IP Office 2.1

Manager Application

40DHB0002USAU Issue 15c (6th May 2004)

Table of Contents

Overview of Manager

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.

Using Manager, you can extract and then view and alter the configuration file in the system's RAM memory. Having received a configuration file you can archive it on the PC or modify it using Manager. When you are finished with the new configuration, you can use Manager to send the configuration back to the Control Unit's flash memory and then reboot the Control Unit to activate the changes.

Manager

Installing Manager

Manager is installed as one of the applications from the IP Office Administrator Applications CD. It is highly recommended that Manager is kept on the same version number as the IP Office Control Unit software.

- **Operating System:**
  Manager is supported on the following Windows platforms:
  - Windows 2003
  - Windows XP Professional & XP Professional Server,
  - Windows 2000 Professional (SP2) & Server (SP2),
  - Windows NT4 Workstation (SP6) & NT4 Server (SP6),
  - Windows 98 (2nd Edition)
- Network Settings:
  - The PC should be in the same IP domain as the IP Office Control Unit, ie. it should have the same subnet mask.
  - A fixed IP address is strongly recommended.
-  WARNING:
  If the Manager PC is to be used for software upgrades or to support Avaya 4600 Series IP telephones then a fixed IP address is required. Note also that software upgrades through Manager are not supported over WAN or RAS links.
  - **Installation with Other Applications:**
    If IP Office Feature Key Server and/or IP Office Voicemail (Lite or Pro) are being installed, it is recommended that they are installed onto the same PC and that Manager is installed onto that PC. The required PC specifications for those applications exceed those required by Manager.
  - **Security:**
    Though Manager and the IP Office Control Units both require passwords for access, it is recommended that Manager is not installed on a PC in a public/general use area. The Manager PC will hold copies of the IP Office configuration and other important files.
  - **Regional Settings:**
    The regional settings (**Start | Settings | Control Panel | Regional Options** or **Regional Settings**) should be set correctly. These control the options shown with the Manager application. For a new IP Office installation, the regional setting of the Manager PC is used to set the Locale within the IP Office configuration when first loaded.
  - **Time & Date Settings:**
    Initially the IP Office takes its time and date from whichever PC it finds running Manager. Therefore the time and date on the Manager PC should be set correctly (**Start | Settings | Control Panel | Date/Time**). See How the System Receives Time .

Daily Backup

Using short codes, applications such as Phone Manager and the menus on digital telephones, users can make changes to the configuration running in the system's RAM.

In order to ensure that such changes are saved, the system copies the RAM configuration into the Flash memory once each day. This occurs at between 12:00 AM and 12:30 AM (it only occurs if user changes to the RAM have been made).

Default LAN Settings

When an un-configured Control Unit is switched on, it requests IP information from a DHCP Server on the network.

- Note: This means that the Control Unit must be physically connected to the LAN before being switched on. If connecting to the LAN via another hub, then connect via LAN port 8 with the UPLINK button out.

- If there is a DHCP server on the LAN, the control unit defaults to being a DHCP client and uses the IP address information that the DHCP server supplies.
- If no DHCP Server replies, then the Control Unit defaults to being the DHCP server for the LAN. It then does the following:
  - It allocates itself the IP address 192.168.42.1 and IP Mask 255.255.255.0.
  - By default, the Control Unit supports 200 DHCP clients. Any PC that connects to the LAN as a DHCP client is given an address between 192.168.42.2 and 192.168.42.201 plus 255.255.255.0 as its IP mask and 192.168.42.1 (the Control Unit's address) as its default gateway settings.
  - Note: Address for device on the LAN are allocated from the bottom of the DHCP range upwards. Addresses for dial-in connections are allocated from the top of the DHCP range down.
  - Any PC or device that needs to connect to the Control unit and have a fixed IP address should use IP addresses between 192.168.42.202 and 192.168.42.254.
  - The address 192.168.42.255 is a broadcast address.

Any of these LAN settings can be altered using Manager. For more information see Connecting to the LAN.

Default Telephony Settings

The Control Unit comes with a default configuration.

- No prefix is required for dialing external telephone numbers.
- Various default short codes are available to enable user's to utilize system features via their telephone, see Default System Short Code List.
- Each extension is associated with a User and the user name defaults to "Extn201", "Extn202" etc. The user name appears in the Caller Display so you may want to change these to real names. These are configured using the User configuration form.
- All incoming voice calls are routed to a group called Main (200), which contains the first 16 extensions. Use the Incoming Call Route Form to create incoming call routes to other destinations (extension, fax machines, etc.).

How the System Receives Time

Whenever the Control Unit reboots, it requests the time using the standard Internet Time protocol (RFC868).

Time servers may give the time in local format or in UTC (Universal Time Coordinates) format. If the Control Unit receives the time in local time format it uses that time. Otherwise if it receives the time in UTC format, it uses that time plus the Time Offset configured through Manager in the System Form.

The Voicemail Server, Voicemail Pro Server or Manager programs can all act as Time servers, giving the time as set on their host PC's. They all give the time in both local time format and UTC format.

Following a reboot the Control Unit repeats its request every hour. It first makes the request using the Voicemail Server IP address in its configuration and if it receives no reply it then does a broadcast request.

If you are running Manager when the Voicemail Server starts, then Voicemail does not start as a time server. It is therefore highly recommended that you have no copy of Manager running when you start or restart the Voicemail Server.

You can check the time held by the Control Unit on any phone with a suitable display. Alternatively you can run the **Monitor** application and enable the option **System | System Resource Status Prints** to see the Control Unit's time.

Upgrading Manager and IP Office

Introduction - Upgrading IP Office

Because Manager is an application used for managing the IP Office control unit, upgrading the Manager application does not update the control unit's core software. It is highly recommended that when the IP Office control unit software is upgraded, the Manager application is upgraded as well.

Before attempting an upgrade, ensure that you have performed all the necessary Pre-Upgrade Checks. Certain IP Office control units require additional steps and procedures.

Note: The processes in this document are generic upgrade processes only. When upgrading it is your responsibility to check for and refer to any relevant Avaya Technical Bulletins and other instructions relating to the particular upgrade being performed.

Validated Upgrade

If you are running Manager 2.1 or later and IP Office 2.1 or later, 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 ticked (default) before performing the upgrade. With the **Validate** box ticked, the system will check that it has received the new .bin files and then give you the option to upgrade. If you untick 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 earlier, 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.

Pre-Upgrade Checks

Before proceeding with the upgrade, check the following:

1. Are your Manager PC and the IP Office on the same LAN segment?

   If you are running Manager 2.1 or later and IP Office 2.1 or later, then a validated upgrade will be available. If you are running Manager 2.0 or earlier or if you are running Manager 2.1 but the control unit is still running IP Office 2.0, a validated upgrade will not be performed. If the latter situation applies, make sure your Manager PC and the IP Office are on the same LAN segment and the upgrade is not being performed across WAN or RAS links.

   - Ensure that the Manager PC has a fixed (static) IP address.
   - In Manager, select **File | Preferences**. The current setting (shown in bold) should be **255.255.255.255** in order to test broadcast routing between the Manager PC and IP Office. If not, select that setting and then check that Manager can see and receive the configuration from the IP Office being upgraded.
   - Check the Manager's programs working directory is the folder containing the bin files. The directory is shown in the Manager's title bar and can be set using **File | Change Working Directory**.

2. Upgrade the IP Office Admin & User Software Suites if necessary.
   If upgrading between software levels, for example from 1.1 to 1.3, you should also upgrade the IP Office Administration suite of software to match. The new level of .bin software is likely to need the matching level of Manager software to allow access to new configuration fields. See Upgrading IP Office Application Software.

3. Manager PC IP Address.
   The PC running IP Office Manager should be given 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.

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

5. Copy the Latest IP Office Configuration.
   Always ensure that you have received and made a copy of the latest configuration from the IP Office system before attempting any upgrade.

6. Obtain the Bin files.
   If you have upgraded the IP Office Manager application, then the appropriate .bin files are copied to the Manager's working directory (in 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.

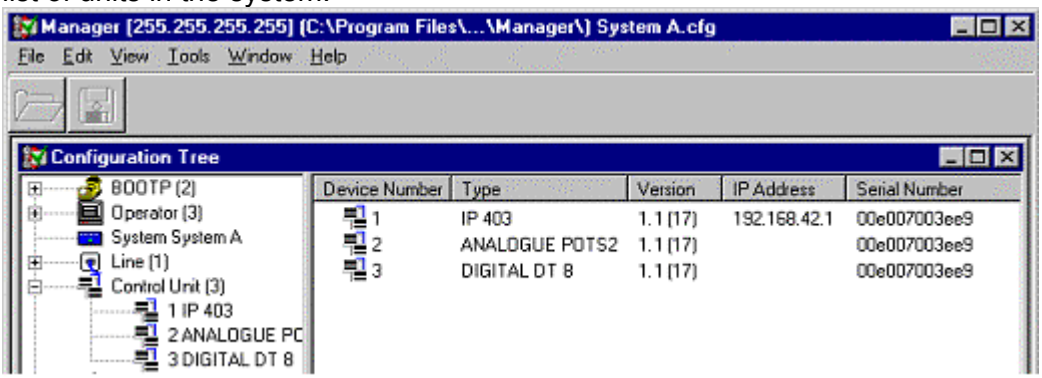
   - Upgrading IP403 Systems to 2.0

     IP403 control units must be upgraded to 2.0 in a two stage process. The first stage involves using the ip403.bin file found in the Manager IP403V1_99 sub-folder. Copy this file to the Manager folder and then perform the upgrade. The second stage involves using the **ip403.bin** file found in the **Manager IP403V2_0** sub-folder. Copy this file to the Manager folder and repeat the upgrade.

   - If you have obtained .bin files from another source check that you have a copy of any instructions provided with those bin files and check that the system complies with those instructions. Backup the existing .bin files and then copy the new files into the Manager's Working Directory.

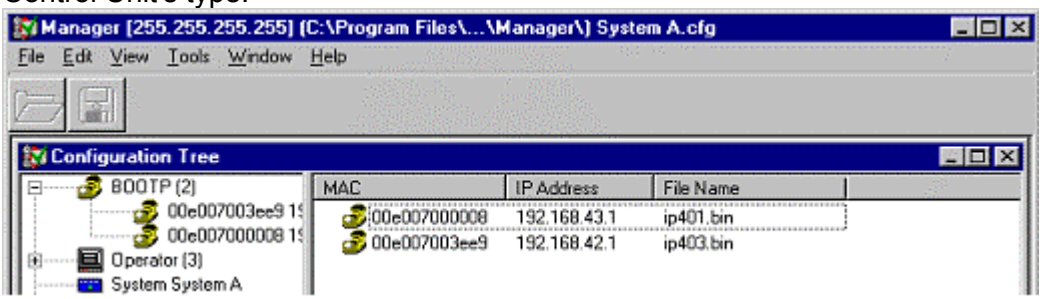
7. Check the Manager BOOTP Entries.
   BOOTP is part of the process by which the IP Office restarts and requests new software. The Manager PC acts as the IP Office's BOOTP server and must have a BOOTP entry for the IP Office.

a. In Manager, receive the IP Office's configuration file. Click on **Control Unit** to display a list of units in the system.



b. Device Number 1 is the Control Unit (ie. 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.

c. Click on **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.



d. If an entry does not exist right-click on the displayed list and select **New**. Enter the required details and click on **OK**. You do not need to send the configuration back to the IP Office as BOOTP entries are stored on the Manager PC.

e. Double-check the entry as this is a critical setting for the upgrade process.

Upgrading IP Office Application Software

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 uninstalling and then reinstalling the software.

The uninstallation 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.

1. Open the Windows Control Panel (**Start | Settings | Control Panel**).
2. Select **Add/Remove Programs**.
3. Select the IP Office application suite to be removed, eg. IP Office Admin Suite, IP Office User Suite, Voicemail Pro.
    - If removing Voicemail Pro, ensure that you have backed up the existing call flow database first, see the "Voicemail Pro Installation" manual for further details.
4. Click on **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. When the process has completed, select another IP Office suite to remove if necessary.
8. Click on **OK** to finish and close the Control Panel.
9. The new versions of the application suites can now be installed.

.bin Files for Control and Expansion Units

The software for IP Office Control Units and Expansion Units is provided in the form of .bin files. These are normally copied to the Manager application's working directory during installation of Manager.

This table describes the different .bin files.

File	Description
ip401.bin	Core software for IP401 Control Units.
ip403.bin	Core software for IP403 Control Units.
ip406.bin	Core software for IP406 Control Units.
ip412.bin	Core software for IP412 Control Units.
naatm16.bin	Software for Analog Trunk Expansion Modules.
nadcp-16.bin	Software for Digital Station Expansion Modules.
nadt-16.bin	Software for Digital Terminal Expansion Modules.
nas0-16.bin	Software for S0 Expansion Modules.
nawan3.bin	Software for older 10Mbps WAN3 Modules.
avpots16.bin	Software for Phones Expansion Module (analog extensions).
ipwan3.bin	Software for 10/100Mbps WAN3 modules supported from IP Office 1.4 onwards.

The following .bin files, also found in the Manager folder, are for Avaya 4600 Series IP telephones.

File	Description
ap4602rx_y.bin	ap4602rx_y.bin Boot file software for 4602 Telephones. The **x_y** indicates the software level, eg. ap4602r1_6.bin.
bbxxxxx.bin	Boot file software for 4600 Series IP Phones.
defxxryy.bin	Telephony software for 4602, 4606, 4612 and 4624 telephones. **xx** indicates the phone type and **yy** the software level, eg. def24r1_70.bin.

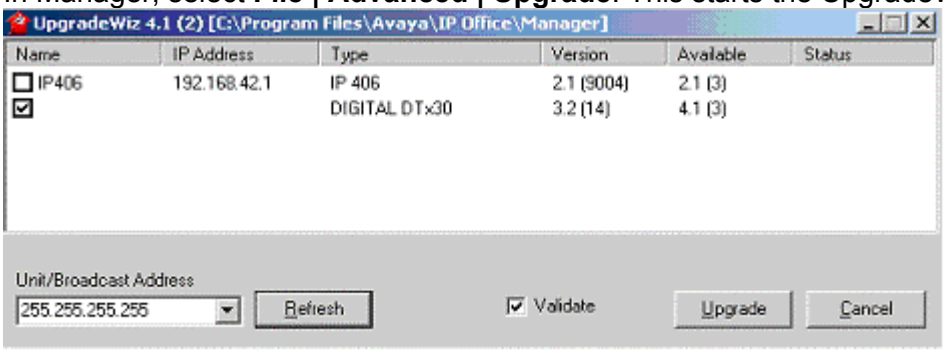
Upgrading Control and Expansion Unit Software

Upgrading IP 401 Systems 2.1 or Later

The 401 control units that are currently running IP Office 2.1 or later have an automatic rollback feature as part the upgrade process. The rollback occurs if the new software is broken or does not work with the control unit during the trial period – 5 minutes (default) after the system has rebooted and is running the new software. The rollback will restore the previous IP Office software version and the configuration that was in place at the time of the upgrade. An asterisk (*) will appear next to the Transferred status for the IP Office 401 unit to indicate that rollback is available. **Note:** Trial time is configurable within the .bin file.

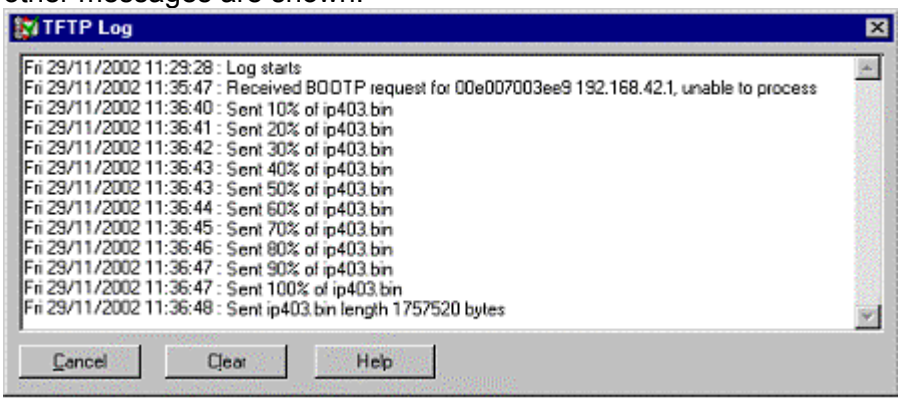
To upgrade an IP Office control and/or expansion unit software:

1. Ensure that you have followed the Pre-Upgrade Checks.
2. Ensure that you have received and made a copy of the IP Office's configuration. If the upgrade fails the current configuration may be erased so a backup copy is an essential precaution.
3. In Manager, select **File | Advanced | Upgrade**. This starts the UpgradeWiz application.



4. After a few seconds the wizard should list 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.
5. 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. Tick 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 ticked by default. Leave the box ticked 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 on **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. The unit will continue operating as if an upgrade was never attempted.

12. An example TFTP log for a successful upgrade is shown below. Refer to Troubleshooting if any other messages are shown.



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

Troubleshooting

If the IP Office does not reboot after the upgrade or goes into a reboot loop, then the upgrade has not been successful.

Some clues as to the cause may be given by the entries in the TFTP Log that was running during the upgrade process.

1. **Unable to Send**
   The following or similar in the TFTPLog indicates that the required .bin file was not in the Manager's Working Directory:

```
: 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
```

   - If this occurs check the setting for Manager's Working Directory (File |Change Working Directory). Then check that the file detailed by the BOOTP entry is in that folder. A set of .bin files is also available in the \bin folder on the IP Office Administration CD. Then remove and reapply power from the IP Office to force a reboot attempt.

2. **Unable to Process**
   The following or similar in the TFTPLog indicates that a matching BOOTP entry was not found.

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

   - If this occurs use Manager to add or edit the required BOOTP entry. Then remove and reapply power from the IP Office to force a reboot attempt.

If these actions do not resolve the issue, the IP Office will have to be reset via the DTE port. For details refer to the Job Aid "DTE Port Maintenance".

Using Manager

Operators

Operators are people who use Manager to configure the system. Operators can be created with different levels of access to the configuration file.

A configuration form represents each entry in the system's configuration. Each operator can be given the rights to View different types of forms, Edit those forms, create New entries and Delete entries. Some forms consist of a number of tabs and operators can be restricted to which of those tabs they can access. All the configuration forms are discussed in more detail in their respective sections.

Each Operator has a user name and a password. Once an Operator has logged on to Manager, they can open configuration files held on the PC or received from the Control Unit. Access to the configuration forms within the configuration file will be dependent on the Operator's rights.

Each Operator can change their password by doing the following:

1. Select **Change Password** from the **File** menu and enter your new password.
2. Click **OK**.
3. Select **Logoff** from the **File** menu and the "Enter Operator Name and Password" dialogue box returns.
4. Log on using your new password.

Default Operators

When Manager is installed it creates five default operators, whose user name and passwords match. The default operators can access the following configuration forms:

- **Administrator:**
  The Administrator has full access to all configuration forms and can create, edit and delete Operators.
- **Manager:**
  Line (View, Edit and Delete only), Extension (View and Edit only), Service (IP, AutoConnect, Quota and PPP tabs only), Firewall Profile (Standard tab only), System, User, Hunt Group, Short Code, Incoming Call Route, Directory, Time Profile, Least Cost Route and Account Code.
- **Operator:**
  User (view and edit the Voicemail, DND, Telephony and Forwarding tabs only), Hunt Group (view and edit the Hunt Group tab only), Time Profile (view and edit only), Directory and Account Code.

Creating Operators

The top-level operator, called "Administrator" has rights to create new operators, change operator settings and delete operators. This is done by accessing the Operator form after logging onto Manager as the Administrator. See Operator Form.

Receiving a Configuration

With each start-up or reboot of Manager, it needs to get the current configuration from the Control Unit. The configuration is copied from the system's RAM and includes any user changes made since the last reboot of the system. The system's current configuration can be received from the Control Unit using either of the methods below.

To Receive and Open a Configuration

1. Click on the 🗁 icon or select **File** and then **Open**.
2. Manager scans the LAN for Control Units.
3. If only one Control Unit is detected, the **Receiving Config From** dialogue box appears - go to step 5; otherwise, the **Select unit to read configuration from** dialogue box will appear.
4. The Control Units found are listed in the box. Select the Control Unit required and then select **OK**.
5. Enter the system password. The configuration is then read and opened in Manager. The following message appears in the Manager status bar - "*filename*.cfg Received OK Size xxxx".
    - If no configuration file is loaded, the most likely cause is an incorrect system password.
6. A copy of the configuration file is also saved in the Manager's Working Directory as a .cfg file. The System name is used for the file name.

To Receive, Name and Open a Configuration

This method of opening a configuration allows you to rename the configuration file if so desired before opening it. It also allows you to see the file being received and then you can open it by clicking the 🗁 icon.

1. Select **File** and then **Offline**.
2. Select **RecvConfig**. Manager scans the LAN for Control Units.
3. If only one Control Unit is detected the Default File Name dialogue box appears - go to step 5, otherwise the "Who Is" dialogue box appears.
4. The Control Units found are listed in the box. Select the Control Unit required and then select **OK**.
5. Enter the name you wish to give the configuration file in the Default File Name dialogue box (by default the System name is used).
6. Select **Yes** in the "About to Receive *filename*.cfg from..." dialogue box
7. Enter the system password. The configuration is then received by Manager (the configuration file is received into the Manager program file). The follow message appears in the Manager status bar - "*filename*.cfg Received OK Size xxxx".
8. Click the 🗁 icon or select **File** and then **Open**.
9. Enter the system password.

Editing a Configuration

Manager displays the Control Unit's configuration as a series of icons in two panels.

The left-hand panel contains a configuration tree, with icons used to group different types of configuration entries. Double-click on a top-level icon within the configuration tree to expand or collapse the display of matching entries under each icon. Click on the top-level icon to display the matching entries in the right-hand panel.

Double-click on an entry in either the left or right-hand panel to display the configuration form for that entry. Each form contains a range of settings appropriate to the type of entry. Each form may consist of a number of tabbed pages (referred to as 'tabs'). For details of the various forms see The Configuration Tree .

In the right-hand panel you can select an entry in the right-hand panel and then right-click to View, Edit, Copy or Delete the entry. Additionally, you can right-click to Add a new entry.

This is a brief overview of the commands that can be used to view and alter the configuration. For details of additional commands, see Toolbar .

- **Right Mouse Button**
  The right mouse button can be used within the right hand side pane of the configuration tree and you are given a menu with options for View, Edit, New and Delete. These allow you to view, edit or delete an existing entry or create a new entry.
- **Sorting**
  Each branch of the Configuration Tree lists its entries under column headings (Users are listed by Name, Extension, Options and Forwarding etc.) To change the entry order, either ascending or descending, click on the column heading, eg. to view your Users in descending order click on the Name column.
- **Drag and Drop**
  Entries can be copied between configuration forms using drag and drop. For example, a short code created for a user can be copied to another User by dragging the short code between the two open forms.
- **Direct Access**
  In most cases where a list box is used to select a Hunt Group, Time Profile, Firewall Profile etc., it is possible to double-click on this entry to enable you to view or edit the relevant form.

Sending/Saving a Configuration

After making any configuration changes, the new configuration needs to be saved before the changes are reflected. When saving a configuration, what actually happens is that the new configuration is sent back to the Control Unit for updating. Hence, the terms "saving" and "sending" a configuration are used interchangeably within Manager. There are two ways to send a configuration, via a system merge or a full reboot of the Control Unit.

A reboot/merge configuration list tells you which configuration form can be merged or and which requires a reboot.

Instructions for sending a configuration back to the system apply to both the merge and reboot method. Each time a live configuration is sent back to the system, you can choose between a merge and a reboot.

Configuration Sizes can effect the sending of configuration forms back to the different IP Office Control Units.

Instructions for Sending a Configuration

Certain configuration changes require sending the new configuration back to the Control Unit via a reboot. Though this only takes a few seconds, it cuts off any calls in progress. To avoid upsetting users, select the **Reboot When Free** option.

The configuration file is sent from the PC to the system's Flash memory. The reboot then causes the Flash configuration to be copied to the system's RAM memory.

If you are working with a configuration received from the Control Unit by selecting **File | Open**.

1. Click on the  icon or choose **File | Save**.
2. Select the reboot action required:
    - **Immediately** - Reboots the Control Unit immediately and will cut off any calls in progress.
    - **When Free** (default) - Reboots the Control Unit when the system is free (no calls in progress).
    - **Merge Config** - The Control Unit will not be rebooted, but only certain configuration changes can be merged. See Sending a Configuration via Merge.
    - **None** - Does not send any configuration to the Control Unit.
3. If you did not enter a system password when you received the configuration, then a password MUST be entered at this point to send the configuration to the Control Unit.
4. Select **OK**.

Configuration Sizes

There are maximum size limits to the configuration that can be loaded into the different IP Office Control Units. These are:

- **IP401:** 64KB.
- **IP403:** 192KB.
- **IP406:** 192KB.
- **IP412:** 1.0MB.
- **Small Edition:** 192KB.

Attempting to load a configuration that exceeds the limits above will cause the system to lock and require resetting via the DTE port.

Figures for all individual entries in the configuration cannot be given as they vary between software releases. The list below gives typical values, in bytes, for common entries:

- **Extension:** 70.
- **User:** 170.
- **Short code:** 40.
- **DSS button:** 20.
- **RAS:** 110.
- **Intranet Service:** 240.
- **WAN Service:** 400.
- **IP Route:** 30.
- **Account Code:** 40.
- **Directory Entry:** 70.
- **Internet Service:** 220.
- **Hunt Group:** 100 (+ 10 per member).
- **Firewall:** 40 (+ 80 per custom entry).
- **Time Profile:** 40 (+ 20 per entry).
- **Licence:** 40.

Reboot/Merge Configuration List

Certain configuration changes can be merged and become active without a reboot and others require a full reboot. Merged changes are copied to both the system's RAM and Flash memory.

Manager tracks the changes made to the configuration so that if all changes made can be merged, then the option for sending the configuration will automatically be selected to **Merge Config**.

The table below shows which configuration form can be merged and which requires a system reboot:

✔ : Configuration changes can be merged.

X: Configuration changes require a system reboot.

	Merge	Reboot
BootP	N/A	N/A
Operator	N/A	N/A
System		X
Line	✔	
Unit		X
Extension		X
User	✔	
Hunt Group	✔	
Short code	✔	
Service	✔	
RAS	✔	
Incoming Call Route	✔	
WAN Port		X
Directory	✔	
Time Profile		X
Firewall Profile	✔	
IP Route	✔	
Least Cost Route	✔	
License	✔	
Account Code	✔	
User Restriction	✔	
E911		X
Wireless		X
Logical LAN		X
Tunnel		X
Auto Attendant		X

Supported Country and Locale Settings

- When a new or defaulted system's configuration is first opened in Manager, the system's Locale is set to match that of the PC running Manager. This Locale can be changed through the System form if required.
- The system's Locale sets the default ringing patterns and caller display settings.
- The locale also controls the language that a voicemail server will use for prompts. Note however that the range of languages installed and supported on the voicemail server may differ from those supported by the Control Unit. For details refer to the Voicemail Installation & Administration Manual.

This list indicates locale settings supported within the Control Unit software. Note: This does not necessarily indicate support, availability or approval for IP Office within that country.

Country	Locale(s)	Default Caller Display
Argentina	ess	FSK-D
Australia	ena	UK20
Belgium	frb, nlb	FSK-D
Brazil	ptb	DTMF-D
Canada	enc, frc	FSK-D
Chile	esl	FSK-D
Columbia	eso	UK20
Denmark	dan	DTMF-C
Finland	fi, fin	DTMF-A
France	fr, fra	FSK-D
Germany	de, deu	FSK-D
Greece	ell	FSK-D
Holland	nl, nld	DTMF-D
Hungary	hu, hun	FSK-D
Iceland	isl	
Italy	it, ita	FSK-D
Korea	ko, kor	FSK-D
Mexico	esm	FSK-D
New Zealand	enz	UK20
Norway	no, non, nor	UK
Peru	esr	FSK-D
Poland	pl, plk	FSK-D
Portugal	pt, ptg	UK20
Russia	ru, rus	
South Africa	ens	
Spain	es, esp, esn	FSK-D

Sweden	sv, sve	DTMF-A
Switzerland	frs	FSK-D
UK	en, eng	UK20
USA	enu	FSK-D
Venezuela	esv	FSK-D

Offline Files

Working with Offline Files

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.

Another use for offline files is if for any reason, your live configuration gets erased, you can open an offline configuration file (if you have saved a version offline) and send it to your live system without needing to re-configure your system from scratch.

Saving an Offline File to a Live System

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.

If you are working with an offline configuration and are now ready to merge it with the live system:

1. Click on the  icon or choose **File | Save**
2. Go to **File** menu, select **Offline | Send Config**
3. Manager program scans the LAN for all Control Units (The LAN can be defined in Preferences)
4. If only one Control Unit is detected the **Sending Config To** dialogue box appears - go to step 6 otherwise Manager then offers a list of the Control Units found
5. Select the Control Unit you wish to send the configuration to
6. Enter the System password in the **Sending Config To** dialogue box and select the **Reboot** mode - See Reboot.
7. 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.

Installing and Configuring Ports

Port Types

The IP Office supports a wide range of ports. The types of port supported vary from country to country. For details of the IP Office ports supported in a particular country, contact Avaya in that country.

- **BRI:** *Basic Rate Interface*
  These are provided for BRI line connection or via the S0 Expansion module for BRI device connection.
- **DS:** *Digital Station*
  Provides support for Avaya 4400 and 6400 Series telephones.
- **DT:** *Digital Terminal*
  Provides support for Avaya 20 Series telephones. Not supported in the United States.
- **Expansion:**
  These are used for connection to IP Office Expansion Modules.
- **LAN:** *Local Area Network*
  These are 10/100MBps auto-detect Ethernet LAN ports.
- **POT:** *Plain Ordinary Telephone*
  Provide support for analog telephones.
- **WAN:** *Wide Area Network*
  See Installing and Configuring WAN Ports and Voice over IP - Overview.

Installing and Configuring DT Ports

Installing and Configuring DT Ports

Some Control Units are equipped with DT ports. These can also be added to a system by installing a DT Expansion Module.

DT ports are used to support Avaya 20 Series telephones. Further details on the use of these phones are given in the User Guide for each phone.

Note that DT ports are not supported within the United States.

More:

- Installing a DT Expansion Module
- Configuring DT Features

Installing a DT Expansion Module

1. Using the blue expansion cable supplied, connect the DT Module to the Control Unit via the next available Expansion port.
2. Power up the DT Module via the power supply provided.
3. Reboot the Control Unit, the Control Unit will not see the DT module until after a reboot.
4. Receive the configuration from the Control Unit.
5. Check under Control Unit that the DT module is now listed. Check that the additional Extensions and Users are listed. These can be renumbered and renamed as per normal extensions.
6. Connect the DT handsets to the extension ports required.

Configuring DT Features

Using INDEX

The **INDeX** facility on a DT display telephone allows a user to speed dial other users on the system. It lists all Users configured on the Control Unit. If a User has a Full Name configured then that appears instead of their User Name.

Account Codes

Once account codes have been created in the configuration, the **ACCOUNT** option on DT display telephones can be selected during an external call. The user can then enter an account code that matches any of those on the system. This account code is recorded with the call information in the systems call log output.

If the **Force Account Code** option has been set for a User, **NO ACCOUNT CODE** appears on their DT handset if they try to make an external call without first entering an account code.

Call Pickup

The **PICKUP** option on a DT display telephone allows a user to pick up and answer calls to a pre-configured Pickup Group. The user can set the Pickup Group through their telephone or it can be done via a short code as shown below. The user does not have to be a member of the group they select as their Pickup Group.

This configuration is stored as a User Short Code as per the following example:

- **Short Code:** *PICKUP
- **Telephone Number:** 300
- **Line group ID:** 0
- **Feature:** CW

DIVERT

The **DIVERT** key on DT telephones allows the user to switch forwarding on/off and to select the number to which calls are forwarded. It is also used to program the numbers to which calls are forwarded. These settings appear in the Forwarding tab of the User configuration form.

NO CALLS

The **NO CALLS** key on DT telephones allows the user to switch Do Not Disturb on/off. This then uses the options set in the User's DND tab.

The users can also use the key to program the Outgoing Call Bar option in the Telephony tab of the User configuration form.

Using Speed Dials

When a user presses **Speed Dial** on a 20 Series handset they are given three choices as shown below.

- **INDEX**
  Allows the user to select entries from the system's Directory. DT display telephones display the Directory Name and allow the user to speed dial the associated number.
- **SYSTEM**
  Allows the user to select from pre-configured system speed dials numbered 100 to 999. These are created as System Short Codes as per the example below:
  - Short Code: *SD100
  - Telephone Number: 01923123456
  - Line group ID: 0
  - Feature: Dial (or DialExt if internal)
- **OWN**
  Allows the user to select from personal pre-configured speed dials numbered 0 to 9. These are created as User Short Codes as per the example below:
  - Short Code: *SD01
  - Telephone Number: 01923123456
  - Line group ID: 0
  - Feature: Dial (or DiaExt if internal)

Forward

The **Forward** facility on DT telephones allows users to set their Follow Me option from any DT telephone on the system. The setting then appears in the User's Forwarding tab.

DSS Keys

The DSS keys on a DT telephone (if available) can be programmed to an extension or group number. These settings appear as User Short Codes but are set through the Button Programming tab.

GROUP

The **GROUP** key can then be used to disable/enable the User's membership of any groups. See Enable/Disable Membership .

LOG ON

By default, **LOG ON** is available on all DT display telephones. Only users with a login code can access this user. While logged in a LOG OFF option is available. **NOT LOGGED ON** is displayed when no specific user is logged on. See Hot Desking .

Passcode

When changes are made to User options, eg. forwarding, or to phone features, eg. Ringer volume, via a 20 Series handset, the user has to enter a passcode. By default the passcode is 0000. The **PASS** option allows the user to change their passcode. This is then stored in the Telephony tab of the User's configuration form as the Login Code.

Directory Name

When a user changes their Directory Name on a 20 Series handset this is stored in the User Form as their Full Name. Note - Phone Manager always uses the Full Name in preference to the User Name.

Language

When a user changes the Language being used on their 20 Series handset this is stored in the User Form as their Locale.

Voicemail

When dialing an internal extension from a 20 Series handset the call will not be automatically passed to Voicemail if the extension is busy or not answered within the **Allocated Answer Interval**. The **VOICE** or **VMAIL** option is used to access the Voicemail Server. The options then available are dependent on the type of voicemail server being run.

Installing and Configuring DS Ports

Installing and Configuring DS Ports

Some Control Units are equipped with DS ports. These can also be added to a system by installing a DS Expansion Module.

DS ports are used to support Avaya 4400 and 6400 Series telephones. Further details on the use of these phones are given in the User Guide for each phone.

- **Note: 4400/6400 Ringing Tones**
  The 4400 and 6400 telephones store ringer cadences internally and so cannot be altered by settings within Manager.

More:

- Configuring Softkeys
- Assigning Functions to DSS Keys
- Using DisplayMsg
- Call Coverage

Configuring Softkeys

The 4412D+, 4424D+ and 6400 series phones display a number of softkey functions. The default softkey menu is:

- Dir, Drop, HfAns, Timer, DpkUp, AutCB, Prog, CFrwd, Cpark, SAC, TmDay, Admin.

Other functions may be substituted for the default function. See Installing and Configuring DS Ports for a list of functions. Alternatively an Abbreviated Dial may be configured for the SoftKey. The softkey menu is changed either through the phone (using **Menu | Admin**) or by adding entries in the User's Short Code table.

- **Changing a Softkeys Function:**
  The example below configures softkey 1 to be "**GrpPg**" (function number 138) for hunt group 200. This replaces the default softkey 1 function "**Dir**".
  - **Short Code:** *SK1 *(Softkey 1)*
  - **Telephone Number:** 138/200 *(function number 138 with parameter 200)*
  - **Feature:** CW

- **Using a Softkey for Abbreviated Dialing:**
  The softkey menu may include Abbreviated Dial elements. Again this can be done via an entry in the User's Short Code table. For example:
  - **Short Code:** *SK2 *(Softkey 2)*
  - **Telephone Number:** Lewis/217 *(the text to display above the softkey (max 5 characters) and the number to dial)*
  - **Feature:** Dial

Assigning Functions to DSS Keys

Functions can also be made available via the DSS keys. This is done through the User's **Button Programming** tab. This allows you to select an action for the DSS key and to enter the telephone number or parameters for that action.

- Note that for each DSS key setup, a short code of the form ***DSS** appears in the User's **Short Codes** tab. Changes made these short codes are ignored and overwritten by the settings in the Button Programming tab.

The actions supported are **Dial**, **Group**, **Park**, **User, Emulation** and **Advanced**.

- **Dial**:
  This is an abbreviated dial where the LED illuminates for the duration of the call, giving the user some feedback as to what was pressed. Abbreviated Dial may be partial dialing strings. For example it may contain "732" and be labeled "NJ", with the user being required to complete the dialing.
- **Group**:
  Monitor the status of a Hunt-group queue. Flashes green if a call is incoming to the group, flashes red if calls for the group are being queued. Put the name of the group, surrounded by quotes, in the Telephone Number field.
- **Park**:
  Monitor a park slot. The red LED is lit if the park slot is occupied by a call parked by another station, or green if the park slot is occupied by a call parked by the station with the programmed PARK BLF button. If you are the user who parked the call, pressing this button reconnects you to the call. If another party parked the call, pressing this button once provides call information and pressing it a second time connects you to the call. Select Answer from this menu to pickup call.
- **User:**
  Monitor a user. This is a Busy-Lamp-Field. Put the name of the person, surrounded by quotes, in the Telephone Number field.
- **Emulation:**
  Gives access to number of functions that emulate operation on other telephone systems. See Emulation Functions.
- **Advanced:**
  Gives access to a range of short code functions which can be assigned to DSS keys. See Short Code Features.

Users can setup the Dial, Group, Park and User actions through their telephone using **Menu | Menu | ProgA | DSS**.

Using DisplayMsg

There is an additional method for starting DS functions. This is via a specially formatted "DisplayMsg". Other users may send the DisplayMsg, CTI applications may send it, or a user may send a message to themselves. The format of the display message is as follows: [0)nnn/ppppppp

To set a short code up:

- **Short Code:**
- **Telephone Number:** xxxx;[0)nnn/ppppppp
  - xxxx is the destination. If empty, DisplayMsg is self-directed.
  - nnn is the function number
  - ppppppp is the parameter data (if required)
- **Feature:** DisplayMsg

Call Coverage

Call Coverage

Call coverage allows calls ringing at one extension (the 'Sender') to also be presented and answered at other extensions at the same time (called the 'Covering Extensions').

Senders

Senders are extensions that share their alerting calls with another extension(s), referred to as their Covering Extension.

The only calls that are not shared are:

- Hunt Group calls that alert at the sender.
- Automatic Intercom calls.
- Calls that have been forwarded/diverted to the sender.
- Paging calls.
- Calls that are being covered for another station.
- Calls from one of their covering extensions.

Covering Extensions

When the Senders extension rings, the Covering Extensions also ring and show the call on a free Call Appearance button. The display indicates that the call is from the sender by showing the incomings call's name or number and the sender's name.

Covering Extensions can receive their own calls as well as calls for the Sender. A Covering Extension can receive a call when:

- Send All Calls/Do Not Disturb is not active.
- Forwarding/Divert is not active.
- They have an available Call Appearance button to accept the call.

Notes

To help Covering Extensions handle coverage calls efficiently it is suggested that the following buttons are programmed. See Setting Up Call Coverage for further details.

- **Program additional Call Appearance buttons :** Covering Extensions must have enough Call Appearance buttons for their own calls and for the extensions they are covering. By default each extension has three Call Appearance buttons. A suggested minimum extra is one less than the number of Call Appearance buttons on the Sender's extension.
- **Program a Voicemail Collect button for the Sender :** This will allow the Covering Extension to transfer a call directly to the Sender's Voicemail.
- **Program an Automatic Intercom button for the Sender :** This allows the Covering Extension to place a Voice Announce. If you do not wish to make Voice Announce calls, use Dial Intercom instead.
- **Program a Send All Calls button**
- **Program a Drop Button :** This helps in transferring calls.

Call Alerting Scenarios

Listed below are examples of how calls to the Sender's extension are handled in specific scenarios.

- **Sender and Covering Extensions available:**
  An incoming call alerts both the Sender and Covering Extension's on Call Appearance buttons. It alert the Sender's extension for their set Allocated Answer Interval and then alerts the Covering Extension only until the call is answered or the caller hangs up.
- **Sender available/Covering Extension not available:**
  An incoming call alerts the Sender only. The call remains alerting until it is answered or the caller hangs up.
- **Sender not available/Covering Extension available:**
  The call will alert the Covering Extension but not the Sender. The call remains alerting until the call is answered or the call hangs up.
- If voicemail is available and enabled for the Sender, then in all the above scenarios, following the Sender's Allocated Answer Interval timeout the call is redirected to the Sender's voicemail.
- **Sender and Covering Extension not available:**
  The caller hears busy tone or is redirected to the Sender's voicemail.

Setting Up Call Coverage

Within IP Office Manager, the following configuration screens need to be amended to enable Call Coverage.

