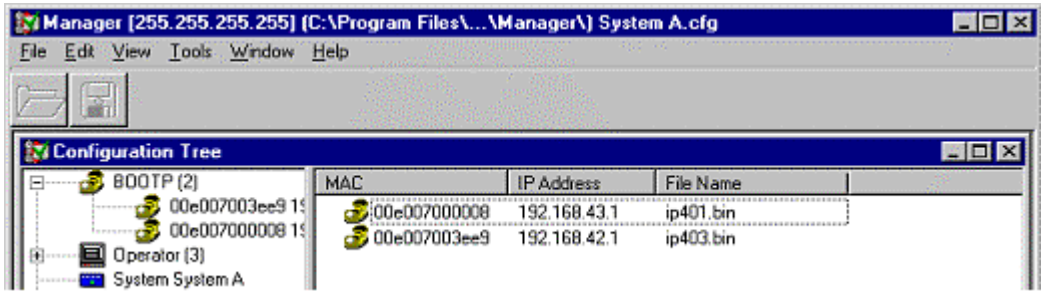
VIII. Check the Manager **BOOTP** entries. BOOTP is part of the process by which the IP Office restarts and requests new software. The Manager PC acts as the IP Office's BOOTP server and must have a BOOTP entry for the IP Office.

To verify the BOOTP entries:

1. Log onto Manager and receive the IP Office configuration.
2. Click **Control Unit** to display a list of units in the system. The list of units should look similar to the screenshot below.



3. Device Number 1 is the Control Unit (i.e. IP401, IP403, IP406 or IP412). Note its type, software version, IP address and the serial number. The **Serial Number** is the Control Unit's MAC address.
4. Click **BOOTP** to display a list of BOOTP entries. There should be one for every IP Office ever configured from the Manager PC. Check that the list includes the MAC and IP address of the Control Unit you want to upgrade and that the **.bin** file listed matches the Control Unit's type.



5. If an entry does not exist right-click the displayed list and select **New**. Enter the required details and click **OK**. You do not need to send the configuration back to the IP Office as BOOTP entries are stored on the Manager PC.
6. Double-check the entry as this is a critical setting for the upgrade process.

Upgrading IP Office and Manager

If you are running IP Office and Manager 2.1 or newer, a validated upgrade is available through the Upgrade Wizard within the Manager interface. To invoke a validated upgrade, the **Validate** box on the Upgrade Wizard must be checked (default) before performing the upgrade. With the **Validate** box checked, the system will check that it has received the new .bin files and then give you the option to upgrade. If you uncheck the **Validate** box, a validated upgrade will not be performed. The validated upgrade function can be performed on both a remote and local upgrade.

If you are running Manager 2.0 or older, the **Validate** box and hence the remote upgrade functionality is not available. If you are running Manager 2.1 but the control unit is still running IP Office 2.0, a validated upgrade will not be available and the **Validate** box will be grayed out on Manager.

I. Follow the **Pre-Upgrade Checks**.

II. Remove the existing **IP Office Admin Suite**. When upgrading an IP Office system from one core software level to another, the recommended process is to upgrade all existing IP Office application software as well. This is done by un-installing and then reinstalling the software. The un-install process below only removes those files installed during each applications original installation. Any other files added since (user files, system configurations files, voicemail messages, etc.) are not removed.

PROCEDURE

To un-install the **IP Office Admin Suite**:

1. Open the Windows Control Panel (**Start | Settings | Control Panel**).
2. Select **Add/Remove Programs**.
3. Select **IP Office Admin Suite**.
4. Click **Add/Remove**.
5. From the options offered select **Remove**. This process only removes those files installed during the application suites original installation. Any other files added since (user files, system configurations files, voicemail messages, etc.) are not removed.
6. Follow any prompts given during the removal process.
   - **Note:** The removal of some applications (for example TAPI, Feature Key Server, etc) will require the PC to be rebooted.
7. Click **OK** to finish and close the Control Panel.
8. The new versions of the application suites can now be installed.

III. Install the new application suite.

PROCEDURE

To install the **IP Office Admin Suite**:

1. Insert the **Administrator CD** into the PC's CD drive. The CD autoruns. You are initially presented with the option to select which language you wish to use. Select the language from the pull down list and click **OK**.
2. The **Destination** folder location option menu is displayed. Either accept the default location (click **Next**) of where the **Administration Suite** is to be installed or change the location by clicking **Browse** and entering a new location.
3. Select which components you wish to install by selecting the appropriate boxes and click **Next**.
4. Name the program folder or accept the default (**Manager**), click **Next** and wait for the Administration Suite installation to be completed.
5. Installation runs and on completion select **Restart now** and click **Finish** twice.

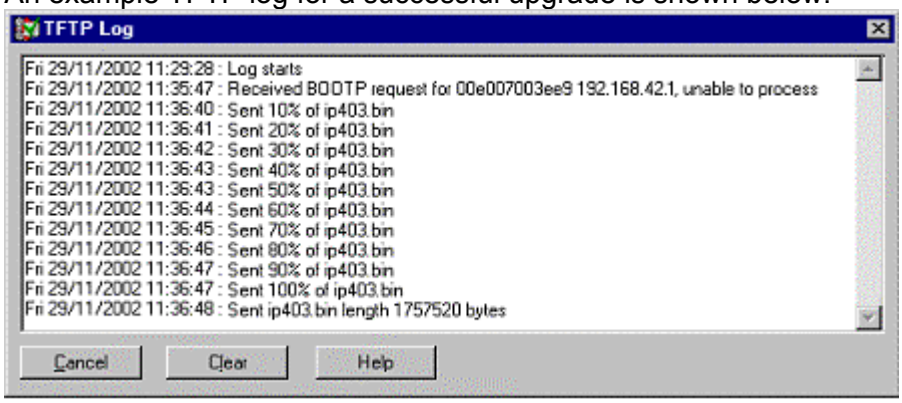
IV. With all the necessary files in the proper directory on the Manager PC, perform the upgrade.

PROCEDURE

To start the upgrade:

1. Log onto Manager.
2. Click **File | Advanced | Upgrade**. The Upgrade Wizard window opens.

3. The wizard lists the Control Units and Expansion Modules found.
   - **No Units Listed**
     If this occurs using the Broadcast Address of 255.255.255.255 it implies that the Manager PC is not connected to any local IP Office units. At this point, you should enter the specific IP address of the unit you wish to upgrade or check the network settings.
4. The list shows the current software level of the units and the level of the appropriate bin file it has available for each unit from those in the Manager's working folder.
5. Check the boxes for those control units that you want to upgrade.
6. If you are running Manager 2.1 or later, a **Validate** box will be available and checked by default. Leave the box checked if the control unit you are updating is currently running IP Office 2.1 or later because this will perform a validated upgrade. If the control unit you are updating is currently running IP Office 2.0 or earlier, the **Validate** box will be grayed out.
7. In Manager select **View | TFTP Log**. This will allow you to see the file transfer processes. Arrange the windows so that you can see both the TFTP Log and the UpgradeWiz.
8. In the UpgradeWiz click **Upgrade**.
9. You will be asked to enter the **System Password**.
10. After the system has received and validated the new .bin files, you will be given the option to continue with the upgrade, where the process of erasing, downloading and installing will begin. If you want the to continue, click **OK**. Clicking **Cancel** will erase all the new .bin files from the RAM of the control unit. The unit will continue operating as if an upgrade was never attempted.
11. An example TFTP log for a successful upgrade is shown below.



12. Following the upgrade the IP Office Control Unit should return to normal operation.

Upgrading IP Office 403 Systems to 2.0 or Newer

IP Office 403 control units running any software level older than 2.0 must be upgraded in a two stage process. You **MUST** upgrade this specific control unit via this method or else the upgrade will fail.

I. Follow the **Pre-Upgrade Checks**.

II. Remove the existing **IP Office Admin Suite**. When upgrading an IP Office system from one core software level to another, the recommended process is to upgrade all existing IP Office application software as well. This is done by un-installing and then reinstalling the software. The un-install process below only removes those files installed during each applications original installation. Any other files added since (user files, system configurations files, voicemail messages, etc.) are not removed.

PROCEDURE

To un-install the **IP Office Admin Suite**:

1. Open the Windows Control Panel (**Start | Settings | Control Panel**).
2. Select **Add/Remove Programs**.
3. Select **IP Office Admin Suite**.
4. Click **Add/Remove**.
5. From the options offered select **Remove**. This process only removes those files installed during the application suites original installation. Any other files added since (user files, system configurations files, voicemail messages, etc.) are not removed.
6. Follow any prompts given during the removal process.

   Note: The removal of some applications (for example TAPI, Feature Key Server, etc) will require the PC to be rebooted.
7. Click **OK** to finish and close the Control Panel.
8. The new versions of the application suites can now be installed.