Senders

For the Sender, the following changes should be made to their **User** form settings:

- **Telephony:**
  - Enable **Call Waiting**.
- **Call Coverage:**
  - Set the Covering Extensions: Right-click and select the required extension from the list shown.
- **Button Programming/Digital Telephony:**
  - Add at least two additional Call Appearance buttons (**Emulation | Appearance**).
  - Add a Send All Calls buttons (**Emulation | Send All Calls**).

Covering Extensions

For the covering extensions, the following changes should be made to their **User** form settings:

- **Button Programming/Digital Telephony:**
  - Add additional **Call Appearance** buttons.
    1. Click an unused button and select **Emulation** | **Appearance**.
  - Add a **Drop** button.
    1. Click an unused button and select **Emulation** | **Drop**.
  - Add a **User** button.
    1. Click an unused button and select **User**.
    2. In the Telephone Number field, enter the Sender's extension name in quotes; eg. "Extn201".
  - Add a **Voicemail Collect** button for the sender.
    1. Click an unused button and select **Advanced | Voicemail | Voicemail Collect**.
    2. In the Telephone Number field, enter the sender's extension name preceded by # and in quotes, eg. "#Extn201".
  - Add an **Automatic Intercom** button for the Sender.
    1. Select **Emulation | Automatic Intercom**.
    2. In the Telephone Number field, enter the sender's extension number. If automatic intercom is not required then the Dial Intercom function can be used instead.
  - Add a **Send All Calls** Button (ie. toggle DND Button).
- **Telephony:**
  - Enable **Call Waiting**.

Installing and Configuring S0 Ports

Installing and Configuring S0 Ports

The S0 module provides ISDN BRI outputs so you can share out ISDN access from say your PRI line to ISDN2 devices like Video Conferencing Control Units or ISDN PC Cards.

An S0 module appears as S0 lines in the system configuration. DID numbers on the main line can be routed out to devices attached to the S0. To add S0 lines the configuration should be received from a Control Unit, which will then update the configuration file with the correct hardware detail.

1. Attach the S0 module to one of the Control Unit's expansion ports and power up the module
2. Reboot the Control Unit.
3. Open the configuration from the Control Unit. Check that the extra lines have been added to the configuration.
4. The default line configuration is probably totally usable/acceptable apart from changing the line group IDs.
5. Any call from the ISDN device attached to the S0 should be able to make external calls. The outgoing rules are the same as apply to any extension.

Example Configurations

To route incoming calls on, eg. DID 123456 to the first port, eg. Line Group ID 701:

1. **Configure an Incoming Call Routing:**
   The destination (type this in) represents the short code to be used to direct the call to the correct line group ID. Note that the Bearer Capability has been set to Any, to allow data and voice via this route.
   - **Line Group ID:** 0
   - **Incoming Number:** 123456
   - **Destination:** 123456
   - **Bearer Capability:** Any
2. **Create a System Short Code:**
   This matches the destination in the Incoming Call Route.
   - **Short Code:** 123456
   - **Telephone Number:** 123456
   - **Line Group ID:** 701
   - **Feature:** Dial
3. Send the configuration to the Control Unit.

Any call coming into the main system on DID 123456 will now be passed directly to the first port.

If you wish to assign DID's from your main pool to individual ports and avoid network charges when dialing between them try variations on the following:

1. You have **DID** ranges, eg. 7325551000 to 7325551099. You wish to assign 7325551000-19 to port 1 and 7325551020-20 to port 2 etc.
2. **Configure Incoming Call Route:**
   The # is used here instead of "n" to avoid problems with, eg. "Main". The minus sign means the number is processed from the left and so will wait for the whole number.
   - **Line Group ID:** 701
   - **Incoming Number:** -100x
   - **Destination: #**
3. Repeat for Line Group ID 702 etc.
4. Create Short codes, eg.
   - **Short Code:** 100x
   - **Telephone Number:** .
   - **Line Group ID:** 701
   - **Feature:** Dial

S0 calls dialed without the area code are handled locally without network charges. Calls with area calls will go via the network.

Installing and Configuring WAN Ports

Installing and Configuring WAN Ports

The Control Unit has a Wide Area Network (WAN) port that can be connected to a digital leased line service using either V.11 or V.24 or V.35 interface at speeds up to 2048kbps.

Point-to-Point protocol (PPP) is used over this link. ISDN links can also be used in the event of failure of the WAN link to provide alternate or top up bandwidth on demand.

The link can use CHAP (encrypted passwords) to verify the end users (preferred) or PAP giving no authentication. If the link is to provide no authentication use identical names for the RAS, Service and User and do not enable the Encrypted Password option. If the link is to provide authentication the RAS name must match the User name at the remote end and enable Encrypted Password in the Service and RAS.

Installing a WAN3 Module

The WAN3 module provides an additional 3 WAN ports. The interface of these ports is identical to the WAN port on the Control Unit.

- Note:
  Installation of a WAN3 module requires allocation of an IP address to the WAN3 unit via DHCP, ie. a DHCP server must be present on the LAN. Following installation the allocated IP address can be changed if required.

1. Switch off power to the IP Office Control Unit.
2. Connect the WAN3 module to the Control Unit using the LAN cable supplied with the unit. This connects to a LAN port on the front of the Control Unit.
3. Apply power to the WAN3 module.
4. Switch on power to the IP Office Control Unit.
5. Run Manager and check under **File | Preferences** that the broadcast address being used is ***255.255.255.255***.
6. Click on the Manager folder icon or select **Open** from the **File** menu. The list of available units should include both the Control Unit and the WAN3 module.
   - If the WAN3 module icon appears indented from the Control Unit icon then it is associated with the Control Unit. Go to Step 13.
   - If the WAN3 module icon appears in-line with the Control Unit icon then the WAN3 module is not associated with the Control Unit. Go to Step 7.
7. Select and load the configuration from the Control Unit.
8. Double-click on the Unit icon to display the installed units.
9. Right-click on the right-hand panel and select **New**.
10. Click on the WAN3 unit to be added.
11. Send the new configuration to the Control Unit and reboot (do not use **Merge**).
12. Click on the Manager folder icon or select **Open** from the **File** menu. The list of available units should include both the Control Unit and the WAN3 module.
    - The WAN3 module icon should now appear indented to the right of the Control Unit icon. If this is not the case then repeat Steps 7 to 12.
13. You can now proceed with configuring the ports on the WAN3 module by selecting and loading the configuration from the Control Unit.

Configuring a WAN Link

To create a data link from Site A to Site B via the WAN port configure the Control Unit as per the following example:

At Site A on IP address 192.168.43.1.

1. **Create a Normal Service:**
   The Service name can be any text and is used to identify this particular Service. The Account Name and password are presented to the remote end, therefore must match the User name and password configured at Site B. The Encrypted Password option can only be used if the remote end also supports CHAP.
2. **Create a User:**
   Under the Dial In tab tick Dial In On. This User account is used to authenticate the connection from the Site B. Note that if the Service and User have the same name these two configuration forms are automatically linked and become an Intranet Service. The User password is displayed at the bottom of the Service tab as the Incoming Password.
3. **Setup RAS:**
   If CHAP is to be used on this link then the Encrypted Password option must be checked in the Service and in the RAS service. The name of the RAS service must match the name of the Service at Site B. Note that if the RAS settings are given the same name as the Service and User they are automatically linked and become a WAN Service. Ensure that the Encrypted Password option is not checked when using a WAN Service.
4. **Edit the WANPort:**
   Note: Do not create a new WANPort, this is automatically detected. If a WANPort is not displayed, connect the WAN cable, reboot the Control Unit and receive the configuration. The WANPort configuration form should now be added.
5. **Create an IP Route:**
   In the IP Address field enter the network address of the remote end, not the IP address of the Control Unit. Under Destination select the Service created above.

At Site B on IP address 192.168.45.1

1. Repeat the above process but altering the details to create a route from Site B to Site A

PBX Features and Functions

Notes

This section covers many of the system features of the Control Unit.

- **Digital Telephones.**
  Note that this section chiefly covers the use of short codes dialed by the user from any type of phone. The Control Unit's DS or DT ports support digital phones, which may access these functions through special keys and display menus. Refer to the separate User Guide for these types of phone.
- **RECALL Button.**
  Many sections make reference to the **RECALL** button on telephones. On some phones this may be marked as **R** or **HOLD**.
- **Calls without CLI.**
  Many features of the PBX utilize the ICLID that accompanies the call. These features (such as external call auto-answer and trusted source mailbox access) will not work if the incoming line provides no ICLID.

Extension versus User

Within Manager, there are configuration forms for both extensions and users. The following paragraphs discuss the relationship between the two within Manager and the IP Office control units.

Extensions refer to physical telephone ports, their characteristics and connection. The Manager configuration tree displays the list of physical extensions available on the system.

Users are the people who use the system and Dial In users for data access. A system User does not have to have an Extension Number that physically exists - this can be useful if the user does not require their own extension but does require to use other system features such as Voicemail, call forwarding, etc.

By default, each Extension is associated with a User. The User Name is used to identify the caller in the display of suitable phones and PC programs. These User Names can be changed via the User Form .

Physical extensions are associated with an extension number through their Extension Form . A User is associated to that extension, by setting that extension number in their User form.

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".

Related Topics:

- Extension Form
- User Form

Account Codes

Account Codes

Account codes are commonly used to control cost allocation and out-going call restriction. Once a successful call has been completed using a certain account code, that account code information will be removed from the internal call information. This means that using the redial button will not re-activate the account code; the user must re-enter the account code each time the restricted number is dialed.

The method for entering account codes depends on the type of phone used.

Account codes can also be made mandatory for users via Force Account Code.

The account code used on a call is included in the call information output by the system's call log. Incoming calls can also trigger account codes automatically by matching the Caller ID stored with the account code.

- To create an account code:
  1. Click **Account Code** to display a list of existing account codes.
  2. Double-click on an existing account code to edit it or right-click on the displayed list and select **New**.
  3. In the **Account Code** field, enter the code to be used to track specific calls.
     - Alphabetic characters can be used in account codes for users dialing from Phone Manager.
     - Wildcards can be used within the account code. The wildcard ***?*** matches a single character, for example 123??? matches any 6 digit account code starting 123. The wildcard ***** matches any digits, for example 456* matches any account code beginning with 456.
  4. In the **CLI** field (optional), entering a Caller ID means that the account code is automatically assigned to incoming or outgoing calls with the same Caller ID.
  5. Send the configuration changes to the Control Unit via Merge.

An account code can be entered before the number is dialed if the user knows the number to be dialed is restricted. If the account code is entered before the number is dialed, a dial tone is supplied to indicate the line is ready to accept the phone number. If the phone number is dialed first, a re-occurring beep will sound to indicate the request for an account code. There are two ways users can enter an account code prior to dialing the phone number:

- Creating a short code
- Via Phone Manager - See the Phone Manager User Guide

Once the account code is created, it can be used in the following ways:

- To force the use of account codes for individual users
- To force the use of account codes at the system level
- To allow Plain Ordinary Telephone (POT) users to enter account codes

If you have IP Office Phone Manager, the list of account codes can be made available to Phone Manager users. See Account Codes and Phone Manager.

Force Account Code

A user can be forced to enter an account code when making ANY external call. This setting is useful when tracking calls for costing purposes or simply for restricting the use of certain numbers. When used for billing purposes different accounts will be billed depending on the account code entered by the user. The Force Account Code field is available for individual users as well as on a system wide basis.

 **Warning:** Users with POT (Plain Ordinary Telephones) can only enter account codes prior to entering the restricted telephone number and if the Set Account Code short code is created. POT users can not enter account codes at the system prompt.

- To force the use of account codes for individual users:
    1. Receive the system configuration if one is not opened.
    2. Click **User** located in the Configuration Tree panel.
    3. In the list of users, double-click the user name or extension for whom you want to force the use of account codes.
    4. Click the **Telephony** tab.
    5. Tick the **Force Account Code** option.
    6. Click **OK**.
    7. Merge the configuration.
    8. If the user is using Phone Manager and does not enter an account code, they see an error message. 20 Series, 4400 series and 6400 series handset users see a request to enter an account code on the phone's display.

Account codes can also be used as PIN codes to restrict outgoing calls. At the short code level, account codes can be set as a mandatory use in association with outgoing dialed numbers. Once set up, users are required to enter an account/PIN code when the number being dialed is matched to a defined restricted number. These restricted numbers are defined using a short code. Any valid account code can be used as a PIN code.

- To force the use of account codes at the system level:
    1. Click the **Short code** form.
    2. In the list of short codes, right-click one of the short code and select **New**.
    3. Create a short code for a number you want to restrict. For example:
        - Short Code: 00xxxxxxxxxx
        - Telephone Number: 00N
        - Feature: Dial
        - Force Account Code: Ticked

       This example forces the use of account codes when dialing an international number. In this example, wildcards are used in defining the restricted number so that PIN codes are not requested in the middle of dialing a number. In this example, a matching number of **00x xxx xxx xxxx** will request the PIN code after the entire number has been dialed. If we had entered a matching number of **00**, the system would request the PIN code in the middle of dialing the number, as it would be matched after just 2 digits.
    4. Click **OK**.
    5. Merge the configuration.

Account Codes and Phone Manager

If you have IP Office Phone Manager, the list of account codes can be made available to Phone Manager users. To make the list of account codes available, set up the following within Manager:

1. Open the **System** form for your IP Office Control Unit.
2. Click the **Telephony** tab.
3. Tick the **Show Account Code** field.
4. Click **OK**.
5. Send the configuration changes to the Control Unit via Reboot.

If the Show Account Code field is left unticked, Phone Manager displays asterisks in the account code field to signify that account code digits are being withheld from view.

Call Restriction

Simple call barring can be applied using short codes. This uses the fact that the IP Office checks dialed numbers for short code matches in a specific order, see Matching Order.

Example:
We want to allow only selected users to dial numbers starting 91900. To do this, we must set up 2 short codes. The first one is a system short code that stops all general users from dialing numbers starting with 91900:

System short code: **Short code | Right-click | New**

- **Short Code:** 91900N
- **Telephone:** blank
- **Feature:** Busy

To allow a specific user to override the above system short code and dial 91900 numbers, we should add the following to their user short codes:

User specific short code: **User | Double-click a specific user | ShortCodes tab | Right-click | Add**

- **Short Code:** 91900N
- **Telephone:** 1900N
- **Feature:** Dial

Using User Restrictions

Within Manager, users can be grouped by the types of numbers they are allowed to dial or not allowed to dial. For example, those who are allowed to dial 1900 or international numbers.

The **User Restriction** form allows named groups of dialing short codes/restrictions to be created. These short codes can then be applied to a user by associating them with the **User Restriction** name rather than having to recreate the short codes for each user.

To set up a restriction within the **User Restriction** form:

1. Click **User Restriction** form within the Configuration Tree.
2. Enter a name for the restriction.
3. Click the **Short Code** List tab and create a short code.
4. Merge the configuration.

For a description of all the fields within this form, see User Restrictions Overview.

To apply a User Restriction to a specific user:

1. Click the **User** form within the Configuration Tree.
2. Double-click the user for whom you want this restriction applied.
3. Within the **User** tab, click the **Restriction** drop down box and select the **User Restriction** you want applied to this user.
4. Merge the configuration.

Example:

Through **User Restrictions**, we can create a new **Group** called ***Standard***. To this group, we would add the short code for barring 91900 numbers:

- **Short Code:** 91900N
- **Telephone:** 1900N
- **Feature:** Busy

To apply this short code to a specific user, select the **User** formand in the **Restrictions** drop-down list for that user, select ***Standard***.

Conferencing

Conferencing Overview

IP Office systems support the following conference capabilities:

Control Unit Conference Capabilities

Note: *The term conference party refers to both internal and external callers.*

- **IP401 & IP Office- Small Office Edition:**
  Supports a single 3-way conference.
- **IP403 & IP406:**
  Supports multiple conferences totaling up to 63 parties. For example:
  - 21 x 3-way conferences.
  - 1 x 10-way conference (10 parties) plus 11 x 3-way conferences (33 parties) and free capacity for 20 more conference parties to join new or existing conferences.
- **IP412:**
  Supports multiple conferences totaling up to 126 parties but with no more than 63 parties in any one conference.
  - The IP412 supports two 63 party conference banks. When a new conference is started, the bank with the most free capacity is used for that conference. However once a conference is started on one conference bank, that conference cannot use any free capacity from the other conference bank.
- **Analog Line Restriction:**
  In conferences that include external analog line calls, only a maximum of two analog line calls are supported.

Note: System features such as call intrusion, call recording and silent monitoring all use conference resources. This includes automatic recording if enabled.

When any of these features is active, the number of slots available for conference parties is reduced.

Default Conference Handling

The methods below use the IP Office's default system short codes.

To start/add to a conference:

1. Place your first call or the existing conference on hold. Existing conference parties will still be able to talk to each other.
2. Call the new party.
   - If not answered, or diverted to voicemail, or answered but the party does not want to join the conference; put them on hold and dial ***52** to clear the call.
3. If answered and the other party wants to join the conference, put them on hold and dial ***47**.
4. All held calls are now in conference.
   - Digital display extensions will see **CONF** followed by the conference number.

To exit a conference:

1. Any party wanting to leave a conference can simply hang-up.

Using Conference Meet Me

Each conference on the IP Office is assigned a conference number. This number is displayed on suitable display phone extensions (eg. Avaya 20, 4400, 4600 and 6400 display phones).

Conference Meet Me allows users to join or start a specific numbered conference. This method of operation allows you to advertise a conference number and then let the individual parties join the conference themselves.

Through the **Button Programming** tab (also called **Digital Telephony**) within IP Office Manager, the **Conference Meet Me** function can be assigned to a DSS key (select **Advanced | Call | Conference Meet Me**). This allows simple one key access by internal users to specific conferences.

- **Note:** Conference Meet Me can create conferences that include only one or two parties. These are still conferences using slots from the IP Office's conference capacity.

Example 1: Meet Me to any conference

The following example system short code allows any extension to dial *67* and then the number of the conference which they want to join followed by #. For example dialing *67*600# will put the user into conference 600.

- **Short Code:** *67*N#
- **Telephone Number:** N
- **Feature:** Conference Meet Me

Example 2: Meet Me to a specific conference number

The following example system short code allows the dialing extension to join a specific conference, in this case 500.

- **Short Code:** *500
- **Telephone Number:** 500
- **Feature:** Conference Meet Me

If you are asked to add a party to a conference, having a conference meet me short code is very useful. With the conference in progress, call the new party. When they answer, hold the call, dial the conference meet me short code and then hang-up.

Conferencing with 4400, 4600 and 6400 Series Display Phones

These phones support the following features for conference calls on IP Office.

To add another caller to a call or conference:

1. During the existing call or conference, press **Conf** .
2. Dial the other party.
    - If not answered, end the call either by pressing the **Drop** or **Hold** button, then press **Conf**.
    - When answered, press **Conf** again. Any call that was put on Hold is now conferenced in.

To drop a caller from a conference:.

Note: If the conference only contains four parties (including yourself), using Drop to remove the last caller added will end the whole conference.

1. During the conference, press **Menu** .
2. Using the ◀ and ▶ keys, display and then select **Drop**.

To display calls in a conference:

1. **CONF** on your display indicates that you are in a conference call.
2. Press **Menu** twice.
3. Select **HC&P** (held, conference and parked).
4. The ▼ above **Confs** indicates a conference call. Select **Confs**.
5. Use the ◀ and ▶ keys to see the details of the different callers in the conference.
    - **To remove a caller from the conference:** Select **Drop**.

Note that 4600 series telephones cannot add callers to a conference when working handsfree. They can return to handsfree once they have completed adding a call to the conference.

Conferencing with 20 Series Display Phones

The 20 series display phones support the following features for conference calls on IP Office:

1. Press **HOLD** to put your first call or the existing conference on hold. Existing conference parties will still be able to talk to each other.
2. Call the new party.
    - If not answered, or diverted to voicemail, or answered but the party does not want to join the conference; put them on hold and dial ***52** to clear the call.
    - If answered and the other party wants to join the conference, press **SCROLL** and then **CONFER**.
3. All held calls are now in conference.

Conferencing with Phone Manager

The IP Office Phone Manager application can be used to setup and control a conference. Even if the conference is started by other methods, the conference parties will appear in the Phone Manager's Conference tab.

1. Make an outgoing call or answer an incoming call.
2. Place the call on hold (click on).
3. Make a call to the required third party (click on).
4. Place that call on hold also (click on).
5. Repeat steps 3 and 4 until all parties required for the conference are on hold.
6. Click on .
7. The **Conference** tab will appear in Phone Manager. This shows you all the conference parties.
8. To remove a caller from the conference, right-click on their entry in the Conference tab and select **Hang Up**.

Conference Recording

WARNING

The use of call recording is normally subject to local laws and regulations. Before using call recording, you must ensure that you have complied with all applicable local laws and regulations. Failure to do so may result in severe penalties.

If your IP Office also has Voicemail Pro installed, then it can support call recording. Call recording can be applied to conference calls and is not controlled by the intrude settings of the internal conference parties.

The Voicemail Pro has an "Advice of Call Recording" setting. If this is enabled, then all parties in the conference will hear a message that the call is being recorded. Note: Once recording has been started, if a further participant is added to the conference the recording will stop, the new party having not heard the advice of call recording message.

Remember that the Voicemail Pro counts as an additional conference party so recording will not work if all conference slots are in use.

To start recording:

- 20 Series display phone users can press **SCROLL** and then **RECORD**.
- 4400 and 6400 Series display phones users can press **Menu** twice, then **Func** and **Recor**.
- Users running IP Office Phone Manager can select **Functions** and then **Record**.
- For other users, a call record short code must first be setup via Manager. They can then put the conference on hold, dial the short code and when recording begins they are returned to the conference.

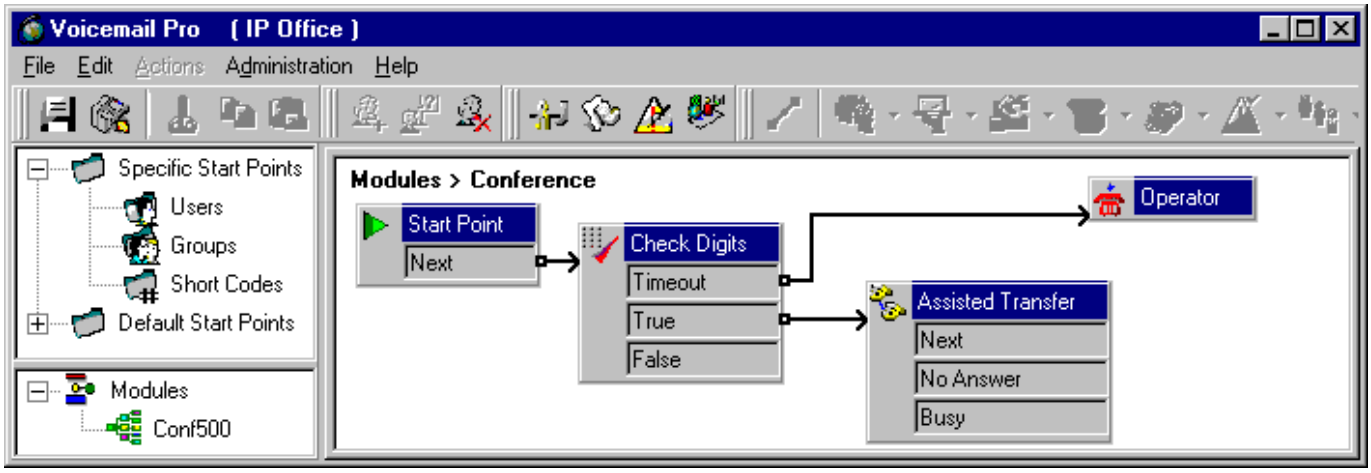
Conferencing and Voicemail Pro

The Voicemail Pro can be used to route callers into a conference.

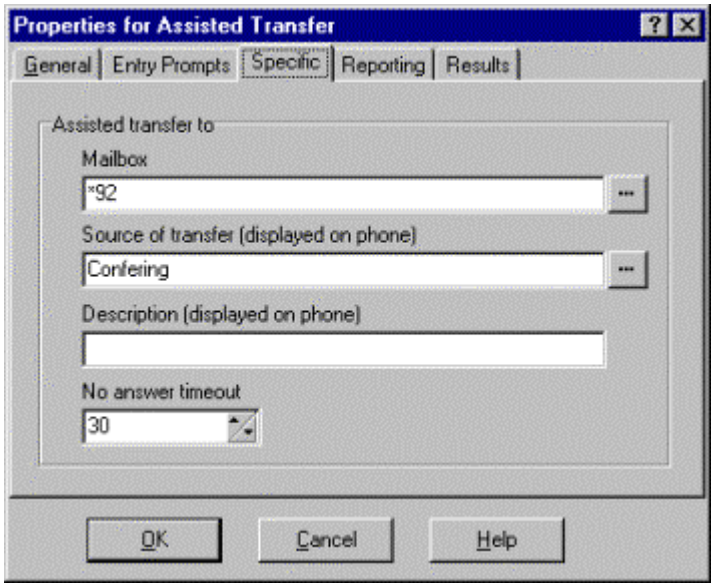
Example 1

In this example callers are routed into conference 500.

1. Using IP Office Manager, a new short code was created. This code allows callers to indicate the conference they want to join.
    - **Short Code:** *92
    - **Telephone Number:** 500
    - **Feature:** Conference Meet Me
2. In Voicemail Pro, a new module called ***Conf500*** was created.
3. The following actions were then added to the module.



- The **Check Digits** action forces callers to match a PIN code.
- The **Assisted Transfer** action contains the short code created above. This will place the caller into conference 500 in this example.

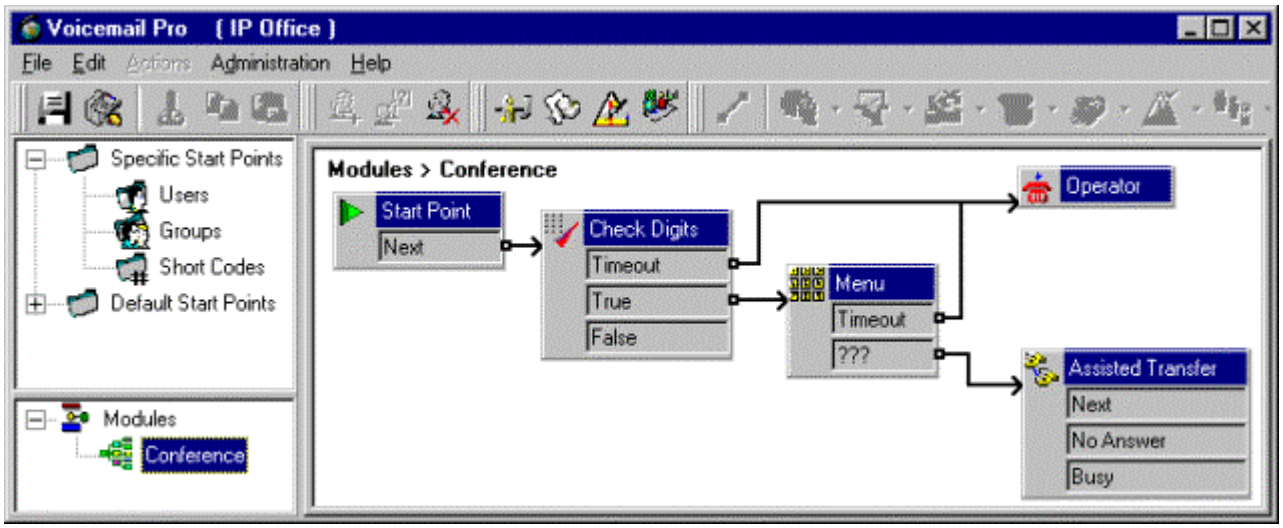


4. External callers can be routed to the module by entering its name in an Incoming Call Route or making the module an option in an existing auto attendant call flow.

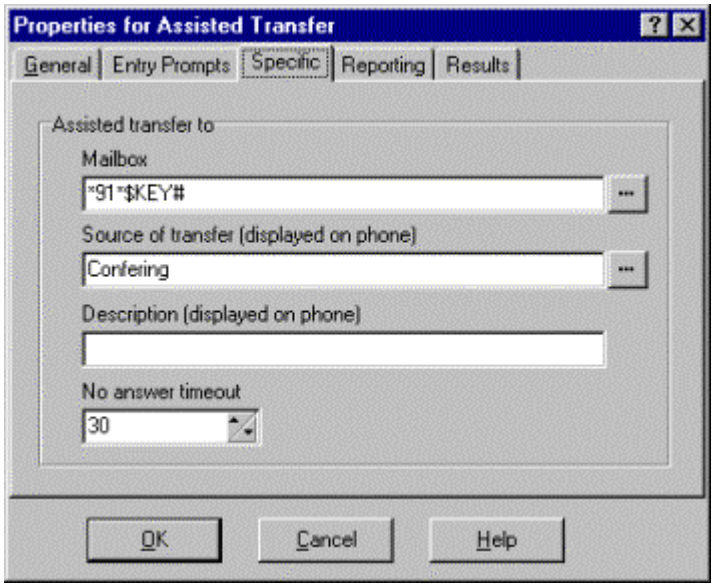
Example 2

In this example, callers are able to specify the conference they want to join.

1. Using IP Office Manager, a new short code was created. This short code allows callers to indicate the conference they want to join. In this example conference 500.
    - **Short Code:** *91*N#
    - **Telephone Number:** N
    - **Feature:** Conference Meet Me
2. In Voicemail Pro, a new module called ***Conference*** was created.
3. The following actions were then added to the module.



- The **Check Digits** action forces callers to match a PIN code.
- The **Menu** action has been configured to expect 3 digits, indicated by the ***???***.
- The **Assisted Transfer** action uses the short code created above. ***$KEY*** part uses the digits the caller entered in the **Menu** action.



4. External callers can be routed to the module by entering its name in an Incoming Call Route or making the module an option in an existing auto attendant call flow.
5. Adding another short code to the IP Office system lets internal callers also access the call flow.
    - **Short Code:** *90
    - **Telephone Number:** "Conference"

- **Feature:** Voicemail Collect

Caller Display

Caller Display uses Incoming Caller Line Identification (ICLID) passed by the Telephone Company via the line. It shows up on phones with display windows and is also passed to your PC programs, and the PC TAPI interface.

Extensions can be configured to enable or disable Caller Display via their Extension Form. Note that the presentation of Caller Display information can delay the ringing of the phone. Also if used on some non-Caller Display phones, it can cause a slight ringing at the start and end of calls. If this is not desired then disable the caller display on the extension.

The Control Unit's Directory allows you to associate names to numbers that you may receive on the system.

- **Note: Caller ID can not be forwarded**
  If an extension is forwarded to another extension the Caller ID of the forwarded extension is received, not the Caller ID of the original call.

Call Forwarding

This is the ability to forward a User's calls to another extension or external number. Calls can be forwarded when there is no answer, when the extension is busy or for all calls. This can be enabled/disabled by dialing short codes or via the Phone Manager application.

The following default Short Codes are available to make use of Forwarding:

- **To set the number for forward all calls and forward on no answer**
  - *07*N# - The user should enter the number in place of the N, eg. *07*208# or *07*5551234#.
- **To set the number for forward on busy**
  - ***57*N#** - The user should enter the number in place of **N**, eg. *57*208#.
- **To set forwarding for all direct station (ie. not Hunt Group) calls**
  - ***01** enables forwarding.
  - ***02** disables forwarding.
- **To set forwarding when the user's extension is not answered**
  - ***05** enable.
  - ***06** disable.
- **To set forwarding when the user's extension is busy**
  - ***03** enable.
  - ***04** disable.

A forwarded call cannot, by default, be transferred back to the original destination. To allow this facility, set Do Not Disturb and enter the Forward Number as a Do Not Disturb Exception.

A forwarded call is processed through all extensions' forwarding path. For example, if extension 201 forwards to 202 and 202 forwards to 203 a call to 201 rings at 203.

When forwarding all is enabled, a user can also forward their Hunt Group calls via Phone Manager or by using the default short codes as follows:

- ***50** - Enable Forward Hunt Group calls.
- ***51** - Disable Forward Hunt Group calls.

Call Intrusion

The Call Intrude short code feature allows a user to join an existing conversation, whether this is an internal or external call.

To set up this facility, a System or User short code such as the example below must be created:

- **Short Code:** *90**N*#*
- **Telephone No:** *N*
- **Feature:** CallIntrude

Based on the above example where N = extn. 201, a user can intrude into a call at extension 201 by dialing *90*201#.

For a user to intrude, **Can Intrude** must be selected on their **Telephony** tab. By default this is not selected. In addition, the users that they are trying to intrude on must not have their **Cannot be Intruded** option checked.

If a user wants to prevent anyone intruding on their calls, the **Cannot be Intruded** option on the user's **Telephony** tab should be checked, which is the default.

The **Dial Inclusion** short code feature is similar to **Call Intrude** but allows the intruding party and the intrusion target to talk without the other party hearing them. During this type of intrusion, all parties hear a repeated intrusion tone. When the intruder hangs-up the original call parties are reconnected.

Directory

The Directory is a list of numbers and associated names stored centrally in the configuration. A Directory Entry can be used to identify a incoming call on a caller display telephone or via a PC application, or give a system wide list of frequently used numbers for speed dialing via Phone Manager or a 20 Series, 6400 series, 4412 and 4424 handset.

An example entry would display "HeadOffice" in a user's caller display when a call from 5551234 is received. Users will see "HeadOffice" in the Directory List in Phone Manager or via INDeX function on a 20 Series, 6400 series, 4412 and 4424 handsets and can speed dial that number.

Call Pickup

A user can answer a call to another extension by using Short Codes.

The following default short codes can be used:

- ***30 - Call Pickup Any**:
  To allow a user to pick up any (the first available) call ringing on another extension.
- ***31 - Call Pickup Group**:
  This allows a user to pick up a Hunt Group call ringing on another extension. The user must be a member of that Hunt Group.
- ***32*N# - Call Pickup Extn**:
  Pick up a ringing call from the specified Extension. N representing the specific Extension.
- ***53*N# - Call Pickup Members**:
  Pick up any call ringing on another extension that is a member of the Hunt group specified. The incoming call can be as a result of a DID call to that extension, an internal call to that extension, an internal or external call to the Hunt Group, a call to a phone from another Hunt Group etc. N represents the extension number of the Hunt Group.

Acquire Call

The Acquire Call facility allows a user to take over the call currently on the Extension Number specified.

Using the default short codes a call can be acquired by dialing -

- ***45*N#**
  N representing the extension number from which the call is to be acquired, eg. ***45*205#**
- ***46**
  This short code takes over the last call from your Extension. This function is useful when you want to catch a call you have just missed that has gone off to Voicemail. The **RECLAIM** function in the Phone Manager application also performs this function.

Call Waiting

Enabling Call Waiting allows a user who is already on a call to be made aware of another call to their extension. An intermittent call waiting tone is played (the tone varies according to locale) and depending on the phone type, information about the new caller may be displayed.

To answer a call waiting, either end the current call or put the current call on hold, and then answer the new call. Hold can then be used to move between calls.

On phones with multiple call appearance buttons, pressing the appropriate button allows you to move between calls. This can also be done through IP Office applications such as Phone Manager.

Call waiting can also be provided for hunt group calls if the hunt group Ring Mode must be Group. The group members personal call waiting must also be enabled.

The following default short codes are available when using Call Waiting. The short code features they use can also be assigned to DSS buttons.

- ***15 - Call Waiting On**:
  Enables call waiting for the user. An intermittent beep indicates a waiting incoming call.
- ***16 - Call Waiting Off**:
  Disables call waiting for the user.
- ***26 - Clear CW**: (Clear & Pickup Call Waiting)
  Clear the current call and pick up the waiting call.
- ***27*N# - Hold CW**: (Hold & Pickup Call Waiting)
  Place the current call on hold and pick up the waiting call.
- ***28*N# - Suspend CW**: (Suspend & Pickup Call Waiting)
  Suspend the current call into the specified slot and pick up the waiting call.

Do Not Disturb

This is the ability to temporarily stop incoming calls to a user's telephone. It prevents the user from receiving Hunt Group calls and give direct callers either busy or Voicemail if available (Note that if Call Forwarding and Do Not Disturb are active, the call is not forwarded, but does receive Voicemail). This can be enabled/disabled by dialing short codes or via the Phone Manager application.

If, however, specific numbers are required to override Do Not Disturb, internal and external phone numbers can be added to an exception list.

The following default Short Codes are available to make use of Do Not Disturb:

- **To turn Do Not Disturb on**
  - ***08** enable.
  - ***09** disable.
- **To add an internal or external number to the Exception List**
  - ***10*_N_#** - The user should enter the number in place of the N, eg. ***10*5551234#**
- **To delete a number from the Exception List**
  - ***11*N#** - The user should enter the number in place of the N, eg. ***11*5551234#**

Follow Me

The **Follow Me To** facility allows a user to take his calls from another location, whether this is an internal or external number. This feature can be set at the user's extension using Short Codes or via the Phone Manager application.

The **Follow Me Here** facility allows a user to take his calls from another extension. This feature can be set at the destination extension using Short Codes.

In both cases if the redirected call receives busy tone or is not answered then the call behaves as though the User's extension had failed to answer, eg. Forward settings take effect.

The following default Short Codes are available to make use of Follow Me:

- **To set Follow Me To at the user's extension**
  ***14*N#** - The user should enter the destination number in place of the N, eg. ***14*208#**
- **To cancel Follow Me To at the user's extension**
  ***14*#**
- **To set Follow Me Here at the destination extension**
  ***12*N#** - The user should enter his extension number in place of the N, eg. ***12*204#**
- **To cancel Follow Me Here at the destination extension**
  ***13*N#** - The user should enter his extension number in place of the N, eg. ***13*204#** or dial ***14*#** at the user's extension.

Holding a Call

Pressing **Alternate Call** on a telephone places a call on hold and dial tone is provided. Music On Hold is played if this facility is available. Reconnect to the call by pressing **Alternate Call** again, or if the handset has been replaced the system will call the extension back after approximately 2 minutes.

See Parking a Call .

Music on Hold

Music on Hold (MOH)

The IP Office can provide music on hold (MOH) in one of two ways:

- **Internal MOH:**
  During a reboot, the IP Office downloads a .wav file called **holdmusic.wav** from Manager; this file is not permanently stored in the Control Unit. If the main Control Unit receives a **holdmusic.wav** file on reboot, the Audio port is ignored. **Note:** Internal music on hold is not supported by the IP401.
- **External MOH:**
  Connect an audio source to the 3.5mm audio port on the back of the IP Office control unit.
    - If an internal MOH file has been downloaded, the IP Office will not recognize any external MOH input until it is rebooted without the internal MOH file.

If the message "Unable to send Hold Music" appears in the TFTP Log or on the status bar of Manager, this means that a "holdmusic.wav" file could not be found in the Working Directory. Ignore this message if you are using the Audio Port. This message can also be an indication that communication between the main Control Unit and LAN has been lost since reboot.

Checking Music on Hold

The IP Office has a default system short code that allows you to listen to a system's current music on hold.

1. At an idle extension, dial ***34**.
2. You will hear the system's music on hold.

Note: You must ensure that any MOH source you use complies with copyright, performing rights and other local and national legal requirements.

Internal Music on Hold

The IP Office supports internal music on hold by using a .wav audio file that it downloads during a reboot. **Note:** Internal music on hold is not supported by the IP401.

The preferred .wav file properties are:

- PCM, 8kHz 16-bit, mono.
- Maximum length 30 seconds.

- **? How do I get a suitable .wav file**
  There are many suppliers of music on hold files. Though many of these require a single payment they are then free of copyright and public performance issues. Do an internet search on MOH and 'wav'.
- **? How do I check and change my .wav files**
  Use Windows Sound Recorder to check and change the .wav files properties. Select **Start | Programs | Accessories | Entertainment | Sound Recorder**.
  - Open your .wav file and then select **File | Properties** to view its properties. Use **Convert Now** to change the properties to those required by IP Office.
  - If the file is too long, you can use the slider and the **Edit | Delete After Current Position** option to shorten the file.
  - Use **Save as** and rename the file as ***holdmusic.wav***.
- **? How do I download the file to the IP Office**
  Use the following process:
  - Copy the .wav file to the IP Office Manager folder (**c:\Program Files\Avaya\IP Office\Manager**) and name it **holdmusic.wav**.
  - Select **View | TFTP Log** and arrange the windows so that you can see it and Manager at the same time.
  - Use **File | Advanced | Reboot** to send a reboot command to the IP Office. You will be asked for the system password.
  - During the reboot, in the TFTP Log you should see a request for holdmusic.wav and the file then being downloaded.
  - Following the reboot you should be able to test the music on hold by dialing ***34** at an extension.
- **! I do all the above but the file is not downloaded**
  If running Manager over a WAN link, a RAS connection or from different LAN domain, then the default TFTP request for the music on hold file during reboot won't work. See "Internal MOH and Remote Maintenance".

Notes:

1. *The IP Office will accept .wav files in other formats and then attempt a suitable conversion. However the results and range of formats that it will convert cannot be guaranteed. Additionally, higher quality audio .wav files will have larger files sizes that lengthen the reboot time whilst losing the extra quality after conversion.*

External Music on Hold

The Audio port of the IP Office control unit is a standard 3.5mm audio jack socket. It accepts input using standard 3.5mm audio stereo or mono jack plugs.

- **? Can I connect a personal music player**
  Yes, if it has an auto-repeat mode. Simply connect the headphone sockets to the IP Office audio port. Note however that these devices are not normally designed for continuous 24/7 operation.

- **? What device should I use**
  We recommend that you use a dedicated hold music device. These are available from most telecommunications installers and distributors.

- **? Can I Use Internal Music on Hold as well**
  No, the IP Office only allows one music on hold source. If it downloads an internal music on hold file it will ignore any input from the Audio port. To remove the internal music on hold file, you must delete 'holdmusic.wav' found in the Manager program folder and reboot the IP Office.

The IP Office audio port accepts a maximum 200mV RSM input and provides an impedance of 10kΩ per channel.

Internal MOH and Remote Maintenance

During its reboot, the IP Office sends out a broadcast TFTP request for the **holdmusic.wav** file.

Since it is a broadcast request, it typically will not be forwarded by any network routers. Also because the IP Office is rebooting, any existing WAN or RAS connection are broken until the reboot is complete.

These are the possible resolutions (apart from using external music on hold):

- **If the Manager PC is on a LAN connection to the IP Office:**
  In the IP Office configuration, set the TFTP Server Address on the System form to the IP Address of the PC running Manager.
- **Run a Second TFTP Server on the Same LAN as the IP Office:**
  Using a second TFTP server with a copy of ***holdmusic.wav*** file in its file directory and on the same LAN as the IP Office ensures that the file is available to the IP Office during its reboot.
- **Use Manager:**
  Install a second copy of Manager on the IP Office's local LAN and set this copy of Manager to run permanently. Whilst remote maintainers may frown upon this, we always recommend that Manager is installed somewhere on the IP Office local LAN to support local maintenance when remote connection is not working.
- **Use another TFTP Server Program:**
  Any TFTP server can be used to provide the ***holdmusic.wav*** file. We have tested operation with **TFTP32** (*http://tftp32.jounin.net* - disable its DHCP after install) and **TFTP Server 2000** *(http://support.avaya.com)*.

Incoming Call Routing

Incoming Call Routing

By default all incoming voice calls are sent to the hunt group Main (extension 200), which contains the first 16 extensions. All incoming data calls are sent to a RAS service called DialIn, see IP Route Form .

The **Incoming Call Route** form allows entries to be created to route incoming calls to different groups, extensions, RAS services or voicemail. These routes can be based on the incoming line group, the type of call, incoming digits or the caller's CLI.

Each call route has a Destination. The **Destination** field allows selection of any existing user, hunt group and RAS service in the configuration. ***Voicemail*** can also be selected to prompt the caller for their mailbox number and mailbox code.

In addition short codes can be manually entered into the Destination field. If Voicemail Pro is installed, ***VM:*** followed by a Voicemail Pro module name can be entered to route calls directly to that Voicemail Pro module. On Avaya IP Office - Small Office Edition systems with integral voicemail, ***AA:*** followed by an auto-attendant name can be used to route callers directly to a Avaya IP Office - Small Office Edition Auto-Attendant service. Note: ***VM:*** and ***AA:*** entries are restricted to a maximum of 15 characters length in total.

More:

- Night Service Destinations
- Fallback Extension
- Incoming Call Priority

Night Service Destinations

IP Office 2.1 allows a time profile to be used to define when an incoming call route should use an alternate Night Service Destination field rather than the normal Destination field.

The time profile must already exist in the configuration before it can be selected as the **Night Service Profile** for an incoming call route. The time profile defines when the night service destination should be used.

The **Night Service Destination** field is used the same as the normal **Destination** field in the Incoming Call Route form.

Fallback Extension

Defines an alternate destination which should be used when the current primary destination (set in the Destination or Night Service Destination field) cannot be obtained. For example if the primary destination is a hunt group returning busy and without queuing or voicemail.

Incoming Call Priority

Incoming calls can be assigned a priority level between 1 (lowest) and 3 (highest). When calls to the same destination are queued, those calls with the highest priority will go before those with a lower priority. Internal calls are treated as having no priority over external calls.

Note: The routing of calls with different priority levels into a queue supported by a Voicemail Pro using a **Speak Position** action is not recommended. Having spoken a queue position to a caller, the Voicemail Pro will not speak a higher queue position to that caller after higher priority callers have gone ahead in the queue.

Using Least Cost Routes

By configuring a Least Cost Route you are able to route calls via an alternative carrier. Time profiles can also be used to allow you to take advantage of cheaper rates at specific times.

Note: Least Cost Routing is not compatible with short codes using [ ] and ; characters.

Short Codes can be configured in the Least Cost Route form. The following are the only kind of features allowed in the feature field.

- Dial, Dial3K1, Dial56K, Dial64K, DialEmergency, Dial Speech, DialV110, DialV120, DialVideo, Busy.

To Route Calls via an Alternative Carrier During Specific Hours

1. Create a Time Profile for the required hours.
2. Create a Least Cost Route that uses that Time Profile and with a short code that will route all calls via the required carrier, eg.
    - **Short Code:** ?
    - **Telephone Number:** 1234. (1234 being the carriers required prefix)
    - **Feature:** Dial

To Use Multiple Carriers

If you wish to use multiple carriers, for example, local calls and international calls are to go through one carrier between specific hours, all calls to UK through an alternative carrier and all other calls via a third carrier.

1. Create a Least Cost Route and create short codes for all local dial codes and international calls, eg. short codes for 732n, 609n, etc.
2. All other calls will use the system short code used for dialing out.

2-Stage LCR Set-up (In-band DTMF)

To take advantage of the Least Cost Routing services offered by second-tier carriers/PTOs/Telcos/etc. who utilize older Central Office switches, a second string of digits needs to be presented, in-band to them after the call is initially set-up. To set this up, use the following Short Code features:

- **D** = wait for the connection then send the following DTMF
- **,** = one second pause in between DTMF digit dialing, eg. 18005551234D12345,N
  This represents the carrier's telephone number, then D, then the digits required by the carrier, eg. an account number, then comma and N representing the number dialed.

Note: A DTMF tone will not be produced if you are running IP Office 401 control unit.

Parking a Call

Parking a call is an alternative to holding a call. The call is parked on the telephone system and so can be retrieved by another extension.

Each parked call requires a park slot number. Attempting to park a call into a park slot that is already occupied cause intercept tone to be played.

Calls left parked for too long will recall to the original extension that parked the call. The **Park Timeout** is set through the **System | Telephony** tab. Its normal default is 5 minutes.

There are several different methods by which calls can be parked and unparked. These are:

Using Short codes

The short code features **ParkCall** and **RideCall** can be used to create short codes to park and unpark calls. The default short codes that use these features are:

- ***37*N#** - Parks a call in park slot ***N***, eg. ***37*300#**
- ***38*N#** - Unparks a call from park slot ***N***, eg. ***38*300#**

Using the Phone Manager and SoftConsole Applications

The Phone Manager and SoftConsole applications all support park buttons. Clicking on these allows the user to park or unpark calls in the park slot associated with each button.

In addition, when a call is parked in one of those slots by another extension, the application user can see details of the call and can unpark it at their extension.

By default the application park buttons are associated with park slots 1 upwards. However these park buttons can be reconfigured to match different park slot numbers.

Using DSS Keys

The ParkCall feature can be used to associate a DSS button on a telephony with a particular park slot number. The DSS button can then be used to park and unpark calls from that park slot. The DSS buttons BLF lamps will indicate when a call is parked in the associated park slot.

Phone Defaults

Some telephones support facilities to park and unpark calls through their display menu options (refer to the appropriate telephone user guide). In this case parked calls are automatically put into park slots matching the extension number. For example, the first call parked by extension 201 would go into park slot 2010, the next into park slot 2011 and so on.

Configuring Personal Fax Numbers

Individuals and departments can have their own fax numbers. DTMF tones, which identify individuals are passed to the fax server, which could have as few as one or two lines.

In the following example, when someone dials 5551234, the system dials 501, which is then rerouted to the fax server:

1. Attach the fax modem to extension 216
2. Configure extension 216 with Caller Display type = DTMFB
3. Create a Hunt Group 500 with extension 216 as a member.
4. Create a User, eg. Fax501 with an extension of 501 and set Forwarding Unconditional to 500

5. Create an Incoming Call Route to extension 501 where the Incoming Number is the user's required personal fax number. Repeat for each user's personal fax number.
    - **Incoming Number:** 5551234
    - **Destination:** 501 Fax 501

Ring Back When Free

If an extension is busy and the user wants to be informed when the extension becomes free, the user can dial any digit and put the telephone down to set Ring Back When Free.

The system periodically checks if that extension is still busy. When it becomes free the system rings the user's telephone and give the appropriate Caller Display information to advise that the destination is free. When the telephone is picked up a call is automatically made to the extension.

This can also be done via the Phone Manager program.

Transferring a Call

Transferring a Call

Put the caller on hold. They will hear music on hold if installed. You can now dial the intended transfer number.

- The **User | Telephony | Busy on Held** setting, if set, stops any additional incoming call arriving whilst the user has a call on hold.

After dialing another number, if the user hangs up before the called number answers, the held caller is automatically transferred and hears ringing. This is called a 'blind' or 'unscreened' transfer.

Alternatively, with the caller still on hold, wait for the called number to answer and then ask if they wish to take the call. If Yes hangup. If No then do one of the following:

1. Use hold to toggle between calls.
2. If the call has been connected to voicemail or is just ringing, put the call on hold and dial ***52**. This will clear the last connected call. Use hold again to retrieve the original call.

The **User | Telephony | Transfer Return** time can be used to set how long a transferred call should ring unanswered before returning to the transferrer. If set, it will only work if set shorter than the any divert to voicemail settings at the transfer destination.

When calls are transferred the original Caller ID is passed onto the destination. By default a forwarded call cannot be transferred back to the original destination. To allow this facility set Do Not Disturb and enter the Forward Number as a Do Not Disturb Exception.

Hot Transfer

Hot transfer is the ability to transfer a call without personally answering the call. A user can perform a Hot Transfer via a PC application, for example, Phone Manager. This displays information regarding the caller, which may assist the user to decide who to pass the call on to. Select the Transfer function on the PC application and enter the destination number. The extension receiving the transferred call is informed via Caller Display where the call was transferred from and passes any available information regarding the original caller.

Queuing a Call to a Busy extension

If an extension is busy and a caller wants to hold for that person, the call can be queued for that extension. The caller is put on hold until the extension is free. This is achieved by pressing **Alternate Call** and dialing ***33*201#** (default).

Ring Tones

Selectable Ring Tones

The Control Unit supports a number of ring patterns. These ringing patterns indicate the following different call types:

- **Outside Ring Pattern:** The ring pattern used to indicate an external call.
- **Inside Ring Pattern:** The ring pattern used to indicate an internal call.
- **Ring Back Pattern:** A call ringback from voicemail.

The **System | Telephony** tab is used to set the default ring pattern for each call type. The setting for an individual user can be altered from the system default through each user's **User | Telephony** tab.

The selectable ringing patterns are:

- **RingNormal**
  This pattern varies to match the **Locale** set in the **System | System** tab, see "Other Ring Patterns". This is the default for external calls.
- **RingType1:** 1s ring, 2s off, etc. This is the default for internal calls.
- **RingType2:** 0.25s ring, 0.25s off, 0.25s ring, 0.25s off, 0.25s ring, 1.75s off, etc. This is the default for ringback calls.
- **RingType3:** 0.4s ring, 0.8s off, …
- **RingType4:** 2s ring, 4s off, …
- **RingType5:** 2s ring, 2s off, …
- **RingType6:** 0.945s ring, 4.5s off, …
- **RingType7:** 0.25s ring, 0.24 off, 0.25 ring, 2.25 off, …
- **RingType8:** 1s ring, 3s off, …
- **RingType9:** 1s ring, 4s off, …
- **RingType0:** Same as RingNormal for the locale "eng".
- **Default Ring:** Shown on the **User | Telephony** tab. Indicates follow the settings on the **System | Telephony** tab.

The following are the default ring normal settings if the locale is not supported:

- **Dial Tone:** 350Hz + 450Hz.
- **Ring Tone:** 400Hz + 450Hz.
- **Busy Tone:** 400Hz.
- **Minimum/Maximum Flash:** 25mS/350mS.
- **Ring Cadence:** 40Hz.
- **Ringing Pattern:** 0.4s On, 0.2s off, …
- **Call Waiting Pattern:** 0.1s on, 30s off, …
- **Busy Pattern:** 0.375s on, 0.375 off, …

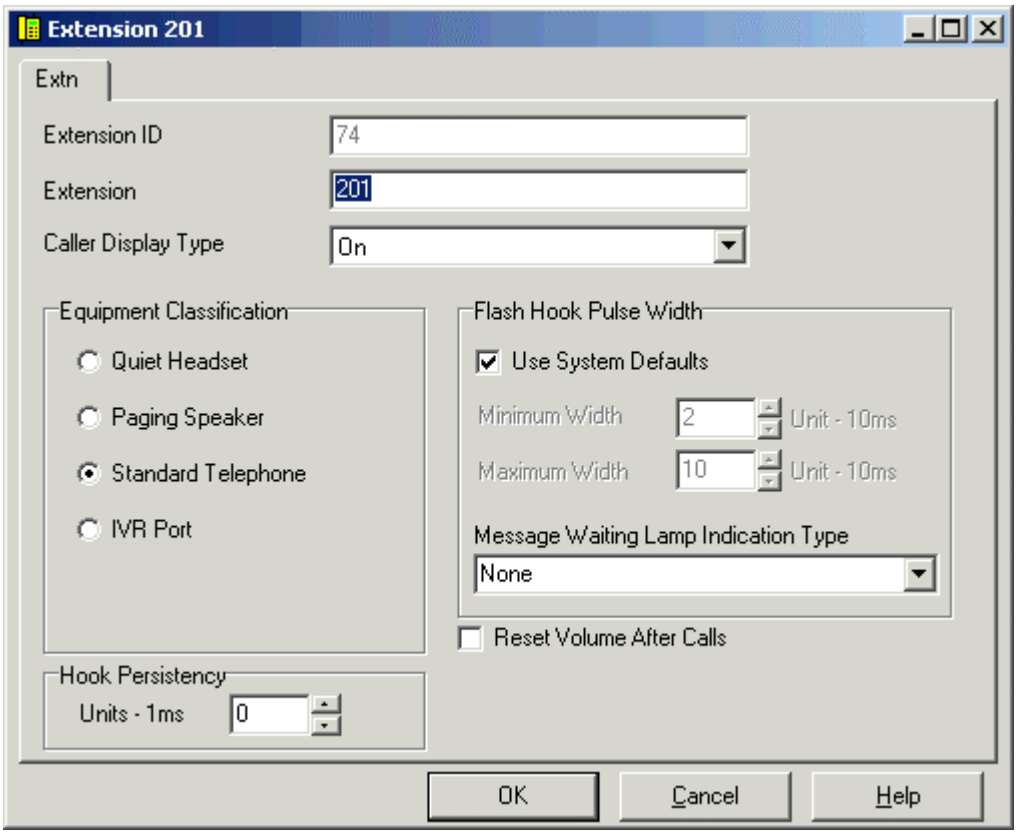
Notes:

1. Avaya 4400, 4600 and 6400 series telephones only support **Ring Normal**.
2. Different types of phone may support their own methods of setting the ring tone, volume and/or pattern.

Flash Hook Pulse Width

The system **Locale** defines the default setting for extension flash hook pulse width, see "Other Ring Patterns".

If necessary, the flash hook pulse width for individual extensions can be altered. This is done through each extension's **Extension** form.



Trusted Locations

A "trusted location" can be set via the Source Numbers tab in the User's configuration form. Note that external numbers used as trusted locations must provide ICLID.

These are locations that the System allows either data access, eg. a user dialing in from home, or access to Voicemail without a Voicemail Code, eg. a user collecting his Voicemail messages from a cell phone, or the location the Voicemail Server calls to inform the user of a new message.

Allow Direct Voicemail Access

To allow a User to collect Voicemail without being prompted for their Voicemail Code (not supported by Voicemail Pro using Intuity Mailbox mode). Prefix the number with a "V".

- V202 - This example allows the user to collect their VoiceMail from extension 201 without being prompted for their Voicemail Code
- V7325551234 - This example allows a user to collect their VoiceMail from an external number (home number), without being prompted for a Voicemail Code.

By default, each user is configured with their extension as a "trusted location" which enables them to dial *17 (default) from their own extension to collect Voicemail messages.

Allow RAS/Data Access from a Specified number

To allow RAS/data access only from a specified number, prefix the number (defined in the **Source Numbers** tab) with a "R".

Instruct Voicemail to Call the User

To have the Voicemail Server call the user when a new message has arrived for a Hunt Group, prefix the Hunt Group name with a "H".

When the hunt group receives a new message, the Voicemail Server rings the extension and informs the user.

Instruct Voicemail to Call the User at Another Location

To have the Voicemail Server call the user at a location other than their own extension when a new message is received, prefix the number (defined in the **Source Numbers** tab) with a "P".

This facility is only available if using Voicemail Pro and through which the user has a Callback start point set.

Hot Desking

When adding a user with no physical phone (See Extension versus User), you must add the Source Numbers in for those users.

CCC Operation Notes

CCC is a suite of software that works in conjunction with the Control Unit to report on call status and call handling. To be effective, those extensions, users and groups used with CCC should be programmed as follows:

- The users should all use login codes. This is important for the default user associated with the extension, who should be set to forced login. Use of the **Login Idle Period** is also recommended. See Hot Desking .
- None of the groups used with CCC should set have their **Ring Mode** set to ***Group***.
- CCC expects the names of agents (users), hunt group, services, etc to be unique from each other. Failure to do this can affect the correct presentation and storage of call data.

BRI Line Settings

BRI lines can be used in either Point-to-Point or Point-to-MultiPoint mode. Point-to-Point lines are used when only one device terminates a line in a customer's office. Point-to-MultiPoint lines are used when more than one device may be used on the line at the customer's premises.

There are major benefits in using Point-to-Point lines: -

1. The exchange knows when the line/terminal equipment is down/dead, thus it will not offer calls down that line. If the lines are Point-to-MultiPoint calls are always offered down the line and fail if no response from the terminal equipment. So if you have two Point-to-MultiPoint lines and one is faulty 50% of incoming calls fail.
2. You get a Green LED on the Control Unit when the line is connected. With Point-to-MultiPoint lines some exchanges will drop level/layer 1/2 signals when the line is idle for a period.
3. The timing clock is locked to the exchange. If level/layer 1/2 signals disappear on a line then the Control Unit will switch to another line, however this may result in some audible click when the switchover occurs.

The system will typically work when defaulted on either Point-to-Point or Point-to-MultiPoint lines. This is because our Terminal Equipment Identifier (TEI), which is used by the exchange to chat to the equipment, is set to 0 (TEI = 0). If you intend to connect multiple devices (simultaneously) to an ISDN line, then the TEI should be set to 127. With a TEI = 127 the Control Unit will ask the exchange to allocate a TEI for operation.

- Note: When connected to some manufactures equipment, which provides an S0 interface (BRI), a defaulted Control Unit will not bring up the ISDN line. Configuring the Control Unit to a TEI = 127 for that line will usually resolve this.

External Output Port

Introduction - Using the External Output (Door) Port

All the IP Office control units are equipped with a external output port. This port, also called the "door relay port", can be used to control up to two external devices.

The port is marked as **EXT O/P** and is located on the back of the control unit adjacent to the power supply input socket. It provides two relay connections.

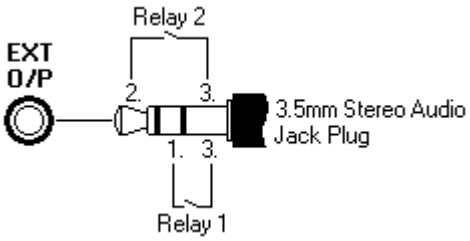
Through the IP Office, the two relays can be switched on, off or pulsed (on for 5 seconds). This can be done using short codes, through the Door tab in Phone Manager Pro or via the Open Door action in Voicemail Pro.

As the alternate name for the port suggests, the usual application for these relays is to activate door release systems. However, as long as the criteria for maximum current and voltage are meet, the relays can be used for other applications.

Wiring Connection

The pin numbers used in the diagram below relate to those used in the IP Office Installation Manual.

3.5mm stereo audio jack plugs are frequently sold as pre-wired sealed units. It may be necessary to use a multi-meter to determine the wiring connections from an available plug. Typically 3 (common to both relays) is the cable screen.



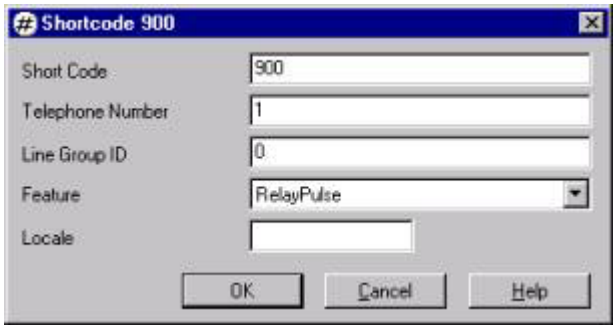
- Switching capacity: 0.7A
- Maximum voltage: 55V dc.
- On state resistance: 0.7Ω.
- Short circuit current: 1.0A
- Reverse circuit current capacity: 1.4A
- Ensure that 1 and 2 are always at a positive voltage with respect to 3.

Short Code Controls

The IP Office is installed with a number of default short codes for external output operation. These are:

Relay State	Relay 1	Relay 2
- On	*39	*42
- Off	*40	*43
- Pulse	*41	*44

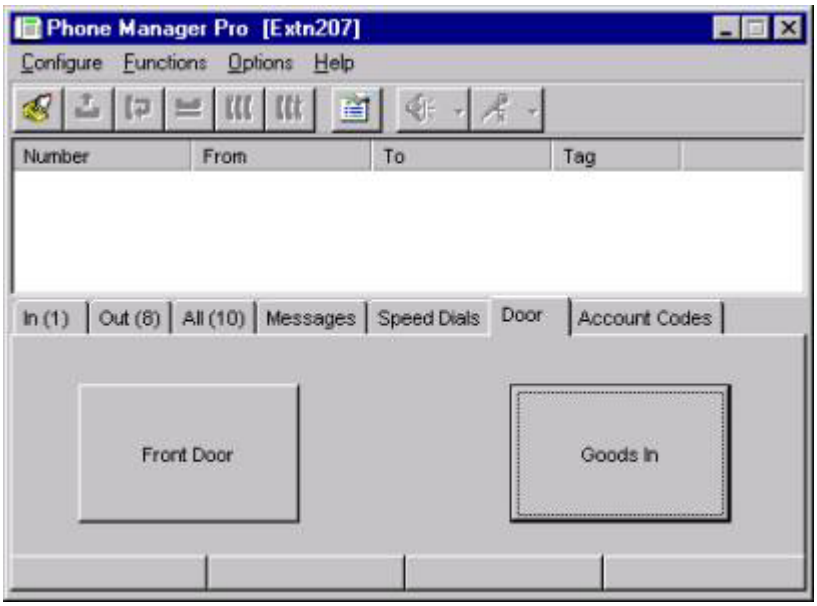
If necessary these short codes can be deleted and a new system or user short code added. The short code will be similar to the form shown below



- **Short Code:** Replace with whatever dialing should trigger the relay action.
- **Telephone Number:** Enter either ***1*** for relay 1 or ***2*** for relay 2.
- **Feature:** Select ***Relay On***, ***Relay Off*** or ***Relay Pulse***.

Phone Manager Pro

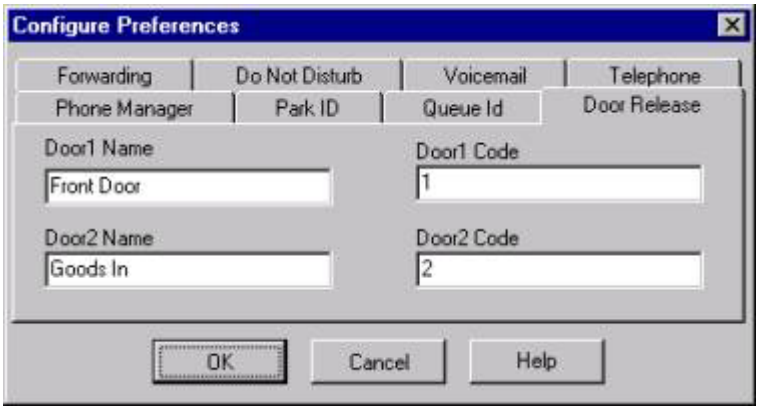
IP Office Phone Manager Pro can be used to pulse either of the external relays. This is done through the **Door** tab on the Phone Manager application. This tab is only shown when a door entry button is configured.



Note: The Phone Manager Pro user can trigger the door relays through this tab even when they are on a call.

Configuration

1. Within Phone Manager Pro, click on the **Configure Preferences** icon.
2. Select the **Door Release** tab.



3. For **Door1 Name** and **Door2 Name**, enter the text to display on buttons in the Phone Manager Pro's **Door** tab.
4. In the **Door1 Code** and **Door2 Code,** enter the relay number that each button on the **Door** tab should pulse. If no number is entered the button is not shown.
5. Select **OK**.
6. The **Door** tab can now be selected to display the door buttons and activate the appropriate relay.

Voicemail Pro

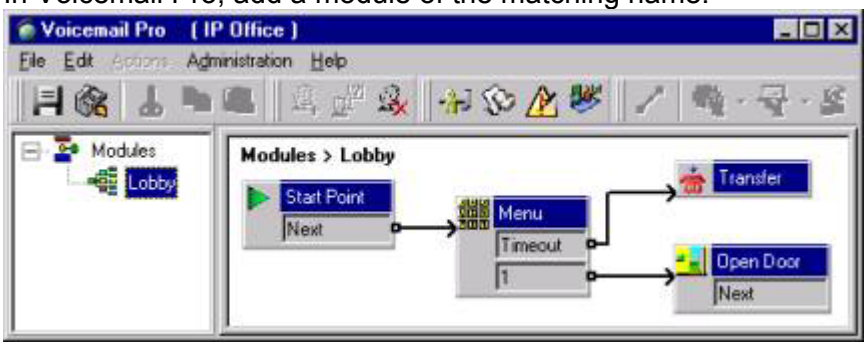
The Open Door action can be used to pulse either relay 1 or relay 2. It can be incorporated into call flows where required.

An example scenario could be a lobby phone which, when picked up immediately, either calls the receptionist (who can manually activate the door release) or allows the caller to enter a code to release the door themselves.

Do the following to incorporate the Open Door action into a call flow:

1. In Manager, open the configuration for the **User** associated with the lobby phone. Add a short code similar to the following:

2. Whenever the user extension goes off hook, this short code will call a Voicemail Pro module, in this example one called Lobby.
3. In Voicemail Pro, add a module of the matching name.



4. In the **Menu** action's properties:
   - In the **Entry Prompts** tab record a prompt such as *"Please hold for reception"* and tick **Allow prompts to be interrupted by Tone**.
   - In the **Touch Tones** tab set a short timeout since callers who know the door access code can interrupt the entry prompt. Select a key for door access, in this example we used 1.
   - Link the **Timeout** result to a **Transfer** to the reception number.
   - Link the 1 key press result to the **Open Door** action.
5. In the **Open Door** action's properties:
   - In the **General** tab enter a **Pin** for the action. Callers who press 1 for entry will hear *"Please enter your access code"*.
   - In the **Specific** tab select the door relay that should be triggered by successful pin entry.

Hot Desking

Hot Desking

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.

- To create a Hot Desk user:

  This will enable the user you are configuring to be able to hot desk.

  1. Receive the system configuration.
  2. Click **User** located in the Configuration Tree panel.
  3. In the list of users, double-click the user name or extension for whom you want to create/enable Hot Desking.
  4. Click the **Telephony** tab.
  5. In the **Login Code** field, enter at least 4 digits. Inform the user of this Login Code because it must be used by the User for Hot Desking.
  6. Click **OK**.
  7. Merge the configuration.

- To use Hot Desking as a user:

  1. After the system administrator has set you up as a Hot Desk user, you can log onto any phone that is on the system by:
     - If the phone has display buttons/keys:
       i. Dial the button that corresponds to **Login**.
       ii. Dial the extension number you want to log onto (usually it is your own extension).
       iii. Dial the button that corresponds to **Next**.
       iv. Dial the **Login Code** (ask your system administrator if you do not know it).
       v. You are now logged onto your extension.
     - If the phone does not support display buttons/keys, default system short codes can be used:
       i. Dial ***35*N*C#**, where **N** represents the extension number you want to log onto and **C** represents the **Login Code** (ask your system administrator if you do not know it).
  2. When you are ready to log off the phone:
     - On a phone with display buttons/keys, dial the button that corresponds **Logoff**.
     - On a phone without display buttons, dial ***36**.

- Hot Desking Example:

  Example: Extension 201 is to be used for Hot Desking.

  1. Create the number of users required and give each a **Login Code**.
     - **User 1:** Extension 401, Login Code 123.
     - **User 2:** Extension 402, Login Code 456.

- **User 3:** Extension 403, Login Code 789.

2. At extension 201, each user can now log in to use the extension with their own user settings. They can do this using the default system short codes.
    - **For User 1 to log in:** *35*401*123#
    - **For User 2 to log in:** *35*402*456#
    - **For the current user to log out:** *36

    The user associated with extension 201 (through their **User** form) does not normally need to log on. They are automatically re-associated with extn. 201 whenever *36 is dialed at the extension or following a reboot of the Control Unit. If you want that person to also have to log on, then in their **User** tab you should enter a **Login Code** and select **Forced Login**.

When using DT, 4412, 4424 or 6400 series display telephones, you can set the extension to have no extension number. It then displays **NOT LOGGED ON** between log on's.

For each log in user, you can configure how long an extension can remain idle before they are automatically logged out. This is done using the **Login Idle Period** in their **User | Telephony** tab. This option should only be used in conjunction with **Force Login**.

Force Login

Force Login forces the user to log back onto his phone after any logoff, including a system reboot. For example, when a Hot Desking user logs off a phone, the system (by default) attempts to re-associate the phone with the default user; if that user is set to **Force Login**, then they must enter their **Login Code** to complete the re-association. By default Force Login is not enabled for users.

To set up **Force Login**:

1. Receive the system configuration.
2. Click **User** located in the Configuration Tree panel.
3. In the list of users, double-click the user name or extension for whom you want to create a Force Login.
4. Click the **Telephony** tab.
5. Tick **Force Login**.
6. A **Login Code** must be set when **Force Login** is enabled. In the **Login Code** field, enter at least 4 digits. Inform the user of this Login Code.
7. Click **OK**.
8. Merge the configuration.

Login Idle Period

Login Idle Period sets the length (in seconds) in which a user can be logged onto an idle phone. If the telephone is not used within this time frame, the user currently logged on is automatically logged off. Because of the potential for an automatic logoff, **Login Idle Period** must be used in conjunction with **Force Login**.

Login Idle Period is useful for call centers where tracking of time spent on the phone is important.

To set a login idle length in seconds:

1. Receive the system configuration.
2. Click **User** located in the Configuration Tree panel.
3. In the list of users, double-click the user name or extension for whom you want to set a Login Idle Period.
4. Click the **Telephony** tab.
5. Enter the seconds you want to set the idle period for.
6. Tick the **Force Login** field.
7. A **Login Code** must be set when **Force Login** is enabled. In the **Login Code** field, enter at least 4 digits. Inform the user of this Login Code.
8. Click **OK**.
9. Merge the configuration.

Hunt Groups

Overview of Hunt Groups

A Hunt Group is a collection of users, eg. Sales - a group to handle all sales related calls

An incoming caller wishing to speak to Sales can ring one number but the call can be answered by any number of extensions that are members of the Sales Hunt Group.

By default all incoming voice calls are sent to a Hunt Group called Main (extension 200), which is configured in Group mode, and contains the first 16 extensions. Therefore all incoming calls ring each extension simultaneously. This is set up as an initial starting point for the telephone system while individual user extensions are configured.

The Hunt Group can be given an extension number. This extension number can be used internally or linked to an Incoming Call Route. All the calls received by this extension number can be answered using either:

- **Group Mode:** All telephones in the Extension List ring simultaneously.
- **Linear Mode:** Each extension is rung in order, one after the other, starting from the first extension in the list each time.
- **Circular Mode:** Each extension is rung in order, one after the other. However, the last extension used is remembered. The next call received rings the next extension in the list.
- **Most Idle Mode:** The extension that has been unused for the longest period rings first, then the extension that has been idle second longest rings, etc.

If all extensions in the Hunt Group are busy (ie. on a call, logged out or membership is disabled) or not answered, another Hunt Group, called an Overflow Group, can be used to take the calls. The Overflow Time can be used to stipulate how long a call will ring round the members of the Hunt Group before being passed to the Overflow Group.

If preferred, calls can be held in a queue and passed to the first available extension in the group. If an Overflow Group is used, a call is sent to the Overflow Group after it has been held in the queue for the time specified by the Overflow Time.

A Time Profile can be used to indicate when a Hunt Group is operational, (9:00 to 5:00), and another hunt group called a Night Service Fallback Group can be used to provide cover outside of these hours.

If you wish a Night Service Fallback Group to provide cover at irregular times, a Short Code can be used. Once this is done, the status of Night Service can only be changed back via a Short Code (and not Time Profile).

During a holiday period, the Hunt Group can be put into Out of Service mode and another Hunt Group called the Out of Service Fallback Group can be used to provide cover.

Voicemail can also be used in conjunction with Hunt Groups to take all group related messages, play an announcement when the Hunt Group is in Night Service or Out of Service mode and give announcements while a call is held in a queue. Hunt Groups also support Voicemail Email - to pass messages to an email account, and a Voicemail Code that can be used to verify a user when messages are retrieved remotely.

Examples

These examples explain how to use a basic Hunt Group and how Voicemail and Queuing act with the Hunt Group when a Voicemail Server is operational. There is also an example of how to use an Overflow Group, a Night Service Fallback Group and a Time Profile.

Basic Hunt Group

Scenario - all sales related calls must be answered by staff in the Sales department, first by Jane, then by Peter, and finally, if necessary, by Anne.

1. Create a hunt group called "Sales"
2. Assign the extension no, eg. 300
3. Add extensions, ie. Jane (201), Peter (204) and Anne (205)
4. Set the Ring Mode to Linear

Result - all calls received by the Sales Hunt Group first go to Jane's phone. If Jane is busy or does not answer her extension within 15 seconds (default) the call moves to Peter's phone. If Peter is also unable to answer the call, it goes to Anne's phone. If Anne does not answer the call it passes back to Jane's phone. The call continues in this manner until the call is answered or the caller hangs up. (This example assumes that a Voicemail Server is not available, see below).

Using Voicemail

Scenario - if the Sales department is unable to answer a call, the caller is given the option to leave a message. (A Voicemail Server must be operational for this facility to be available).

- Ensure the **Voicemail On** option in the Sales hunt group created above is checked (default).

Result - when the Sales Hunt Group receives a call and cannot be answered by any member, the caller is sent to the Voicemail for the Sales Hunt Group.

Using the Queuing Facility

Scenario - if the Sales department is **all** busy on calls, further calls are held in a queue until one of the Sales team become free. (In order for a caller to receive the Hunt Group queue messages a Voicemail Server must be operational).

1. Ensure the **Queuing On** option in the Sales Hunt Group created above is checked (default).
2. The **Queuing Ring Time** is set to 10 seconds by default.

Result – when the Sales Hunt Group receives a call and all members are on calls, the call remains in queue. If, for example, Peter's extension becomes free the first call in the queue is passed to Peter's extension.

When the call is placed in the queue, the caller first hears 10 seconds of ringing tone and then is given the first "Queue" message. Music On Hold (if this facility is available) is then played for 20 seconds followed by the second "Queue" message. Music On Hold is then played for a further 20 seconds and followed by the second "Queue" message again. This sequence is repeated until the call is answered.

Please note - the Voicemail On, Queuing On and Queuing Ring Time of 10 seconds options are all set by default when creating a Hunt Group but these facilities are not available unless a Voicemail Server is operational.

Using an Overflow Group

Scenario - When the Sales department is attending their weekly sales meeting the receptionists must answer calls.

1. Create a new Hunt Group called "Reception".
2. Assign an extension, ie. 301.
3. Add extensions, ie. Katie (202) and Richard (206).
4. Set the **Ring Mode** to **Group**.
5. In the Sales Hunt Group created above, add the **Reception** Hunt Group to the **Overflow Group** list.

Result - when the Sales Hunt Group receives a call and the members are unable to answer the call, the call is sent to the Reception Hunt Group. Katie's and Richard's extensions will ring simultaneously.

If both Katie and Richard are unable to answer the call within 15 seconds (default) the caller is sent to Voicemail for Sales.

Overflow Group List - Select Required Items

Select the Hunt Group to act as the Overflow Group

CTRL or SHIFT can be used to select multiple entries. A Hunt Group may be added more than once, eg. Main, Sales, Main, etc.

Using a Night Service Fallback Group

When the Sales department is attending their weekly sales meeting, the receptionists who will take messages must answer calls.

- In the Sales Hunt Group created above, set the **Reception** Hunt Group as the **Night Service Fallback Group**.

Result - either Jane, Peter or Anne can dial the relevant short code on their phones to put the Sales Hunt Group into Night Service. If the default short codes are being used, the short code dialed will be *20*300#. All calls received by the Sales Hunt Group are sent to the Reception Hunt Group and can be answered by either Katie or Richard.

When the Sales team has finished their meeting, either Jane, Peter or Anne can dial the relevant short code to return the Sales Hunt Group to In Service. If the default short codes are being used, the short code dialed will be *21*300#. Jane, Peter or Anne can now answer All Sales Hunt Group calls.

Using a Time Profile

Office hours are 9.00 am to 5.00 pm, Monday to Friday. Outside of these hours sales related calls must be passed to Voicemail to give the caller the option to leave a message. (A Voicemail Server must be operational for this facility to be available).

1. Create a **Time Profile** for 9.00 am to 5.00 pm, Monday to Friday called "Office Hours".
2. In the Sales Hunt Group created above, enter the "Office Hours" time profile.
3. Ensure that a Night Service Fallback Group has not been entered.

Result - all calls received by the Sales Hunt Group between 9 am and 5 pm on Monday through Friday are answered by the group. When calls are received before 9 am or after 5 pm Monday to Friday or all day Saturday or Sunday the call is sent to Voicemail and played the Out of Hours Greeting.

Enable/Disable Membership

A User's membership to a Hunt Group can be disabled temporarily.

- Right-click on the required User and select Disable. An asterisk appears to the left of the User's name. Right-click on the User and select Enable to reverse this option.

This facility can also be activated via Short Codes using the features HuntGroupDisable and HuntGroupEnable. This allows users to disable and enable their membership to a Hunt Group from their own phones.

For example, the following short codes could be created. **N** represents the Hunt Group the user wishes to disable or enable themselves from.

- **To Disable Group Membership:**
  - **Short Code:** *90*N#
  - **Telephone Number:** N
  - **Line Group ID:** 0
  - **Feature:** HuntGroupDisable

- **To Enable Group Membership:**
  - **Short Code:** *91*N#
  - **Telephone Number:** N
  - **Line Group ID:** 0
  - **Feature:** HuntGroupEnable

Hunt Group Call Waiting

Call waiting indication is normally provided to users for hunt group calls. Instead the call should ring at and be answered by another free group member.

For hunt groups using the **Ring Mode** of ***Group***, call waiting indication can be enabled. This is done by ticking the **Call Waiting** option on the **Hunt Group | Hunt Group** tab.

Note that for the group member to receive call waiting indication, their personal call waiting setting must also be enabled.

Hunt Group Voicemail

Refer to the "Voicemail Installation and Maintenance Manual".

Forwarding Hunt Group calls

A user can forward his Hunt Group calls to an internal or external number. See Call Forwarding .

How to Monitor Calls

Monitoring allows a user to listen in to the call being handled by another user without being heard.

-  **WARNING**
  Monitoring is not enabled by default. The use of monitoring is normally subject to local laws and regulations. Before enabling monitoring you must ensure that you have complied with all applicable local laws and regulations. Failure to do so may result in severe penalties.
- Monitoring can be accompanied by a repeated tone heard by all parties. In some locales it may be a requirement to provide this tone. Use of the tone is controlled by the **Beep on Listen** setting on the **System | System** tab.

Note that monitoring is separate from call intrusion. It is not affected by the intrusion settings of any of the users involved.

Monitoring is setup by selecting a Monitor Group for a user. The user can then listen to any calls made or received by the members of that group. A short code is also required to trigger the monitoring.

Example:
User 'Extn205' wants to be able to monitor calls received by members of the Hunt Group 'Sales'.

1. In the Telephony tab of the user 'Extn205', select 'Sales' in the **Monitor Group** list box.
2. Create a User Short Code to allow Extn205 to start monitoring. This could also be done as a System short code if desired.
   - **Short Code:** *99*N#
   - **Telephone Number:** N
   - **Line Group ID:** 0
   - **Feature:** CallListen

Now when a member of the 'Sales' hunt group is on a call, Extn205 can replace N in the short code with the extension number of that member and monitor their call. Note: Monitoring includes calls direct to/from a user in addition to hunt group calls.