III. Install the new application suite.

PROCEDURE

To install the **IP Office Admin Suite**:

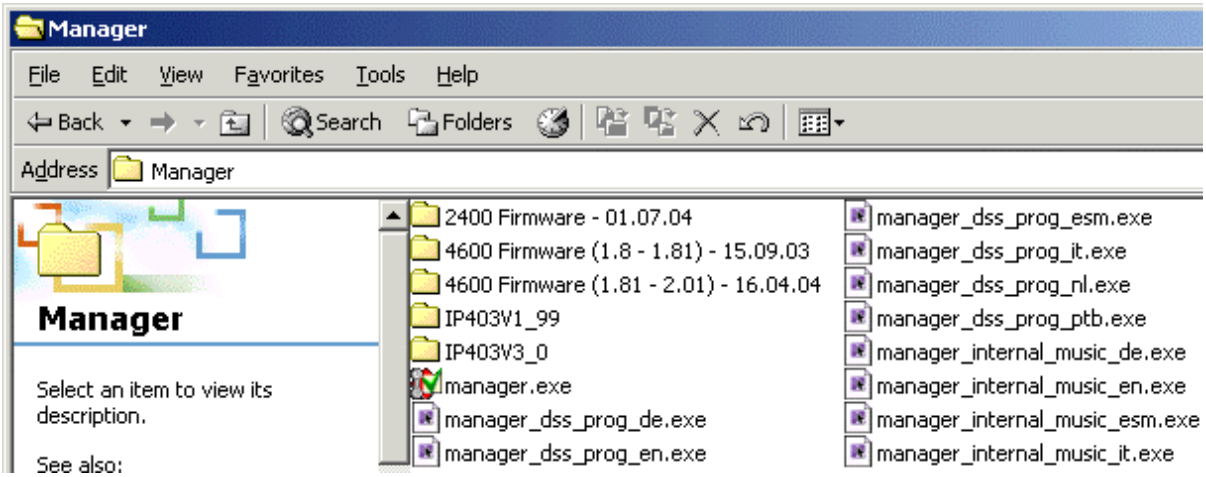
1. Insert the **Administrator CD** into the PC's CD drive. The CD autoruns. You are initially presented with the option to select which language you wish to use. Select the language from the pull down list and click **OK**.
2. The **Destination** folder location option menu is displayed. Either accept the default location (click **Next**) of where the **Administration Suite** is to be installed or change the location by clicking **Browse** and entering a new location.
3. Select which components you wish to install by selecting the appropriate boxes and click **Next**.
4. Name the program folder or accept the default (**Manager**), click **Next** and wait for the Administration Suite installation to be completed.
5. Installation runs and on completion select **Restart now** and click **Finish** twice.

IV. Perform the first stage of the upgrade by using the **ip403.bin** file found in the **Manager / IP403V1_99** sub-folder.

PROCEDURE

To perform the first stage of the upgrade:

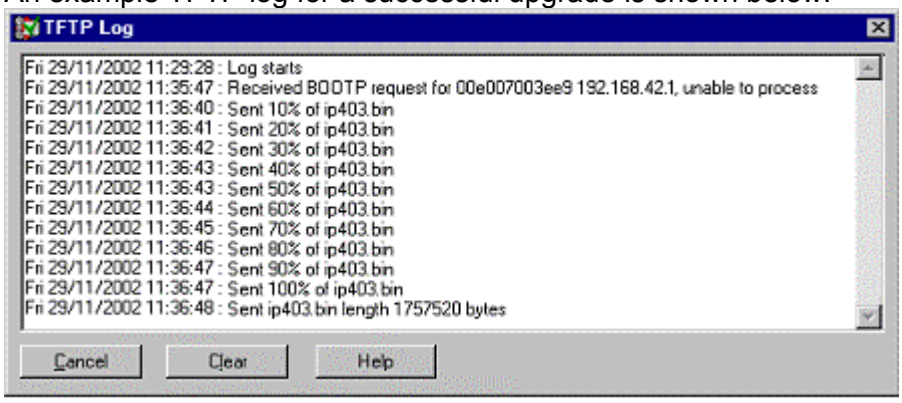
1. Open an explorer window and browse to the directory where Manager is stored. The directory should look similar to the following



2. Open an explorer window and browse to the directory where Manager is stored. Open the **IP403V1_99** sub-folder. Copy the **ip403.bin** file from the sub-folder to the top level Manager working directory opened in the other explorer window.
3. Log onto Manager.
4. Click **File | Advanced | Upgrade**. The Upgrade Wizard window opens.
5. The wizard lists the Control Units and Expansion Modules found.
    - **No Units Listed**
      If this occurs using the Broadcast Address of 255.255.255.255 it implies that the Manager PC is not connected to any local IP Office units. At this point, you should enter the specific IP address of the unit you wish to upgrade or check the network settings.

   The list shows the current software level of the units and the level of the appropriate bin file it has available for each unit from those in the Manager's working folder.
6. Check the boxes for those control units that you want to upgrade.
7. If you are running Manager 2.1 or later, a **Validate** box will be available and checked by default. Leave the box checked if the control unit you are updating is currently running IP Office 2.1 or later because this will perform a validated upgrade. If the control unit you are updating is currently running IP Office 2.0 or earlier, the **Validate** box will be grayed out.
8. In Manager select **View | TFTP Log**. This will allow you to see the file transfer processes. Arrange the windows so that you can see both the TFTP Log and the UpgradeWiz.
9. In the UpgradeWiz click **Upgrade**.
10. You will be asked to enter the **System Password**.
11. After the system has received and validated the new .bin files, you will be given the option to continue with the upgrade, where the process of erasing, downloading and installing will begin. If you want the to continue, click **OK**. Clicking **Cancel** will erase all the new .bin files from the RAM of the control unit.

12. An example TFTP log for a successful upgrade is shown below.



13. Perform the second stage of the upgrade by following the instructions below.

V. Perform the second stage of the upgrade by using the **ip403.bin** file found in the **Manager / IP403V...** (version number is dependent on the software version being upgraded) sub-folder. Repeat the upgrade steps outlined above, but using the bin file in the new subfolder.

VI. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Manager is running the upgraded software version.

Telephones

IP Phone Displays "Invalid set Type" or "Wrong set Type"

Issue

When installing or restarting an IP phone, the display shows "Invalid set Type" or "Wrong set Type".

Potential Cause

For IP phones to function properly, one of the following two process must take place:

- An IP extension is created and the user logs onto the IP phone with that assigned extension number.
- No IP extension is created via Manager and the user of the IP phone enters an unused extension number and the IP extension is automatically created.

Actions

To resolve this issue, perform either action I or II and then action III if necessary.

I. Via Manager, check that there is an IP extension created for the IP phone in question.

PROCEDURE

To check for an IP extension and create a new one if necessary:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Extension**. A list of configured extensions are displayed. Look for an IP extension, represented by the icon.
    i. If there is one, check that it is not assigned to another IP phone or user, then have the user log onto the IP phone using this extension number.
    ii. If there is no IP extension or not one available for use, create one by doing the following:
        a. Right-click within the Extension window and select **New**.
        b. In the **Extension** field of the **IP Extension** configuration window, enter a new extension number (one that is not currently listed). By default, any manually created extension becomes an IP extension.
        c. Click **OK**.
        d. Click and reboot the system.
        e. Use the newly created extension number to log onto the IP phone.

II. Alternatively, you can have the user log onto the IP phone by entering a new extension number (one that is NOT associated with a non-IP extension). By doing this, an IP extension number is automatically created (if the **Auto-create Extn Enable** function is checked - it is checked by default).

PROCEDURE

To check that the **Auto-create Extn Enable** function is checked, do the following:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **System**. Open the IP Office system being configured.
3. On the **Gatekeeper** tab, check that the **Auto-create Extn Enable** function is checked.

III. If this extension number needs to be associated with a particular user, do the following:

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **User**.
   - If the user is already created, associate the new extension to the user by doing the following:
     i. Double-click the user in question.
     ii. Enter the extension number into the **Extension** field. Note that changing a user's extension number affects the user's ability to collect Voicemail messages from their own extension. Each user's extension is set up as a "trusted location" under the Source Numbers tab of the User configuration form. This "trusted location" allows the user to dial *17 to collect Voicemail from his own extension. Therefore if the extension number is changed so must the "trusted location".

     The following related configuration items are automatically updated when a user extension is changed:
     - Hunt group membership (disabled membership state is maintained).
     - Coverage lists containing this user.
     - Diverts to this user.
     - Incoming call routes to this destination.
     - Internal auto-attendant transfer-targets.
     - Dial in source numbers for access to user's own voicemail.

     iii. Click **OK**.
     iv. Click  and merge the updates back to the system.

   - If the user has not been created, create the user by doing the following:
     i. Right-click within the User window and select **New**.
     ii. Enter the user's name in the Name field.
     iii. Enter the extension number into the **Extension** field.
     iv. Click **OK**.
     v. Click  and merge the updates back to the system.

IV. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Log onto the IP phone using the appropriate extension number and then restart the phone again to verify that it logs back on correctly.

IP Phones Not Restarting

Issue

The Avaya IP phones using DHCP from the IP Office will not automatically restart after a system reset or power cut.