Using Queuing

Queuing allows callers to a Hunt Group to be held in a queue when **all** extensions in the Extension List are busy. When an extension becomes free a queued call is then presented to that extension.

If voicemail is operational, the caller is played queue messages. Refer to the Voicemail Installation & Administration Manual for full details.

Using the Fallback Tab

Hunt Groups are defined in the Hunt Group configuration form. A Hunt Group has three service modes:

In Service

When this field is selected within the Hunt Group tab, it implies that the hunt group is enabled. This is the default mode.

Night Service

When a Hunt Group is in Night Service, callers hear busy tone or if VoiceMail is operational they are played the Out of Hours greeting. Alternatively you can pass the callers to another Hunt Group, containing a manned extension or a user forwarded to a cell phone etc., by entering that Hunt Group as the Night Service Fallback Group.

Select the option in the Fallback tab and send the configuration to the Control Unit or use a short code to place a Hunt Group into Night Service. Short Codes can be created using the **SetHuntGroupNightService** and **ClearHuntGroupNightService** features. Note that if the group is also using a time profile, these features cannot override when the time profile sets the group into night service mode.

The default short codes include two short codes that already use those features:

- ***20*N#** - Puts group ***N*** into Night Service mode.
- ***21*N#** - Takes group ***N*** out of Night Service mode.

Once you have used Short Codes to change the status, it can only be changed back via a Short Code (and not Time Profile).

Out of Service

When a Hunt Group is Out of Service, callers hear busy tone or if VoiceMail is operational they are played the Out of Hours greeting. Alternatively you can pass the callers to another Hunt Group, containing a manned extension or a user forwarded to a cell phone etc., by entering that Hunt Group as the Out of Service Fallback Group.

To place a Hunt Group into Out of Service select the option in the Fallback tab and send the configuration to the Control Unit. Alternatively the short code features SetHuntGroupOutOfService and ClearHuntGroupOutofService could be used to create short codes for this action.

Using a Time Profile

A Time Profile can be assigned to a Hunt Group. During the in service hours, the Hunt Group performs as configured in the HuntGroup tab. Outside of these hours the group it follows the groups Night Service settings.

Please note:

- The Time Profile does not change the groups Service Mode setting.
- Short codes cannot be used to override the time profile action.

Short Codes

Understanding Short Codes

Short Codes allow an administrator to configure features that can be accessed on a system-wide or user basis. A list of these features are available under Short Code Features.

Short Codes can be used for:

- Speed Dials.
- Activating and deactivating features for an individual phone (eg. Do Not Disturb) or for the entire system (eg. Night Service).
- Call Routing and Restriction.

Short codes can be set within several configuration forms, depending on how a particular short code is to be used. For example, a Forward on Busy short code that is created directly from the Short code configuration form applies to all users on the phone system, but the same short code created within the User configuration form applies only to that user.

Because short codes can be set within several configuration forms, an order of priority is put in place for situations where short codes settings contradict. For example, if a system short code states that *08 is for Do Not Disturb On, but if a user programs for her phone to recognize *08 for Voicemail Ringback On, then the user short code overrides the system short code for that particular user. The priority level are as follows:

- **User Short Codes**
  Takes priority over short codes set for user restrictions, the system as a whole, least cost routing and lines. 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, least cost routing and lines. 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 and lines. 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**
  Takes priority over short codes set for lines. Least cost routing short codes are matched against any dialing that results in a number to be dialed.
- **Line Short Codes**
  Short codes can also be configured on some types of line.

To create a short code, the following parameters need to be understood:

- How short code matching is performed
- List of valid short code characters
- Valid characters that can be used in the Telephone Number field
- Short code features

Matching Order

The number dialed by a user is treated in the following order:

1. If the number dialed matches an internal extension, go to step 6.
2. If the number matches a ***User short code***, apply the short code. If the result is a number for dialing proceed to Step 5. Otherwise go to step 3.
3. If the number matches a short code in the user restriction set associated with the user, apply the ***User restriction short code***. If the result is a number for dialing proceed to Step 5. Otherwise go to step 4.
4. If the number matches a ***System short code***, apply the short code. If the result is a number for dialing proceed to Step 5.
5. If the number matches a ***Least Cost Route short code***, dial the number as per the Least Cost Route rules.
6. Dial the number.

Getting the Dialed Number

Getting the Dialed Number

This section describes how a dialed number is determined and how short code matching is performed. Routing of the short code begins based on a couple of parameters set in the System Telephony tab (see Telephony).

- The **Dial Delay Count** is the number of digits that are dialed by the user before the system begins to process the dialed string. Matching against the short code table occurs when this number had been reached.
- The **Dial Delay Time** is the interval allowed between dialed digits. It is reset after a new digit is dialed. It serves two purposes:
  - It sets the time since the last digit dialed, after which dialing is assumed to have ended.
  - It is used to detect short codes that are less than the Dial Delay Count in length.

The Dial Delay Count and Dial Delay Timer work together to get the dialed string, that is examined by IP Office. The Dial Delay Count is what takes precedence. Once that number of digits in the Dial Delay Count has been dialed, the system starts to match the digits against Short Codes. The dialed string is considered complete when there are no more digits dialed within the Dial Delay Time.

Example: Dial Delay Time

An example of the first use of the Dial Delay Count is the following:

- Dial Delay Count = 0
- Dial Delay Time = 4000 msec (4 seconds)

A user dials the number "97325551212".

The Dial Delay Count is 0, so the system immediately starts looking for a match against Short Codes even though dialing has not been completed..

As long as the user dials each digit within 4 second of the previous digit, the Dial Delay Time reset after each digit. Only after the last "2" is dialed does the Dial Delay Timer expire and the complete number dialed to evaluate is stored.

User may see the effect of this in the short delay between dialing a neighboring extension and that extension ringing.

Example: Short Dialing

An example of the second use is:

- Dial Delay Count = 4
- Dial Delay Time = 4000 msec (4 seconds)

A user dials "911". The dial string is less than the Dial Delay Count. However 4 seconds after the final 1, the Dial Delay Time expires. The switch assumes that dialing is complete and process the number "911".

Example: Overlap Dialing

When the Dial Delay Count is greater than zero, overlap dialing can be supported. Consider the following:

- Dial Delay Count =4
- Dial Delay Time = 4000 msec (4 seconds)
- Short Code 1 = 01
- Short Code 2 = 0123

Short Code 2 is matched because the Dial Delay Count is reached. Short Code 1 is matched because the Dial Delay Time is met.

If the above example had a Dial Delay Count of 0, only Short Code 1 would be used because the matching would occur immediately.

Example: Single Digit Short Codes

IP Office supports Single Digit Short Codes, but they are treated in a different way than other short codes and should be used with extreme care. Single Digit Short Codes rules can be summarized by the following. They are acted on immediately regardless of the Dial Delay Count and Dial Delay Time. Consider the following short codes:

- Dial Delay Count =2
- Dial Delay Time = 2000 msec (2 seconds)
- Short Code 1 = 1
- Short Code 2 = 12
- Short Code 3 = 123

If Single Digit Short Codes did not receive special treatment, a user could dial any one of the three short codes listed and the switch would translate the dialed short code after the 2 second *Dial Delay Time* interval. However, because there is special treatment, the only short code that is recognized is Short Code 1 (single digit 1). The switch does not wait for the Dial Delay Time interval. As soon as the first digit is dialed a match is recognized and the switch translates immediately.

An administrator must choose Single digit short codes with digits that are not used as the first digit for any other short code. They should be defined only after all other short requirements are satisfied.

Short Code Parameters

Short Codes are made up of a combination the following, depending on what short code you are creating:

- **Short Code**: *Default = blank*
  The dialing digits used to trigger the short code. Maximum length is 33 characters. See Short Code Characters for a list of valid characters.
- **Telephone Number**: *Default = blank*
  The number output by the short code. The number dialed by the short code or parameters for the short code feature. This field can contain numbers and characters. For example, it can contain Voicemail Pro start point names, user names, hunt group names and telephone numbers (including those with special characters). Maximum length 33 characters. See Telephone Number Characters for a list of valid characters.
- **Line Group ID**: *Default = 0*
  For external calls, this is the set of lines that are used when making the call. Which group a line belongs to is set through the **Line** form for each line.
- **Feature**: *Default = Dial*
  This is what the short code does. See Short Code Features .
- **Locale**: *Default = blank*
  Some features can support country specific variations if needed.

Telephone Number Characters

In relation to short codes, the Telephone Number field can reflect the number dialed by the short code or parameters for the short code feature. For example, this field can contain Voicemail Pro start point names, user names, hunt group names and telephone numbers (including those with special characters).

The **Telephone Number** field can contain numbers and the following characters:

- **C** – Place digits following the "C" in the outgoing call's Called Number field rather than Keypad field (this is the default).
- **D** – Wait for connection, then send the following as DTMF. (See Using Least Cost Routes for an example). Note: A DTMF tone will not be produced if you are running IP Office 401 control unit.
- **E** – Replace with the Extension Number dialing the Short Code.
- **I** - Send data in an Information Packet rather than Set-up Packet (for advance use).
- **K** - Place the digits following the "K" in the outgoing call's Keypad field rather than Called Number field. Only supported on ISDN/QSIG.
- **L** - Use the last number dialed.
- **N** - Substitute with digits dialed for N or the string of "X"s in the Short Code field. For example use the Hunt Group extension number entered as part of the short code. (See default short code ***20*N#** for an example.)
- **S** - Place the digits following the "S" into the outgoing call's Calling Number field. See Short Code Examples .
- **SS -** Pass through the Calling Party Number on VPN lines. For example, to provide the incoming ICLID at the far end of a VoIP connection, a short code **?** with telephone number **.SS** should be added to the line.
- **t** - Set 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. See Maximum Call Length.
- **U** - Replace with the User Name of the User dialing the Short Code. See default short code ***17** for an example.
- **W** – Set flag in packet to withhold outgoing Caller ID (operation is PSTN network dependent.
- **@** – Enter following digits into sub-address.
- **.** – Replace with current dialed digits, ie. those that have been dialed so far and triggered the short code match.
- **,** – One second pause in between DTMF digit dialing (See Using Least Cost Routes for an example).
- **" "** – Any text must be surrounded by quotation marks, eg. User or Hunt Group Names.
- **?** – In conjunction with the Voicemail Collect feature. Indicates collect messages.
- **#** – In conjunction with the Voicemail Collect feature. Indicates leave messages.

Short Code Characters

When creating a short code, the **Short Code** field can contain dialed numbers plus ***** and **#** and the following non dialed characters:

- **?** – Signifies that this is the default entry and is used in the absence of any other match or partial match.
- **?D** – Same as **?** except that if no other Short Codes match, this Extension is directly patched to an outside line. Thus Extensions configured with this parameter act as though they are pure direct lines. See Dial on Pick up .
- **N** - Signifies a sequence of one or more digits dialed and then followed by a ***** or **#**. The * or # are entered separately in Short Code field (ie. N* or N#).
- **X** – Match a single digit. When a group of "X"s is used, the short code matches against the total length of "X"s (for example if there are 10 "X"s, the user would have to dial 10 digits for it to match the short code).
- **[n]** – Expect secondary dial tone, where "n" represents the short code configured to trigger secondary dial tone.
- ; – Receive sending complete. This must be the last character in the short code string. It indicates to the system wait for the number to be fully dialed (based on the Dial Delay Time) before acting on the short code.
    - In the United States, this MUST be used when the line group for the short code contains PRI lines or T1 lines emulating analog lines.

Using Special Characters

Using Special Characters

For all short codes in this section, "Y" is the number of the Line Group that the calls will be routed to. Throughout this section, the short codes start with "9".

Secondary Dial Tone and [n] Characters

If you wanted to have secondary dial tone, the following short code would need to be added.

- **Short Code**: 9
- **Telephone:** .
- **Feature:** SecondaryDialTone
- **Line Group ID:** 0

The Line Group ID should be "0", versus Y. With this additional short code in place other short codes that would be used for dialing out on lines would start with "[9]" rather than "9". Thus, the other short code examples in this section (see below) would start with

- [9]N;
- [9]xxxxxxxxxx;
- [9]1800N;

'N' and 'X'

When Short Codes contain only digits, matching is straightforward. It is when special characters are being used. One question is can Short Codes that have "X"s in them be used in conjunction with ones that just have "N"? The answer is yes. The "X"'s in the Short Code field match against a specific string length.

Consider the following two short codes.

- **Short Code**: 9N;
- **Telephone:** N
- **Feature:** Dial
- **Line Group ID:** Y

- **Short Code:** 9xxxxxxxxxx;
- **Telephone:** N
- **Feature:** Dial
- **Line Group ID:** Y

In the above case, dial strings that are less than 10 digits use the first short code, while strings that are 10 digits or greater use the second short code. This scheme can be used to send local versus long distance calls out over different line, without the user being aware of this.

In the above example, if only the "9xxxxxxxxxx;" short code existed, any number dialed that was less than 10 digits would not be matched.

Dialed Digits and Outgoing Digits

Another thing that needs to be understood is what is going to get sent to the Central Office. If you have separated out digits to match against and you want those digits sent out to the Central Office, you must add them in the **Telephone Number** field. Consider the following.

- **Short Code**: 91800N;
- **Telephone:** 1800N
- **Feature:** Dial
- **Line Group ID:** Y

The user dials "918005551212". The match is made on the string to the above short code. If the "1800" did not appear in the Telephone Number field, "5551212" would be what got sent out.

If the line requires "*" codes to access features, or you would like to make use of your line Provider's features (Call ID Block), simply add the appropriate "*" code as part of the Telephone Number field (See Blocking Caller ID).

The same holds true for long distance carrier access code numbers. Simply add the access code as part of the Telephone Number field.

- In the United States, short codes that use Line Groups that contain PRI lines need to have the Short Code end with a ";", because the PRI protocol must have certain parameters that require the entire dialed number. Analog (Loop and Ground Start) lines do not require this, so short codes associated with only these types of lines can be configured without the ";". If you have a group that contains either PRI or T1 emulating analog lines, use the ";".

Default System Short Code List

This section lists the default system short codes. It shows the **Short Code**, the **Telephone Number**, the **Feature** and the **Line Group ID**. Blank indicates that the field is left blank.

Code	Telephone Number	Feature	Line Group
*00	Blank	CancelAllForwarding	0
*01	Blank	ForwardUnconditionalOn	0
*02	Blank	ForwardUnconditionalOff	0
*03	Blank	ForwardOnBusyOn	0
*04	Blank	ForwardOnBusyOff	0
*05	Blank	ForwardOnNoAnswerOn	0
*06	Blank	ForwardOnNoAnswerOff	0
*07*N#	N	ForwardNumber	0
*08	Blank	DoNotDisturbOn	0
*09	Blank	DoNotDisturbOff	0
*10*N#	N	DoNotDisturbExceptionAdd	0
*11*N#	N	DoNotDisturbExceptionDel	0
*12*N#	N	FollowMeHere	0
*13*N#	N	FollowMeHereCancel	0
*14*N#	N	FollowMeTo	0
*15	Blank	CallWaitingOn	0
*16	Blank	CallWaitingOff	0
*17	?U	VoicemailCollect	0
*18	Blank	VoicemailOn	0
*19	Blank	VoicemailOff	0
*20*N#	N	SetHuntGroupNightService	0
*21*N#	N	ClearHuntGroupNightService	0
*22*N#	N	SuspendCall	0
*29	Blank	ToggleCalls	0
*30	Blank	CallPickupAny	0
*31	Blank	CallPickupGroup	0
*32*N#	N	CallPickupExtn	0
*33*N#	N	CallQueue	0
*34	Blank	HoldMusic	0
*35*N#	N	ExtnLogin	0
*36	Blank	ExtnLogout	0

*37*N#	N	ParkCall	0
*38*N#	N	RideCall	0
*39	1	RelayOn	0
*40	1	RelayOff	0
*41	1	RelayPulse	0
*42	2	RelayOn	0
*43	2	RelayOff	0
*44	2	RelayPulse	0
*45*N#	N	AcquireCall	0
*46	Blank	AcquireCall	0
*47	Blank	ConferenceAdd	0
*48	Blank	VoicemailRingbackOn	0
*49	Blank	VoicemailRingbackOff	0
*50	Blank	ForwardHuntgroupOn	0
*51	Blank	ForwardHuntgroupOff	0
*52	Blank	Cancel or Deny	0
*53*N#	Blank	CallPickupMembers	0
*57*N#	N	ForwardOnBusyNumber	0
*70*N#	N	DialPhysicalExtnByNumber	0
*71*N#	N	DialPhysicalExtnByID	0
*DSSN	";[0]151 – ERR'-N	DisplayMsg	0
*SDN	";[0]151 – ERR'-N	DisplayMsg	0
*SKN	";[0]151 – ERR'-N	DisplayMsg	0
[9]0N;	0N	Dial3K1	0
[9]1N;	1N	Dial3K1	0
[9]N;	N	Dial3K1	0
[9] xxxxxxxxxxx;	N	Dial3K1	0
9	.	SecondaryDialTone	0
911	911	Dial	0

Suggested minimum configuration

Code	Telephone Number	Feature	Line Group
*17	?U	VoicemailCollect	0
*30	Blank	CallPickupAny	0

?	.	Dial	0

- Note: The "Follow Me Here" (***12*N#**) and "Follow Me To" (***14*N#**) functions can be canceled by using ***14*#** on the user's original extension.

With the default short codes, the following will happen:

- All calls preceded by 9 will receive secondary dial tone.
- International numbers follow the "[9]0N;" short code.
- Long Distance numbers use the "[9]1N;" short code.
- Local (7 digits) numbers use the '[9]N;" short code.
- Local (10 digit) numbers use the "9xxxxxxxxxx" short code.

Short Code Features

Short Code Feature Overview

The options within the Feature field represent what the short code does when the user dials it. Every short code requires a selected feature. Information relating to each feature takes the following form:

- **Feature name:** Busy, Busy on Held, Call Intrude, etc. for example.
- A short description of the feature's usage.
- **Telephone Number:** Data required by the feature. Some features do not any data entered in this field.
- **Button Programming:** Path to the feature when applying to a DSS key.
- **DSS Toggles:** States whether the DSS key reverses the feature when pressed again or not. A Yes implies that the feature has toggle capability and a No implies it does not.
- **Label:** Name shown next to the display key if set on 2420 or 4620 telephones.

The available features are presented in the table below:

- Busy
- Busy On Held
- Call Intrude
- Call Listen
- Call Pickup Any
- Call Pickup Extn
- Call Pickup Group
- Call Pickup Members
- Call Queue
- Call Record
- Call Steal
- Call Waiting On
- Call Waiting Off
- Call Waiting Suspend
- Cancel All Forwarding
- Cancel Ring Back When Free
- Channel Monitor
- Clear Call
- Clear CW
- Clear Hunt Group Night Service
- Clear Hunt Group Out Of Service
- Clear Quota
- Conference Add
- Follow Me Here
- Follow Me Here Cancel
- Follow Me To
- Forward Hunt Group Calls On
- Forward Hunt Group Calls Off
- Forward Number
- Forward On Busy Number
- Forward On Busy On
- Forward On Busy Off
- Forward On No Answer On
- Forward On No Answer Off
- Forward Unconditional On
- Forward Unconditional Off
- Headset Toggle
- Hold Call
- Hold CW
- Hold Music
- Hunt Group Disable
- Hunt Group Enable
- Off Hook Station
- Park Call
- Priority Call
- Record Greeting

- Conference Meet Me
- CW
- Dial
- Dial 3K1
- Dial 56K
- Dial 64K
- Dial CW
- Dial Direct
- Dial Emergency
- Dial Extn
- Dial Inclusion
- Dial Paging
- DialPhysicalNumberByExtension
- DialPhysicalNumberByID
- Dial Speech
- Dial V110
- Dial V120
- Dial Video
- Display Msg
- Do Not Disturb Exception Add
- Do Not Disturb Exception Delete
- Do Not Disturb On
- Do Not Disturb Off
- Extn Login
- Extn Logout
- Flash Hook
- Relay On
- Relay Off
- Relay Pulse
- Resume Call
- Retrieve Call
- Ride Call
- Ring Back When Free
- Secondary Dial Tone
- Set Absent Text
- Set Account Code
- Set Hunt Group Night Service
- Set Hunt Group Out Of Service
- Set Inside Call Seq
- Set No Answer Time
- Set Outside Call Seq
- Set Ringback Seq
- Set Wrap Up Time
- Suspend Call
- Suspend CW
- Toggle Calls
- Voicemail Collect
- Voicemail Node
- Voicemail On
- Voicemail Off
- Voicemail Ringback On
- Voicemail Ringback Off

Busy

Provide busy signal to the user. This is useful for barring numbers - it provides busy tone when the barred number is dialed. See Call Restriction .

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Busy | Busy.
- **Label:** Busy.

Busy On Held

When on, busy on held returns busy to new calls when the user has an existing call on hold.

- **Telephone Number:** Y or 1 for on, N or 0 for off.
- **Button Programming:** Advanced | Busy | Busy on Held.
- **Label:** BusyH

Call Intrude

Intrudes on the existing call of the specified target extension. All call parties are put into a conference and can talk.

Use of this feature is subject to the **Can Intrude** status of the intruder and the **Cannot be Intruded** status of the other call parties.

- **Telephone Number:** Target extension number.
- **Button Programming:** Advanced | Call | Call Intrude.
- **Label:** Intru.

Call Listen

This feature will allow a user to listen to another conversation. The extension the user is listening to must be a member of their Monitor group. See How to Monitor Calls .

- **Telephone Number:** Target extension number.
- **Button Programming:** Advanced | Call | Call Listen.
- **Label:** Listn.

Call Pickup Any

Pick up any (the first available) ringing call. See Call Pickup .

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Call | Call Pickup Any.
- **Label:** PickA

Call Pickup Extn

Pick up a ringing call from a specific Extension.

- **Telephone Number:** Target extension number.
- **Button Programming:** No.

Call Pickup Group

Pick up a call ringing any hunt group of which the user is a member.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Call | Call Pickup Group.
- **Label:** PickG.

Call Pickup Members

This feature can be used to pick up any call to an extension that is a member of the Hunt Group specified. The incoming call can be as a result of a **DID** call to that extension, an internal call to that extension, an internal or external call to the Hunt Group, a call to a phone from another Hunt Group etc. See Call Pickup .

- **Telephone Number:** Group number or "Group name".
- **Button Programming:** Advanced | Call | Call Pickup Members.
- **Label:** PickM

Call Queue

Queue the current call to the destination phone, waiting for the phone to become free. This is the same as a transfer except it allows you to transfer to a busy phone.

- **Telephone Number:** Target extension number.
- **Button Programming:** Advanced | Call | Call Queue.
- **Label:** Queue.

Call Record

This feature allows you to record a conversation on the extension specified in the short code. To make use of this refer to the Voicemail Pro documentation.

- **Telephone Number:** Target extension number.
- **Button Programming:** Advanced | Call | Call Record.
- **Label:** Recor.

Call Steal

Takes over the call currently on the specified extension number or reclaim the user's last transferred call. . See Acquire Call .

- **Telephone Number:** Target extension number or blank for last call transferred.
- **Button Programming:** Advanced | Call | Call Steal.
- **Label:** Steal.

Call Waiting On

Enables call waiting on the user's extension. See Call Waiting .

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Call | Call Waiting On.
- **DSS Toggles:** Yes
- **Label:** CWOn.

Call Waiting Off

Disables Call Waiting on this Extension.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Call | Call Waiting Off.
- **Label:** CWOff.

Call Waiting Suspend

This uses the Q.931 Hold facility and "holds" the incoming call at the ISDN exchange, freeing the ISDN B channel. The current call is placed in slot 0 at the exchange or the slot specified. Only available if supported by the ISDN exchange.

- **Telephone Number:** Blank or specific exchange slot number.
- **Button Programming:** Advanced | Call | Call Waiting Suspend.
- **Label:** CWSus

Cancel All Forwarding

Cancels all forms of forwarding on the user's extension including "Follow Me" and Do Not Disturb".

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Call | Cancel All Forwarding.
- **Label:** FwdOf.

Cancel Ring Back When Free

Cancels any existing ringback set by the user.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Miscellaneous | Cancel Ring Back When Free.
- **Label:** RBak-.

Channel Monitor

For Avaya use only.

- **Telephone Number:** *Channel.*
- **Button Programming:** Advanced | Call | Channel Monitor.
- **Label:** ChMon.

Clear Call

This feature can be used to end the current call. See Transferring a Call .

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Call | Clear Call.
- **Label:** Clear.

Clear CW

End the user's current call and answer any their call waiting. See Call Waiting .

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Call | Clear CW.
- **Label:** ClrCW.

Clear Hunt Group Night Service

Changes the specified hunt group from 'Night Service' mode to 'In Service' mode. Note: This will not override a time profile if set.

- **Telephone Number:** Group number.
- **Button Programming:** Advanced | Call | Clear Hunt Group Night Service.
- **Label:** HGNS-.

Clear Hunt Group Out Of Service

Changes the specified hunt group from 'Out of Service' mode to 'In Service' mode Note: this will not override time profile settings.

- **Telephone Number:** Group number.
- **Button Programming:** Advanced | Call | Clear Hunt Group Out of Service.
- **Label:** HGOS-.

Clear Quota

Refreshes the quota for all services or a specific service. See Quotas and Timebands .

- **Telephone Number:** "Service name" or "" (all services).
- **Button Programming:** Advanced | Call | Clear Quota.
- **Label:** Quota.

Conference Add

Places all calls the user's has on hold into a conference with the user.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Call | Conference Add.
- **Label:** Conf+.

Conference Meet Me

This feature allows a user to join a specific conference.

- **Telephone Number:** Conference number.
- **Button Programming:** Advanced | Call | Conference Meet Me.
- **Label:** CnfRV.

CW

Pick up the waiting call. Provides same functionality as pressing the Recall or Hold key on the phone.

- **Telephone Number:** *None.*
- **Button Programming:** No.

Dial

Dials the number specified to an outside line.

- **Telephone Number:** Telephone number.
- **Button Programming:** Dial
- **Label:** *Telephone number.*

Dial 3K1

Set the call protocol Async PPP, ISDN rate is set to 64000 bps. The call is presented to local exchange as a "3K1 Speech Call". Useful in some where voice calls cost less than data calls.

- **Telephone Number:** Telephone number.
- **Button Programming:** Advanced | Call | Dial 3K1.
- **Label:** D3K1

Dial 56K

Sets the call protocol to Sync PPP, ISDN rate is set to 56000 bps. The call presented to local exchange as a "Data Call".

- **Telephone Number:** Telephone number.
- **Button Programming:** Advanced | Call | Dial 56K.
- **Label:** D56K

Dial 64K

Sets the call protocol to Sync PPP, ISDN rate is set to 64000 bps. The call is presented to local exchange as a "Data Call".

- **Telephone Number:** Telephone number.
- **Button Programming:** Advanced | Call | Dial 64K.
- **Label:** D64K

Dial CW

Call the specified extension number and force call waiting indication on if the extension is already on a call.

- **Telephone Number:** Extension number.
- **Button Programming:** Advanced | Call | Dial CW.
- **Label:** DCW.

Dial Direct

Call the extension specified and force automatic answer if supported by the telephone type. .

- **Telephone Number:** Extension number.
- **Button Programming:** Advanced | Call | Dial Direct.
- **Label:** Dirct.

Dial Emergency

Dials the number specified regardless of any call barring applicable to the user.

- **Telephone Number:** Telephone number.
- **Button Programming:** Advanced | Call | Dial Emergency.
- **Label:** Emrgy.

Dial Extn

This feature can be used to dial an internal extension number.

- **Telephone Number:** Extension number.
- **Button Programming:** No.

Dial Inclusion

Intrudes on the existing call of the specified target extension. The intruder and the target extension can then talk but cannot be heard by the other party.

During the intrusion all parties hear a repeated intrusion tone. When the intruder hangs-up the original call parties are reconnected.

Use of this feature is subject to the **Can Intrude** status of the intruder and the **Cannot be Intruded** status of the other call parties.

- **Telephone Number:** Target extension number.
- **Button Programming:** Advanced | Dial | Dial Inclusion.
- **Label:** Inclu.

Dial Paging

Makes a paging call to an extension or group. The target extension or group members must support page calls.

- **Telephone Number:** Extension or group number.
- **Button Programming:** Advanced | Dial | Dial Paging.
- **Label:** Page.

DialPhysicalNumberByExtension

Dial a specified extension number regardless of the current user logged on at that extension and any forwarding, follow me or do not disturb settings applied by the extension user.

This function is currently only available on US based systems as part of E911 requirements.

- **Telephone Number:** Extension number.
- **Button Programming:** Advanced | Dial | Dial Physical Extn By Number.
- **Label:** PhyEx.

DialPhysicalNumberByID

Dial a specific extension using its system ID. This may be necessary in hot desking environments where some extensions have been created with no default extension number.

This function is currently only available on US based systems as part of E911 requirements.

- **Telephone Number:** Extension ID.
- **Button Programming:** No.

Dial Speech

This feature allows a short code to be created to force the outgoing call to use the Speech bearer capability.

- **Telephone Number:** Telephone number.
- **Button Programming:** Advanced | Dial | Dial Speech.
- **Label:** DSpch.

Dial V110

Sets the call protocol to Async PPP using V.110 which runs at 9600 bps. The call is presented to local exchange as a "Data Call". It is ideal for some bulletin boards.

- **Telephone Number:** Telephone number.
- **Button Programming:** Advanced | Call | Dial V110.
- **Label:** DV110

Dial V120

Sets the call protocol to Async PPP using V.120. The call is presented to local exchange as a "Data Call". This will run at speeds up to 64K per channel but has a slightly higher Protocol overhead than pure 64K operation. Useful for some bulletin board systems as it allows the destination to run at a different asynchronous speed to the calling end.

- **Telephone Number:** Telephone number.
- **Button Programming:** Advanced | Call | Dial V120.
- **Label:** DV120

Dial Video

Sets the call protocol to Sync PPP, ISDN rate is set to 64000 bps. The call is presented to the local exchange as a "Video Call".

- **Telephone Number:** Telephone number.
- **Button Programming:** Advanced | Call | Dial Video.
- **Label:** Dvide

Display Msg

Allows the sending of special functions to DS port display phone extensions. The telephone number takes the format xxxx;[0)nnn/ppppppp where:

- xxx is the target extension.
- nnn is the Definity feature number.
- ppppppp is the parameter data (if required).

- **Telephone Number:** *See above.*
- **Button Programming:** Advanced | Dial | Display Msg.
- **Label:** Displ.

Do Not Disturb Exception Add

Adds a number to the user's "Do Not Disturb Exception List". This can be an internal extension number or external CLI.

- **Telephone Number:** Telephone number or CLI.
- **Button Programming:** Advanced | Do Not Disturb | Do Not Disturb Exception Add.
- **Label:** DNDX+.

Do Not Disturb Exception Delete

Removes a number from the user's "Do Not Disturb Exception List".

- **Telephone Number:** Telephone number or CLI.
- **Button Programming:** Advanced | Do Not Disturb | Do Not Disturb Exception Delete.
- **Label:** DNDX-.

Do Not Disturb On

Places the users into 'do not disturb' mode. See Do Not Disturb .

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Do Not Disturb | Do Not Disturb On.
- **DSS Toggles:** Yes
- **Label:** DNDOn.

Do Not Disturb Off

Cancels the user's 'do not disturb' mode if set.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Do Not Disturb | Do Not Disturb On.
- **Label:** DNDOf.

Extn Login

This feature allows a user to take over ownership of an Extension. The Telephone Number entered is the "Extension*Login Code" of the required User.

- **Telephone Number:** Extension Number*Login Code of agent or hot desk user.
- **Button Programming:** Advanced | Extn | Extn Login.
  Note: Currently only supported on DT port phones.
- **DSS Toggles:** Yes
- **Label:** Login.

Extn Logout

Logs out a User from a telephone to which they had previously logged on.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Extn | Extn Logout.
- **Label:** Logof.

Flash Hook

Sends a hook flash signal to the currently connected analog line.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Miscellaneous | Flash Hook.
- **Label:** Flash.

Follow Me Here

Causes calls to the extension number specified, to be redirected to the extension initiating the 'Follow Me Here'. See Follow Me .

- **Telephone Number:** Extension to redirect.
- **Button Programming:** Advanced | Follow Me | Follow Me Here.
- **Label:** Here+

Follow Me Here Cancel

Cancels any 'Follow Me Here' set on the specified extension. Only works if entered at the extension from which the original "Follow Me Here" was initiated.

- **Telephone Number:** Extension being redirected.
- **Button Programming:** Advanced | Follow Me | Follow Me Here Cancel.
- **Label:** Here-.

Follow Me To

Causes calls to the extension initiating the 'Follow Me To' to be redirected to the extension specified. This feature can be canceled at the redirected extension by using the same feature but leaving the target extension number blank.

See Follow Me .

- **Telephone Number:** Target extension number or blank to cancel.
- **Button Programming:** Advanced | Follow Me | Follow Me To.
- **Label:** FolTo.

Forward Hunt Group Calls On

Forward the user's hunt group calls to their forward number. Only works when a forward number is set (see Forward Number) and forward unconditional is also on (see Forward Unconditional).

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Forward | Forward Hunt Group Calls On.
- **DSS Toggles:** Yes
- **Label:** FwdH+.

Forward Hunt Group Calls Off

Cancels the forwarding of the user's hunt group calls.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Forward | Forward Hunt Group Calls Off.
- **Label:** FwdH-.

Forward Number

Sets the extension number to which calls are forwarded when using 'Forward Unconditional'. Also used for 'Forward Hunt Group'.

- **Telephone Number:** Telephone number.
- **Button Programming:** Advanced | Forward | Forward Number.
- **Label:** FwdNo.

Forward On Busy Number

Sets the extension number to which calls are forwarded when using 'Forward on Busy' and/or 'Forward on No Answer'.

- **Telephone Number:** Telephone number.
- **Button Programming:** Advanced | Forward | Forward on Busy Number.
- **Label:** FwBNo.

Forward On Busy On

Enables forwarding to the 'Forward on Busy Number' when the user's extension is busy.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Forward | Forward on Busy On.
- **DSS Toggles:** Yes
- **Label:** FwBOn

Forward On Busy Off

Disables forwarding when the user's extension is busy.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Forward | Forward on Busy Off.
- **Label:** FwBOf.

Forward On No Answer On

Enables forwarding to the 'Forward on Busy Number' when the user's extension is not answered within the period defined by their 'No Answer Time'.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Forward | Forward on No Answer On.
- **Label:** FwNOn.

Forward On No Answer Off

Disables forwarding when the user's extension is not answered.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Forward | Forward on No Answer Off.
- **Label:** FwNOff.

Forward Unconditional On

Enables forwarding of all calls, except group calls, to the 'Forward Number' set for the user's extension. To also forward hunt group calls to the same number 'Forward Hunt Group Call On' must also be used.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Forward | Forward Unconditional On.
- **DSS Toggles:** Yes
- **Label:** FwUOn.

Forward Unconditional Off

Disables forwarding of all calls from the user's extension. Note: This does not disable 'Forward on No Answer' and/or 'Forward on Busy' if also on.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Forward | Forward Unconditional Off.
- **Label:** FwUOf.

Headset Toggle

- **Telephone Number:** *None.*
- **Button Programming:** Miscellaneous | Headset Toggle.
- **Label:** HdSet.
- **Toggles:** Yes.

Hold Call

This uses the Q.931 Hold facility, and "holds" the incoming call at the ISDN exchange, freeing up the ISDN B channel. The Hold Call feature "holds" the current call to a slot. The current call is always automatically placed into slot 0 if it has not been placed in a specified slot. Only available if supported by the ISDN exchange. See also Retrieve Call .

- **Telephone Number:** Exchange hold slot number or blank (slot 0).
- **Button Programming:** Advanced | Hold | Hold Call.
- **Label:** Hold.

Hold CW

Place the user's current call on hold and answers the waiting call.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Hold | Hold CW.
- **Label:** HoldCW.

Hold Music

Plays to the user the system's music on hold source. See Music On Hold .

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Hold | Hold Music.
- **Label:** Music.

Hunt Group Disable

Disables the user's membership of the specified hunt group. They will no longer receive call to that hunt group until their membership is enabled again.

- **Telephone Number:** Group number.
- **Button Programming:** Advanced | Hunt Group | Hunt Group Disable.
- **Label:** HGDis.

Hunt Group Enable

Enables the user's membership of a hunt group. They will then begin to receive calls to the specified hunt group.

- **Telephone Number:** Group number.
- **Button Programming:** Advanced | Hunt Group | Hunt Group Enable.
- **DSS Toggles:** Yes
- **Label:** HGEna.

Off Hook Station

Enables or disables whether the user's extension acts as a fully hands free unit. Typically this is used when the answering and clearing of calls is done through an application such as Phone Manager.

- **Telephone Number:** "Y" for on or "N" for off.
- **Button Programming:** Advanced | Miscellaneous | Off Hook Station.
- **Label:** OHStn.

Park Call

Parks the user's current call into the specified park slot number. The call can then be retrieved by other extensions (refer to the appropriate telephone user guide). The 'Ride Call' feature can be used to retrieve calls from specific park slots.

Note: When programmed to a DSS key, the key's BLG lamp indicates when a call is parked in that park slot. The key can also be used to retrieve the parked call.

- **Telephone Number:** Park slot number.
- **Button Programming:** Park.
- **DSS Toggles:** Yes
- **Label:** Park.

Priority Call

Allows the user to call an extension that is set to 'do not disturb'.

- **Telephone Number:** Target extension number.
- **Button Programming:** Advanced | Call | Priority Call.
- **Label:** PCall.

Record Greeting

For use with integrated Voicemail on Avaya IP Office - Small Office Edition systems. Allows the recording of the greetings used by auto-attendant services.

- **Telephone Number:** AA:Name.x where Name is the auto-attendant service name and x is the greeting (1 = morning, 2 = afternoon, 3 = evening and 4 = options menu).

Relay On

Closes the specified switch in the system's external output (EXT O/P) port.

- **Telephone Number:** Switch number (1 or 2).
- **Button Programming:** Advanced | Relay | Relay On.
- **Label:** Rely+.

Relay Off

Opens the specified switch in the system's external output (EXT O/P) port.

- **Telephone Number:** Switch number (1 or 2).
- **Button Programming:** Advanced | Relay | Relay Off.
- **Label:** Rely-.

Relay Pulse

Closes the specified switch in the system's external output (EXT O/P) port for 5 seconds and then opens the switch.

- **Telephone Number:** Switch number (1 or 2).
- **Button Programming:** Advanced | Relay | Relay Pulse.
- **Label:** Relay.

Resume Call

Resume a call previously suspended to the specified ISDN exchange slot. The suspended call may be resumed from another phone/ISDN Control Unit on the same line. See also Suspend Call and Suspend CW.

- **Telephone Number:** Exchange suspend slot number.
- **Button Programming:** Advanced | Call | Resume Call.
- **Label:** Resum.

Retrieve Call

Retrieves a call previously held to a specific ISDN exchange slot. Only available when supported by the ISDN exchange. See also Hold Call .

- **Telephone Number:** Exchange hold slot number.
- **Button Programming:** Advanced | Call | Retrieve Call.
- **Label:** Retriv.

Ride Call

Retrieve a parked call from a specified system park slot.

- **Telephone Number:** System park slot number.
- **Button Programming:** Advanced | Call | Ride Call.
- **Label:** Ride.

Ring Back When Free

Sets a ringback on the specified extension. This sets a 'ringback when free' on an extension currently on a call or a 'ringback when next used' for an extension that is free but doesn't answer.

When the target extension is next used or ends its current call, the users is rung and when they answer a call is made to the target extension.

- **Telephone Number:** Target extension number.
- **Button Programming:** Advanced | Miscellaneous | Ring Back When Free.
- **Label:** RBak+.

Secondary Dial Tone

This feature can be used to provide secondary dial tone to a user before dialing. See Secondary Dial Tone and [n] Characters .

- **Telephone Number:** Digit which triggers secondary dial tone.
- **Button Programming:** Advanced | Dial | Secondary Dial Tone.
- **Label:** DTone.

Set Absent Text

This feature can be used select the user's current absence text. Note: The user still has to select Set or Clear on their phone to display or hide the text. This text is then displayed to internal callers who have suitable display phones or applications. See Use the Set Absent Text Short Code Feature .

- **Telephone Number:** The telephone number should take the format "***y,n,text***" where:
  - ***y*** = 0 or 1 to turn this feature on or off.
  - ***n*** = the number of the absent statement to use, see the list below:
    - 0 = None.
    - 1 = On vacation until.
    - 2 = Will be back.
    - 3 = At lunch until.
    - 4 = Meeting until.
    - 5 = Please call.
    - 6 = Dont disturb until.
    - 7 = With visitors until.
    - 8 = With cust. til.
    - 9 = Back soon.
    - 10 = Back tomorrow.
    - 11 = Custom.
  - ***text*** = any text to follow the absent statement.
- **Button Programming:** Advanced | Set | Set Absent Text.
- **Label:** Absnt.

Set Account Code

This short code feature is used to allow system users to enter a valid account code prior to making a phone call. This short code feature is essential for allowing POT users to enter account codes. The example below demonstrates a short code that makes use of the SetAccountCode feature. Once this short code is set up, any account code can be used in conjunction with it.

Example

Short code: **11*N#**

Telephone Number: **N**

Feature: **SetAccountCode**

In the example above, N (within the short code field) = any valid account code, N (within the Telephone Number field) = any telephone number. For the purpose of this example, we will imagine the account code to be **1234**. Once this short code is created, a user can dial **11*1234#** to get a dial tone for dialing the restricted telephone number or the phone number needing to be tracked for billing purposes.

Set Hunt Group Night Service

Puts the specified hunt group into 'Night Service' mode.

- **Telephone Number:** Hunt group extension number.
- **Button Programming:** Advanced | Set | Set Hunt Group Night Service.
- **DSS Toggles:** Yes
- **Label:** HGNS+.

Set Hunt Group Out Of Service

Puts the specified hunt group into 'Out of Service' mode.

- **Telephone Number:** Hunt group extension number.
- **Button Programming:** Advanced | Set | Set Hunt Group Out of Service.
- **Label:** HGOS+.

Set Inside Call Seq

Allows the user to select the ringing used on their extension for internal calls. The number entered corresponds to the ring pattern required. This is 0 for Default Ring, 1 for RingNormal, 2 for RingType1, etc. See Ring Tones .

Note: The 4400 and 4600 series only support the Default Ring type.

- **Telephone Number:** *See above.*
- **Button Programming:** Advanced | Set | Set Inside Call Sequence.
- **Label:** ICSeq.

Set No Answer Time

Allows the user to change their No Answer Time setting (set on the **User | Telephony** tab).

- **Telephone Number:** Time in seconds.
- **Button Programming:** Advanced | Set | Set No Answer Time.
- **Label:** NATim.

Set Outside Call Seq

Allows the user to select the ringing used on their extension for external calls. The number entered corresponds to the ring pattern required. This is 0 for Default Ring, 1 for RingNormal, 2 for RingType1, etc. See Ring Tones .

Note: The 4400 and 4600 series only support the Default Ring type.

- **Telephone Number:** *See above.*
- **Button Programming:** Advanced | Set | Set Outside Call Sequence.
- **Label:** OCSeq.

Set Ringback Seq

Allows the user to select the ringing used on their extension for ringback calls. The number entered corresponds to the ring pattern required. This is 0 for Default Ring, 1 for RingNormal, 2 for RingType1, etc. See Ring Tones .

Note: The 4400 and 4600 series only support the Default Ring type.

- **Telephone Number:** *See above.*
- **Button Programming:** Advanced | Set | Set Ringback Call Sequence.
- **Label:** RBSeq.

Set Wrap Up Time

Allows the user to change their Wrap-up Time setting (set on the User | Telephony tab).

- **Telephone Number:** Time in seconds.
- **Button Programming:** Advanced | Set | Set Wrap Up Time.
- **Label:** WUTim.

Suspend Call

Uses the Q.931 Suspend facility. Suspends the incoming call at the ISDN exchange, freeing up the ISDN B channel. The call is placed in exchange slot 0 if a slot number is not specified. Only available when supported by the ISDN exchange. See also Resume Call .

- **Telephone Number:** Exchange slot number or blank (slot 0).
- **Button Programming:** Advanced | Suspend | Suspend.
- **Label:** Suspe

Suspend CW

Uses the Q.931 Suspend facility. Suspends the incoming call at the ISDN exchange and answer the call waiting. The call is placed in exchange slot 0 if a slot number is not specified. Only available when supported by the ISDN exchange. See also Resume Call .

- **Telephone Number:** Exchange slot number or blank (slot 0).
- **Button Programming:** Advanced | Suspend | Suspend CW.
- **Label:** SusCW.

Toggle Calls

Cycle through each call that the user has on hold on the IP Office.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Call | Toggle Calls.
- **Label:** Toggl.

Voicemail Collect

Connects to the voicemail server. The telephone number must indicate the name of the Voicemail box to be accessed, eg. "?Extn201" or "#Extn201". The ? indicates "collect Voicemail" and the # indicates "deposit Voicemail".

When using Voicemail Pro, names of specific callflow start points can also be used to directly access those start points via a short code. In these cases ? is not used and # is only used if ringing is required before the start points callflow begins.

- Note: Short codes using the **Voicemail Collect** feature, with either **"Short Codes.*name*"** and **"#Short Codes.*name*"** entries in the **Telephone Number** field, will be automatically converted the **Voicemail Node** feature and *name*.

- **Telephone Number:** *See above.*
- **Digital Telephony:** Advanced | Voicemail | Voicemail Collect.
- **Label:** VMCol.

Voicemail Node

Similar to Voicemail Collect but used for calls being directed to a Voicemail Pro Short Codes start point. If ringing is required before the start point callflow begins then a **#** should be included before the name.

- **Telephone Number:** *Voicemail Pro Short Code start point name.*
- **Digital Telephony:** *Not applicable.*
- **Label:** –.

Voicemail On

Enables the user's voicemail mailbox to answer calls which ring unanswered or arrive when the user is busy.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Voicemail | Voicemail On.
- **DSS Toggles:** Yes
- **Label:** VMOn.

Voicemail Off

Disables the user's voicemail box from answering calls.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Voicemail | Voicemail Off.
- **Label:** VMOff.

Voicemail Ringback On

Enables voicemail ringback to the user's extension. Voicemail ringback is used to call the user when they have new voicemail messages. The ringback takes place each time the extension is used.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Voicemail | Voicemail Ringback On.
- **DSS Toggles:** Yes
- **Label:** VMRB+.

Voicemail Ringback Off

Disables voicemail ringback to the user's extension.

- **Telephone Number:** *None.*
- **Button Programming:** Advanced | Voicemail | Voicemail Ringback Off.
- **Label:** VMRB-.

Short Code Examples

Short Code Examples

Short codes are a flexible and quick way of setting up certain features. Because of their flexibility, the procedure for setting up short codes can seem a little vague for people who are unfamiliar with them. To help you get familiar with them, we have provided several examples of useful short codes for you to use directly or build upon.

Creating a Speed Dial

In this example 401 will dial the New Jersey Office on 212 555 0000.

- **Short Code:** 401
- **Telephone Number:** 1 212 555 0000
- **Line Group ID:** 0
- **Feature:** Dial

Replace Outgoing Caller ID

To force outgoing **Caller ID** to 123 (assuming 123 is a valid MSN/DID for your outside line).

- **Short Code:** ?
- **Telephone Number:** .s123
- **Feature:** Dial

External Dial Prefix

This is for dialing a prefix for an outside line.

The example below is for a group that contains PRI lines.

- **Short Code:** 9N;
- **Telephone Number:** N
- **Feature:** Dial

The following example is for analog (Loop or Ground Start) and T1 lines or a combination of the two.

- **Short Code:** 9N
- **Telephone Number:** N
- **Feature:** Dial

Blocking Caller ID

This is for blocking Caller ID for external calls.

- **Short Code:** 9N
- **Telephone Number:** NW
- **Feature:** Dial

Retrieve Messages from Specific Mailbox

To allow a user to retrieve messages from the specified Voicemail box, eg. the Sales Hunt Group.

- **Short Code:** *99
- **Telephone Number:** ?Sales
- **Feature:** VoicemailCollect

Record Message to Specific Mailbox

To allow users to deposit a message directly to Extn201's Voicemail box.

- **Short Code:** *201
- **Telephone Number:** "#Extn201"
- **Feature:** VoicemailCollect

Individual Hot Desking

To allow a user associated with extension 201 to take over the telephone on which they dialed 299, assuming their login code is 1234.

- **Short Code:** 299
- **Telephone Number:** 201*1234
- **Feature:** Extnlogin

Internal Extension Speed Dial

When the user dials 100 this Short Code rings the internal extension 201.

- **Short Code:** 100
- **Telephone Number:** 201
- **Feature:** DialExtn

Switch Call Waiting On

A user can force Call Waiting on the specified extension even if that extension does not have Call Waiting set.

- **Short Code:** *94*N#
- **Telephone Number:** N
- **Feature:** Dial

User Selected Internal Ringing Type

This Short Code allows a User to change their Inside Call Pattern. N represents the number corresponding to the Call Sequence the user wishes to choose, the numbering starts at 0 selecting Default Ring, 1 selects RingNormal, 2 selects RingType1, etc.

- **Short Code:** *80*N#
- **Telephone Number:** N
- **Feature:** SetInsideCallPattern

User Set Allocated Answer Interval

This allows a User to change their Allocated Answer Interval. N represents the number of seconds.

- **Short Code:** *81*N#
- **Telephone Number:** N
- **Feature:** SetAllocatedAnswerInterval

User Set Wrap Up Time

This Short Code allows a User to change their Wrap-up Time. N represents the number of seconds.

- **Short Code:** *82*N#
- **Telephone Number:** N
- **Feature:** SetWrapUpTime

Switch Auto-Answer On

This allows the extension specified to be automatically answered.

- **Short Code:** *83*N#
- **Telephone Number:** N
- **Feature:** DialDirect

Cancel Ring Back When Free

This example Short Code will cancel Ring Back When Free on the specified extension.

- **Short Code:** *84*N#
- **Telephone Number:** N
- **Feature:** CancelRingBackWhenFree

Use the Set Absent Text Short Code Feature

The following short code can be used to turn an absent text message on:

- **Short Code:** *88
- **Telephone Number:** "1,5,my assistant on 208"
- **Line Group ID:** 0
- **Feature:** SetAbsentText

The following short code could be used to turn this facility off. In the Telephone Number the first 0 is used to turn this facility off and the second 0 is used to select the absent statement "None".

- **Short Code:** *89
- **Telephone Number:** "0,0"
- **Line Group ID:** 0
- **Feature:** SetAbsentText

Use Dial Emergency

To allow access to emergency services (eg. 911) even though Call Restriction barring has been set for a User, a short code should be created for each emergency number.

For example:

- **Short Code:** 911
- **Telephone Number:** 911
- **Line Group ID:** 0
- **Feature:** DialEmergency

The DialEmergency Short Code feature can be used to allow any number to override the Outward Restricted option.

Maximum Call Length

The character **t** can be used in dialing short codes to set the maximum allowed duration of a call.

For example, the following short code will dial a number but then disconnect the call after 20 minutes (plus or minus a minute).

- **Short Code:** 9N
- **Telephone Number:** Nt(20)
- **Line Group ID:** 0
- **Feature:** Dial

Dial on Pick up

The following User Short Code dials the extension specified the moment the User's handset it is picked up.

- **Short Code:** ?D
- **Telephone Number:** 201
- **Line Group ID:** 0
- **Feature:** DialExtn

Log In and Log Off

The default short code for logging in is configured as shown below. N represents the users extension number followed by a * and then their login code, eg. *35*401*123#.

- **Short Code:** *35*N#
- **Telephone:** N
- **Feature:** ExtnLogin

The default short code for logging off is shown below.

- **Short Code:** *36
- **Feature:** ExtnLogout

To create new Short Codes to be used for Hot Desking, the Telephone Number field (the information processed by the Control Unit) must consist of the Extension Number followed by an * and then the Login Code, as per the following example:-

- **Short Code:** *80
- **Telephone Number:** 401*123
- **Feature:** ExtnLogin

Directing Incoming Calls to Voicemail Pro

The destination field of an Incoming Route form can be used to direct calls to a specific Voicemail Pro start point.

a) Module Start Point

In the Incoming Call Route form, enter the destination as the name of the module start point preceded by VM: and enclosed in quotes, eg. "VM:AutoAttend". Note that there is a maximum of 15 characters allowed in this entry.

A hunt group should also be created that has the same name as the module start point. In case where Voicemail Pro is not available, incoming calls will be directed to that hunt group as an alternate destination. eg. For the example above create a group called ***AutoAttend***.

b) Short Code Start Point

Once a short code start point has been created in Voicemail Pro, a matching short code should be created on the IP Office, eg:

- **Short Code:** *96
- **Telephone Number:** "#Short Codes.*Main" *(include quote marks)*
- **Feature:** VoicemailCollect

The above short code will allow internal users to access a Voicemail Pro short code start point named Main. To route external incoming calls to the same start point, enter the short code *96 as the **Destination** in the **Incoming Call Route** form.

Creating User Short Codes

User short codes are created within a specific user's settings and apply only to that user. All the rules relating to telephone number characters, short code characters and special characters still apply.

To create a user short code:

1. Click the **User** form within the Configuration Tree.
2. Double-click the user for whom you want to create the short code.
3. Click the **ShortCodes** tab.
4. Double-click or right-click within the panel.
5. Enter information in the necessary fields:
    - **Short Code**: *Default = blank*
      The dialing digits used to trigger the short code. Maximum length is 33 characters. See Short Code Characters for a list of valid characters.
    - **Telephone Number**: *Default = blank*
      The number output by the short code. The number dialed by the short code or parameters for the short code feature. This field can contain numbers and characters. For example, it can contain Voicemail Pro start point names, user names, hunt group names and telephone numbers (including those with special characters). Maximum length 33 characters. See Telephone Number Characters for a list of valid characters.
    - **Line Group ID**: *Default = 0*
      For external calls, this is the set of lines that are used when making the call. Which group a line belongs to is set through the **Line** form for each line.
    - **Feature**: *Default = Dial*
      This is what the short code does. See Short Code Features .
    - **Locale**: *Default = blank*
      Some features can support country specific variations if needed.
6. Merge the configuration.

Short codes created within the User Restriction configuration form can also be applied to individual users.

Creating System Short Codes

System short codes apply to and can be used by all users on the system. A list of default system short codes have been created for your convenience.

To create a new system short code:

1. Click the **Short code** form within the Configuration Tree.
2. Double-click within the short code panel or right-click and select **New**.
3. Enter information in the necessary fields:
    - **Short Code**: *Default = blank*
      The dialing digits used to trigger the short code. Maximum length is 33 characters. See Short Code Characters for a list of valid characters.
    - **Telephone Number**: *Default = blank*
      The number output by the short code. The number dialed by the short code or parameters for the short code feature. This field can contain numbers and characters. For example, it can contain Voicemail Pro start point names, user names, hunt group names and telephone numbers (including those with special characters). Maximum length 33 characters. See Telephone Number Characters for a list of valid characters.
    - **Line Group ID**: *Default = 0*
      For external calls, this is the set of lines that are used when making the call. Which group a line belongs to is set through the **Line** form for each line.
    - **Feature**: *Default = Dial*
      This is what the short code does. See Short Code Features .
    - **Locale**: *Default = blank*
      Some features can support country specific variations if needed.
6. Merge the configuration.

Creating User Restriction Short Codes

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. These short codes have the same properties and parameters as the other short codes, with the exception that you can assign specific names to them for re-use.

To set up a restriction within the **User Restriction** form:

1. Click **User Restriction** form within the Configuration Tree.
2. Enter a name for the restriction.
3. Click the **Short Code** List tab and create a short code.
4. Merge the configuration.

For a description of all the fields within this form, see User Restrictions Overview.

Routing Features and Functions

Overview of Routing

The Control Unit is a network router. In this role it can extend a local area network by using WAN links and PSTN connections, so that users on the LAN can access remote addresses.

Additionally it allows users to dial-in and then act as if they were using a PC on the LAN.

Internal Data Channels

As well as being a network router, the Control Unit is a telephone system. These dual roles allow it to support a range of functions that involve traffic between the network and telephony interfaces. These functions use internal data channels.

The number of internal data channels that can be connected from the system's LAN interface to its telephony interface at any time is restricted.

- An internal data channel is a B-channel connected between the system's telephony and LAN interfaces. For example a Voicemail connection, an internet connection or a RAS user.
- The number of data channels in use does not necessarily match the number of users:
- Several network users, browsing the internet using the same ISP connection would be a single data channel.
- Several dial-in network users would each have a separate data channel.
- An additional restriction is in place to limit the number of data channels that can be simultaneously in use for Voicemail at any time.

The restriction depends on the type of Control Unit being used.

Control Unit	Maximum Number of Internal Data Channels	Maximum Number of Internal Data Channels for Voicemail
IP 401	2	2
Avaya IP Office - Small Office Edition	18	10
IP 403	18	10
IP 406	24	20
IP 412	100	30

- Note: Calls using a VCM channel (eg. VoIP calls and Avaya 4600 Series phones) do not use a data channel.

Connecting to the Internet

You require an account with an Internet Service Provider (ISP). By using the Network Address Translation feature a simple single address ISDN dial up account provides all your users access to the Internet. The ISP provides you with an account name, password, address of a DNS service (this is not required if the Request DNS option is selected), and ISDN number to call. You can use the Installation Wizard to enter these details, or configure a Service and an IP route (this is not required if the Default Route option is checked).

Example Configuration

This example shows how to set up a connection to an ISP:

1. Create a service:
    - **Name:** Internet (any name to identify the Service).
    - **Account Name:** As provided by the ISP.
    - **Password:** As provided by the ISP.
    - **Telephone Number:** As provided by the ISP.
    - Only select the Encrypted Password option if the ISP also supports CHAP.
2. Create an IP Route. This is not required if the Default Route option is selected, as shown above.
    - Enter only the Destination as "Internet" (this is the Service created above). This becomes the default route, in other words, if a packet is received for a network where a route has not been configured it is sent via this Service.
3. Under DNS tab of the System configuration form enter the DNS Server IP Address as provided by the ISP. Note that this is not required if the Request DNS option is selected under the Service's IP tab.
    - If the Request DNS option is enabled a PC sends DNS requests to the Control Unit. The Control Unit then forwards these requests to the correct DNS server. This is useful if your system is using different ISPs at different times of the day or for backup.
4. The Quota time (default 240 minutes) limits the amount of call time allowed for this Service per day, week or month. This time can be refreshed via a short code using the ClearQuota feature.
5. Each PC that is used to access the Internet requires the IP address of the DNS Server whether this is the Control Unit or the ISP's DNS server. If DHCP is being used the Windows 95/98 utility, winipcfg, can be used to release and renew the IP configuration of a PC.

To enable dial up using both channels of an ISDN BRI line, first you must make sure that the ISP you are dialing supports Multilink (bonding channels). Then you must set two modes of operation by using AT commands.

- **ATB1** - this will set MLPPP
- **AT*A*_n_** - where ***n*** is either 1 or 0.
    - 1= Permanent bonding of channels
    - 0= the bonding of channels on demand.

Connecting to the LAN

Connecting to the LAN

Computers in an office communicate via a LAN (Local Area Network), which may at its simplest be a length of coaxial cable connecting all the computers or by twisted pair cables going into a central hub. In our case the Control Unit is a LAN hub with a number of LAN ports for computer connection. The Control Unit communicates with the LAN via TCP/IP (Transmission Control Protocol / Internet Protocol).

The computers communicate by putting data into packets marked with the source and destination IP address. The sending computer does not care where the destination is, it simply places the packet onto its LAN. It is the destination computer's task to see the packets and collect them.

Separate LANs are connected together using routers. Routers use WAN (Wide Area Network) links on leased telephone lines or data calls across the public telephone network (PSTN) to route traffic from one network to another. The Control Unit is a router, which can be setup with information about where to route traffic to and from other LANs.

IP Addressing

Each computer/host on a TCP/IP network must have a unique IP Address. The address is 32 bits long, eg. 11000000101010000010101000000001.

As this is impossible for humans to remember, we split it into 4 groups of 8 bits and convert those groups from binary into decimal numbers, with dots between the groups.

For example:

- 11000000101010000010101000000001 becomes
- 11000000.10101000.00101010.00000001 becomes
- 192.168.42.1.

Note: Occasionally IP addresses may also be seen in hexadecimal format, in this case 192.168.42.1 becomes C0.A8.2A.01.

Sending Traffic to the Router: Subnet Masks

Each computer on a TCP/IP LAN requires three values; an IP address, a subnet mask (also called an IP Mask) and a default gateway address. The first two are used to decide whether a data packet for another computer is on the same LAN. If it is not then the third, the default gateway address, is the address of the router, which will forward the packet to its correct destination outside the LAN

To decide this, the computer does a binary AND of its IP address and mask and compares that to the binary AND of the destination's IP address and mask. If the result is not the same then the destination is not on the LAN. The packet is sent to the PC's default gateway address, where the original destination address is looked at to determine how to get the packet to its final destination. Our gateway or router is the Control Unit, which contains in its IP Route table instructions to get the packet to the destination.

For example:

- **Source PC1:**
  IP address 192.168.42.201, Subnet mask 255.255.255.0, ANDing gives 192.168.42.0.
- **Destination PC2:**
  IP address 192.168.42.202, Subnet mask 255.255.255.0, ANDing gives 192.168.42.0, same as PC1 so on the same LAN as PC1.
- **Destination PC3:**
  IP address 158.152.1.43, Subnet mask 255.255.255.0, ANDing gives 158.152.1.0, which is different from PC1 so the packet is sent to the Control Unit which must have a entry for address of PC2 in its IP Route table.

There are special IP addresses called broadcast addresses, which are seen by all computers on a LAN, eg. 255.255.255.255 or 192.168.42.255.

Dynamic Host Configuration Protocol (DHCP)

Originally IP addresses were allocated manually to each computer/host by network administrators. A protocol called Dynamic Host Configuration Protocol (DHCP) allowed this to be done automatically. When a computer is switched on, it sends out a broadcast on the LAN asking for an IP address, subnet mask and default gateway. A DHCP server replies, thus simplifying the allocation process.

A major benefit of DHCP is that a PC can be set to be a DHCP client. It can then be connected to any LAN with a DHCP server, switched on and it will automatically be correctly configured. There should only be one DHCP server on any LAN.

The Control Unit can act as a simple DHCP server. When switched on with a defaulted configuration, the Control Unit request IP information from a DHCP server. If it gets no response to its request then it assumes the role of DHCP server for the LAN.

In DHCP Server mode, by default the Control Unit issues itself the address 192.168.42.1. It allocates 200 addresses for DHCP clients, 192.168.42.1 to 19.168.42.200. This leaves 192.168.42.201 to 192.168.42.254 available for any computers that need to be allocated a fixed or static IP address. 192.168.42.255 is not used as this is a broadcast address for the LAN.

Getting it Working!

A major factor is what IP address range the customer wants the Control Unit to have. If the default of 192.168.42.1 to 254 is acceptable with the Control Unit acting as DHCP server, connect the Control Unit system to the LAN and switch it on. Then connect the PC's to the LAN and switch them on.

If the Customer wants you to work to a specific address range and has a DHCP server machine on his LAN that is okay. Connect the Control Unit to the LAN and switch it on. It should see the DHCP server and configure itself as a client.

Configuration is more complex if the customer wants the Control Unit to have a specific address but does not have a DHCP server on the LAN. First, establish communications with the Control Unit from a PC configured with a specified IP address 192.168.42.201, subnet mask 255.255.255.0. Use that to configure the Control Unit to the IP address, IP mask and DHCP mode required.

Address ranges

The following addresses will never appear on the Internet and are thus free for use within a private network.

- 10.0.0.0.
- 172.16.0.0 through 172.32.0.0.
- 192.168.0.0 through 192.168.255.0.

If you pick one of these you should have no address problems with the Internet. We picked 192.168.42.0 and 192.168.43.0 out of the hat!

Viewing Your PCs IP configuration

In Windows 95/98 there is a program called WINIPCFG, which displays the IP configuration of the PC. This is useful when the PC is obtaining the configuration from a DHCP server. To view this information run **winipcfg** or **winipcfg /all**

If DHCP is being used, winipcfg also allows you to change your PC's IP configuration without rebooting by using Release and Renew.

On Windows NT/2000 and XP the information can be obtained using **ipconfig** or **ipconfig /all** via the command prompt.

Domain Name System

This is the system used on the Internet to match computer names to IP addresses.

Internet users request specific hosts using names such as www.avaya.com. These names are sent to a Domain Name Server (DNS), which converts the name to the IP address so the computers can pass data.

Typically your ISP will give you the address of their DNS server and this information can be entered in the DNS tab of the System configuration form.

If you are using multiple ISPs the Control Unit can pass on DNS requests to the correct DNS Server, tick **Request DNS** in the IP tab of the Service configuration form.

Whichever method is used, each PC on the network should renew their IP configuration either using the Windows 95/98 utility called *winipcfg* or next time the PC requests an IP address from the DHCP server.

Firewalls

Firewalls

The Control Unit can act as a firewall. The firewall access software allows you to control who can access external resources, while isolating your private networks from the Internet. The firewall also performs Network Address Translation allowing access to the Internet using a single pre-configured or dynamically assigned IP address, yet still allows **all** your PCs and workstations simultaneous access if and when required.

Different firewall profiles can be created and then assigned to Services and to Dial In users.

To create a firewall, right-click within the Firewall Profile entries and select **New**. There are 2 levels of configuration, the Radio buttons on the Standard tab then the additional filters you wish to apply via the Custom tab.

The firewall works by allowing permitted packets to punch holes in the wall (start a session) and then allowing the responses through. After a period these holes heal and prevent further packets getting through.

When a packet comes along and there are no holes on the wall, the following checks take place:

1. Is there an existing hole/session - let it through and also check for end/timeout.
2. Will ANY of the additional filters drop the packet - Yes, then drop it and go onto next packet.
3. Is there an additional filter that allows this packet through - Yes, then let it through and move onto next packet.
4. Will any of the radio buttons let the packet through - Yes, then let it through and move onto next packet.
5. If Network Address Translation (NAT) is used with the firewall (which it typically is), then you must also configure a Primary Incoming Translation Address (see IP tab of the Service configuration form) if you wish sessions to be started into your site (typically for SMTP) from the Internet.

Example Firewall Filters

Dropping NetBIOS searches on an ISPs DNS

We suggest that the following filter is always added to the firewall facing the Internet to avoid costly but otherwise typically pointless requests from Windows machines trying to find friends by making DNS searches on the DNS server at your ISP.

Add the following in a custom firewall entry.

- **Direction:** Drop
- **IP Protocol:** 6
- **Match Offset:** 20
- **Match Length:** 4
- **Match Data:** 00890035
- **Match Mask:** FFFFFFFF

Browsing Non-Standard Port Numbers

The radio button for HTTP permits ports 80 and 443 through the firewall. Some hosts use non-standard ports for HTTP traffic eg. 8080, 8000, 8001,8002, etc. You can add individual filters for these ports as you find them. (The Monitor program can identify which packets are being blocked by the Firewall. Using the Firewall Fail information obtained from the trace and the data in RFC1700 - Assigned Numbers, firewall entries can then be created.)

You wish to access a Web page but you cannot because it uses TCP port 8000 instead of the more usual port 80, use the entry below.

- **Direction:** Out
- **IP Protocol:** 6
- **Match Offset:** 22
- **Match Length:** 2
- **Match Data:** 1F40
- **Match Mask:** FFFF

A more general additional entry given below allows all TCP ports out.

- **Direction:** Out
- **IP Protocol:** 6
- **Match Offset:** 0
- **Match Length:** 0
- **Match Data:** 00000000000000000000000000000000
- **Match Mask:** 00000000000000000000000000000000

Routing All Internet Traffic Through a WinProxy

If you wish to put WinProxy in front of all Internet traffic via the Control Unit. The following firewall allows only the WinProxy server to contact the Internet : -

1. Create a new Firewall profile and select **Drop** for all protocols
2. Under **Custom** create a new Firewall Entry
3. In Notes enter the name of the server allowed. Then use the default settings except in Local IP Address enter the IP address of the WinProxy Server, in Local IP Mask enter 255.255.255.255 and in Direction select Bothway
4. **Stopping PINGs**
   You wish to stop pings - this is ICMP Filtering. Using the data below can create a firewall filter that performs the following; Trap Pings; Trap Ping Replies; Trap Both.
   - **Trap Pings:** Protocol = 1, offset = 20, data = 08, mask = FF
   - **Trap Ping Replies:** Protocol = 1, offset = 20, data = 00, mask = FF
   - **Trap Both:** Protocol = 1, offset = 20, data = 00, mask = F7, Traps Both.

Understanding IP Routing via ISDN

Understanding IP Routing via ISDN

This is a mechanism for taking IP packets from one LAN transporting them across an ISDN data call and depositing the packets on a distant LAN. The data call is made automatically when packets require transporting and is cleared when the flow of packets stops. The user is not aware of the individual "Bandwidth on demand" calls happening. The data within the ISDN call uses the Point-to-Point Protocol (PPP) which is used by the vast majority of manufacturers for linking routers, particularly if it is not the same router manufacturer at each end of the link.

- For outbound calls, eg. to the Internet, configure a Service and IP Route - for further information refer to Connecting to the Internet .
- For inbound calls, eg. a user dialing in from home to the office, configure an Incoming Call Route, a RAS service, a User, and an IP route for the return data.
- For calls both ways between two sites, configure a Service, a User, a RAS, an Incoming Call Route and an IP Route at both ends - see the example below.

It is possible to have several different routing destinations active at any time. The Control Unit can handle simultaneous active data routes dependent on the number of data calls supported by the system.

The basic decision on how to route a packet is set by the IP routing table (see IP Route Form) which looks for the best route in its tables and selects the appropriate destination. The Default Route is typically to the Internet where the vast majority of IP addresses exist. These are static routes. RIP (I or II) and OSPF are not supported.

Configuration Example

To create a data link between two sites via ISDN configure the Control Unit as per the following example:

At Site A on IP address 192.168.43.1

1. **Create a Normal Service:**
   The Service name can be any text and is used to identify this particular Service. The Account Name and password are presented to the remote end, therefore must match the User name and password configured at Site B. The Telephone Number is the number of the remote end.
2. **Create a User:**
   Under the **Dial In** tab tick **Dial In On**. This User account is used to authenticate the connection from the Site B. Note that as the Service and User have the same names, these two configuration forms are automatically linked and become an Intranet Service. The User password is displayed at the bottom of the Service tab as the Incoming Password.
3. **Setup RAS:**
   Check the default RAS settings "DialIn" are available, otherwise create a new one. If the RAS settings are given the same name as the Service and User they are automatically linked and become a WAN Service. Ensure that the Encrypted Password option is not checked when using a WAN Service.
4. **Setup an Incoming Call Route:**
   Check the default Incoming Call Route is available, otherwise create a new one. If the Incoming Number is left blank, the Incoming Call Route accepts data calls on any number. Under **Destination** select the RAS service created above. The Bearer Capability should be AnyData.
5. **Create an IP Route:**
   In the IP Address field enter the network address of the remote end, not the IP address of the Control Unit. Under Destination select the Service created above.

At Site B on IP address 192.168.45.1

1. Repeat the above process but altering the details to create an route from Site B to Site A

Network Address Translation (NAT)

NAT is a mechanism that allows you to pretend to have a different IP address than you actually have. You may have an established network using your own numbering scheme, and would like to access the Internet. There are many cost effective Internet Service Providers (ISP) but they want you to use a different IP address. By using NAT between your machine and their network everyone is satisfied, and no need to renumber your network. An additional benefit is that all your machines can use the NAT facility and access the Internet via the one address.

NAT is the translation of an IP address within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one (or more) global outside IP address and unmaps the global IP address on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and it lets the company use a single IP address in its communication with the world.

Configuring NAT

The use of NAT is automatically enabled if the Service being used includes an IP address that is not in the same domain as the Control Unit's IP address. See IP.

An exception to the above applies for the IP412 Control Unit. This unit displays an **Enable NAT** check box on its System LAN1 and LAN2 forms.

Point to Point Protocol (PPP)

This is an industrial standard protocol for data links, particularly useful when connecting equipment from differing vendors. Options within the protocol, eg. data compression can be negotiated, thus avoiding the need for a manager to set these independently for each destination.

PPP (Point-to-Point Protocol) is a Protocol for communication between two computers using a Serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP) and is designed to handle others. It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a Full Duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle Synchronous as well as Asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

Quotas and Timebands

Quotas place a time limit on outgoing calls to a particular IP Service. This avoids excessive ISDN call charges when perhaps something changes on your network and call frequency increases unintentionally.

See the Quota tab of the Service configuration form

To refresh the Quota time, create a short code using the ClearQuota feature as per the following example or use "" to represent all Services.

- **Short Code:** *75
- **Telephone Number:** "Internet"
- **Line Group:** 0
- **Feature:** ClearQuota

Timebands apply to incoming calls. You can specify what hours you are open for external users. See the Dial In tab of the User configuration form.

Using a Fallback Service

A Fallback Service provides an alternative route while a Service is In Fallback. For example, you may wish to connect to your ISP during working hours and at other times take advantage of varying call charges from an alternative ISP. You could therefore set up one Service to connect during peak times and another to act as fallback during the cheaper period.

You need to create an additional Service to be used during the cheaper period and select this service from the **Fallback Service** list box (open the Service form and select the **Fallback** tab).

If the original Service is to be used during specific hours and the Fallback Service to be used outside of these hours, a Time Profile can be created. Select this Time Profile from the Time Profile list box. At the set time the original Service goes into Fallback and the Fallback Service is used.

A Service can also be put into Fallback manually using short codes, eg:

- **Put a service into fallback**
  - **Short Code:** *85
  - **Telephone Number:** 800
  - **Line Group ID:** 0
  - **Feature:** SetHuntGroupNightService

- **Take a service out of fallback**
  - **Short Code:** *86
  - **Telephone Number:** 800
  - **Line Group ID:** 0
  - **Feature:** ClearHuntGroupNightService

Using a Service

A Service is configured to provide remote data access for local users. A Service is needed when configuring, for example, connection to an ISP for Internet access, connection to a remote Control Unit via ISDN or via a WAN link. See Service Form .

When creating a new Service, you are given several options:

- A **Normal Service** should be selected when configuring, for example, a connection to an ISP.
- A **WAN Service** can be selected when creating a WAN link. A User and RAS Service will also be created with the same name. These three entries are automatically linked and each open the same form. Note however, that this type of Service cannot be used if the Encrypted Password option is checked. In this case the RAS Service name must match the Account Name. Therefore either create each entry manually or create an Intranet Service.
- An **Intranet Service** can be selected to automatically create a User with the same name at the same time. These two entries are linked and will each open the same form. Note that the Dial In tab is now added to the Service configuration form and the Dial In On option is assumed. The User's password is entered in the Incoming Password field at the bottom on the Service tab.

Bandwidth on Demand

This is the ability to make data calls between sites only when there is data to be sent or sufficient data to warrant an additional call. The calls are made automatically without the users being aware of when calls begin or end. Using ISDN it is possible to establish a data call and be passing data in less that a second. The rules for making calls, how long to keep calls up, etc. are configurable via the Bandwidth of the Service configuration form.

Gatekeeper

Gatekeepers provide network services to H.323 terminals, MCUs, and gateways. H.323 devices register with gatekeepers to send and receive H.323 calls. Gatekeepers give permission to make or accept a call based on a variety of factors.

Note: H.323 gatekeeper (Call Servers) is supported on the LAN1 address only.

Gatekeepers can provide network services such as:

- Controlling the number and type of connections allowed across the network.
- Helping to route a call to the correct destination.
- Determining and maintaining the network address for incoming calls.

The Gatekeeper tab in the System configuration form can be used to configure Gatekeeper support.

LDAP

LDAP

LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network. LDAP is lighter because in its initial version it did not include security features. LDAP originated at the University of Michigan and has been endorsed by at least 40 companies. Netscape includes it in its latest Communicator suite of products. Microsoft includes it as part of what it calls Active Directory in a number of products including Outlook Express. Novell's NetWare Directory Services interoperates with LDAP.

In a network, a directory tells you where in the network something is located. On TCP/IP networks (including the Internet), the Domain Name System (DNS) is the directory system used to relate the domain name to a specific network address (a unique location on the network). However, you may not know the domain name. LDAP allows you to search for an individual without knowing where they're located (although additional information will help with the search).

An LDAP directory is organized in a simple "tree" hierarchy consisting of the following levels:

- The "root" directory (the starting place or the source of the tree), which branches out to
- Countries, each of which branches out to
- Organizations, which branch out to
- Organizational units (divisions, departments, and so forth), which branches out to (includes an entry for)
- Individuals (which includes people, files, and shared resources such as printers)

An LDAP directory can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically. An LDAP server is called a Directory System Agent (DSA). An LDAP server that receives a request from a user takes responsibility for the request, passing it to other DSAs as necessary, but ensuring a single coordinated response for the user.

LDAP Directory Synchronization allows the telephone number Directory held in the Control Unit to be synchronized with the information on an LDAP server. Although targeted for interoperation with Windows 2000 Server Active Directory, the feature is sufficiently configurable to interoperate with any server that supports LDAP version 2 or higher.

Telephone numbers obtained via the LDAP mechanism are held dynamically in the Directory. Each record retrieved creates a Directory Entry for use with Phone Manager. Please note that the entries are not stored in the configuration and therefore will not be visible via Manager. A maximum of 500 records can be retrieved due to size restraints. Records with exactly the same data in the Name and Number fields will not be duplicated.

LDAP Configuration

LDAP support can be configured in the LDAP tab within the System configuration form as follows:

- **LDAP Enabled**
  Default: disabled. Simple check box to enable LDAP operation.
- **User Name**
  The name used to authenticate access to the LDAP server.
  For a Windows 2000 Active Directory server, the user name is of email format (ie. with a domain suffix). To determine the domain-name of a particular Windows 2000 user look on the "Account" tab of the user's properties under "Active Directory Users and Computers". Note that this means that the user name required is not necessarily the same as the name of the Active Directory entry.

There should be a built-in account in Active Directory for anonymous Internet access, with prefix "IUSR_" and suffix server_name (whatever was chosen at the Windows 2000 installation). Thus, for example, the user name entered is this field might be: IUSR_CORPSERV@acme.com

- **Password / Confirm Password**
  The password used to authenticate access to the LDAP server.
  Enter the password that has been configured under Active Directory for the above user.
  Alternatively an Active Directory object (i.e. the User container) may be made available for anonymous read access. This is configured on the server as follows:
  In "Active Directory Users and Computers" enable "Advanced Features" under the "View" menu. Open the properties of the object to be published and select the "Security" tab. Click "Add" and select "ANONYMOUS LOGON", click "Add", click "OK", click "Advanced" and select "ANONYMOUS LOGON", click "View/Edit", change "Apply onto" to "This object and all child objects", click "OK", "OK", "OK".
  Once this has been done on the server, any entry can be made in the User Name field in the System configuration form (however this field cannot be left blank) and the Password field left blank. Other non-Active Directory LDAP servers may allow totally anonymous access, in which case neither User Name nor Password need be configured.
- **Server IP Address**
  The IP address of the server storing the database
- **Authentication Method**
  This field defines the format of the password. Choice of three:
- **Simple:** Password is clear text.
  - **Kerberos 4 LDAP:** Password is kerberos ticket.
  - **Kerberos 4 DSA:** Password is kerberos ticket.
  - Note that only simple authentication is currently implemented so neither of the kerberos methods should be selected.
- **Resync Interval -** Default value: 3600
  The period, expressed in seconds, at which the Control Unit will resynchronize the directory with the server.

  This value also affects some aspects of the internal operation. The LDAP search inquiry contains a field specifying a time limit for the search operation and this is set to 1/16th of the resync interval. So a server should terminate a search request if it has not completed within 225 secs (default). The client end will terminate the LDAP operation if the TCP connection has been up for more than 1/8th of the resync interval (default 450 secs). This time is also the interval at which a change in state of the "LDAP Enabled" configuration item is checked.
- **Search Base / Search Filter**
  These 2 fields are used together to refine the extraction of directory entries. Basically the Base specifies the point in the tree to start searching and the Filter specifies which objects under the base are of interest. The search base is a distinguished name in string form (as defined in RFC1779).
  The Filter deals with the attributes of the objects found under the Base and has its format defined in RFC2254 (except that extensible matching is not supported).
  If the Search Filter field is left blank the filter defaults to "(objectClass=*)", this will match all objects under the Search Base.
  The following are some examples applicable to an Active Directory database:
- To get all the user phone numbers in a domain:
  Search Base: cn=users,dc=acme,dc=com
  Search Filter: (telephonenumber=*)
- To restrict the search to a particular Organizational Unit (eg office) and get cell phone numbers also:
  Search Base: ou=holmdel,ou=nj,DC=acme,DC=com
  Search Filter: (|(telephonenumber=*)(mobile=*))

- To get the members of distribution list "group1":
  Search Base: cn=users,dc=acme,dc=com
  Search Filter: (&(memberof=cn=group1,cn=users,dc=acme,dc=com)(telephonenumber=*))
- **Number Attributes**
  The Search Base/Filter combination determines what objects on the server are returned. This field defines which attributes the server should return for those entries.
- The default value is:
  "telephoneNumber,otherTelephone,homePhone=H,otherHomePhone=H,mobile=M,otherMobile=M"
- This means that the server only returns the following number attributes: TelephoneNumber otherTelephone homePhone otherHomePhone mobile otherMobile
- The optional "=string" sub-fields define how that type of number is tagged in the directory. Thus, for example, a cell phone number would appear in the directory:
- John Birbeck M 7325551234

The above attribute names are ones used by Active Directory for Contacts. Additional ones are:

- IpPhone
- otherIpPhone
- facsimileTelephoneNumber
- otherfacsimileTelephoneNumber
- pager
- otherPager

None of the attribute names are case sensitive. Other LDAP servers may use different attributes.

The person names are obtained from the "cn" (common name) attribute and this is always requested in addition to the number attributes that have been specified.

Virtual CAPI

CAPI (Common Application Programming Interface) is an international standard interface that application programs can use to communicate directly with ISDN equipment. Using CAPI, an application program can be written to initiate and terminate phone calls in computers equipped for ISDN. Computer telephony (CTI) applications can be written for ISDN users.