Actions

I. Check with the site's IT manager that the IP Office is not providing more than five IP addresses through DHCP to IP phones or computers. The IP Office only supports five simultaneous DHCP client requests.

II. Have the site's IT manager check that any static IP addresses on the LAN subnet are outside the IP Office DHCP scope.

III. If the IP hard phones are using a different DHCP server or have statically assigned addresses, then you need to verify that the IP phones are set to using the IP address of the PC running Manager as the TFTP server.

Procedure

Check that the TFTP server IP address is that of the PC running Manager.

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **System** and double-click the IP Office system you are configuring.
3. In the **TFTP Server IP Address** field, make sure it contains the IP address of the PC running Manager.
4. If any updates have been made and needs to be saved, click and accept the selected reboot mode by clicking **OK**.

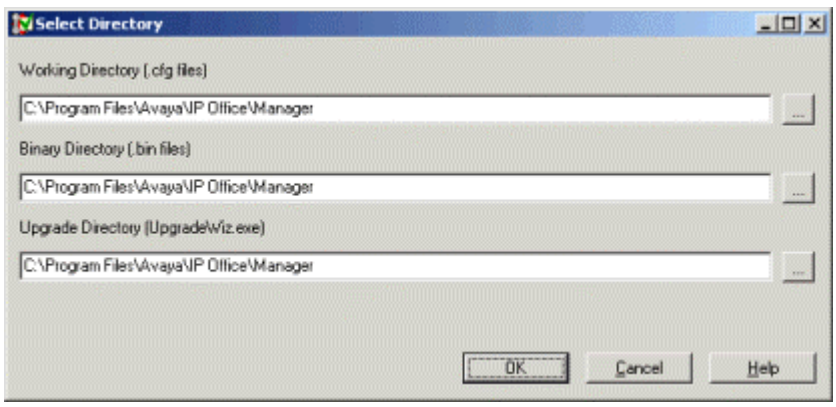
IV. Check the **Preferences** setting on Manager. There should be one set to **255.255.255.255** (a broadcast address).

V. Check that the binary directory (bin files) of the Manager program is directed to the location of the IP hard phone bin files. Bin files are stored in the root of the Manager directory, so the binary files' directory needs to point to the Manager directory.

Procedure

To verify the directory location (and update it if necessary):

1. Log onto Manager.
2. Click **File|Change Working Directory**. A **Select Directory** window appears.



3. In the **Binary Directory (.bin files)** field, make sure that it contains the file path of where the Manager application was installed. If it does not, click the Browse icon to the right of the text box to browse to the correct location.
4. Click **OK**.

VI. If the IP phones are connected through third party switches, have the IT Manager check that spanning tree is turned OFF on the third party switches.

VII. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Restart the IP Office after the updates have been made and check that the IP phones restart correctly.

Time & Date is Incorrect on Handsets

Issue

Time and date information is incorrect on user handsets.

Actions

By default, phones connected to the IP Office system get their time and date information from the Voicemail Pro or Manager program (unless otherwise specified). However, Voicemail Pro or Manager will only act as a time server when the application itself is open. When a time server is defined and available, the phones get an updated time and date from the time server approximately every 10 minutes. Check to see where the users are getting their time and date information from/what is acting as the time server.

I. If you are unsure where the phones are getting their time and date information, check the **Time Server IP Address** setting within Manager.

PROCEDURE

To check the Time Server IP Address setting:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **System** and double-click the IP Office system you are configuring.
3. On the **System** tab, look at the information in the **Time Server IP Address** field. Go to the PC that is acting as the time server and check the following:
   - The correct time and date is set.
   - The time must be set in 24 hour format.
   - If the Manager or Voicemail Pro is acting as the time server, ensure that the application is running.
4. If the **Time Server IP Address** field is blank or set to 0.0.0.0, it means Voicemail Pro will be used as the default time server if the service is running.
5. Check the **Time Offset (hours)** field. This field is used to compensate for the time difference between the time server and the IP Office if they are in different time zones. For example, if the time server is 5 hours ahead of the IP Office, then this field must be configured with **-5** to make the adjustment.

II. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Monitor the clock over a 24 hour period for time slips.

Time Profiles

Configured Time Profile Not Activating

Issue

The configured time profile is not activating at the set time.

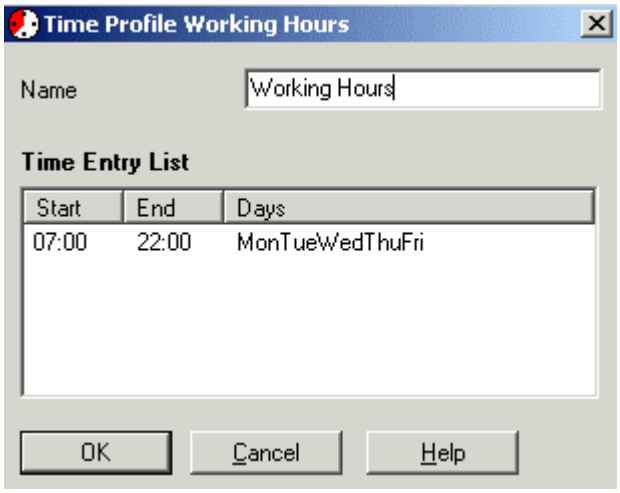
Actions

Time Profiles are used by different IP Office services to define when their settings are used. For example, a time profile can be used to define where Hunt Group calls are routed outside of office hours. Outside of a Time Profile, voice calls are re-routed according to the configuration but any currently connected calls at the time the Time Profile changes are not affected.

I. Check that the correct time and date are configured for the time profile in question.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Time Profile**. A list of configured profiles are displayed.
3. Double-click the time profile in question. A configuration window for that specific time profile displays.



4. Under the **Time Entry List**, check that the **Start** and **End** time and **Days** are set as required and that there are no duplicate or conflicting settings.
   i. If the information needs to be updated, right-click the time entry and select **Edit**.
   ii. Make the necessary changes. Remember that IP Office uses the 24 hour time format.
   iii. Click **OK**.
5. Click **OK** again and then to save the changes.

II. Check that there are not two Time Profiles with the same name.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Time Profile**. A list of configured profiles are displayed.
3. If there are two profiles with the same name, one must be renamed or deleted.
4. If you rename the profile in question, remember to update the service in which this Time Profile is applied.

III. Verify that the correct **Time Profile** is set against the required service. For example, a time profile can be applied to a Hunt Group, a Least Cost Route, a particular Service or an Account Code.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, open the configuration form in which the Time Profile in question is applied.
3. Navigate to the **Time Profile** field and make sure it contains the correct profile name.
4. Click **OK** and then  if any changes have been made that you want to save.

IV. Verify that the users reporting the problem are expecting the service within the configured time profile.

V. Check that the PC being used as the time server is using the 24 hour time format. By default, the IP Office system uses the Manager PC as the time server.

PROCEDURE

To view the time server configuration on Manager:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **System** and double-click the system being configured.
3. On the **System** tab, look at the **Time Server IP Address** field.
   - If there is an IP address defined, check that the PC assigned to that address is set to the 24 hour time format.
   - If left blank or set to **0.0.0.0**, it means Voicemail Pro will be used as the default time server if its service is running.
4. Click **OK** and then  if any changes have been made that you want saved.

VI. If the time profile issue is in relation to a Hunt Group, verify that the customer is not trying to override the time profile defined for a Hunt Group's night service or out of service setting. If a Hunt Group's night service or out of service is defined via a time profile, a short code can be used to manually put that Hunt Group into night or out of service mode before the defined time. However, that same Hunt Group can not be taken out of night service or out of service mode prior to the End time defined within the Time Profile.

PROCEDURE

To view a Hunt Group's service and time profile settings:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Hunt Group**.
3. Double-click the Hunt Group in question. A configuration window for that Hunt Group displays.
4. On the **Fallback** tab, see if there is a profile selected within the **Time Profile** field; if there is, a Hunt Group should be selected within the **Night Service Fallback Group** or **Out of Service Fallback Group** field to correspond with the time profile.
5. Click **OK** and then  if any changes have been made that you want saved.

VII. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Make the necessary changes and retest the time profile application.

Trunks

Analog Trunk Lines Remain Connected

Issue

Analog trunk lines remain connected after the call has ended.

Possible Causes

Analog lines will clear after a call ends if disconnect clear is configured with the Central Office/Network Provider and is also configured for the analog line within Manager. Additionally, if the call routing on a voicemail action does not have a disconnect defined, this may also cause the line to remain open.

Action

I. Check for Disconnect Clear.

Procedure

1. Disconnect the IP Office
2. Pug your test butt in (such as a Ziad)
3. Place a call to the line.
4. Clear the call from the calling end.
5. If you have two clicks close together. This will indicate the network removing & reinstating loop current.

II. Via Manager, check the setting for the analog trunk.

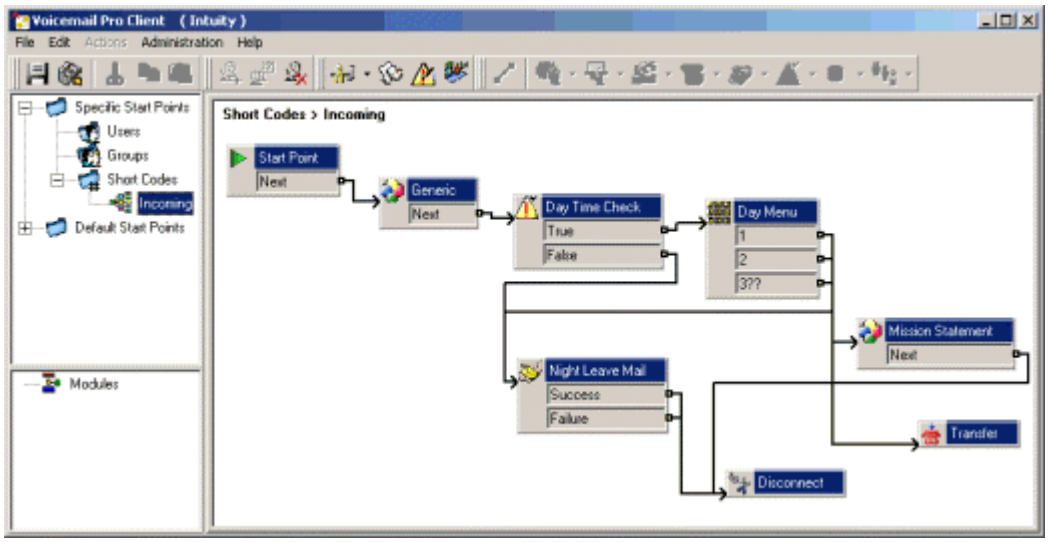
Procedure

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Line** and double-click the analog trunk in question.
3. On the **Analog** tab:
    i. Check that the **Disconnect Clear** check box is checked. Disconnect clear is a technique used to signal to the IP Office from the carrier/exchange that the call should clear. We recommend leaving this checked to make use of the disconnect clear function. Note: not all providers support the disconnect clear function.
    ii. Check the **Disconnect Clear Timer**. The default value is 500ms. If this default value needs to be changed, check with Central Office/Network Provider. Keep in mind that the detection time must be less than the actual disconnect time period and the value entered must be the desired time minus the internally defined *150ms* de-glitch time period. For example, the Central Office/Network Provider may give you the value of 750ms, but consider the actual disconnect time period minus the de-glitch time and the value to be entered will be less than 750ms.
4. Click **OK**.
5. If any configuration changes have been made and needs to be saved, click  and accept the selected reboot mode by clicking **OK**.

III. Via Voicemail Pro, check the call routing for the voicemail action.

Procedure

1. Log onto Voicemail Pro.
2. For the call flow, check that a **Disconnect** action has not been added to the end of the call flow. As sample call flow is provided below.



3. To add a **Disconnect** action to a call flow:
   i. Open the call flow in question.
   ii. Click within the call flow window.
   iii. Click  and select  **Disconnect**.
   iv. Click within the call flow window. This places the action into the call flow.
   v. Click  to connect the **Disconnect** action to the appropriate action.
6. Save the configuration change by clicking  .

IV. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

The analog trunk clears at the end of a call.

E1 PRI 30 Lines

Issues/Symptoms

On an E1 PRI 30 line, if users are experiencing any of the following issues/symptoms, then the steps within the Actions heading need to be followed.

- Low connection speeds on modems and faxes.
- Elongated text within faxes.
- Remote access connection problems.
- Disconnected calls.

Actions

I. Confirm that the ISDN settings within Manager are consistent with the those provided by the Central Office/Network Provider.

PROCEDURE

To look at the settings within Manager:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Line** and double-click then PRI trunk in question.
3. On the **Line** tab, check the following:
   - The **Line SubType** matches that provided by the Central Office/Network Provider.
   - The **Number of Channels** setting matches that provided by the Central Office/Network Provider.
4. On the **Advanced** tab, check the following:
   - The **Clock Quality** is correctly set.
     - If there is only one PRI line/trunk, set the **Clock Quality** to **Network**.
     - If there are more than one PRI line/trunk, set one of the line/trunk to **Network** and the others to **Fallback**.
   - The line **Signalling** field should be set to **CPE**.
   - If CRC is enabled at the Central Office/Network Provider, then the **CRC Checking** field on this window should also be checked/enable.
5. Click **OK**.
6. If any updates have been made and needs to be saved, click  and accept the selected reboot mode by clicking **OK**.

II. Use the System Monitor application to check for clocking problems on the IP Office.

To use the System Monitor application:

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 following trace settings:
   - Ensure that the **Print** option (within the **System** tab) is enabled.
   - Ensure that the following fields are enabled within the **ISDN** tab:
     - **Layer 1** under the **Events** heading.
     - **Layer 1 Send** and **Layer 1 Receive** under the **Packets** heading.

3. Click **OK**.
4. If the following statement appears on the Monitor trace, it means a frame slippage has been detected on line 5 (Falc 5).

```
11529987mS PRN: Falc 5 slip
```

5. If you determine that a frame slippage has occurred, the following actions can be taken to address it:
    - Replace the PRI card in the control unit.
    - If this still does not address the issue, it is most likely a fault on the Central Office/Network Provider's line. Call the Central Office/Network Provider and confirm.

III. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Verify that users are no longer experiencing the issues reported.

Incoming Calls have no Caller ID Information on Analog Trunks

Issue

No caller ID or name information is displayed for calls coming in on analog trunks.

Actions

Caller ID and name information is not necessarily the same. Name information is not displayed on analog trunks. Caller ID is the number designated to be displayed. In most regions, the display of caller ID information must be purchased from the Central Office/Network Provider before it becomes available to users.

I. Check with the Central Office/Network Provider that Number sending is being sent from the Central Office/Network Provider. In some countries, this feature must be purchased from the Central Office/Network Provider before it is activated.

II. Verify that the trunk type selected is correct based on information from the Central Office/Network Provider. The trunk type must match the type defined by the Central Office/Network Provider.

PROCEDURE

To check the trunk type setting on the analog trunk:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Line** and double-click the analog trunk in question.
3. Via the **Analog** tab, check the selection within the **Trunk Type** field. Make sure it matches the type defined by the Central Office/Network Provider.
4. Repeat the above steps for all configured analog trunks.

III. Via the System Monitor application, check for caller ID information being sent from the Central Office/Network Provider.

PROCEDURE

To use the System Monitor application:

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.
   - On the **System** tab, make sure the **Print** check box is checked.
   - On the **ATM** tab, make sure the **Channel**, **CM Line** and **I/O** check box is checked.
   - On the **Call** tab, make sure the **Targeting** check box is checked.
3. Click **OK**.
4. Below is an explanation of how to read the trace codes:

   Channel tracing produces traces which start with -

   - **PRN: AtmTrunk** for an ATM4 in version 2.1 and below.
   - **PRN: AtmChannel** for an ATM4 in version 3.0 and above.
   - **PRN: AtmLine** for an ATM16 irrespective of version.

   Note that the **AtmTrunk1: CLI Message Rx'd:** or the **AtmChannel1: CLI Message Rx'd:** message is followed by one or more **PRN: 0xWXYZ** messages. The decode rules for these messages are shown in the step entitled “How to decode the **CLI Message Rx'd PRN: 0xWXYZ** messages”.

   - CM Line tracing produces traces which start with **PRN: AlogLine**

- I/O tracing produces traces which start with **PRN: AtmIO**
- Targeting tracing produces traces which start with **CMTARGET**

To identify the Line Number on ATM Tracing

Channel tracing:

- **AtmTrunkB3** where **B3** is the Line Number [in version 2.0(16)].

```
A0 = Line 1,
A1 = Line 2,
 .      .
 .      .
B3 = Line 7,
B4 = Line 8
```

- **AtmTrunk1** where **1** is the Line Number [in versions 2.0(18) and all versions of 2.1]
- **AtmChannel1** where **1** is the Line Number [in version 3.0 and above].
- **AtmLine701** where **701** is the Line Number on an ATM16 module.

```
A0 = Line 1,
A1 = Line 2,
 .      .
 .      .
B3 = Line 7,
B4 = Line 8
```

CM Line tracing:

- **AlogLine8** where **8** is the Line Number [in version 2.1 and below].
- **AtmLine8** where **8** is the Line Number [in version 3.0 and above].

I/O tracing:

- **AtmIOB3** where **B3** is the Line Number [in version 2.0(16) and below].

```
A0 = Line 1,
A1 = Line 2,
 .      .
 .      .
B3 = Line 7,
B4 = Line 8
```

- **AtmIO1** where **1** is the Line Number [in version 2.0(18) and above].