Officially, CAPI is referred to as Common-ISDN-API and is embodied in ETS 300 838. ETS refers to standards from the European Telecommunication Standards Institute (ETSI). The standard is internationalized by recommendation T.200 from the International Telecommunications Union (ITU).

CAPI can be compared with the Intel-Microsoft "standard" programming interface, the Telephony Application Program Interface (TAPI). CAPI includes signaling and data exchange protocols not included in TAPI. TAPI services are also provided by CAPI and a TAPI application can be mapped to CAPI functions.

Because ISDN is widely used in Germany, the Netherlands, and Scandinavia, users there are accustomed to receiving a CAPI software program or driver along with their ISDN computer card. Not all CAPI driver versions support all functions. CAPI provides functions that are independent from physical signaling protocols that vary among different countries. CAPI supports these protocols: HDLC, HDLC inverted, SDLC, LAPD, X.75, Voice (PCM), Fax group 3 (T.30), V.110/V.120, and compression (V.42bis).

CAPI support is provided via RVS-COM. RVS-COM provides a Central communications server on the network: communications hardware (ISDN-CAPI adapter, ISDN TA, ISDN router) connected to the server can be used by PCs on the network for G3/G4 fax, file transfer/Eurofile transfer, remote control, e-mail, answerphone, telephony, Internet and T-Online. Receiving messages (G3 and G4 fax, answerphone, PC Mail) takes place centrally on the server. Operates on smaller networks as standalone communications server (Windows 95/98/NT); on larger networks connects to MS Exchange Server (Windows NT) via the RVS Exchange Connector.

RIP

RIP

Routing Information Protocol (RIP) is a protocol which allows routers within a network to exchange routes of which they are aware approximately every 30 seconds. Through this process, each router becomes adds routes in the network to its routing table.

Each router to router link is called a 'hop' and routes of up to 15 hops are created in the routing tables. When more than one route to a destination exists, the route with the lowest metric (number of hops) is added to the routing table.

When an existing route becomes unavailable, it is marked as requiring 'infinite' (16 hops). It is then advertised as such to other routers for the next few updates before being removed from the routing table. The IP Office also uses 'split horizon' and 'poison reverse'.

RIP is a simple method for automatic route sharing and updating within small homogeneous networks. It allows alternate routes to be advertised when an existing route fails. Within a large network the exchange of routing information every 30 seconds can create excessive traffic. In addition the routing table held by each IP Office is limited to 100 routes (including static and internal routes).

RIP is supported with IP Office system's from Level 2.0 upwards. The normal default is for RIP to be disabled. It can be enabled on LAN1, LAN2 and individual services. The supported RIP options are:

- **Listen Only (Passive):**
  The IP Office listens to RIP1 and RIP2 messages and uses these to update its routing table. However the IP Office does not respond.
- **RIP1:**
  The IP Office listens to RIP1 and RIP2 messages. It advertises its own routes in a RIP1 sub-network broadcast.
- **RIP2 Broadcast (RIP1 Compatibility):**
  The IP Office listens to RIP1 and RIP2 messages. It advertises its own routes in a RIP2 sub-network broadcast. This method is compatible with RIP1 routers.
- **RIP2 Multicast:**
  The IP Office listens to RIP1 and RIP2 messages. It advertises its own routes to the RIP2 mulitcast address (249.0.0.0). This method is not compatible with RIP1 routers.

Broadcast and multicast routes (those with addresses such as 255.255.255.255 and 224.0.0.0) are not included in RIP broadcasts.

Static routes (those in the **IP Route** table) take precedence over a RIP route when the two routes have the same metric.

The full routing table currently held by an IP Office system can be viewed using the IP Office Monitor application, see Viewing the Routing Table.

Viewing the Routing Table

An IP Office's routing table can be viewed using the IP Office Monitor application. This application can be installed from the IP Office Admin CD. Full details of using Monitor are not covered here.

Note: This method can be used to view the IP Office's routing table regardless of whether RIP is being used.

1. Start **Monitor** and select the IP Office system whose routing table you want to view.
2. Select **Filters | Trace Options**.
3. Select the **Routing** tab.
4. Tick **Routing Table**.

5. If required you can also select to view **Routing Table Changes** plus **RIP In** and **RIP Out** messages.
6. The routing table is sent to the monitor trace once every minute.

```
Destination     Netmask         Gateway      Interface    Metric Type
0.0.0.0         0.0.0.0         0.0.0.0      LAN1          0      S
255.255.255.255 255.255.255.255 0.0.0.0      LAN1          0      I
192.168.44.0    255.255.255.0   0.0.0.0      LAN1          0      I
192.168.99.0    255.255.255.0   0.0.0.0      RemoteManager 0      S
192.168.42.0    255.255.255.0   192.168.44.1 LAN1          0      S
```

The **Type** indicates:

- **I** = Internal routes.
- **S** = Static route set in the IP Route table.
- **R** = RIP route resolved from RIP messages.
- **T** = Temporary route to a specific IP address accessed via a service.

Voice over IP

Overview of VoIP

The Control Unit supports a maximum of 20 VoIP channels, which can be compressed using voice compression channels. These are pre-installed in Avaya IP Office - Small Office Edition controls units. On other units they are added by installing 5, 10, 20 or 30 channel Voice Compression Modules. Note: The type and number of VCM modules supported by each control unit type varies.

The voice compression channel improves call quality and can be used to compress voice down to either 6k3 (G723) or 8k (G729/Netcoder) and provides echo cancellation (required for high latency circuits).

The bandwidth required for a VoIP call is made up of two parts, one of which is due to the actual digitization of the analog voice the other is required by the protocol which is used to wrap the digitized voice up and transport it to the remote site. VoIP calls require an overhead of 40 bytes per packet (RTP/UDP/IP Header overhead) this overhead is increased on a LAN by a further 12 bytes Ethernet or by 7 bytes over a PPP WAN link.

When transporting voice over low speed links (WANs) it is possible that normal data packets (eg. 1500 byte IP packets) can prevent or delay the voice data from getting across the link. This can cause a very unacceptable speech quality. Thus it is vital that the routers in the network that carry voice have some form of Quality of service mechanism (QoS).

The Control Unit supports the DiffServ (RFC 2474) Quality of Service mechanisms (QoS) which is based upon a Type of Service (ToS) field in the IP header. The software will prioritize voice, fragment large packets and provide VoIP header compression to minimize the WAN overhead.

Typically the VoIP WAN overhead is 47 bytes on 20 byte payload this is 235% overhead. On the WAN protocol this is reduced to 11 bytes (8 bytes data, 2 bytes CRC and 1 byte HDLC flag) on the same 20-byte packet this is only 55%, and 180% saving. This overhead must be included when calculating the actual link speeds required to support voice traffic, eg. an 8Kbps compression voice path actually required 12.4Kbps of WAN bandwidth when using QoS or 26.8Kbps if using standard non QoS routers.

QoS routers are also required to ensure low speech latency and to maintain sufficient audible quality. At present our header compression is based upon the latest standards (RFC 2507/2508/2509). For efficiency we operate below PPP (non-standard) - reducing the overheads further and allow data fragmentation to be performed more effectively (keeping latency low). It is therefore required to place our equipment at both ends to operate at full efficiency.

VoIP Protocols

The H.323 Stack within the core software supports the following protocols:-

- H.323 (V2)(1998), Packet-based multimedia communications systems
- Q.931, ISDN user-network interface layer 3 specification for basic call control
- H.225.0 (1998), Call signaling protocols and media stream packetization for packet-based multimedia communication systems
- RTP/RTCP
- H.245 (1998), Control protocol for multimedia communication
- Audio CODECs:
    - G.711 A-law/U-law
    - G.723.1 MP-MLQ
    - G.729 Annex A - CS-ACELP (Not supported by NetMeeting)
- Silence Suppression
- Fax Relay
- Local End Echo Cancellation 25ms (except transparent - no cancellation)
- Out of band DTMF
- Internet Standards/Specification (in addition to TCP/UDP/IP)
    - RFC 1889 - RTP/RTCP
    - RFC 2507,2508,2509 - Header Compression
    - RFC 2474 - DiffServ

Performance

The following table is the absolute maximum ratings tested in the lab. For deployment we recommend that more bandwidth be made available for normal data.

	56K	64K	128K	256K	2M	LAN
G729.1 (8k)	4	5*	6	18	20!	20
NetCoder (8k)	4	5*	9*	18!	20	20
G.723 (6.4k)	5	5*	9	18	20	20
ADPCM (32k)	1	1	6	5	20!	20
G.711 (64k)	X	X	1	3	16!	20
Transparent (64k)	X	X	1	3	14!	20

- * - data transfer is affected at higher channel connectivity
- ! - channel connectivity at higher levels is affected by data transfer

Implementation

A Control Unit plays the part of a Gateway between H.323 terminals and phones connected to the Control Unit (and also external lines). H.323 is configured on a Control Unit as a VPN line, specifying the IP address of a remote gateway and the audio compression to be used.

IP phones can be configured as extensions. An example is NetMeeting, which is configured to use the Control Unit as a Gatekeeper, with an account name that should match the name of a user configured on the Control Unit.

IP extensions are automatically created when an IP phone registers with the Gatekeeper (depending on a configuration option). If the user is not found a new user and extension are created, allowing the phone to be used immediately.

Basic call setup (without a Gatekeeper)

- Call setup using H.225.0 encapsulated in Q.931 messages
- Capability exchange using H.245
- Establishment of audio communication using H.245 OpenLogicalChannel
- Audio using RTP/RTCP

Fast connect procedure

- Call setup using H.225.0 in Q.931 messages, with H.245 OpenLogicalChannel messages embedded in the H.225.0 messages
- Audio using RTP/RTCP

Overlap sending

- Support for overlap sending, where a SetupAck is sent in response to the Setup message

Gatekeeper

- Gatekeeper support allows IP extensions to be automatically configured when they register with the gatekeeper.

Jitter buffer

- 5 frames of jitter buffer

Quality of Service

- Layer3 - DiffServ TOS Field set to DSCP 6 on generated packets. WAN links optimize for this traffic when set to "PPPSyncVoice". At present normal LAN and normal ISDN traffic is not prioritized.
- Layer4 - UDP Port Marking - all RTP/UDP traffic is sent within UDP port range of C000-CFFF (hex) (49152-53247)

Voice Packet Payload Sizing/Latency (Default)

Codec	Payload	Latency
Transparent 64K G711	80bytes	10ms
ADPCM 32K	40bytes	10ms
ADPCM 16K	20bytes	10ms
G.711 ALAW	160bytes	20ms
G.729A	20bytes	20ms
G.723 (6K3)	24bytes	30ms
Netcoder 8K	20bytes	20ms

G.726-32K	80bytes	20ms
G.726-16K	40bytes	20ms

Creating a VoIP Link via the LAN

At Site A on IP address 192.168.43.1

1. **Create a new line:**
   The Line Number and Line Group ID must be unique, in other words, not used by any other line. The Gateway IP Address is the IP Address of the Control Unit at the remote end.
2. **Create an IP Route:**
   The IP Address is the network address of the remote end. The Destination will either be LAN1 or LAN2.
3. **Create a Short Code:**
   This routes all calls where the number dialed starts with 8 via Line Group ID 1, therefore via the VPN Line created above.
   - **Short Code:** 8N
   - **Telephone Number:** N
   - **Line Group ID:** 1
   - **Feature:** Dial

At Site B on IP address 192.168.45.1

1. Repeat the above steps for VoIP traffic from Site B to Site A.

Creating a VoIP Link via the WAN Port Using PPP

A VoIP link across a leased line requires the Control Unit at both ends to have a Voice Compression Module installed. These provide for a fixed number of channels to use VoIP at any time. They are used to compress voice down to either 6k3 (G723) or 8k (G729/Netcoder) and provide echo cancellation.

Both ends must using the same version of software and configured to use the same speed and compression.

At Site A on IP address 192.168.42.1.

1. **Create a Normal Service:**
   The Account Name and password is presented to the remote end, therefore must match the User name and password configured at Site B. The Encrypted Password option can only be used if the remote end also supports CHAP.
2. **Create a User:**
   Under the Dial In tab tick Dial In On. This User account is used to authenticate the connection from the Site B. As the Service and User have the same name these two configuration forms are automatically linked and become an Intranet Service. The User password is displayed at the bottom of the Service tab as the Incoming Password.
   - **Name:** SiteB
   - **Dial In | Dial In On:** Enabled.
3. **Create a RAS service:**
   If CHAP is to be used on this link, then the **Encrypted Password** option must be checked in the Service and in the RAS service. The name of the RAS service must match the name of the Service at Site B. If the RAS service is given the same name as the Service and User, they are automatically linked and become a WAN Service. Ensure that the Encrypted Password option is **not** checked when using a WAN Service.
4. **Edit the WANPort:**
   Note - do not create a new WANPort, this is automatically detected. If a WANPort is not displayed, connect the WAN cable, reboot the Control Unit and receive the configuration. The WANPort configuration form should now be added.
   - **RAS Name:** SiteA
5. **Create an IP Route:**
   The IP Address is the network address of the remote end. Under Destination select the Service created above.
6. **Create a new Line:**
   The Line Number and Line Group ID must be unique, in other words, not used by any other line. The Gateway IP Address is the IP Address of the Control Unit at the remote end. The Compression Mode used is dependent on the Voice Compression Card the Control Unit is running and the speed of the link.
7. **Create a Short Code:**
   To route all calls where the number dialed starts with 8 via Line Group ID 1, therefore via the VPN Line created above.
   - **Short Code:** 8N
   - **Telephone Number:** N
   - **Line Group ID:** 1
   - **Feature:** Dial

At Site B on IP address 192.168.45.1

1. Repeat the above steps for VoIP traffic from Site B to Site A.

- Note: For the IP401 Control Unit, enabling Local Tones under the Line and Extension VoIP tabs is recommended.

Creating a VoIP Link via the WAN Port Using Frame Relay

To create a VoIP link via the WAN port using frame relay, the first step is to attach a WAN cable and reboot the Control Unit. After this, receive a copy of the configuration.

Both ends must using the same version of software and configured to use the same speed and compression.

At Site A

1. Create a WAN Service:
    - On the Service Tab:
      The Name is "FR_link". The Account Name should be "FR_Link" and all password fields (both Password and Incoming Password) should be left blank.
    - On the **PPP** Tab:
      Check the **MultiLink/QoS** box.
      Set the **Header Compression Mode** to ***IPHC***.
    - On the Dial In Tab:
      If you are using a WAN 3 module, you must add "WAN" as the Dial In Service number.
2. On the **Wan Port** Form:
    - In the WanPort Tab
      Set the speed to match the link. Set the **RAS Name** to ***DialIn***. Set the **Mode** as ***SyncFrameRelay***.
    - In the FrameRelay Tab
      Set the appropriate Frame Relay Management Type. The other default settings are appropriate for a basic Frame Relay Connection.
    - In the DCLI tab
      Set the RAS Name to "FR_link".
      Frame Link Type = PPP
      DLCI set to the network setting
3. **Create a RAS service:**
   Encrypted Password option is **not** checked when using a WAN Service. Have the Name = "FR_Link"
4. **Create an IP Route:**
   The IP Address is the network address of the remote end. Under Destination select the "FR_link" that was created above.
5. **Create a new Line:**
   The Line Number and Line Group ID must be unique, in other words, not used by any other line. The Gateway IP Address is the IP Address of the Control Unit at the remote end.
6. **Create a Short Code:**
   To route all calls where the number dialed starts with 8 via Line Group ID 1, therefore via the VPN Line created above.
    - **Short Code:** 8N
    - **Telephone Number:** N
    - **Line Group ID:** 1
    - **Feature:** Dial

At Site B

1. Repeat the above steps for VoIP traffic from Site B to Site A.

- Note: For the IP401 Control Unit, enabling Local Tones under the Line and Extension VoIP tabs is recommended.

Dedicated T1 Service

At the IP Office

1. **Create a Service:**
   - On the Service Table:
     Add an entry and click on the radio button for WAN. The Name value is "isp_service".
   - On the Bandwidth Tab:
     Set the Minimum Number of Channels value to 1 and set the Maximum Number of Channels to the number to be used in Step 2.
   - In the IP Tab
     Set the IP Address field to the IP address of the subscriber's end of the T1 cable (this is assigned by the ISP at subscription time).
   - On the PPP Tab:
     Check the MultiLink box.
     Disable Compression Mode.
     Disable Callback Mode.
   - Click OK at the bottom
     This action automatically adds an entry to the RAS table with the name "isp_service" and automatically adds a User with the name "isp_service".
2. **On the WAN Port Form**
   - **Create a WAN Service:**
     Add an entry with a Name value like **LINE5.0** with no spaces where LINE in capital letters is mandatory. The digit 5 indicates that the PRI/T1 card is in slot B. If the PRI/T1 card were in slot A, the digit 1 would be used. The dot is mandatory. The digit(s) after the dot is (are) determined by the formula: the lowest numbered channel used for dedicated service minus one. If the PRI/T1 card is in slot B and channels 1 through 12 are used for dedicated service, the Name value must be LINE5.0 with no spaces. If the PRI/T1 card is in slot A and channels 21 through 24 are used for dedicated service, the Name value must be LINE1.20 with no spaces.
   - Set the Speed value, e.g. 768000 (depending on the channels used, in multiples of 64000, e.g. 12 channel used).
   - Set the Mode value to SyncPPP.
   - Set the RAS Name value to "isp_service".
   - Click OK to save the changes.
3. **Create an IP Route**
   - **In IP Route Table:**
     Add an entry with a blank IP Address value, a blank IP Mask value a blank Gateway value and a Destination value of "isp_service".
   - Click OK to save the changes.
4. **Line Changes**
   - **In the Line Table:**
     Edit the Line 01 or Line 05 entry, depending on the value entered in step 2, such that each channel from the lowest numbered of the of the dedicated channels, e.g. 1, to the highest numbered dedicated channel, eg. 12.
   - Set the Type value to Clear Channel 64K.
   - Click OK to save the changes.

5. **System Changes**
   - **In the LAN1 Tab on the System Form:**
     Change the IP address to the IP address of the IP Office.
   - Set the IP Mask to the that required by the network configuration.
   - **In the DNS Tab on the System Form:**
     Set the DNS Server IP Address to the value in the network.
   - Set the Type value to Clear Channel 64K.
   - Click OK to save the changes.
6. Save the configuration file to the Control Unit, choose to reboot immediately.

At the PC

1. Use **Start | Settings | Control Panel | Network | Protocols Tab | TCP/IP entry | Properties**. Set the IP address to the IP address of the IP Office the IP Mask to that required by the network configuration and the Gateway IP Address to the IP Address of the IP Office as Specified in Step 5 of the previous list and the DNS Server IP Address to the value in the network.
2. In Internet Explorer, under Tools->Internet Options, set the home page as required.
3. Open the configuration file from the Control Unit.
4. Connect the span to the slot in the back of the Control Unit as determined by the value assigned in Step 2 of the previous list.
5. In the Browser, click on the Home button.

Using a Dedicated T1/PRI ISP Link

Using a Dedicated T1/PRI ISP Link

This document shows by example the configuration to create a dedicated WAN PPP link to an Internet Service Provider (ISP) over a set of T1 or PRI line channels.

- Note
  The ISP must support this mode of connection and will need to provide details of the required settings. If multiple channels are to be used, then the ISP must support Multilink PPP.

The basic steps are:

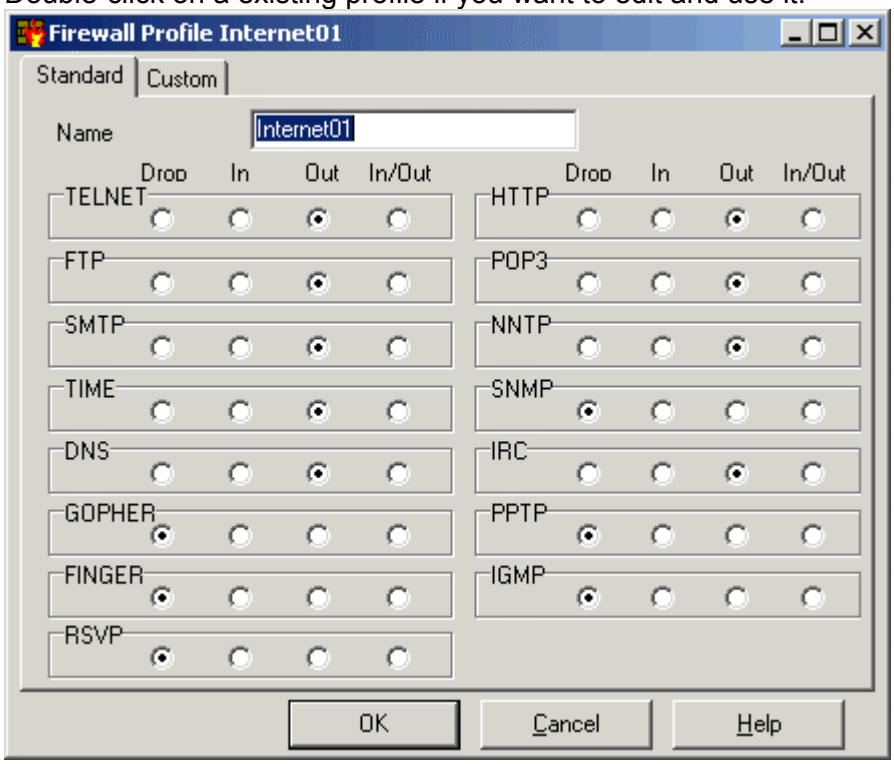
1. Create a Firewall
2. Create a Service
3. Create a Virtual WAN Port
4. Create an IP Route
5. Configure the Line Channels

1. Create a Firewall

- **WARNING: WAN connections can be used without a firewall. However, for any WAN connection to or through the Internet, Avaya strongly recommends that a firewall is setup and used to control the types of traffic allowed.**

The normal installation process for IP Office creates a default firewall for internet access. We are repeating the process here in case a firewall was not setup during original installation or if you want to apply different firewall settings to the T1 PPP link.

1. Start Manager and load the IP Office configuration.
2. In the left-hand panel, click **Firewall Profile** to display the list of the existing profiles.
3. Right-click on the displayed list and select **New**.
    - Double-click on a existing profile if you want to edit and use it.

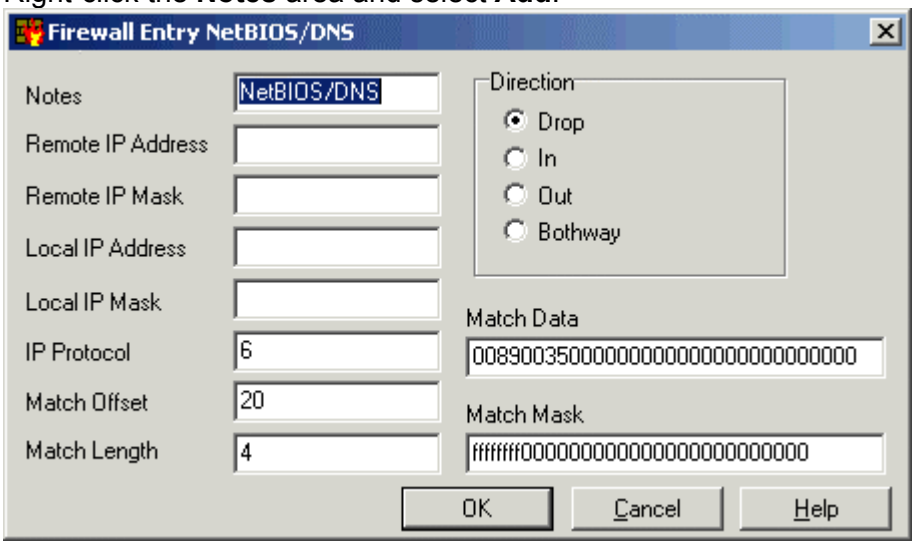


4. Enter an appropriate name, such as "***Internet01***", in the **Name** field.
5. Set the protocols settings as required by the customer. The defaults, are shown above.
6. Proceed to step 1a following.

1a. Block NetBIOS/DNS Access

NetBIOS and DNS traffic from your network to the internet is normally not needed and causes unnecessary line usage and costs. You can block it by adding a custom filter to the internet firewall profile.

1. With the firewall profile open, click on the **Custom** tab.
2. Right-click the **Notes** area and select **Add**.



3. In the **Notes** field, enter an appropriate name such as ***Drop NetBIOS/DNS***.
4. Set the **Direction** to ***Drop***.
5. In the **IP Protocol** field, enter **6** (TCP).
6. In the **Match Offset** field, enter ***20***.
7. In the **Match Length** field, enter ***4***.
8. In the **Match Data** field, enter ***00890035*** (the IP Office will insert the remaining zeros).
9. In the **Match Mask** field, enter ***ffffffff***.
10. Click **OK**.

1b. Allow Ping for Testing

Sending pings through the firewall may be useful for testing the internet connection. Remember to remove this custom entry afterwards unless the customer also want to be able to send pings.

1. With the firewall profile open, click on the **Custom** tab.
2. Right-click on the **Notes** area and select **Add**.
3. In the **Notes** field, enter an appropriate name such as ***Allow ICMP (PING)***.
4. Set the **Direction** to ***Bothway***.
5. Set the **IP Protocol** to ***1*** (ICMP).
6. Set the **Match Offset** to ***20***.
7. Set the **Match Length** to **0**.
8. Set the **Match Mask** to ***F7***.
9. Click **OK** to save the custom setting and **OK** to save the profile.

2. Create a WAN Service

The service defines features such as the ISP assigned IP address, the bandwidth required and the firewall to use.

2a. Create a New WAN Service

1. In the left-hand panel, click on **Service** to display the list of existing services.
2. Right-click on the list and select **New**.
3. Select **WAN Service** and then click on **OK**.
4. The configuration form for a service should appear.

2b. Configure the WAN Service – Service Tab

1. Select the **Service** tab.
2. In the **Name** field enter an appropriate name, such as "**Internet**".
    - **Note:** This will also automatically create a RAS entry with the same name.
3. Enter the **Account Name**, **Password** and **Telephone Number** details provided by the ISP.
4. For the **Firewall Profile** select the firewall created previously.

2c. Configure the WAN Service Bandwidth Tab

1. Click the **Bandwidth** tab.
2. Set the **Maximum No. of Channels** to the maximum number of channels that the service should use. In this example, 12 channels were used.
    - **Note:** The maximum number of channels that can be used will be limited by the number of data channels supported by the IP Office Control Unit and not already in use.
3. Leave all the other entries at their default values.

2d. Configure the WAN Service – IP Tab

If the ISP has allocated IP address details then enter them through this tab. If the IP Address and IP Mask define a different domain from the IP Office's own LAN settings (those in the **System | LAN1** or **LAN2** tab), then NAT is automatically applied.

1. Click the **IP** tab.
2. In the **IP Address** field, enter the IP address specified by the ISP.
3. In the **IP Mask** field, enter the IP Mask specified by the ISP.

2e. Configure the WAN Service – PPP Tab

The settings shown are typical. The actual settings must match those required by the ISP. For example, if Cisco routers are being used then IPHC needs to be ticked.

1. Click the **PPP** tab.
2. Ensure that the following options are selected. Leave all other options at their default settings.
    - **Multilink.**
    - **Compression Mode: Disable.**
    - **Callback Mode: Disable.**
    - **Access Mode: Digital64**
3. Click **OK**.

3. Create the Virtual WAN Port

1. In the left-hand panel, click **WAN Port** to display a list of existing ports.
2. Right-click on the displayed list and select **New**.
3. In the **Name** field, enter either ***LINEx.y*** where:
   - ***LINE*** must be in uppercase.
   - ***x*** is the line number. For a PRI/T1 module in Slot A, this will be ***1***. For a PRI/T1 module in Slot B, this will be ***5***.
   - ***y*** is the lowest numbered channel number to be used by the WAN link minus 1. For example, if the lowest channel to be used is channel 1 then y = 1 - 1 = 0.
4. In the **Speed** field, enter the total combined speed of the maximum number of channels sets in the Service. In this example, 12 channels x 64000 bits = 76800.
   - Note: The maximum number of channels that can be used will be limited by the number of data channels supported by the IP Office Control Unit and not already in use.
5. Set the **Mode** to **SyncPPP**.
6. In the **RAS Name** field, select the RAS name created when the new Service of that name was created.
7. Click **OK**.

4. Create an IP Route

Note: By leaving the IP address details blank, this becomes the default route for any IP traffic not for the IP Office's LAN. To route IP traffic via other WAN routes, specific IP address details need to be entered in the IP Route form for those routes.

1. In the left-hand panel, click on **IP Route** to display the list of existing routes.
2. Right-click on the list area and select **New**.
3. In the **Destination** field, select the name given to the WAN Service created previously.
4. Leave the **Metric** at default value of **1**.
5. Click **OK**.

5. Configure the Line Channels

This stage of the process differs according to the type of line being used.

5a. T1 Line

1. In the left-hand panel, click **Line** to display the list of existing lines.
2. Double-click on the line previously entered in the WAN Port settings.
3. Check that the **Channel Allocation** order matches that required by the ISP. Cisco routers typically use ***1->24***.
4. Select the channels to be used in the WAN PPP link and change their **Channel Type** to "***Clear Channel 64k***". Use the Shift key to select and edit the appropriate channels all at the same time.
5. Click **OK**.
6. Click **OK** again.
7. Send the configuration to the IP Office and reboot.

5b. T1 PRI Line

1. In the left-hand panel, click on **Line** to display the list of existing lines.
2. Double-click on the line previously entered in the WAN Port settings.
3. Check that the **Channel Allocation** order matches that required by the ISP. Cisco routers typically use ***1->23***.
4. Select the channels to be used in the WAN PPP link and change their **Admin** to "***Out of Service***". Use the Shift key to select and edit the appropriate channels all at the same time.
5. Click **OK**.
6. Click **OK** again.
7. Send the configuration to the IP Office and reboot.

SNMP

SNMP Introduction

SNMP (Simple Network Management Protocol) is a standard network protocol that allows the monitoring and management of data devices across a network.

An SNMP agent can be built into network devices such as routers and hubs. An SNMP manager application (for example CastleRock or HP OpenView) can then communicate with those devices.

This communication can be:

- **Polling:** *Supported by IP Office 2.0*
  Some SNMP manager applications send out polling messages to the network. They then record the responds of any SNMP enabled devices (agents). This allows the manager to create a network map and to raise an alarm when devices previously present do not respond.
    - Most SNMP manager applications can also do simple IP address polling to locate non-SNMP enabled devices. However this method of polling does not identify the device type or other information.
    - SNMP polling including details about the responding device. For example an IP Office control unit's response includes the control unit type, level of software, routing table information, up time, etc.
- **Traps:** *Supported by IP Office 2.0*
  When certain events occur, a devices SNMP agent can send details of the event to the SNMP manager. This is called an SNMP 'trap'. These appear in the event log of the SNMP manager. Most SMNP manager's can be configured to give additional alerts in response to particular traps.
- **Management:** *Not supported by IP Office 2.0*
  Some SNMP agents support device management and configuration changes through the SNMP manager interface.

IP Office 2.0 allows IP Office Control Units to act as read-only SNMP v1 agents. It can include the sending of events traps to up to two different SNMP manager addresses.

IP Office SNMP operation has been tested against Castle Rock SNMPc-EE 5.1.6c and HP OpenView Network Node Manager 6.41.

Installing the IP Office MIB Files

To allow full communication between an SNMP agent and an SNMP manager, the SNMP manager must load MIB files (Management Information Base) specific to the SNMP agent device and the features it supports. These MIB files contain details of the information the agent can provide and the traps that it can send. Full details of the structure of the IP Office MIB files, MIB groups within those files and event traps can be found in the "IP Office Installation Manual".

The MIB files for IP Office operation are included on the IP Office Admin CD in the folder ***C:\smnp_mibs***. The actual files required and the method of loading depend on the SNMP manager application being used. The details below cover the two SNMP manager applications tested.

CastleRock SNMPc

1. Copy the following MIB files from ***C:\smnp_mibs*** to the applications MIBs folder. Note: The order matches the order in which the MIBs should be added in step 4 below.

	MIB File	Source
a.	entity-mib.mib	*snmp_mibs\Standard folder on IP Office Admin CD.*
b.	avayagen-mib.mib	*snmp_mibs\IPOffice folder on IP Office Admin CD.*
c.	ipo-prod-mib.mib	*snmp_mibs\IPOffice folder on IP Office Admin CD.*
d.	ipo-mib.mib	*snmp_mibs\IPOffice folder on IP Office Admin CD.*
e.	inet-address-mib.mib	*snmp_mibs\Standard folder on IP Office Admin CD.*
f.	integrated-services-mib.mib	*snmp_mibs\Standard folder on IP Office Admin CD.*
g.	diffserv-dscp-tc.mib	*snmp_mibs\Standard folder on IP Office Admin CD.*
h.	diffserv-mib.mib	*snmp_mibs\Standard folder on IP Office Admin CD.*
i.	ipo-phones-mib.mib	*snmp_mibs\IPOffice folder on IP Office Admin CD.*

2. Start the CastleRock SNMP console.
3. Select **Config | MIB Database**.
4. Select **Add**. Select and add each MIB in the shown above.
5. Select **Compile**.

HP Open View Network Node Manager

1. Copy the following MIB files from ***C:\smnp_mibs*** to the applications MIBs folder.

	MIB File	Source
a.	rfc2737-entity-mib.mib	*snmp_mibs\standard folder on OpenView Install CD.*
b.	avayagen-mib.mib	*snmp_mibs\IPOffice folder on IP Office Admin CD.*
c.	ipo-prod-mib.mib	*snmp_mibs\IPOffice folder on IP Office Admin CD.*
d.	ipo-mib.mib	*snmp_mibs\IPOffice folder on IP Office Admin CD.*
e.	inet-address-mib.mib	*snmp_mibs\Standard folder on IP Office Admin CD.*
f.	rfc2213-integrated-services-mib.mib	*snmp_mibs\standard folder on OpenView Install CD.*
g.	diffserv-dscp-tc.mib	*snmp_mibs\Standard folder on IP Office Admin CD.*
h.	diffserv-mib-hpov.mib	*snmp_mibs\Standard folder on IP Office Admin CD.*
i.	ipo-phones-mib.mib	*snmp_mibs\IPOffice folder on IP Office Admin CD.*

2. Start the OpenView Network Node Manager console.
3. Select **Options** and then **Load/Unload MIBs: SNMP**.
4. Select **Load** and select all the MIB files listed above.
5. Select **Compile**.

Enabling SNMP and Polling Support

In order for the IP Office control unit to be discovered and polled by an SNMP manager, its SNMP agent must be enabled and placed in the same read community as the SNMP manager.

To enable the SNMP agent:

1. In Manager, receive the control unit's configuration.
2. Double-click **System** from the Configuration Tree panel and select the **SNMP** tab.
3. Tick **SNMP Enabled**.
4. In **SNMP Port**, enter the UDP port number used by the IP Office SNMP agent to listen for and respond to SNMP traffic. The normal default is ***161***.
5. In **Community (Read-only)**, enter the community to which the device belongs for read access. This community name must match that used by the SNMP manager application when sending requests to the device. The community ***public*** is frequently used to establish communication and then changed (at both the SNMP agent and manager ends) for security.
6. Click **OK**.
7. Send the configuration back to the IP Office and select reboot.
8. Following the IP Office reboot, the SNMP manager should be able to discover the control unit.
9. The control unit's response will include details of the control unit type and the current level of core software.

Enabling SNMP Trap Sending

In Manager, receive the control unit's configuration.

1. Double-click **System** from the Configuration Tree panel and select the **SNMP** tab.
2. Ensure that **SNMP Enabled** is ticked.
3. Using either **Trap Destination 1** or **Trap Destination 2**, enter the following information:
    - Enter the **IP Address** of the PC running the SNMP manager application.
    - Enter the **Port** on which the traps messages should be sent. This is the UDP port on which the IP Office sends SNMP trap messages. The default is ***162***.
    - Set the **Community** that will be used by the agent and the SNMP manager. The community ***public*** is frequently used to establish communication and then changed (at both the SNMP agent and manager ends) for security.
    - Select the **Events** which should be sent:
        - **Generic:**
          Events such as soft reboot (warm start), hard reboot (cold start), links up/down (transition in the status of a PPP or frame relay interface) or SNMP community mismatch.
        - **Entity:**
          Failures, errors and changes of state in IP Office modules and trunk interfaces. Note: Does not include WAN3, Modem2 and ATM4.
        - **Licence:**
          Changes of state in the communication with the Feature Key Server.
        - **Phone Change:**
          Changes to the type of DS, DT or IP phone connected to a port.
8. Click on **OK**.
9. Send the configuration back to the IP Office and select reboot.

Configuration Forms

The Configuration Tree

The left-hand panel of the Manager window shows various icons arranged in a configuration tree. Click on an icon to display related entries in the right-hand panel. You can double-click on icons to expand or contract the entries within the configuration tree.

Once you have selected a configuration form from the configuration tree, the within the right-hand panel, you double-click on entries to display their configuration form or right-click to select various options (typically **View**, **Edit**, **New** and **Delete**).

Through the configuration tree, you configure the following via their respective forms:

- Configure a BootP entry.
- Configure an Operator.
- Configure the System.
- Configure a Line. This form varies according to the type of line.
- Configure a Control Unit.
- Configure an Extension.
- Configure a User.
- Configure a Hunt Group.
- Configure a Short Code.
- Configure a Service.
- Configure a Remote Access Service (RAS).
- Configure an Incoming Call Route.
- Configure a WAN Port.
- Configure a Directory Entry.
- Configure a Time Profile.
- Configure a Firewall Profile.
- Configure an IP Route.
- Configure a Least Cost Route.
- Enter License keys.
- Configure an Account Code.
- Configure an E911 System. This configuration form is only available when the system locale is set to **enu** - U.S.
- Configure Wireless 802.11b. This configuration form is only available if you are running IP Office - Small Office Edition.
- Configure User Restrictions.
- Configure a Logical LAN.
- Configure Tunnels.
- Configure an Auto Attendant.

BOOTP Form

BOOTP is used to upgrade the operational software on the Control Unit. BOOTP entries are generated automatically and stored in the registry of the local PC. You may need to create a BOOTP entry manually if you have a Control Unit that has not previously been upgraded from the local PC.

- Note: The BOOTP entry for a system is used for software upgrades. It is also used for emergency recovery. Therefore it is important to check that an entry has been created for the system you are managing.
- Note: The BOOTP information is not saved as part of the system configuration. It is saved on the Manager PC and may contain information for several systems if managed through the same PC.

- **Enabled :** *Default = Enabled*
  If unticked, disables BOOTP support of the IP Office system from this Manager PC. This may be necessary when managing multiple IP Office systems on different networks.
- **MAC :**
  The hardware MAC address of the Control Unit. This is the same as the Serial Number displayed in the Unit form. Alternatively this information is available during the upgrade process via the **TFTP log** (see View Menu) or in the status bar of Manager.
- **IP Address :**
  Enter the IP address of the Control Unit.
- **File Name :**
  Enter the name of the .bin software file to be sent to the Control Unit during upgrades. This file must exist in the Working Directory.
- **Time Offset (hours) :** *Default = 0.*
  Use if the Manager application is being used as the time server for the IP Office system. Sets the offset between the PC time and the time sent to the IP Office system in response to a time request. Do not use if an alternate time server has been set in the System form.

Operator Form

Operators are people who configure the system. Rather than allowing full access to the configuration, Operators can be created with different levels of access to the configuration file. Each Operator should be given a name and a password.

- **Name :**
  The name of the Operator
- **Password :**
  The password to be used by the Operator
- **Confirm Password :**
  Type the password entered above to ensure the correct password has been used.

Define what access you are going to give to the Operator on this configuration form, the following four rights define this access: -

- **View:** This allows the Operator to view existing entries.
- **Edit:** This allows an Operator to make changes to entries in a form.
- **New:** This allows an Operator to create new entries.
- **Delete:** This allows an Operator to delete existing entries.

The other tabs represent the various configuration forms. Use the check boxes to select what access the operator should have to which parts of each form.

The operator settings are stored on the Manager PC in .ops files in the Manager directory. As this is not part of the Control Units configuration no send or reboot is necessary following operator changes.

System Form

System Form Overview

This form enables the configuration of system settings and the system's main features such as DHCP and the Voicemail Server PC.

The following tabs correspond to the System Form:

- System
- LAN1
- LAN2 - Applies only to the IP412 and Avaya IP Office - Small Office Edition.
- DNS
- Voicemail
- Telephony
- Gatekeeper
- LDAP
- SNMP

System

Fields within this tab allow you to configure settings related to the Control Unit. The following fields are configurable:

- **Name:** *Default = System MAC Address*
  A name to identify this system. This is typically used to identify the configuration by the location or customer's company name. Some features such as Gatekeeper require the system to have a name. This field is case sensitive and within any network of IP Offices must be unique. Do not use punctuation characters such as #, ?, /, -,. and ,.
- **Locale:**
  This option sets country and language variations based on a three letter value. The main purpose is to set the default ringing and caller display types for the system. See Supported Country and Locale Settings.
- **Password:** *Default = password*
  A password for controlling access to the operation of the Control Unit. This is required to upgrade and reboot and to send or receive configurations from the Control Unit. This is a required option and a prompt is given if left blank.
  - **Confirm Password:**
    This is used to check that the password entered in the Password field has been entered correctly. A warning message appears requesting you to re-confirm the password if the fields differ.
- **Monitor Password:** *Default = blank*
  This password is used by the Monitor and Call Status applications to allow communication with the main unit. If left blank these applications will use the System Password above.
  - **Confirm Monitor Password:**
    This is used to check that the password entered in the Monitor Password field has been entered correctly. A warning message appears requesting you to re-confirm the password if the fields differ.
- **Time Server IP Address:** *Default = Blank*
  Sets a specific address for the Control Unit's time server requests. Blank or 0.0.0.0 means default operation as above. 0.0.0.1 disables time server updates.
- **Time Offset (Hours):** *Default = Blank*
  If a specific address of a time server other than a Voicemail Server or Manager PC is set, then the **Time Offset** field should be used.
- **TFTP Server IP Address:** *Default = Blank*
  When Manager is running, it acts as a TFTP server for the IP Office Control Unit. An entry is only required here if you want to force the Control Unit to use a particular device as its TFTP server. This field must be filled in with the IP address of the PC running Manager on systems using 4600 Series IP phones. On Avaya IP Office - Small Office Edition systems this can be the IP Address of the control unit if fitted with a local memory storage card.
- **License Server IP Address:** *Default* = 255.255.255.255
  The IP address of the server PC providing license key validation for the Control Unit. For a serial licence key plugged directly into a Avaya IP Office - Small Office Edition control unit the field should be left blank. Note that each IP Office Control Unit requires a separate server PC for license validation. See License Form .
- **AVPP IP Address :** *Only necessary if using the 3600 series wireless handsets.*
  The address of the Avaya Voice Priority Processor (AVPP) used to support 3600 series wireless handsets (SpectraLink).

- **File Writer IP Address :**
  The address of the TFTP server able to send files to any writable media card installed on Avaya IP Office - Small Office Edition systems.
- **Conferencing Center IP Address :**
  The IP address of the Conferencing Center server PC. This address is used by the IP Office and by Voicemail Pro server.
- **Conferencing Center URL :**
  The root URL of the web server being used to support Conferencing Center. This address is then used by Conferencing Center links within Phone Manager and SoftConsole.
- **DSS Status:** *Default = Off*
  Affects phones with a display and DSS keys. Controls whether pressing a DSS key set to another user, who is on a call, display details of their calling/called party. When not selected, off, no called/calling party information is displayed.
- **Beep on Listen:** *Default = On (USA)/On (ROW)*
  Controls whether call parties hear a repeating tone when their call is monitored by another party using the Call Listen feature. See How to Monitor Calls .
- **Hide auto record:** *Default = On (USA)/Off (ROW)*
  During call recording by Voicemail Pro, some Avaya terminals display **REC** to show that the call is being recorded. When on, **Hide auto record** suppresses this recording indication.
- **Favour RIP Routes, over static routes:** *Default = Off*
  If enabled and a static route is configured for a specific destination and a RIP route is received for that same destination, the RIP route will be added to the routing table and used, regardless of the metric it has. If this field is not enabled, then a RIP route that is received at the same destination to a configured static route will be discarded.

LAN1

This configuration form is used to configure IP addressing for the LAN. Note: The IP412 and Avaya IP Office - Small Office Edition control units support two LANs, appearing as LAN1 and LAN2. On the IP412 each LAN is represented by a separate physical LAN port. On the Avaya IP Office - Small Office Edition the LAN ports are switched as appropriate.

The following fields are configurable:

- **IP Address:** *Default = 192.168.42.1*
  This is the IP address of the Control Unit on LAN1. If the Control Unit is also acting as a DHCP server on LAN1 then this address will be the DHCP Starting address.
- **IP Mask:** *Default = 255.255.255.0*
  This is the Subnet mask used on LAN1.
    - Do not enter **IP Address** and **IP Mask** values if running in DHCP Client mode. The fields will be filled automatically with the values received from the DHCP server.
- **Primary Trans. IP Address:** *Default = blank* **[IP412 and IP Office - Small Office Edition only]**
  This address acts as the primary address for the LAN. Any incoming IP packets without a session are translated to this address.
- **Number of DHCP IP Addresses:** *Default = 200*
  This defines the number of sequential IP addresses, including the Control Unit IP address, that is allocated via DHCP on LAN1 and/or to Dial in users. Addresses are only allocated if the DHCP mode is set to Server or DialIn.
    - Note: If the Control Unit is acting as a DHCP Server (DHCP mode set to Server or DialIn) on both the LAN1 and LAN2, Dial in users are allocated their address from the LAN1 pool of addresses first.
- **DHCP Mode:**
  This controls the Control Unit's DHCP state on the LAN1.
    - **Server:** When selected the Control Unit is acting as the DHCP Server on LAN1, allocating address to other devices on the network and to PPP Dial in users.
    - **Disabled:** When selected the Control Unit will not use DHCP, therefore it will not act as a DHCP server or obtain an IP address from a DHCP server on this LAN.
    - **Dial In:** This option allows the Control Unit to allocate IP addresses to PPP Dial In users only. It will not allocate IP addresses to local devices on this LAN.
    - **Client:** The Control Unit obtains its **IP Address** and **IP Mask** from a DHCP server on the LAN.
- **Enable NAT:** *Default = Off*
  This option is only shown on the LAN1 and LAN2 tabs of IP412 and Avaya IP Office - Small Office Edition Control Units. It controls whether NAT should be used for IP traffic from LAN1 to LAN2. Note: Not supported on the same LAN interface as WAN3.
- **RIP Mode :** *Default = None*
  Routing Information Protocol (RIP) is a method by which network routers can exchange information about device locations and routes. RIP can be used within small networks to allow dynamic route configuration as opposed to static configuration.
    - **None:** The LAN does not listen to or send RIP messages.

- **Listen Only (Passive):** Listen to RIP-1 and RIP-2 messages in order to learn RIP routes on the network.
- **RIP1:** As above plus send RIP-1 responses as a sub-network broadcast.
- **RIP2 Broadcast (RIP1 Compatibility):** As above but send RIP-2 responses as a sub-network broadcast.
- **RIP2 Multicast:** As above but send RIP-2 responses to the RIP-2 multicast address.

LAN2

This configuration form is similar to LAN1 . It appears on the IP412 and Avaya IP Office - Small Office Edition which support two separate LAN's.

Note: For Manager 2.1, DHCP will always give the LAN1 address, even if you have a LAN2 configured.

The following additional field is shown on the LAN2 tab:

- **Firewall:**
  Allows the application of an IP Office firewall to traffic between LAN2 and LAN1.

DNS

DNS is the system used on the Internet to match computer names to IP addresses. Internet users request specific hosts using names such as www.avaya.com. These names are sent to a Domain Name Server, which converts the name to the IP address, which the computers can pass data.

Within the context of Manager, this tab is used to enter the DNS and WINS information that is given to each host on LAN1 and LAN2 when the main unit is acting as the DHCP server on either or both LANs.

See Domain Name System .

- **DNS Service IP Address:** *Default = Blank*
  This is the IP address of an DNS Server. Your Internet service provider or network administrator provides this information. Alternatively leave this field blank and the main unit will offer itself as a DNS server and will then forward DNS requests to the ISP's DNS server. With the second method, tick **Request DNS** in the IP tab of the Service Form. The form includes fields for primary (1) and secondary (2) address entries.
- **DNS Domain:** *Default = Blank*
  This is the domain name for your IP address. Your Internet service provider or network administrator provides this. Typically this field is left blank.
- **WINS Server IP Address:** *Default = Blank*
  This is the IP address of your local WINS server. This is only used by Windows PCs, and normally points to an NT server nominated by your network administrator as your WINS server. Setting a value will result in also sending a mode of "hybrid". The form includes fields for primary (1) and secondary (2) address entries.
- **WINS Scope:** *Default = Blank*
  This is provided by your network administrator or left blank.

Voicemail

If Voicemail or VoiceMail Pro applications are being used with your system, the system must know where the Voicemail Server is located. Fields in this tab allow you to define the Voicemail Server.

The following fields are configurable:

- **Voicemail Type:** *Default = PC*
  Sets the type of voicemail system being used.

- **None :** No voicemail operation.
- **PC :** The Voicemail server is being run on a networked PC.
- **Line :** Used for centralized voicemail.
- **Integral :** Voicemail running on an integral card in the Control Unit.
- **Group :** Not currently supported.
- **Audix:** Communicate with an Avaya Intuity Audix voicemail system.

- **Voicemail Destination :** *Default = blank*
  Only used if the Voicemail type is set to ***Line, Group*** or ***Audix***. The drop-down selector displays the available options.
- **Audix UDP :**
  Available if the voicemail type Audix is selected. Needs to be completed with a four digit number from the Universal Dial Plan.
- **Voicemail IP Address :** *Default = 255.255.255.255*
  This is the IP address of the PC that is running the Voicemail Server or Voicemail Pro application.
  - If set as 255.255.255.255, Control Unit broadcasts on the LAN to see if it can discover the Voicemail Server. If set to a specific IP address, the system connects to the Voicemail Server running on that specific IP address only.
- **Voicemail Password :** *Default = blank*
  The Voicemail Password is used by the main unit to confirm connection has been made to the correct Voicemail Pro Server. The password entered must correspond to the password set via the Voicemail Pro software. This entry must be left blank when using the standard Voicemail application supplied on the Admin CD.
  - **Confirm Password :**
    The password must be retyped to ensure it has been correctly entered.

System Telephony

Information within this tab allows you to set the system defaults for telephony operation. These can also be set per user in the Telephony tab of the **User** configuration form.

For details of the ringing tones see Ring Tones.

The following fields are configurable within this tab:

- **Default Outside Call Sequence:** *Default = RingNormal*
  Default Ringing sequence for outside calls. The 4400 and 4600 series only support the RingNormal.
- **Default Inside Call Sequence:** *Default = RingType1*
  Default Ringing sequence for internal (extension to extension) calls. The 4400 and 4600 series only support the RingNormal.
- **Default Ring Back Sequence:** *Default = RingType2*
  Default Ringing sequence for calls that are ringing back an extension, eg. CTI calls, VoiceMail and Ring Back when free. The 4400 and 4600 series only support the RingNormal.
- **Dial Delay Time (ms):** *Default = 4000ms (USA/Japan), 1000ms (ROW)*
  The time the system waits following a dialed digit before it interprets all the digits dialed as a unique number. This allows Short Codes and Extensions to have overlapping numbers, eg. Extension "555" and the telephone number "5551234".)
- **Dial Delay Count:** *Default = 0 digits (USA/Japan), 4 digits (ROW)*
  The number of digits to wait for before interpreting the dialed digits - this acts earlier than the dial delay time if this number of digits has been entered.
- **Default No Answer Time (secs):** *Default = 15 seconds*
  The amount of time allowed after the start of ringing to when the phone has been considered unanswered. This determines the amount of time a call rings at the extension before going to Voicemail and also the amount of time a call rings at the extension when auto callback has been invoked.
- **Hold Timeout (secs):** *Default = 90 seconds*
  The time calls remain on hold before recalling to the user who held the call. Entering **0** disables this feature.
- **Park Timeout (secs):** *Default = 300 seconds*
  The time calls remain parked before recalling to the user who parked the call. Entering **0** disables this feature.
- **Show Account Code:** *Default = Off*
  If enabled, the list of account codes will display in Phone Manager. If disabled, the request for account codes will be blocked.
- **Local Dial Tone:** *Default = On*
  For all normal operation this should be left enabled as it allows the system to provide dial tone to users (essential for MSN working).
- **Local Busy Tone:** *Default = Off*
  Used when local exchange gives busy signal (via Q.931) but provides no Busy Tone. For all normal operation this should be left off.
- **Companding:**
  Used to select the method of audio compression for voice calls between **ALAW** and **ULAW** (also called MU-LAW or -Law).
- **Conferencing Tone:** *Default = Off*
  When off, gives a single tone when a new party joins a conference and double-tone

when a party leave a conference. When on, repeats the conference tone every 10 seconds to all conference parties.

- **Inhibit Off-Switch Calls:** *Default = Off (Italy = On)*
  When on, bars any external trunk calls from being diverted or forwarded off switch, ie. trunk to trunk transfers.
- **Dial By Name:** *Default = On*
  When on, allows the directory features on various phones to match the dialing of full names. When off, the directory features use the pre-IP Office 1.4 method of first character match only.
- **Busy Tone Detection:** Default = System
  Allows configuration of the IP Office's busy tone detection settings.

Gatekeeper

Gatekeepers provide network services to H.323 terminals, MCUs, and gateways. H.323 devices register with gatekeepers to send and receive H.323 calls. Gatekeepers give permission to make or accept a call based on a variety of factors.

Note: H.323 gatekeeper (Call Servers) is supported on the LAN1 address only.

Gatekeepers can provide network services such as:

- Controlling the number and type of connections allowed across the network.
- Helping to route a call to the correct destination.
- Determining and maintaining the network address for incoming calls.

Within the **Gatekeeper** tab, the following fields are configurable:

- **Gatekeeper Enable:** *Default = On*
  This option enables Gatekeeper support.
- **Direct Routed Signaling Enable:** *Default = Disabled*
  When selected, H.323 terminals send audio data directly rather than via the Control Unit.
- **Auto-create Extn Enable:** *Default = On*
  When selected, H.323 terminals automatically register themselves with the Gatekeeper, thus creating an Extension in the configuration.
- **Enable RSVP:** *Default = Disabled (Greyed out)*
  Use this option to turn RSVP support on or off. Note that the default firewall profile settings if applied drop RSVP.
- **DSCP (Hex):** *Default = 0xB8*
  The Quality of Service (DiffServe) setting applied to VoIP calls. For correct operation, especially over WAN links, the same value should be set at both ends.
  - **DSCP:** *Default = 46*
    Decimal value equivalent of DSCP (Hex). These two fields are linked, allowing DSCP entry in either Hex or Decimal.
- **DSCP Mask (Hex):** *Default = 0xFC*
  Allows a mask to be applied to packets for the DSCP value.
  - **DSCP Mask:** *Default = 63.*
    Decimal value equivalent of DSCP Mask (Hex). These two fields are linked, allowing DSCP Mask entry in either Hex or Decimal.
- **SIG DSCP (Hex):** *Default = 0x00*
  The Quality of Service setting applied to VoIP call signaling.
  - **SIG DSCP:** *Default = 0.*
    Decimal value equivalent of SIG DSCP (Hex). These two fields are linked, allowing SIG DSCP entry in either Hex or Decimal.
- **SSON:** *Default = 176*
  Sets the site specific option number (SSON) used by the IP Office's internal DHCP. This should match the SSON used by 4600 Series IP phones to request installation settings (the default being 176). Acceptable values are between 128 and 255.

LDAP

This form is used to configure LDAP operation.

The following fields are configurable within the LDAP tab:

- **User Name:** *Default = blank*
  Enter the user name to be used to authenticate connection with the LDAP database.

  For a Windows 2000 Active Directory server, the user name is of email format (ie. with a domain suffix). To determine the domain-name of a particular Windows 2000 user look on the "Account" tab of the user's properties under "Active Directory Users and Computers". Note that this means that the user name required is not necessarily the same as the name of the Active Directory entry. There should be a built-in account in Active Directory for anonymous Internet access, with prefix "IUSR_" and suffix server_name (whatever was chosen at the Windows 2000 installation). Thus, for example, the user name entered is this field might be: IUSR_CORPSERV@acme.com

- **Password:** *Default = blank*
  Enter the password to be used to authenticate connection with the LDAP database.

  Enter the password that has been configured under Active Directory for the above user.
  Alternatively an Active Directory object (eg the User container) may be made available for anonymous read access. This is configured on the server as follows:
  In "Active Directory Users and Computers" enable "Advanced Features" under the "View" menu. Open the properties of the object to be published and select the "Security" tab. Click "Add" and select "ANONYMOUS LOGON", click "Add", click "OK", click "Advanced" and select "ANONYMOUS LOGON", click "View/Edit", change "Apply onto" to "This object and all child objects", click "OK", "OK", "OK".
  Once this has been done on the server, any entry can be made in the User Name field in the System configuration form (however this field cannot be left blank) and the Password field left blank. Other non-Active Directory LDAP servers may allow totally anonymous access, in which case neither User Name nor Password need be configured.

  - **Confirm Password:**
    Reenter the password to ensure this has been entered correctly.

- **Server IP Address:** *Default = blank*
  Enter the IP address of the server storing the database
- **Authentication Method:** *Default = Simple*
  Select the authentication method to be used.
  - **Simple:** clear text authentication
  - **Kerberos:** Kerberos 4 LDAP and Kerberos 4 DSA encrypted authentication (for future use)
- **Resync Interval (secs):** *Default = 3600 seconds*
  This is the amount of time between each request for updated information.
- **Search Base:** *Default = blank*
  Use this box to define the starting point for the search in order to restrict the search to, eg. company, location etc. (as defined in RFC 1779)
- **Search Filter:** *Default = blank*
  Use this box to define which records are retrieved (as defined in RFC2254). If this field is left blank the filter will default to "(objectClass=*)", this matches all objects under the Search Base.
- **Number Attributes:** *Default = see below*
  Enter the number attributes the server should return for each entry that matches the Search Base and Search Filter. .Other entries could be ipPhone, otherIpPhone,

facsimileTelephoneNumber, otherfacsimileTelephone Number, pager or otherPager. The attribute names are not case sensitive. Other LDAP servers may use different attributes.

- By default the entry is "telephoneNumber,otherTelephone,homePhone=H,otherHomePhone=H,mobile=M,otherMobile=M", as used by Windows 2000 Server Active Directory for Contacts.

- **LDAP Enabled:** *Default = Off*
  This option will turn LDAP support on or off.

Notes:

- A maximum of 500 records can be retrieved due to size restraints.
- Each record retrieved creates a Directory entry for use with Phone Manager. Please note that the entries will not be stored in the configuration and therefore are not visible via Manager.
- All records are merged so that no duplicate entries are created.

SNMP

Simple Network Management Protocol (SNMP) allows network devices (SNMP clients and SNMP servers) to exchange information. SNMP clients are built into devices such as network routers, server PC, etc. SNMP servers are typically PC application which receive and/or request SNMP information.

The IP Office SNMP client allows the IP Office control unit to respond to SNMP polling and to send information about error conditions to SNMP servers.

Note: In order for an SNMP server application to interact with an IP Office, the IP Office MIB files, provided on the IP Office Admin CD, must be compiled into the SNMP server applications database. For details on compiling the MIB files, see Installing the IP Office MIB Files.

The following fields are configurable:

- **SNMP Enabled:** *Default = Off*
  Enables support for SNMP by the IP Office control unit.
- **SNMP Port:** *Default = 161*
  The port on which the control listens and responds to SNMP polling traffic.
- **Community (Read-only):** *Default = Blank*
  The SNMP community, eg. public.
- **Trap Destination 1/2:**
  The control unit supports two SNMP traps, to which it can send specified IP Office events.
- **IP Address:** *Default = Blank*
  The IP address of the SNMP server to which trap information is sent.
- **Port:** *Default = 162*
  The SNMP transmit port
- **Community:** *Default = Blank*
  The SNMP community for the transmitted traps. Must be matched by the receiving SNMP server.
- **Events:** Default = None
  Sets which types of IP Office events should be collected and sent by the trap:
  - **Generic:** Report on cold starts, warm starts and SNMP authentication failure.
  - **Entity:** Report on link up/down changes between IP Office modules (except WAN3), trunks and VCM.
  - **Licence:** Report failure to connect with the Licence Key Server.
  - **CSU Loop-Back:** Only displays when the system locale is set to **enu**. Ticking this field enables the sending of CSU loop-back events, which may then be monitored by an SNMP manager application.
  - **Phone Change:** Send a trap whenever a phone is removed or moved.

Line Form

Line Form Overview

Depending on the types of line installed in the Control Unit, the tabs and options that appear for this form will vary. Manager will recognize the type of line card installed in the Control Unit and make only those corresponding configuration settings available.

Note: The types of lines supported will vary in different countries. For confirmation of the line types supported in a particular country, contact your Avaya representative in that country.

These are the possible line types and their respective symbols within Manager:

- **Analog Line:**
  Indicates that the line is on an Analog card installed in the Control Unit or that analog expansion module(s) are in use. When configuring an analog line on Manager, the Line and Analog tabs will be available for set up. When configuring the line settings, make sure your line settings match those of the exchange line settings.
- **Digital Line:**
  Indicates that the line is a digital line. Each line consists of a single physical connection but may carry a number of channels. To recognize the type of digital line, look at its **Line SubType** setting. Digital line types available are:
  - **T1:** The line is provided by a PRI T1 card installed in the Control Unit and set the T1 operation.
  - **US PRI:** The line is provided by a PRI T1 card installed in the Control Unit and set to PRI operation.
  - **E1 PRI:** The line is provided by a PRI E1 or BRI card installed in the Control Unit.
  - **E1-R2:** The line is provided by an E1-R2 card installed in the Control Unit.
  - **Blank:** The line is a BRI line provided by an S0 expansion port.
- **IP Line:**
  The line is an IP line added manually rather than by the installation of a physical line card in the Control Unit.

Line Form (E1 PRI, BRI)

Line Form (E1 PRI, BRI) Overview

This configuration form is used to configure the E1 PRI and BRI lines installed in the Control Unit.

The following tabs contain configurable information for this line form:

- Line
- Short Codes

Line

Within the Line tab, the following fields are available for configuration:

- **Line Number**
  This parameter is not configurable, it is allocated by the system.
- **Line Sub Type:**
  Select to match the particular line provided by the PSTN.
  - E1 PRI supports ETSI, QSIG A and QSIG B.
  - BRI supports ETSI and AusTS013.
- **Telephone Number:**
  Used to remember the external telephone number of this line to assist with loop-back testing. For information only.
- **Number Of Channels:**
  Defines the number of operational channels that are available on this line. 2 for BRI and up to 30 for PRI - depending upon the number of channels subscribed.
- **Outgoing Channels:**
  This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as Number of Channels field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls.
- **Clock Quality:** *Default = Network*
  Sets whether the Control Unit takes it clock source from the network, use the network as a fallback source or not as a clock source.
- **Data Channels:**
  The number of channels available for data use. If left blank, the value is 0.
- **Voice Channels:**
  The number of channels available for voice use.
- **TEI:** *Default = 0*
  The Terminal Equipment Identifier. Used to identify each Control Unit connected to a particular ISDN line. For Point to Point lines this is typically (always) 0. It can also be 0 on a Point to Multi-Point line, however if multiple devices are sharing a Point to Multi-Point line it should be set to 127 which results in the exchange deciding on the TEI's to be used.
- **Incoming Group ID and Outgoing Group ID:** *Default = 0*
  One group can contain multiple lines. Short Codes and Incoming Call Routes use this number to indicate which line they use.
- **International Prefix:** *Default = 00*
  This indicates the digits to be prefixed to an incoming international call. When a number is presented from ISDN as an "international number" this prefix is added, eg. 441923000000 is converted to 00441923000000.

- **National Prefix:** *Default = 0*
  This indicates the digits to be prefixed to a incoming national call. When a number is presented from ISDN as a "national number" this prefix is added, eg. "1923000000 is converted to 01923000000.
- **CRC Checking:** *Default = On*
- **Prefix:** *Default = Blank.*
  Enter the number to prefix to all incoming calls which are not national (see National Prefix above) or international (see International Prefix above). The addition of prefixes is useful for callbacks, etc. if users must dial a prefix to access an outside line.

Short Codes

A Line Short Code is similar to a User Short Code in that it performs the function on that line only. A Line Short Code is performed once the specific Line has been accessed. See Understanding Short Codes .

- **To add a Short Code:**
  Place the cursor over the Short Code List Box and double-click or right-click and select **Add**.

Line Form (E1-R2)

Line Form (E1-R2) Overview

This form is used to configure E1-R2 lines provided by an E1-R2 card installed in the Control Unit.

The following tabs contain configurable information for this line form:

- Line
- Advanced
- MFC Group

Line (E1-R2)

Within the **Line** tab, the following fields are available for configuration:

- **Line Number:**
  Allocated by the system.
- **Line SubType:** *Default = E1-R2*
  Supported options are **E1-R2**, **ETSI**, **QSIGA** or **QSIGB**.
- **Channel Allocation:** *Default = 30>1*
  The order (30>1 or 1>30) in which channels are used.
- **Country (Locale):** *Default = Mexico.*
  Select the locale that matches the area of usage. Note that changing the locale will return MFC Group settings to their defaults for the selected locale. Currently supported locales are ***Mexico***, ***Brazil***, ***Argentina***, ***Korea***, ***China*** and ***None***.

The table at the base of the form displays the settings for the individual channels provided by the line. For details of the channel settings see Edit Channel (E1-R2).

To edit a channel either double-click on it or right-click and select Edit. To edit multiple channels at the same time select the channels whilst pressing the Shift or Ctrl key. Then right-click and select Edit.

Edit Channel (E1-R2)

Within the Edit Channel section, the following fields are available for configuration:

- **Channel:**
  The channel or channels being edited.
- **Incoming Group & Outgoing Group:** *Default = 0*
  A group can contain multiple lines and channels. Short codes and Incoming Call Routes can indicate which group they should use.
- **Direction:** *Default = Bothway*
  The direction of calls on the channel (Incoming, Outgoing or Bothway).
- **Bearer:** *Default = Any*
  The type of traffic carried by the channel (Voice, Data or Any).
- **Line Signaling Type:** *Default = R2 Loop Start*
  The signaling type used by the channel. Current supported options are:
  - R2 Loop Start, R2 DID, R2 DOD, R2 DIOD, Tie Immediate Start, Tie Wink Start, Tie Delay Dial, Tie Automatic, WAN Service and Out of Service.
- **Dial Type:** *Default = MFC Dialing*
  *The type of dialing supported by the channel (**MFC Dialing, Pulse Dialing or DTMF Dialing).*

Timers

This form display the various timers provided for E1-R2 channels. To change a value either double-click on it or right-click and select **Edit**.

By right-clicking you can also select options to set to default, set to maximum or set to minimum the selected timer or all timers.

Advanced (E1-R2)

- **Line Signaling Timers:**
  To edit one of these timers, either double-click on the timer or right-click on a timer and select the action required.
- **Zero Suppression:** *Default = HDB3*
  Selects the method of zero suppression used (HDB3 or AMI).
- **Clock Quality:** *Default = Network*
  Sets whether the Control Unit takes it clock source from the network, use the network as a fallback source or not as a clock source.
- **Pulse Metering Bit:** *Default = A Bit*
  Sets which bit should be used to indicate the pulse metering signal (**A Bit**, **B Bit** or **C Bit**).
- **Line Signaling:** *Default = CPE*
  Select either **CPE** or **CO**.

  Note: The CO feature is intended to be used primarily as a testing aid. It allows T1 and E1 lines to be tested in a back-to-back configuration, using crossover (Qsig) cables. The **CO** feature operates on this line type by modifying the way in which incoming calls are disconnected for IP Office configuration in Brazil and Argentina. In these locales, the CO setting uses **Forced-Release** instead of **Clear-Back** to disconnect incoming calls. The Brazilian **Double-Seizure** mechanism, used to police **Collect** calls, is also disabled in CO mode.
- **Incoming Routing Digits:** *Default = 4*
  Sets the number of incoming digits used for incoming call routing.
- **CRC Checking:** *Default = Ticked (On)*
  Switches CRC on or off.
- **Default All**
  Default the MFC Group tab settings.

MFC Group (E1-R2)

These tabs show the parameter assigned to each signal in an MFC group. The defaults are set according to the **Country (Locale)** on the **Line** tab. All the values can be returned to default by the **Default All** button on the **Advanced** tab.

To change a setting either double-click on it or right-click and select **Edit**.

Line Form (US T1)

T1 Line Overview

T1 is a standard for digital transmission in the United States and Canada.

This form is used to configure T1 lines provided by T1 PRI card installed in the Control Unit.

The following tabs contain configurable information for your T1 line:

- Line
- Advanced

Line

Within the Line tab, the following fields are available for configuration:

- **Line Number:**
  Allocated by the system.
- **Line SubType:** *Default = PRI*
  Set to ***T1*** for a T1 line. For ***PRI*** see Line Form (US PRI) .
- **Channel Allocation:** *Default = 24 -> 1*
  The order, 24 to 1 or 1 to 24, in which channels are used.
- **Prefix:** *Default = Blank*
  Enter the number to prefix to all incoming numbers for callback. This is useful if all users must dial a prefix to access an outside line, the prefix is automatically placed in front of all incoming numbers so that users can dial the number back.

The settings for each channel can be edited. Users have the option of editing individual channels (for both the T1 Edit Channel and Timer forms) by double-clicking on the channel, or editing multiple channels by the following:

1. Use the standard Window Key to select a continuous group (Shift Key) or Individual Channels (Control Key).
2. After selecting the last item (via either of the above methods, press the right mouse button while still holding down the Control or Shift Key). Select the Edit option.
3. A form comes up with the Channel parameters. The first and last channels that you have selected are listed in the Channel box (ie. 1-8).
4. Make all appropriate changes and then select OK. The changes are applied to all the selected channels.

T1 Edit Channel

- **Channel:**
  Allocated by the system.
- **Incoming Group** and **Outgoing Group:** *Default = 0*
  One group can contain multiple lines. Short Codes and Incoming Call Routes use this number to indicate which line they use.
- **Direction:** *Default = Bothway*
  The direction of calls on the channel (***Incoming***, ***Outgoing*** or ***Bothway***).
- **Bearer:** *Default = Voice*
  The type of traffic carried by the channel.
- **Type:** *Default = Ground-Start*
  The T1 emulates the following connections (***Ground-Start***, ***Loop-Start***, ***E&M - TIE***, ***E&M - DID***,

E&M Switched 56K, ***Direct Inward Dial, Clear Channel 64K*** or ***Out of Service***). When a channel is Out Of Service, set the **Incoming Group** and **Outgoing Group** to 0 (the default).

- **Dial Type:** *Default = DTMF Dial*
  Select the dialing method required (***DTMF Dial*** or ***Pulse Dial***).
- **Incoming Trunk Type:** *Default = Wink-Start*
  Used for E&M types only. The handshake method for incoming calls (***Automatic***, ***Immediate***, ***Delay Dial*** or ***Wink-Start***).
- **Outgoing Trunk Type:** *Default = Wink-Start*
  Used for E&M types only. The handshake method for outgoing calls (***Automatic***, ***Immediate***, ***Delay Dial*** or ***Wink-Start***).
- **Tx Gain:** *Default = 0dB*
  The transmit gain in dB.
- **Rx Gain:** *Default = 0dB*
  The receive gain in dB.

Timers

This form displays the various timer provided for T1 lines. The Timers can be changed for one timer or multiple timers.

Timers can either be changed manually or by clicking the right mouse button. The options are listed below:

- **Edit Value**
  Calls up the edit box to manually enter a value.
- **Default Value**
  Applies a default value, which is hard coded within the box.
- **Default All Values**
  Applies the default value to all parameters listed.
- **Apply Maximum**
  Applies Maximum allowable value to the selected parameter.
- **Apply All Maximum**
  As above but for all timer parameters.
- **Apply Minimum**
  Applies Minimum allowable value to the selected parameter.
- **Apply All Minimum**
  As above but for all timer parameters.

Advanced

- **Framing:** *Default = ESF*
  Selects the type of signal framing used (***ESF*** or ***D4***).
- **Zero Suppression:** *Default = B8ZS*
  Selects the method of zero suppression used (***B8ZS*** or ***AMI ZCS***).
- **Clock Quality:** *Default = Network*
  Sets whether the Control Unit takes it clock source from the network, uses the network as a fallback clock source only or not as a clock source (***Network***, ***Fallback*** or ***Un-suitable***).
- **Line Compensation:** *Default = 0-115 feet*
  Sets the line length to a specific distance.
- **Channel Unit**: *Default = Foreign Exchange*
  The channel signaling equipment provided by the Central Office (***Foreign Exchange***, ***Special Access*** or ***Normal***.
- **CRC Checking:** *Default = On*
  Turns CRC on or off.
- **Line Signaling:** *Default = CPE*
  Note: This field is only available when logged into Manager with the Administrator password. It affects T1 channels set to **Loop-Start** or **Ground-Start**. The field can be set to either ***CPE*** (Customer Premises Equipment) or ***CO*** (Central Office). This field should normally be left at its default of ***CPE***. The setting ***CO*** is normally only used in lab back-to-back testing.
- **Incoming Routing Digits:** *Default=0 (present call immediately)*
  Sets the number of routing digits expected on incoming calls. This allows the line to present the call to the system once the expected digits have been received rather than waiting for the digits timeout to expire. This field only affects T1 line channels set to ***E&M Tie***, ***E&M DID***, ***E&M Switched 56K*** and ***Direct Inward Dial***.
- **CSU Operation:** Tick this field to enable theT1 line to respond to loop-back requests from the line.

Line Form (US PRI)

Line Form (US PRI) Overview

This form is used to configure PRI lines provided by T1 PRI card installed in the Control Unit.

In PRI operation two information elements, TNS (Transit Network Selector) and NSF (Network Specific Facility) are sent in the call setup to the service provider. On IP Office, the values for TNS, NSF and the actual phone number presented to the line are determined by parsing the number dialed through, in sequence, the **TNS**, **Special** and **Call by Call** tabs.

Note also that B-channels within the same line can be brought from different service provides. Additionally some B-channels can be used 'call by call', that is, use a different service provider for each call.

More:

- Line
- Network Selection
- Special
- Call By Call
- Advanced

Line

- **Line Number:**
  Allocated by the system.
- **Line SubType:** *Default = PRI*
  Set to ***PRI***. If set to ***T1*** see Line Form (US T1) .
- **Channel Allocation:** *Default = 23 -> 1*
  The order, 23 to 1 or 1 to 23, in which channels are used.
- **Switch Type:** *Default = NI2*
  Options ***4ESS***, ***5ESS***, ***DMS100*** and ***NI2***.
- **Provider:** *Default = Local Telco*
  Select the PSTN service provider (***AT&T***, ***Sprint***, ***WorldCom*** or ***Local Telco***).
- **Prefix:** *Default = Blank*
  Enter the number to prefix to all incoming numbers for callback. This is useful if all users must dial a prefix to access an outside line. The prefix is automatically placed in front of all incoming numbers so that users can dial the number back.

The settings for each channel can be edited. Users have the option of editing individual channels (for both the T1 Edit Channel and Timer forms) by double-clicking on the channel, or editing multiple channels by the following:

1. Use the standard Window Key to select a continuous group (Shift Key) or Individual Channels (Control Key).
2. After selecting the last item (via either of the above methods, press the right mouse button while still holding down the Control or Shift Key). Select the Edit option.
3. A form comes up with the Channel parameters. The first and last channels that you have selected are listed in the Channel box (ie. 1-8).
4. Make all appropriate changes and then select OK. The changes are applied to all the selected channels.

Edit Channel

- **Channel:**
  Allocated by the system.
- **Incoming Group** and **Outgoing Group:** *Default = 0*
  One group can contain multiple lines. Short Codes and Incoming Call Routes use this number to indicate which line they use.
- **Direction:** *Default = Bothway*
  The direction of calls on the channel (***Incoming***, ***Outgoing*** or ***Bothway***).
- **Bearer:** *Default = Any*
  The type of traffic carried by the channel (***Voice***, ***Data*** or ***Any***).
- **Service:** *Default = No Service or None.*
  If the line provider is set to AT&T, selects the type of service provided by the channel from ***Call by Call***, ***SDN (inc GSDN)***, ***MegaCom800***, ***MegaComWats***, ***Accunet***, ***NLDS***, ***I800***, ***ETN***, ***Private Line***, ***AT&T Multiquest***. For other providers the service options are **None** or **No Service**.
- **Admin:** *Default = In Service*
  Used to indicate the channel status (***In Service***, ***Out of Service*** or ***Maintenance***).
- **Tx Gain:** *Default = 0dB*
  The transmit gain in dB.
- **Rx Gain:** *Default = 0dB*
  The receive gain in dB.

Network Selection

This tab is shown when the line **Provider** is set to ***AT&T***.It allows the entry of the Network Selection settings. These are prefixes for alternative long distance carriers (for example 10XXX). When a number dialed matches an entry in the table, that pattern is stripped from the number before being sent out. This table is used to set field in the TNS information element for ***4ESS*** and ***5ESS*** exchanges. It is also used to set fields in the NSF information element.

- **Network Selection Code:**
  The pattern for the alternate long distance carrier. Right-click the mouse to Add, Delete or Edit entries.
- **Example:**
  Pattern 10xxx is in the **Network Selection** tab. If 10288 is dialed, 10 is removed, 288 is placed in the TNS and NSF information.
- **Altering Entries:**
  Right-click the mouse to **Add**, **Delete** or **Edit** entries.

Special

This tab is shown when the line **Provider** is set to ***AT&T***.This table is used to set additional fields in the NSF information element after initial number parsing by the **TNS** tab. These are used to indicate the services required by the call. If the channel is set to Call by Call, then further parsing is done using the entries in the **Call by Call** tab.

Double-click on an existing entry to edit it or on a blank space to add a new entry.

- **Short code:**
  The number which results from the application of the rules specified in the User or System Short code tables and the Network Selection table and the Call-by-call table to the number dialed by the user.
- **Number:**
  The number to be dialed to line.
- **Special:** *Default = No Operator*
  (***No Operator***, ***Local Operator*** or ***Presubscribed Carrier***).
- **Plan:** *Default = National*
  (***National*** or ***International***).

Typical values would be:

Short code	Number	Service
011N	N	No Operator, International
010N	N	Local Operator, International
01N	N	Local Operator, National
00N	N	Presubscribed Carrier, National
0N	N	Presubscribed Carrier, National
1N	1N	No operator, National

Call By Call

This tab is shown when the line **Provider** is set to ***AT&T***.Settings in this tab are only used when calls are routed via a channel which has its Service set to Call by Call.

It allows short codes to be created to route calls to a different services according to the number dialed. Call By Call reduces the costs and maximizes the use of facilities. Call By Call chooses the optimal service for a particular call by including the Bearer capability in the routing decision. This is particularly useful when there are limited resources.

Double-click on an existing entry to edit it or on a blank space to add a new entry.

- **Short Code:**
  The number which results from the application of the rules specified in the User or System Short code tables and the Network Selection table to the number dialed by the user.
- **Number:**
  The number to be dialed to line.
- **Bearer:** *Default = Any*
  The type of channel required for the call (***Voice***, ***Data*** or ***Any***).
- **Service:** *Default = AT&T.99*
  The service required by the call (***SDN (inc GSDN)***, ***MegaCom800***, ***MegaCom***, ***Inwats***, ***Wats***, ***Accunet***, ***NLDS***, ***I800***, ***ETN***, ***Private Line***, ***AT&T Multiquest***).

Advanced

- **Test Number:**
  Used to remember the external telephone number of this line to assist with loop-back testing. For information only.
- **Framing:** *Default = ESF*
  Selects the type of signal framing used (***ESF*** or ***D4***).
- **Zero Suppression:** *Default = B8ZS*
  Selects the method of zero suppression used (***B8ZS*** or ***AMI ZCS***).
- **Clock Quality:** *Default = Network*
  Sets whether the Control Unit takes it clock source from the network, uses the network as a fallback clock source only or not as a clock source (***Network***, ***Fallback*** or ***Un-suitable***).
- **Line Compensation:** *Default = 0-115 feet*
  Sets the line length to a specific distance.
- **Channel Unit**: *Default = Foreign Exchange*
  The channel signaling equipment provided by the Central Office (***Foreign Exchange***, ***Special Access*** or ***Normal***.
- **CRC Checking:** *Default = On*
  Turns CRC on or off.
- **Line Signaling:**
  Note: This field is only available when logged into Manager with the Administrator password. Not used for PRI, only used for T1.
- **Incoming Routing Digits:**
  Not used for PRI, only used for T1.

Line Form (Analog)

Analog Line Overview

This form is used to configure analog lines installed in the Control Unit or those on expansion modules. When configuring the line settings, make sure your line settings match those of the exchange line settings.

The following tabs contain configurable information for this line form:

- Line
- Analog

Line

Within the Line tab, the following fields are available for configuration:

- **Line Number**
  This parameter is not configurable, it is allocated by the system.
- **Telephone Number:**
  Used to remember the external telephone number of this line to assist with loop-back testing. For information only.
- **Outgoing Channels:** *Default = 1 (not changeable)*
  This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as Number of Channels field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls.
- **Voice Channels:** *Default = 1 (not changeable)*
  The number of channels available for voice use.
- **Incoming Group ID and Outgoing Group ID:** *Default = 0*
  One group can contain multiple lines. Short Codes and Incoming Call Routes use this number to indicate which line they use.
- **National Prefix:** *Default = 0 (not changeable)*
  This indicates the digits to be prefixed to a national call.
- **Prefix:** *Default = Blank.*
  Enter the number to prefix to all incoming calls which are not national (see National Prefix above). The addition of prefixes is useful for callbacks, etc. if users must dial a prefix to access an outside line.