  Note that the above is true for all Analogue Trunks that are terminated on the IP Office Main module. When Analogue Trunks are terminated on an ATM16 module NO tracing is output on the SysMonitor apart from the following:

  - PRN: **AtmTrunkXXX:** bchan=Y: StateChange..... [in V2.1(27) and below]

- PRN: **AtmLineXXX:** bchan=Y: StateChange ..... [in V3.0 onwards]

5. A typical trace taken from an Analogue Trunk that supports ICLID/CLI terminated on an IP Office Main module running 2.1(28) is shown below. The trace has been annotated to show the decode of certain messages and to indicate, where appropriate, what is happening. All trace messages are shown in code-base font and **bold** with the decode/meaning in regular font style.

   108691mS PRN: AtmTrunk1: StateChange CLIPossibleIncoming->Idle

   AtmTrunk1 => Line Number 1.

   The Line interface is primed ready for the possibility of an incoming ICLID/CLI message.

   108692mS PRN: AtmIO1: Block Forward OFF

   AtmIO1 => Line Number 1.

   108692mS PRN: AtmIO1: CLI Detection ON Equaliser ON

   ICLID/CLI detection has been enabled on this Trunk

   109703mS PRN: AtmTrunk1: CLI Message Rx'd:

   The start of a ICLID/CLI message has been detected. The message received is then shown in Hex (0x).

   109703mS PRN: 0x4500

   4500 -> Date (mm dd) and Time(hh mm) info.

   Note - The full decode options for these 4 byte words is given later.

   109704mS PRN: 0x3031

   30(hex) -> 0(ASCII); 31(hex) -> 1(ASCII)

   109704mS PRN: 0x3134

   31(hex) -> 1(ASCII); 34(hex) -> 4(ASCII)

   109704mS PRN: 0x3136

   31(hex) -> 1(ASCII); 36(hex) -> 6(ASCII)

   109704mS PRN: 0x3035

   30(hex) -> 0(ASCII); 35(hex) -> 5(ASCII)

   The resultant Date/Time decode is as follows:

   - Date decodes as 01 14 which is 14th of January
   - Time decodes as 16 05 which is 16:05 (or 4:05pm)

   109705mS PRN: AtmTrunk1: CLI Message Rx'd:

   The start of a second ICLID/CLI message has been detected.

109705mS PRN: 0x4980

4980 -> Calling Party Number

109706mS PRN: 0x3031

30(hex) -> 0(ASCII); 31(hex) -> 1(ASCII)

109706mS PRN: 0x3730

37(hex) -> 7(ASCII); 30(hex) -> 0(ASCII)

109706mS PRN: 0x372d

37(hex) -> 7(ASCII); 2d(hex) -> -(ASCII)

109706mS PRN: 0x3339

33(hex) -> 3(ASCII); 39(hex) -> 9(ASCII)

109706mS PRN: 0x3033

30(hex) -> 0(ASCII); 33(hex) -> 3(ASCII)

109707mS PRN: 0x3931

39(hex) -> 9(ASCII); 31(hex) -> 1(ASCII)

The resultant Calling Party Number (ICLID/CLI) is 01707-390391

109707mS PRN: AtmTrunk1: CLI Message Rx'd:

The start of a third ICLID/CLI message has been detected.

109707mS PRN: 0x5800

5800 -> End of ICLID/CLI detected

09708mS PRN: AtmIO1: CLI Detection OFF Equaliser OFF

ICLID/CLI Detector has been disabled.

109708mS PRN: AtmTrunk1: StateChange CLIAwaitData->CLIDataSettle

109911mS PRN: AtmTrunk1: StateChange CLIDataSettle->CLIAwaitSecondRing

110191mS PRN: AtmTrunk1: StateChange CLIAwaitSecondRing->PossibleIncoming

Line state changes from receiving ICLID/CLI to possible incoming call.

110437mS CMTARGET: LOOKUP CALL ROUTE:3 type=100 called_party= sub= calling=01707-390391 in=1 complete=1

110437mS CMTARGET: LOOKUP INCOMING CALL ROUTE:3, calling party is 01707-390391. Using destination 326

Targeting tracing intimates the ICLID/CLI received as [calling =]. In this case 01707-390391

IV. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Make an incoming call and check that caller ID and/or caller's name is received on the telephone display.

Incoming Calls have no Caller ID Information on ISDN Trunks

Issue

No caller ID or name information is displayed for calls coming in on ISDN trunks.

Actions

Caller ID and name information is not necessarily the same. Caller ID is the number designated to be displayed and name is text information to be displayed. In most regions, both of these features must be purchased from the Central Office/Network Provider before they become available to users.

I. This feature is only available on IP Office 2.0 and newer. Older IP Office software does not accept this information from the Central Office/Network Provider.

II. Check with the Central Office/Network Provider that caller ID information is being sent from the Central Office/Network Provider. In some countries, the caller ID feature must be purchased from the Central Office/Network Provider before it is activated.

III. Check with the Central Office/Network Provider that Name and Number sending is being sent from the Central Office/Network Provider. In some countries, this feature must be purchased from the Central Office/Network Provider before it is activated.

IV. Verify that the trunk type selected is correct based on information from the Central Office/Network Provider. The trunk type must match the type defined by the Central Office/Network Provider.

PROCEDURE

To check the trunk type setting on the analog trunk:

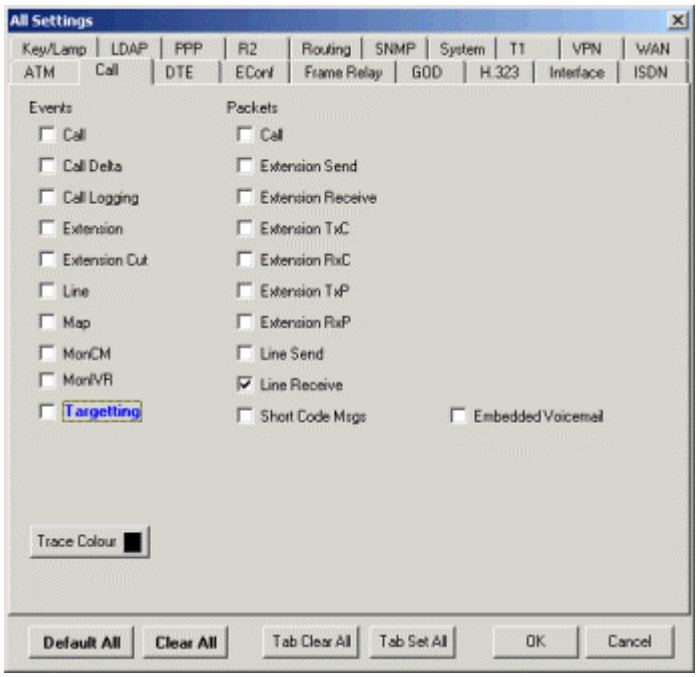
1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Line** and double-click the analog trunk in question.
3. Via the **Analog** tab, check the selection within the **Trunk Type** field. Make sure it matches the type defined by the Central Office/Network Provider.
4. Repeat the above steps for all configured analog trunks.
5. If any configuration changes have been made, click **OK** and then  to save the changes.

V. Via the System Monitor application, check for caller ID information being sent from the Central Office/Network Provider.

PROCEDURE

To use the System Monitor application:

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 checked.



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]

VI. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Make an incoming call and check that caller ID and/or caller's name is received on the telephone display.

User Can Not Page over IP Line to Remote Site

Issue

User is unable to page over a VoIP line to a remote site.

Actions

For paging to a remote site, the correct system short code must be set up at both ends.

I. Verify that the local system has a shortcode directed at the remote site where paging is required. The short code should look similar to the following:

Short Code: *81

Telephone Number: .

Line Group ID: 10 (IP trunk group ID)

Feature: Dial

PROCEDURE

To set up the short code on the local system:

1. Log onto Manager and open the local system's IP Office configuration.
2. From the Configuration Tree, click **ShortCode** and double-click the system to be configured.
3. Verify that there is a short code created for the IP trunk and that it is similar to the above sample short code. If one does not exist, create one.
4. If any configuration changes have been made, click **OK** and then  to save the changes.

II. Verify that the remote system short code for dial paging is set up correctly. The short code should look similar to the following:

Short Code: *81

Telephone Number: 305 (group or extension page number)

Line Group ID: 0

Feature: DialPaging

PROCEDURE

To set up the short code on the remote system:

1. Log onto Manager and open the local system's IP Office configuration.
2. From the Configuration Tree, click **ShortCode** and double-click the system to be configured.
3. Verify that there is a short code with the **DialPaging** feature and that it is similar to the above sample short code. If one does not exist, create one.
4. If paging is set up for a group page number, check the following:
    - A Hunt Group with all the users required as members have been created and that the extension number assigned to that Hunt Group matches the number in the **Telephone Number** field of the short code.
    - The Hunt Group ring mode is set to **Group** and the **Voicemail** and **Queuing** facilities are turned off for that Hunt Group.
5. If any configuration changes have been made, click **OK** and then  to save the changes.

III. The Fast Start option can sometimes effect the audio channel on an IP trunk/line. Fast Start controls the number of messages that need to be exchanged before an audio channel is created. If Fast Start is not enabled, tones may not be passed along in time, and therefore the tones are lost before the connection is made. Check to see if the **Enable Faststart** option on the IP line/trunk (at both the local and remote site) is enabled.

PROCEDURE

To check the **Enable Faststart** option:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, click **Line** and double-click the IP line/trunk to be configured.
3. On the **VoIP** tab, verify that the **Enable Faststart** option is enable/checked.
4. If any configuration changes have been made, click **OK** and then  to save the changes.

IV. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Retest paging to verify that it is working.

Voicemail

Attempts to Access Voicemail from Remote IP Office Site is Unsuccessful

Issue

Within a small community network, when dialing the system short code (*17 by default) from a remote IP Office site to access voicemail, the user gets a busy tone or voicemail is just unobtainable.

Actions

The Voicemail Pro server on a central IP Office system can be used to provide voicemail services for remote IP Office systems. This is called Centralized Voicemail Pro. Centralized Voicemail Pro requires Small Community Networking.

I. Check that voicemail is accessible at the central IP Office site. The quickest ways to verify the accessibility of voicemail are via the system short code or Phone Manager.

PROCEDURE

To verify the accessibility of voicemail via the short code (*17) from the central site:

1. Leave a test message for a volunteer user located at the central site.
2. Have the user dial ***17** to access voicemail. The voicemail system should prompted the user to enter an extension and password.
3. If access to voicemail is successful, it means voicemail is functioning. Continue to Action II.

PROCEDURE

If Phone Manager is set up at the central site:

1. Leave a test message for a volunteer user located at the central site.
2. Have this user log onto Phone Manager and click the messages tab. There should be a test message from you; have the user double click the required mailbox. The voicemail system should prompted the user to enter an extension and password.
3. If access to voicemail is successful, it means voicemail is functioning. Continue to Action II.

II. Verify if it is only the one user or all remote users who are experiencing the problem by having other users at the remote IP Office site attempt to access their voicemail via the VoicemailCollect short code (*17 by default).

III. Verify that the settings for the IP trunks (at both the local and remote sites) being used for small community networking are configured correctly and have matching settings. **Voice Networking** must be enabled at both ends and matching field settings are essential for compatibility and performance.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Line**. Double-click the IP trunk being used for connection to the remote site in question.
3. Within the **VoIP** tab:
    i. Ensure that the **Voice Networking** check box is checked. This enables the exchange of directory and user information between the IP Office systems and is the key enabler of Small Community Networking.

ii. Check that the **Gateway IP Address** field contains the IP address of the remote site in question (if you are making the configuration from the central site). Then at the remote IP Office site, check that the Gateway IP Address field contains the IP address of the central site.

iii. Ensure that the **Compression Mode** selection is the same across all IP Office sites within the network.

iv. Ensure that the **H450 Support** selection is the same across all IP Office sites within the network.

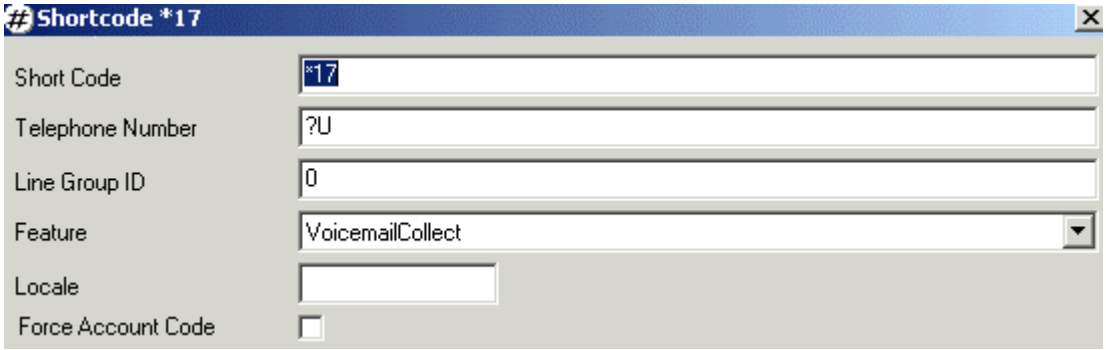
5. If any configuration changes have been made, click **OK** and then to save the changes.

Actions Performed on the Remote IP Office System

IV. On the remote IP Office system, check that the system default (*17) **VoicemailCollect** short code has not been amended. *17 is the default short code for voicemail access; the actual digits (17) is not mandatory for access and may have been amended by the system administrator. Verify that the user in question is using the defined short code number and the short code configuration is accurate.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **Shortcode**. The list of system short codes are displayed.
3. Under the **Feature** heading, look for **VoicemailCollect**. If displayed, double-click it to display the short code configuration. The short code configuration should look similar to the following (with the only possible difference being the short code number).



4. Ensure that the user in question is using the defined VoicemailCollect short code.
5. If any configuration changes have been made, click **OK** and then to save the changes.

V. On the remote IP Office system, check that a conflicting VoicemailCollect short code is not configured individually for the user in question. If the same VoicemailCollect short code is misconfigured within the User configuration form, the user will be unable to access voicemail via this short code, even if it is configured correctly on the system.

PROCEDURE

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **User**. Double-click the user in question and click the **ShortCodes** tab.
3. If there is a **VoicemailCollect** short code configured for the user, verify that it is configured accurately. The short code configuration should look similar to the above sample, with the only possible difference being the short code number.

4. If any configuration changes have been made, click **OK** and then  to save the changes.

VI. For the remote IP Office site to make use of the voicemail system at the central site, the remote site's voicemail settings must be configured correctly.

PROCEDURE

To verify the voicemail settings at the remote IP Office site:

1. Log onto Manager and open the remote IP Office site's configuration.
2. From the Configuration Tree, select **System**. Double-click the IP Office system to be configured.
3. On the Voicemail tab:
   i. Make sure the **Voicemail Type** is set to **Line**.
   ii. The **Voicemail Destination** must be set to the IP trunk that connects the system to the central site.
4. If any configuration changes have been made, click **OK** and then  to save the changes.

VII. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Have the user in question dial the VoicemailCollect short code (*17 by default) to access the central site's voicemail system.

Message Waiting Light Illuminated without Messages

Issue

The message waiting light on the telephone is illuminated even though there are no new messages remaining in the mailbox.

Possible Cause

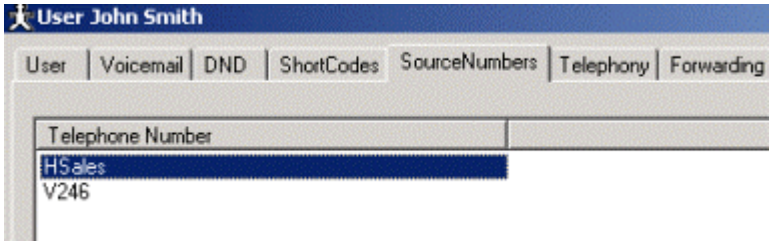
If the user associated with the telephone has been configured to receive message waiting indication for messages left at a Huntgroup's voicemail box, this will cause the message waiting light to be illuminated when a message is left on that Huntgroup's voicemail.

Action

I. Check to see if the user has a message indication relationship to a Huntgroup.

Procedure

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **User** and double-click the user in question.
3. On the **SourceNumbers** tab, see if there is an **H** followed by a Huntgroup name, i.e. HSales, where **Sales** is the name of a Huntgroup.



4. If there is a configuration similar to the above example, then check that Huntgroup's mailbox for new messages. Once the new messages are processed/played, the message waiting light on the user's phone should extinguish.

II. Check that text messages have not been left on the user's telephone. If the user in question has a digital telephone, text messages can be read from the display window. If the customer's digital telephone has a menu button, check for text messages by press pressing **Menu|Menu|Msgs|Recvs**. This displays the types of messages available on the phone and if any is awaiting in the mailbox. If the customer's phone does not have a Menu button, refer to the specific telephone user's guide for instructions.

III. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Listen and delete all messages and verify that the message waiting light does not illuminate.

Message Waiting Light will not Illuminate after a Message is Left

Issue

Message waiting light does not illuminate after a message is left in a user's mailbox.

Actions

I. Duplicate user names on the IP Office system can cause this problem. The duplication of information can happen when, for example, there is an existing John Smith user who is associated with extension 201. Now, if there is a second John Smith user who is associated with extension 208 on the IP Office and the first John Smith user is not deleted from the list of Voicemail Pro list of users, confusion with the message waiting indication may arise. To resolve this issue, delete the old John Smith user name or differentiate it from the new John Smith via Manager; then delete the user from Voicemail Pro and restart Voicemail Pro. This will cause Voicemail Pro to repopulate its list of users with the updated information. Detailed procedures are provided below.

Procedure

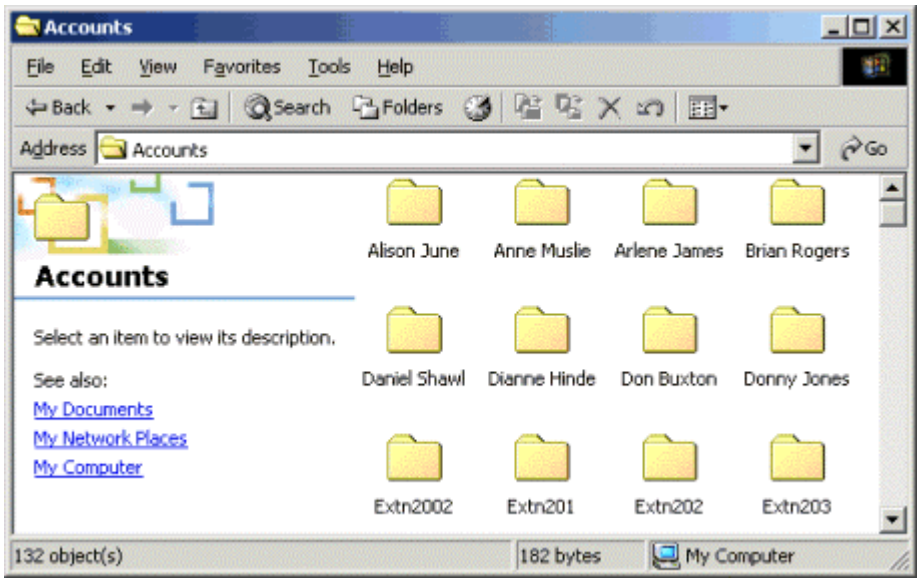
To delete or update the user in question via Manager:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **User** and look for duplicate user names. Delete or update the user in question.
3. Click **OK** and then  to save the changes.

Procedure

To delete the user in question from the Voicemail Pro list of users:

1. Navigate to Voicemail Pro's **Account** directory. Typically, it is located within **Avaya/IP Office/Voicemail Pro/VM/Accounts**.



2. Delete the user account in question. This user will lose all messages and greetings and will need to reset all mailbox preferences.
3. Restart Voicemail Pro.

II. When a user first logs on as an agent, message waiting lights will not illuminate, even when there is a message in the mailbox for that agent. This is because Voicemail does not recognize that the agent has logged on until that agent connects to Voicemail. Therefore, it is highly recommended that the first thing an agent does after logging on is check for Voicemail messages. After this initial interaction with Voicemail, the message waiting light will illuminate when there is a message (for that log on session).

III. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Leave a message for the user in question and verify that the message waiting light illuminates.

User or Hunt Group has Difficulties Receiving Voicemail Messages

Issue

User or Hunt Group has trouble receiving Voicemail messages.

Actions

I. User and Hunt Group name entries must be entered in the correct format. These entries are case sensitive and must be unique. Only alphanumeric characters and spaces are supported. However, spaces after the name are NOT acceptable.

Procedure

To check the User and Hunt Group name entries:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **User** or **Hunt Group** accordingly.
3. Double-click the user or Hunt Group in question and update the name entry as necessary.
4. Click **OK** and then  to save the changes.
5. Restart Voicemail to re-populate the User or Hunt Group names with the updated information.

II. Voicemail must be enabled for the Hunt Group and the Users in question.

Procedure

To check the User and Hunt Group name entries:

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **User** or **Hunt Group** accordingly.
3. Verify that the **Voicemail On** check box is checked/enabled for the users or hunt groups in question.
4. Click **OK** and then  to save if any updates have been made.

III. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Leave a message for a user or hunt group and verify that the message waiting lamp illuminates.

Voicemail Messages have Broken Gaps on Playback

Issue

Users experiencing broken gaps in the voice stream when they play back their voicemail messages.

Actions

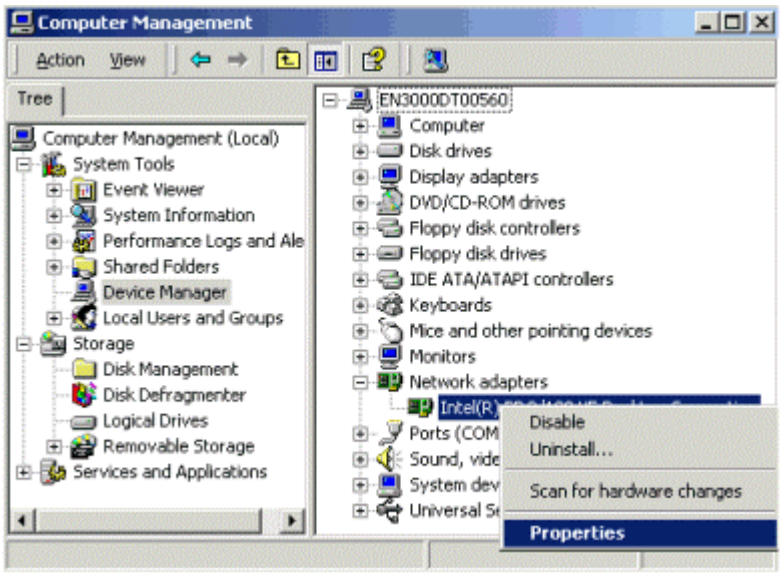
I. Check that the network cabling between the PC running Voicemail and the IP Office is secure and active (the LAN port with the cable plugged in should be lit with intermittent blinking).

II. If the PC running Voicemail is directly connected to an IP Office 403 or 406 system, check that the Network Interface Card (NIC) is set to 100megabit and half duplex. This step is necessary because the IP Office 403 and 406 systems only support half duplex.

PROCEDURE

To check/update the information for the NIC on the PC running voicemail:

1. On the PC running Voicemail, right-click **My Computer** and select **Manage**.
2. Click **Device Manager**. A list of devices recognized by the PC are listed on the right-hand side of the computer management window.
3. Expand the **Network Adapters** option.
4. Right-click the NIC and select **Properties**.



5. A configuration window for the NIC is displayed. On the **Advanced** tab and within the **Property** heading, select **Network Media** or **Network Link** (title varies depending on the specific NIC).
6. Within the **Value** drop-down box, select **100BaseTx**, which means a selection of 100megabit and half duplex.
7. Click **OK**.

III. If the above procedure applies to the customer site, also check that the network switch on the port in which voicemail is connected is also configured for half duplex. Some third party devices are set to full duplex by default.

IV. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Make the necessary changes to the NIC card and restart the computer. Test the same voicemail messages after restart.

Voicemail Pro Server Not Starting or Loses Connection

Issue

The Voicemail Pro server will not start or loses connection to the IP Office control unit after two hours.

Possible Causes

The IP Office system can only interact with one voicemail server at any one time. Voicemail Pro is a licensed voicemail program that builds upon Voicemail Lite by offering a high degree of customization for any mailbox. Unlicensed Voicemail Pro will run for two hours (for demonstration and testing purposes) and then disconnects.

Voicemail Pro consists of both a server program and a client for administration of the server. Some customer sites have Voicemail Pro installed on a separate server PC from that running Manager.

For Voicemail Pro to function properly, the following must be in place:

- Networking configurations between the Voicemail Pro server PC and the IP Office control unit must be correct.
- The Voicemail Pro license key must be properly configured.
- If the customer has remote IP Office systems connected to Voicemail Pro, verify that it is configured for centralized voicemail.

These verifications are discussed in detail below and are sectioned into actions performed on the Voicemail Pro server PC and those performed on the PC running Manager.

Actions Performed on the Voicemail PC

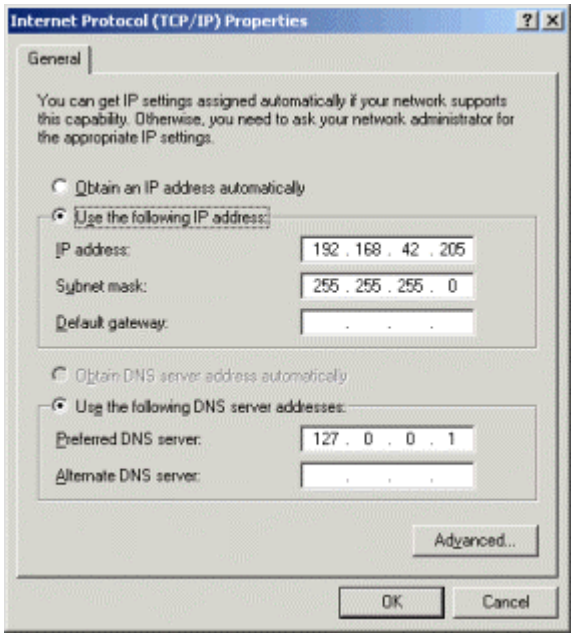
The following verifications are performed on the Voicemail Pro server PC.

I. Verify that the computer running Voicemail Pro has a static IP address and the address is within the IP range and subnet range that the IP Office is configured with. The two IP addresses need to be on the same network. For example, if the IP and subnet range of the IP Office is **192.168.42.1** and **255.255.255.0** respectively, then the IP address of the computer running Manager should be anywhere between **192.168.42.2** to **192.168.42.254**.

Procedure

To check and update the IP address of the computer running Manager:

1. Right-click **My Network Places** and select **Properties**.
2. Right-click **Local Area Connections** and select **Properties**.
3. Select **Internet Properties (TCP/IP)** and click **Properties**.



4. With **Use the following IP address** selected, the fields for IP address and Subnet mask is available for editing. Make the necessary changes based on IP range of the IP Office control unit.
5. Click **OK**.

II. Check the default gateway programmed on the Voicemail Pro computer. The default gateway should be the IP Office.

Procedure

To check and update the default gateway of the Voicemail Pro computer:

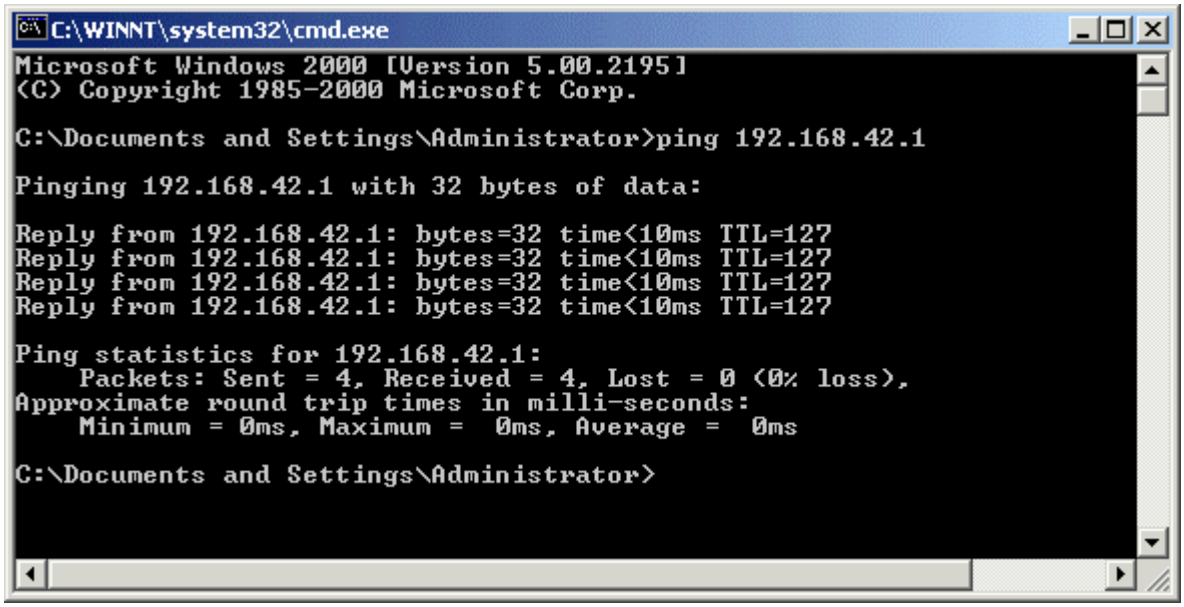
1. Right-click **My Network Places** and select **Properties**.
2. Right-click **Local Area Connections** and select **Properties**.
3. Select **Internet Properties (TCP/IP)** and click **Properties**.
4. With **Use the following IP address** selected, the **Default Gateway** field is available for editing. The default gateway should be the IP Office. Make the necessary updates.
5. Click **OK**.

III. Check that there is a network connection light on the Voicemail Pro computer's network interface card (NIC) and the IP Office or Hub/Switch port at the other end of the cable.

IV. From the PC running Voicemail Pro, check you can ping the IP Office's IP address.

Procedure

1. From the **Start** menu of the computer running Voicemail Pro, select **Run**.
2. Enter **cmd** in the text box.
3. In the Command Prompt window, type **ping xxx.xxx.xxx.xxx** (where x = IP address of the IP Office control unit).
4. A message similar to the following should appear:



5. If the ping results in a Timeout, meaning the Voicemail Pro PC cannot contact the IP Office, check to make sure all network cables are fitted correctly.

Actions Performed on the Manager PC

The following actions must be performed on the PC running Manager.

I. Via Manager, verify that the Voicemail Type and IP address is set correctly.

Procedure

1. Log onto Manager and open the IP Office configuration.
2. From the Configuration Tree, select **System** and double-click the IP Office system you are configuring.
3. Within the **Voicemail** tab:
   i. Check that **PC** is selected under the **Voicemail Type** heading.
   ii. Check that within the Voicemail IP Address field, either the IP address of the Voicemail Pro server is entered or if you have only one voicemail server, a broadcast address of 255.255.255.255 is also acceptable.
2. Click **OK**.
3. Click the icon or choose **File | Save**. Accept the selected reboot mode by clicking **OK**.

II. Check that the license key dongle is fitted properly to the PC running Manager.

Note: If the customer has an IP Office - Small Office Edition or an IP Office 412 control unit, a serial license key can be plugged directly into these control units. If this is the case, check that the serial license dongle is plugged snugly into the correct serial port and the license server IP address is defined properly.

Otherwise, on the PC supporting the feature key, verify the following:

PROCEDURE

Check that the feature key is validated in the tool tray on the PC's task bar. The tool tray typically resides to the left of the clock on your PC monitor. An example is provided below:

- If there is a (red feature key icon) is displayed, it means the feature key (dongle) is connected properly in the back of the PC and is working.
- If the icon is white with a red cross through it, it means the feature key (dongle) is not connected properly or not working. Check that the feature key is connected properly to the back of the PC before continuing with the troubleshooting procedures.

III. Via Manager, verify that a Voicemail Pro 4 ports (Unlimited) license key is installed and the key is valid.

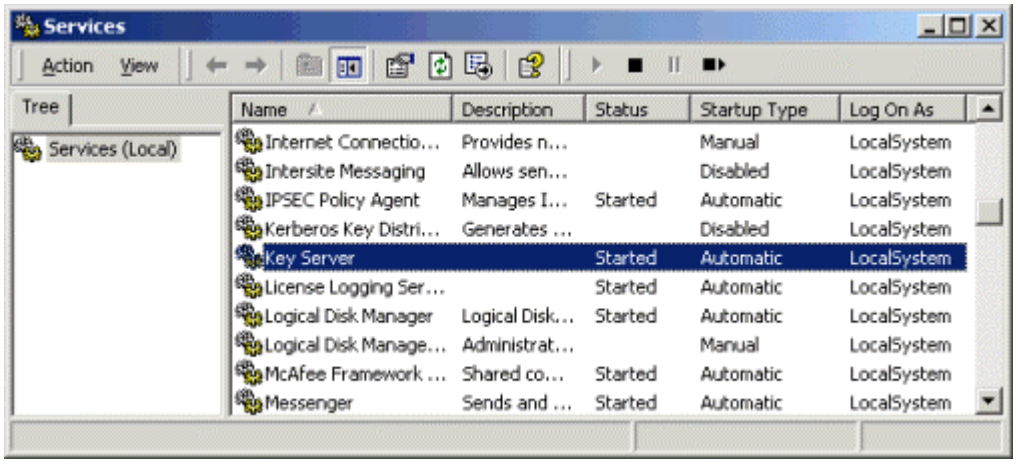
Procedure

1. Log onto Manager and open an IP Office configuration.
2. From the Configuration Tree, select **License**. A **Voicemail Pro 4 ports** (Unlimited) license should be listed with a **Valid** status.
3. If the status is Invalid, refer to Licenses Show Invalid or Unknown.

IV. On the PC running Manager, check that the **Key Server** service is running.

PROCEDURE

1. On the PC running Manager, go to the Windows **Start** menu and select **Settings|Control Panel**.
2. Double-click **Administrative Tools**.
3. Double-click **Services**.
4. Find the **Key Server** service and check that it has a **Started** status.



- If the service is started, right-click it and select **Stop** and then **Restart**. This will ensure that the service is running.
- If it is not started, right-click the service and select **Start**.

V. If the customer has remote IP Office systems connected to Voicemail Pro, verify that the Voicemail configuration on Manager at the remote sites are defined correctly.

PROCEDURE

On the Manager application at each of the remote IP Office sites, do the following:

1. Log onto Manager and open an IP Office configuration.
2. From the Configuration Tree, select **System** and double click the system in question.
3. On the **Voicemail** tab:
   i. Check that the **Voicemail Type** is defined as **Line**. This will define the system to use centralized voicemail.
   ii. In the **Voicemail Destination** field, make sure that the correct IP trunk number is selected.
4. Click **OK**.

VI. If the problem persists after you have performed ALL these troubleshooting steps, gather the following information BEFORE escalating the issue:

- A copy of the IP Office configuration will be useful before escalating to your support organization.
- The username and password of the configuration must be provided to your support organization for testing purposes.
- Any trace codes or log files generated by the System Monitor application (if available).
- Notes relating to the result of each of the verification steps performed above.
- The customer's network diagram (if applicable).

Validation

Monitor the Voicemail Pro system to verify that it starts and continues to function.

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