Analog

Within the Analog tab, the following fields are available for configuration:

- **Channel:**
  Set by the system. Shown for information only.
- **Trunk Type:** *Default = Loop Start*
  Sets the analog line type (**Ground Start**, **Loop Start**, **Loop Start Caller ID**, **Out of Service**).
  - **Note: Ground Start Trunks.**
    Ground Start is only supported on trunks provided by the Analog Trunk 16 expansion module.
  - **Note: Delay Waiting for Caller ID Information.**
    Selecting Loop Start Caller ID on trunks where CLI is not being provided causes a delay in call connection.
- **Signaling Type:** *Default = DTMF Dialing*
  Sets the signaling method used on the line (**DTMF Dialing** or **Pulse Dialing**).

- **Direction:** *Default = Bothway*
  Sets the allowed direction of operation of the line (**Incoming**, **Outgoing** or **Bothway**).
- **Bearer:** *Default = Any*
  Sets the type of traffic carried by the line (**Voice**, **Data** or **Any**).
- **Bearer:** *Default = Any*
  Sets the type of traffic carried by the line (**Voice**, **Data** or **Any**).
- **Impedance:** *[PTB locale only] Default = 900R*
- **Allow Forwarding:** *Default = Not selected (Off).*
  When off, external calls on other trunks cannot be transferred back off-switch via this trunk. This prevents transfers to trunks that do not support disconnect clear. See also **Inhibit Off-Switch Calls** on the **System | Telephony** tab.
- **BCC:** *[PTB locale only] Default = Not selected*
- **Ring Persistency:** *Default = Set according to system locale*
  The minimum duration of signal required to be recognized.
- **Ring Off Maximum:** *Default = Set according to system locale*
  The time required before signaling is regarded as ended.
- **Flash Pulse Width:** *Default = 50 (500ms)*
- **DTMF Mark:** *Default = 80 (80ms)*
- **DTMF Space:** *Default = 80 (80ms)*
- **Intermediate Digit Pause:** *Default = 50 (500ms)*
- **Voicemail Recording Level:** *Default = Low*
  Used to adjust the volume level of calls recorded by voicemail. Options are ***Low***, ***Medium*** and ***High***.
- **Disconnect Clear:**
  We recommend leaving this ticked to make use of the disconnect clear function.
  - **Enable:** Enables use of disconnect clear.
  - **Units:** *Default = 50 (500ms)*
- **Pulse On Width:** *Default = 40 (40ms)*
- **Pulse Off Width:** *Default = 60 (60ms)*
- **Await Dial Tone:** *Default = 15 (1.5second)*
  Sets how long the system should wait before dialing out.
- **BCC Flash Pulse Width:** *[PTB locale only] Default = 100 (1000ms)*
- **Gains:**
  - **Tx (A-D):** *Default = 0dB*
    Set the transmit gain between -4.0 to +3.5dB in 0.5dB steps.
  - **Rx (D-A):** Default = 0dB
    Set the receive gain between -4.0 to +3.5dB in 0.5dB steps.
- **Secondary Dial Tone:** *Default = Off*
  Configures the use of secondary dial tone on analog lines. When selected the following options are accessible.
- **Long CLI Line:** *Default = Off*
  The CLI signal on some long analog lines can become degraded and is not then correctly detected. If you are sure that CLI is being provided but not detected, selecting this option may resolve the problem.
- **Await time:** *Default = 10 (x 100ms = 1 second)*
  Set the transmit gain between -4.0 to +3.5dB in 0.5dB steps.

- **After n Digits:** *Default = 1*
  Sets the delay used before dialing any following digits.
- **Matching Digit:** *Default =0*
  The digit which, when first matched in the dialing string, will cause secondary dial tone delay.
- **Modem Enabled:** *Default = Off*
  The first analog channel on Avaya IP Office - Small Office Edition controls units and on ATM4 trunk modules can be set to modem operation (V.32 with V42 error correction). This allow the receipt of incoming modem calls for system maintenance operation. In addition in systems without a Modem 2 card the channel can also be used for outgoing modem operation.

Line Form (S0)

Line Form (S0) Overview

This configuration form is used for lines added by the installation of an S0 expansion module.

The S0 module provides ISDN BRI outputs so you can share out ISDN access from say your PRI line to ISDN2 devices like Video Conferencing Control Units or ISDN PC Cards.

For details on installation and sample configurations of S0 modules, see Installing and Configuring S0 Ports.

The following tabs contain configurable information for this line form:

- Line
- Short Codes

Line

- **Line Number**
  This parameter is not configurable. It is allocated by the system.
- **Line Sub Type:** *Default = Blank*
  Not used.
- **Telephone Number:**
  Used to remember the telephone number of this line. For information only.
- **Number Of Channels:** *Default = 2*
  Defines the number of operational channels that are available on this line. 2 for BRI and up to 30 for PRI - depending upon the number of channels subscribed.
- **Outgoing Channels:** *Default = 2*
  This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as Number of Channels field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls.
- **Clock Quality:**
  Sets whether the Control Unit takes it clock source from the network, uses the network as a fallback clock source only or not as a clock source (***Network***, ***Fallback*** or ***Un-suitable***).
- **Voice Channels:** *Default = 2*
  The number of channels available for voice use.
- **Data Channels:** *Default = 2*
  The number of channels available for data use. If left blank the value is 0.
- **TEI:** *Default = 0*
  Not used. The Control Unit will ignore any entry.
- **Incoming Group ID** and **Outgoing Group ID:** *Default = 0*
  One group can contain multiple lines. Short Codes and Incoming Call Routes use this number to indicate which line they use.
- **International Prefix:** *Default = 00*
  This indicates the digits to be prefixed to an incoming international call. When a number is presented from ISDN as an "international number" this prefix is added, eg. 441923000000 is converted to 001441923000000.
- **National Prefix:** *Default = 0*
  This indicates the digits to be prefixed to a incoming national call. When a number is presented from ISDN as a "national number" this prefix is added, eg. "7325551234 is converted to 17325551234.
- **Prefix:** *Default = Blank.*
  Enter the number to prefix to all incoming calls which are not national (see **National Prefix** above) or international (see **International Prefix** above). The addition of

prefixes is useful for callbacks, etc. if users must dial a prefix to access an outside line.

Short Codes

A Line Short Code is similar to a User Short Code in that it performs the function on that line only. A Line Short Code is performed once the specific Line has been accessed. See Understanding Short Codes.

- **To add a Short Code:**
  Place the cursor over the Short Code List Box and double-click or right-click and select **Add**.

Line Form (IP)

Line Form (IP) Overview

This configuration form is used for lines added manually, ie. IP lines. These are typically used for VoIP operation.

The following tabs contain configurable information for this line form:

- Line
- ShortCodes
- VoIP

Line (IP)

Within the Line tab, the following fields are available for configuration:

- **Line Number**
  Enter the line number that you wish. Note that this must be unique.
- **Telephone Number:**
  Used to remember the telephone number of this line. For information only.
- **Number Of Channels:** *Default = 20*
  Defines the number of operational channels that are available on this line. 2 for BRI and up to 30 for PRI - depending upon the number of channels subscribed.
- **Outgoing Channels:** *Default = 20*
  This defines the number of channels available, on this line, for outgoing calls. This should normally be the same as Number of Channels field, but can be reduced to ensure incoming calls cannot be blocked by outgoing calls.
- **Data Channels:** *Default = 20*
  The number of channels available for data use. If left blank the value is 0.
- **Voice Channels:** *Default = 20*
  The number of channels available for voice use.
- **TEI:** *Default = 0*
  The Terminal Equipment Identifier. Used to identify each Control Unit connected to a particular ISDN line. For Point to Point lines this is typically (always) 0. It can also be 0 on a Point to Multi-Point line, however if multiple devices are actually sharing a Point to Multi-Point line it should be set to 127 which will result in the exchange deciding on the TEI's to be used by this Control Unit.
- **Incoming Group ID** and **Outgoing Group ID:** *Default = 0*
  One group can contain multiple lines. Short Codes and Incoming Call Routes use this number to indicate which line they use.
- **International Prefix:** *Default = 00*
  This indicates the digits to be prefixed to an incoming international call. When a number is presented from ISDN as an "international number" this prefix is added, eg. 441923000000 is converted to 001441923000000.
- **National Prefix:** *Default = 0*
  This indicates the digits to be prefixed to a incoming national call. When a number is presented from ISDN as a "national number" this prefix is added, eg. "7325551234" is converted to "17325551234".
- **Prefix:** *Default = Blank.*
  Enter the number to prefix to all incoming calls which are not national (see **National Prefix** above) or international (see **International Prefix** above). The addition of prefixes is useful for callbacks, etc. if users must dial a prefix to access an outside line.

Short Codes (IP)

A Line Short Code is similar to a User Short Code in that it performs the function on that line only. A Line Short Code is performed once the specific Line has been accessed. See Understanding Short Codes .

- **To add a Short Code:**
  Place the cursor over the Short Code List Box and double-click or right-click and select **Add**.

VoIP (IP)

This tab is used for configuring the VoIP operation of an IP line. The following fields are available for configuration:

- **Gateway IP Address:** *Default = Blank*
  Enter the IP address of the remote Control Unit.
- **Voice Pkt. Size:**
  This is the number of data bytes contained in a Voice Packet. This is automatically defaulted to match the Compression Mode selected.
- **Compression Mode:** *Default = Automatic Selection*
  This defines the type of compression which is to be used on any Voice call on this Line.
  - **Automatic Selection** - During call setup the IP Office negotiates the compression mode using the following order of preference: G729a, G.723.1, G711 ALAW, G711 ULAW.
  - Other available options are: Transparent 64K, G.711 ALAW 64K, G.711 ULAW 64K, G.729(a) 8K CS-ACELP, G.729 Simple, G.723.1 6K3 MP-MLQ, NetCoder 8K, G726 ADPCM 32K, G.726 ADPCM 16K.
- **H450 Support:** *Default = H450*
  Selects the supplementary service signaling method for use across H.323 connections. Options are None, QSig and H450. Note that the selected method must be supported by the remote end. For IP Office to IP Office connections H450 is preferred.
- **Silence Suppression:** *Default = Off*
  When selected H.323 terminals will not send data if they are silent, this is useful when optimizing data traffic.
- **Enable FastStart:** *Default = Off*
  A fast connection procedure. Reduces the number of messages that need to be exchanged before an audio channel is created.
- **Fax Transport Support:** *Default = Off*
  When selected this option will provide support for faxing over a H.323 connection to another IP Office with the same setting.
- **Local Hold Music:** *Default = Off*
  When selected H.323 terminals use their own hold music.
- **Local Tones:** *Default = Off*
  When selected H.323 terminals use their own ringing tones. For IP401 Control Units this should be switched on.
- **Enable RSVP:** *Default = Disabled (Greyed out)*
  Use this option to turn RSVP support on or off. Note that the default firewall profile settings if applied drop RSVP.
- **Out of Band DTMF:** *Default = On*
  When on, DTMF is sent as a separate signal rather than as part of the encoded voice

stream ("In Band"). This is recommended for low bit-rate compression modes such as G.729 and G.723 where DTMF in the voice stream can become distorted.

- **Allow Direct Media Path:** *Default = On*
  When disabled the media (voice) path always passes through the Control Unit. When enabled the remote end may be told of a new IP address for the media path if for example the call is transferred to a H.323 extension. Enabling this option may cause some vendors problems with changing the media path in mid call.
- **Voice Networking:** *Default = Off*
  Also known as "Small Community Networking". This option enables extension number sharing with the remote IP Office system. Extensions on the remote system can then be dialed from the local system.
    - Note: This requires that extension numbers and names on the two systems are unique. Line and group extension numbers are not shared. Remote extension numbers cannot be included in local groups.
    - Full operation requires H450 Support to be enabled over the links used.

Control Unit Form

Control Unit Form

The Control Unit configuration form gives the specifications for each device connected to the system. This includes modules installed in the Control Unit as well as external expansion modules.

For most units, this information is allocated by the system and is not configurable. The fields displayed are:

- **Device Number:**
  This is automatically allocated by the system.
- **Unit Type:**
  The name of the device, eg. ***IP403***, ***ANALOGUE POTS2***, ***DIGITAL DT 8***.
- **Version:**
  The version of software running on each unit.
- **Serial Number:**
  This is the number the system uses to tie a physical Control Unit to a device configuration (device number). For the Control Unit and WAN3 modules this is the MAC address. For a device connected to an Expansion port it is the Expansion port number plus 1.
- **Unit IP Address:**
  This field should be blank except for the Control Unit and any WAN3 modules installed. Do not change the Control Unit entry (if this is necessary, it should be done via the System form). If the WAN3 module has not obtained an IP address by DHCP, then an entry can be made here for the WAN3.
- **Interconnect Number:**
  The Expansion port used to connect to this device.
- **Interconnect Class:**
  The type of interconnection used between this device and the Control Unit, eg. CPU (itself), TDMInterconnect (Expansion Bus), etc.

Extension Form

Extension Form Overview

Extensions refer to physical telephone ports, their characteristics and connection. The Manager configuration tree displays the list of physical extensions available on the system. Only an IP extension can be manually created.

Users are the people who use the system and Dial In users for data access. A system User does not have to have an Extension Number that physically exists - this can be useful if the user does not require their own extension but does require to use other system features such as Voicemail, call forwarding, etc.

By default, each Extension is associated with a User. The User Name is used to identify the caller in the display of suitable phones and PC programs. These User Names can be changed via the User Form.

Physical extensions are associated with an extension number through their Extension Form . A User is associated to that extension, by setting that extension number in their User form.

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 Extension configuration form allows you to configure the operation of each physical telephone extension.

The following tabs contain configurable information for this form:

- Extn
- VoIP - Only available when a new extension is created.

Extn

Within this tab, the following fields are configurable:

- **Extension ID:**
  The physical ID of the extension port. This parameter is only configurable with an IP extension. With all other extensions, it is allocated by the system and therefore not configurable.
- **Extension:**
  This is the logical extension number and can be up to 9 digits long.
- **Caller Display Type:** *Default = CallerDisplayOn*
  Controls the presentation of caller display information. See Caller Display.
  - **Off:** Disables caller display.
  - **On:** Enables caller display using the caller display type appropriate to the System Locale, see Supported Country and Locale Settings. If a different setting is required it can be selected from the list of supported options. Note: If the line coming in does not support call display and you have this field ON, it will cause a 3 seconds delay between the time the caller hears a ringing tone and when the actual phone at the called extension will ring.
  - To use a standalone Caller Display Control Unit on an extension, set the caller display of that extension to FSKD.
  - For an analog extension connected to a fax server or other device that requires the pass through of DTMF tones, select DTMFB. See Configuring Personal Fax Numbers.
- **Equipment Classification:** *Default = Standard Telephone*
  Select the type of terminal that is connected to the extension port.

- **Standard Telephone:** Use for normal telephone extensions.
- **Paging Speaker:** When enabled this Extension can be used for connection to a paging amplifier. When the Extension is called, no ringing is generated and the call is answered immediately. (When returning this extension back to a standard analog extension the Phone module must also be rebooted.)
- **Quiet Headset:** Use for headset devices attached to PC's.
- **IVR Port:** Provides a disconnect clear signal to the attached device at the end of calls. This is required by some third party devices. When selected the **Disconnect Pulse Width** is displayed and can be adjusted if necessary.

- **Hook Persistency:** *Default = 100ms*

Defines the time frame (in milliseconds) in which the system will wait before determining that the phone is off-hook.

- **Flash Hook Pulse Width:**
  - **Use System Defaults:** *Default = Selected (On)*
    Use the values set as appropriate to the system's Locale.
  - **Minimum Width:**
    Minimum hook flash length sent if **Use System Defaults** is not selected.
  - **Maximum Width:**
    Maximum hook flash length sent if **Use System Defaults** is not selected.
- **Message Waiting Lamp Indication Type:** *Default = None*
  This option is grayed out except for analog extensions. When set to **On** allows the sending of message waiting lamp indication to an analog extension. Due to the number of methods of message waiting indication (mwi) used by different manufacturers, this operation cannot be guaranteed with all analog phones.
  - The IP Office currently only supports lamps using 81V dc signaling. Some analog phones use 90V dc signaling.
- **Reset Volume after Calls:** *Default = None*
  Reset the phone volume after each call.

VoIP

This tab is available when a new IP Extension is created manually. See Voice over IP - Overview.

The following fields are available for configuration:

- **IP Address:**
  Enter the IP address of the H.323 terminal. The default entry accepts connection to any address.
- **Voice Pkt. Size:** *Default = 80*
  This is the number of data bytes contained in a Voice Packet. This is automatically defaulted to match the Compression mode selected.
- **Compression Mode:** *Default = Automatic Selection*
  This defines the type of compression which is to be used on any Voice call on this Line.
  - **Automatic Selection -** During call setup the IP Office negotiates the compression mode using the following order of preference: **G729a**, **G.723.1**, **G711 ALAW**, **G711 ULAW**.
  - Other available options are: **Transparent 64K, G.711 ALAW 64K**, **G.711 ULAW 64K**, **G.729(a) 8K CS-ACELP**, **G.729 Simple, G.723.1 6K3 MP-MLQ, NetCoder 8K, G726 ADPCM 32K, G.726 ADPCM 16K.**
- **MAC Address:** *Default = 000000000000*
  Enter the hardware address of the H.323 terminal. The default entry accepts connection to any terminal.
- **Silence Suppression:** *Default = Off*
  When selected H.323 terminals will not send data if they are silent, this is useful when optimizing data traffic.
- **Enable Fast Start:** *Default = Off*
  A fast connection procedure. Reduces the number of messages that need to be exchanged before an audio channel is created.
- **Fax Transport Support:** *Default = Off*
  When selected this option will provide support for faxing over a H.323 connection to another IP Office with the same setting.
- **Local Hold Music:** *Default = Off*
  When selected H.323 terminals use their own hold music.
- **Local Tones:** *Default = Off*
  When selected H.323 terminals use their own ringing tones. For IP401 Control Units this should be switched on.
- **Enable RSVP:** *Default = Disabled (Greyed out)*
  Use this option to turn RSVP support on or off. Note that the default firewall profile settings if applied drop RSVP.
- **Out of Band DTMF:** *Default = On*
  When on, DTMF is sent as a separate signal rather than as part of the encoded voice stream ("In Band"). This is recommended for low bit-rate compression modes such as G.729 and G.723 where DTMF in the voice stream can become distorted.
- **Allow Direct Media Path:** *Default = On*
  When disabled the media (voice) path always passes through the Control Unit. When enabled the remote end may be told of a new IP address for the media path if for example the call is transferred to a H.323 extension. Enabling this option may cause some vendors problems with changing the media path in mid call.

User Form

User Form Overview

Users are the people who use the system and Dial In users for data access. A system User does not have to have an Extension Number that physically exists - this can be useful if the user does not require their own extension but does require the use of other system features such as Voicemail, call forwarding, etc.

By default, each Extension is associated with a User. The User Name is used to identify the caller in the display of suitable phones and PC programs. These User Names can be changed via the User tab within the User Form.

Physical extensions are associated with an extension number through the Extension Form. A User is associated to that extension by setting that extension number in their User form.

Aside from the standard user, the system also recognizes the following user set up:

- **No User:** Used to apply settings to extensions which have no associated user.
- **Remote Manager:** Used as the default settings for dial in connections.
- **Hot Desking User:** Users with a **Login Code** set within this User form's Telephony tab. This user can use this login code to log onto his extension (and all its associated settings) from any telephone - Hot Desking.

When a new user is created:

- Newly created users are automatically logged into their handsets, provided that the **Forced Login** user configuration parameter is disabled.
- Any calls in progress when the handset is repossessed on completion of the merge now belong to the new user.
- If this is not the behaviour required, then the **Forced Login** parameters should be enabled, and the new user must log into their phone manually.

When a user is deleted:

When a user is deleted, any calls in progress with this user continue without interruption. The owner if the call is transferred to the **NoUser** system user. When the call drops, the call is reported in the call log event stream as originating/terminating at **NoUser**. The handset reports **Not Logged In** when the user is deleted.

Merging the deletion of a user causes all references to that deleted user to be removed from the system. This includes:

- DSS keys set to User.
- Presence on a coverage list.
- Diverts to this user.
- Incoming call routes to this target.
- Hunt group membership.
- Internal auto-attendant transfers.

Note that if the user is logged onto IP Office Phone Manager and/or SoftConsole, the deleted user must terminate and then restart these applications manually utilizing the new user configuration.

Changing a user's extension:

Changing a user's extension automatically logs the user out of their current extension and into their new extension provided that this new extension exists and **Forced Login** is not enabled. If **Forced Login** is enabled, then the user remains on the current extension being used until the user logs out.

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.

The following tabs contain configurable information for the User form:

- User
- Voicemail
- DND
- ShortCodes
- SourceNumbers
- Telephony
- Forwarding
- DialIn
- VoiceRecording
- Digital Telephony/Button Programming
- Coverage

User

Users are the people who use the system or are Dial In users for data access. A system User may or may not have an Extension Number that physical exists - this is useful if users do not require a physical extension but wish to use system features, eg. Voicemail, forwarding etc. See Extension versus User .

- **No User** is used to apply settings to extensions which have no associated user.
- **Remote Manager** is used as the default settings for dial in connections.

The following fields are configurable within the User tab:

- **Name:**
  This is the user's account name, eg. "JohnB" and the one that will be used for RAS Dial In, Caller Display and voicemail mailbox. As the display on Caller Display telephones is normally only 16 digits long it is useful to keep the name short. Only alphanumeric characters and space are supported in this field. Do not use punctuation characters such as #, ?, /, -, _ and ,. This field is case sensitive and must be unique.
  - **Voicemail uses the name to match a user to their mailbox. Changing a user's name will route their voicemail calls to a new mailbox.**
- **Password:** *Default = Blank*
  This password is required when the User has Dial In access, or wishes to monitor/control their Extension with Phone Manager and TAPI applications.
- **Confirm Password:**
  This is used to check that the password entered in the Password field has been entered correctly. A warning message requesting you to re-confirm the password is generated if the Password and the Confirm Password fields differ.
- **Full Name:** *Default = Blank*
  Use this field to enter the entire user's name. The Phone Manager Directory uses this information when the Show Users option is checked and also appears in the title bar of Phone Manager.
- **Extension:**
  Any number up to 9 digits. In general all extensions should have the same number of digits. If left blank then this User has no Extension and is just a Dial In user.
- **Locale:** *Default = Blank*
  On an analog extension this option configures the language used by voicemail prompts to the user (assuming that language is available on the voicemail server). On a digital extension it also controls the display language used on the telephone. See Supported Country and Locale Settings.
- **Priority:** *Default = 5, Range 0 (Lowest) to 5 (Highest)*
  This setting is used by Least Cost Routing to determine which routes the user can use.
- **Restrictions:** *Default = None*
  Sets which set of User Restrictions applies to the user. See User Restrictions.

Voicemail

If a Voicemail Server application is being used on your system, each user has use of a Voicemail box. You can use this form to enable this facility and various user voicemail settings.

The following fields are configurable within the **Voicemail** tab.

- **Voicemail Code:** *Default = Blank*
  A code (1-15 digits) used by the Voicemail Server to validate access to this User's Voicemail box. This is required when users retrieve Voicemail messages remotely, ie. from another user's extension or from an external telephone, eg. a mobile. If remote access is attempted and a Voicemail Code has not been configured the message "Remote access is not configured on this mailbox" is played.
    - **Confirm Voicemail Code:**
      The Voicemail Code must be retyped to ensure it has been correctly entered.
- **Voicemail Email:** *Default = Blank*
  When a new Voicemail message is received by the user, the WAV file created can be sent to an email account. Enter the email address to be used by the Voicemail Server, eg. jbloggs@bloggs.com. This address is passed to the MAPI interface on the Voicemail Server.
    - Refer to the "Voicemail Installation & Administration Manual" for further details. This setting is not required for IMS operation.
- **Voicemail Reception:** *Default = Blank*
  When connected to a User's Voicemail the caller can press 0 to be transferred to either an internal number, eg. Reception or to an external number, eg. a mobile. Enter here the telephone number to be used. The User should announce this facility in their greeting message, eg. "John Smith is not available today, you may leave a message or press 0 for Reception".
- **Voicemail On:** *Default = On*
  Controls if Voicemail is available for this extension.
- **Voicemail Help:** *Default = Off*
  When retrieving Voicemail messages users can be given a recorded message helping them to use the Voicemail facility - "For help at any time press 8." This option turns this facility on or off.
- **Voicemail Ringback:** *Default = Off*
  When enabled and a new message has been received, the Voicemail server calls the User's extension to attempt to deliver the message each time the telephone is put down. Voicemail will not ring the extension more than once every 30 seconds.
- **Voicemail Email Reading:** *Default = Off*
  When you log into you voicemail box, it will detect your email messages and read them to you. This email text to speech feature is set-up through Voicemail Pro. Refer to the "Voicemail Installation & Administration Manual" for further details.
- **Voicemail Email Mode:** *Default = Off*
  Controls the method of operation of Voicemail Email above. These settings are not used by IMS.
    - **Off:** Do not automatically send a new message to the email account
    - **Copy:** Copy all messages to the email account
    - **Forward:** Forward all messages to the email account and delete from the Voicemail Server.
    - **Alert:** Send an email message without attaching the Voicemail file. This may be used with Email gateways to Pagers or Mobile telephone Short Message Services. Includes the caller's **Caller ID** if available.

DND

This is the ability to temporarily stop incoming calls to a user's telephone. It prevents the user from receiving Hunt Group calls and give direct callers either busy or Voicemail if available. (Note that if Call Forwarding and Do Not Disturb are active, the call is not forwarded, but does receive Voicemail). This can be enabled/disabled by dialing short codes or via the Phone Manager application.

If, however, specific numbers are required to override Do Not Disturb, internal and external phone numbers can be added to an exception list.

See Do Not Disturb for default short codes relating to DND.

The following fields are configurable within the **DND** tab:

- **Do Not Disturb Exception List:** *Default = Blank*
  This is the list of telephone numbers that are still allowed through when Do Not Disturb is set, eg. this could be an assistant or an expected phone call. Internal extension numbers or external telephone numbers can be entered.

To add a telephone number to the **Do Not Disturb Exception List**, do the following:

1. Right-click within the Telephone Number box and select **Add**.
2. Enter the telephone number to be exempt from the Do Not Disturb feature.
3. Click **OK**.

If you wish to add a range of numbers, you can either enter each number separately or make use of the variables "N" or "x" in the number, eg. to allow all numbers from 7325551000 to 7325551099, the DND Exception number can be entered as either 73255510xx or 73255510N.

- **Do Not Disturb:** *Default = Off*
  When checked the Extension is considered busy, except for calls coming from sources listed in the Exception List above.

Short Codes

When a Short Code is entered into this list, it operates on behalf of the User's extension only. See Understanding Short Codes for full discussion of short codes.

- **To add a Short Code:**
  Place the cursor within the Short Code List Box, then double-click or right-click and select **Add**.

Note: Short codes of the form ***DSS** relate to entries in the Button Programming tab and should be altered from that tab.

Source Numbers

Use this tab to create "trusted locations" for data and/or voicemail access. For example, a user dialing in from home or accessing to Voicemail without a Voicemail code is making use of trusted locations. to These are locations that the System allows either data access, eg. a user dialing in from home, or access to Voicemail without a Voicemail Code, eg. a user collecting his Voicemail messages from a cell phone, or the location the Voicemail Server calls to inform the user of a new message. See Trusted Locations for more information. Note that external numbers used as source numbers must provide CLI.

The Telephone Number field is available for configuration within the **Source Numbers** tab:

- **Telephone Number:** *Default = V plus own extension number*
  Right-click within the Telephone Number box and select **Add** to enter a telephone number. The following letter-based codes are available to create source numbers:
  - **V<*Callers CLI*> = Voicemail Trusted Source access**
    Allows access to the user's mailbox for a specified CLI number, eg. V201 or V7325551237. The default is the user's own extension number but additional numbers may be added. *Note: Only supported by Voicemail Lite and Voicemail Pro using IP Office mode.*
  - **R<*Caller's CLI*> = Dial in access**
    To allow data access only from a specified number prefix the number with a "R", eg. R7325551234
  - **H<*Group Name*> = Hunt Group Voicemail Indication**
    Allows the user to receive message waiting indication of new group messages. Enter **H** followed by the group name, eg. **HMain**.
    - On suitable display extensions, the hunt group name and number of new messages is displayed (refer to the appropriate telephone user guide).
    - If the user is using Phone Manager, the Messages tab shows the hunt group name and number of new messages.
    - If the user is not a member of the group, a voicemail code must be set for the group's mailbox (see **Voicemail Code** on the **Hunt Group | Voicemail** tab). Refer to the Voicemail Installation & Administration Manual.
  - **P<*Telephone Number*> = Voicemail Ringback Number**
    For user's with voicemail ringback enabled, this entry sets the ringback destination to a number other than the user's own extension. The voicemail server will ring that number when the user has a new voicemail message. Enter **P** followed by the telephone number including any necessary external dialing prefix, eg. ***P917325559876***. This facility is only available when using VoiceMail Pro through which either a default Callback start point or a user specific Callback start point has been setup.
  - **eConsole = eConsole User Return Calls**
    This option has been replaced by **Transfer Return Time** in the **User | Telephony** settings.

User Telephony

This form allows you to set telephony related features per user. These override the settings in the Telephony tab of the System configuration form.

For details of the ringing tones, see Ring Tones. ***DefaultRing*** uses the system default setting set through the **System | Telephony** tab.

The following fields are configurable within this **Telephony** tab:

- **Outside Call Sequence:** *Default = Default Ring*
  Sets the Outside call pattern for the User.
- **Inside Call Sequence:** *Default = Default Ring*
  Sets the Inside call pattern for the User.
- **Ring Back Sequence :** *Default = Default Ring*
  Sets the Ring Back call pattern for the User.
- **Allocated Answer Interval (secs):** *Default = Blank*
  Leave blank to use the System Default **Allocated Answer Interval** (default 15 seconds). This determines the amount of time a call rings at the extension before going to Voicemail and the amount of time a call rings at the extension when auto callback has been invoked.
- **Wrap-up Time (secs):** *Default = 2 seconds*
  Specifies the amount of time before the user can take another call. You may wish to increase this in a "call center" environment where users may need time to log call details before taking the next call. If set to 0 the user does not receive any calls. It is recommended that this option is not set to less than the default of 2 seconds. See Set Wrap Up Time.
- **Transfer return Time (secs):** *Default = Blank*
  Sets the delay after which any call transferred by the user, which remains unanswered, should return to the user. Settable up to 180 seconds.
- **Login Code:** *Default = Blank*
  The code that has to be entered, as part of the Extension Login sequence, to allow a User to make use of any telephone as if it was theirs. This Login Code can be used for Hot Desking as well as loging back onto your phone after it has been used by a hot desker. See Hot Desking.
  This entry must be at least 4 digits for DT or DS users.
- **Login Idle Period (secs):** *Default = Blank (Off)*
  If the telephone is not used for this period, the user currently logged in is automatically logged off. This option should be used only in conjunction with **Force Login** (see below).
- **Monitor Group:** *Default = Blank*
  Sets the Hunt Group the User can monitor. See How to Monitor Calls.
- **Phone Manager Type:** Default = Lite
  Determines the mode in which the user's copy of the Phone Manager application will operate. Modes are Lite, Pro and VoIP. Note that the number of users able to simultaneously use Pro and VoIP modes is controlled by licenses.
- **Call Waiting On:** *Default = On*
  Call waiting attempts to give the user a tone to indicate other calls are waiting. See Call Waiting.
- **Answer Call Waiting on Hold (Analog):** *Default = On*
  Applies to analog extension users only. If the user has a call waiting and places their current call on hold, the call waiting is automatically connected.
- **Busy on Held:** *Default = On*
  If on, when the user has a call on hold, new calls receive busy tone (ringing for incoming analog call) or are diverted to voicemail if enabled, rather than ringing the user. Note this overrides call waiting when the user has a call on hold.
- **Outgoing Call Bar:** *Default = Off*
  Stops external calls from this User's extension. See Call Restriction.

- **Offhook Station:** *Default = Off*
  Indicates whether this extension is used with a hands free or standard handset.
- **Can Intrude:** *Default = Off*
  Check this option if the User can interrupt other user's calls. See Call Intrusion.
- **Cannot be Intruded:** *Default = On*
  If checked, this user's calls cannot be interrupted or acquired.
- **Directory Exclude:** *Default = Off*
  If checked, the user does not appear in the directory list in Phone Manager and suitable telephones.
- **Force Login:** *Default = Off*
  If checked, the user must login to an extension using the **Login Code** created within this tab. For example, if **Force Login** is ticked for User A and after User B has logged off (having used User A's phone for Hot Desking), then User A must log back onto his extension to make use of the phone. If Force Login is not ticked, then after User B logs off, User A's extension will automatically be logged back on.
- **Force Account Code:** *Default = Off*
  If checked, the User must enter an Account Code to make an external call. See Account Codes.
- **System Phone:** *Default = Off*
  Allows the user (on 2030, 2050 telephones and 4400/4600/6400 series phones with a Menu key) to alter the date and time displayed on all phones. On 2030/2050 phones this is then accessed by selecting **Setup** on the display. On other phones it is accessed by pressing **Menu | Menu | Func | Setup**. Also allows SoftConsole users to use the SoftConsole **Send Message** function.
- **Remote Homeworker/Agent:** *Default = Off*
  Select if the user has been configured as a remote extension on an Avaya INDeX telephone system. Refer to INDeX Level 10 documentation for full details. Only available in Locales where INDeX may also be supported.
- **Book a Conferencing Center in Phone Manager:** *Default = Off*
  When enabled, displays links in the user's Phone Manager application for access to Conferencing Center. Note that to book a conference requires the user to have a Conferencing Center user ID and password.
- **Can Accept Collect Calls:** *Default = Off* [PTB Only]
  Determines whether the user is able to receive and accept collect calls.

Forwarding

This is the ability to forward a user's calls to another extension or external number. Calls can be forwarded when there is no answer, when the extension is busy or for all calls. This can be enabled/disabled by dialing short codes or via the Phone Manager application. See Call Forwarding for call forwarding related short codes.

The following fields are configurable within the **Forwarding** tab:

- **Follow Me Number:** *Default = Blank*
  All calls are redirected to the extension number entered. If the redirected call fails or is not answered then the call behaves as though this User's extension had failed to answer, eg. the Forward settings take effect or voicemail is used.
- **Forward Unconditional:** *Default = Off*
  All calls, except group calls, are forwarded to the Forward Number set below.
- **Forward Number:** *Default = Blank*
  The telephone number to which calls are to be forwarded when **Forward Unconditional** is on. This may be an internal or external number, eg. a cell phone.
- **Forward On Busy:** *Default = Off*
  Calls are forwarded to the number set below the user's extension is busy.
- **Forward On No Answer:** *Default = Off*
  Calls are forwarded to the number set below when the user's extension is does not answer within their set No Answer time.
- **Forward Number:** *Default = Blank*
  The number to which calls are forwarded when **Forward On Busy** and/or **Forward On No Answer** are on.
- **Forward HuntGroup Calls:** *Default = Off*
  If the user is a member of a hunt group, the hunt group call can also be forwarded if required. The group's **Ring Type** must be ***Hunt*** or ***Rotary*** (not ***Group*** or ***Idle***). This option only forwards hunt group calls when **Forward Unconditional** is also on and use the same **Forward Number** as **Forward Unconditional**. The call is only forwarded to this number for the period defined by the hunt group's **No Answer Time** after which it returns to the hunt group.

Dial In

Use this dialogue box to enable dial in access for a remote user. An Incoming Call Route and RAS service must also be configured.

The following fields are configurable within the **Dial In** tab:

- **Dial In On:** *Default = Off*
  When enabled, dial in access into the system is available via this User account.
- **Dial In Time Profile:** *Default = Blank*
  Select the Time Profile applicable to this User account. A Time Profile (configured via the Time Profile configuration form) can be used to set time restrictions on dial in access via this User account. Dial In is allowed during the times set in the Time Profile form. If left blank, then there are no restrictions.
- **Dial In Firewall Profile:** *Default = Blank*
  Select the Firewall Profile to restrict access to the system via this User account. If blank, there are no Dial In restrictions. Firewall profiles are created in the Firewall Profile configuration form.

Voice Recording

This tab is used to activate the automatic recording of user's external calls. The recordings are placed in the user's mailbox. This requires Voicemail Pro to be installed and running.

The following fields are configurable within the **Voice Recording** tab:

- **Record Outbound:** *Default = None*
  Select whether outgoing calls are recorded. Options for recording are:
  - **On:** Record the call if possible.
  - **Mandatory:** If not possible to record, return busy tone to the caller.
  - **Percentages of calls:** Various percentages of calls made by the user will be recorded.
- **Record Inbound:** *Default = None*
  The same as Record Outbound but applied to inbound calls to the user.
- **Record Time Profile:** *Default = Blank*
  Used to select a time profile during which calls are recorded.
- **Auto Recording Mailbox:** *Default = <user's own mailbox>*
  Sets the mailbox into which automatically triggered recordings are placed.
- **Manual Recording Mailbox:** *Default = <user's own mailbox>*
  Sets the mailbox into which recordings triggered by the user are place.

Coverage

Call coverage allows calls ringing at one extension (the 'Sender') to also be presented and answered at other defined extensions (the 'Covering Extensions'). See Call Coverage for more information.

- **Covering Extension:**
  The number of the extension that will be receiving the calls from the selected extension.
- **Covering User:**
  This is the user's account name associated with the covering extension.

To add a covering extension:

1. Right-click within the **Coverage** window and select Add.
2. Choose from the list of extension/users.
3. Click **OK**.

Button Programming/Digital Telephony

If the system locale for Manager is set to **enu**, then the tab is labeled as **Digital Telephony**. If the system locale is set to **en**, then the tab is labeled as **Button Programming**. Regardless of the label,the feature has the same functionality.

This tab is currently used to assign functions to the DSS keys of DT, DS and IP telephones. See Installing and Configuring DT Ports and Installing and Configuring DS Ports

- **Note:** Though set through this tab, short codes of the form *DSS1 appear in the User's Short Codes tab. Any changes to those short codes are ignored and overwritten by the contents of the Button Programming tab.

The following settings are available within the **Button Programming/Digital Telephony** tab:

- **Button:**
  The number of the DSS key against which the function is being set. See Button Numbering Layout.
  - ***Menu1*** to ***Menu12*** can be used to override the default display softkey features accessed by pressing **Menu** on suitable 4400, 4600 and 6400 Series telephones.
- **Action:**
  Provides the following:
  - **Dial**:
    This is effectively an Abbreviated Dial. The only difference is that the LED illuminates for the duration of the call, giving the User some feedback as to what was pressed. The dial string administered for this button may be a partial dial string.
  - **Group**:
    Monitor the status of a Hunt-group queue. Flashes Green if a call is incoming to the group, flashes Red if the queue is backing up. Press to show call information, press again to pickup call. Put the name of the group, surrounded by quotes, in the Telephone Number field. This feature only works for groups with queuing enabled.
  - **Park**:
    Monitor a park slot. Monitor a park slot. The green LED is lit if the park slot is occupied by a call parked by the station with the programmed PARK BLF button. The red LED is lit if the park slot is occupied by a call parked by another station. If you are the user who parked the call, or have a 406D+ or 4606D+ station, pressing this button reconnects you to the call. If another party parked the call and you do not have a 4406D+ or 4606D+ station type, pressing this button once provides call information and a menu, and pressing the button a second time connects you to the call. Selecting **Answr** from this menu will also pickup the call.
  - **User:**
    Monitor a user. This is a Busy-Lamp-Field. Put the name of the person, surrounded by quotes, in the Telephone Number field. Note: When the other party is busy on a call, **DSS Status** (on the **System | System** tab) control whether you see details of the user's call.
  - **Emulation:**
    See Emulation Functions .
  - **Advanced:**
    These are short code features that can be assigned to DSS keys. For details of the individual functions, see Short Code Features . TransTalk 9040 MDW sets must access these features through normal dialed short codes.
  - **Telephone Number:**
    The telephone number associated with the action or parameters required by the action. Refer to details of the particular feature for information about required values.

Emulation Functions

Emulation Functions

These functions can be assigned to DSS keys on 4400, 4600 and 6400 Series phones. Where supported, they emulate the action of the same feature when selected on other non-IP Office Avaya telephone systems.

- **Supported Functions:**
  Those features listed as Not supported can be assigned to a DSS key but have no equivalent function on the IP Office. However they can be configured and a CTI application can then override the display. For example, "Stats" could be configured as a soft key and a CTI application run to override it and display suitable agent statistics.

For each emulation function, various features can apply. Depending on the function, the following features will be available, where some will require information to be entered:

- **Telephone Number:**
  Data required by the feature when setup.
- **Button Programming:**
  Path to feature when applying to a DSS button.
- **DSS Toggles:**
  The DSS key reverses the feature when pressed again.
- **Label:**
  Name shown against DSS key if set on 4620 telephone.
- **User Program:**
  Indicates whether the feature can be programmed against keys by the user if their phone has been programmed with access to the **Admin** (Self-Administer) function.
- **Function Number:**
  Definity feature number.
- **Default Softkey:**
  Is the feature a default softkey display feature accessed by pressing **Menu** on suitable 4400, 4600 and 6400 Series phones.
- **9040:**
  Is the feature supported on the TransTalk MDR 9040.

Abbreviated Dial

This allows one touch dialing of a stored number.

- **Telephone Number:** Telephone number or partial telephone number.
- **Button Programming:** Emulation | Abbreviated Dial.
- **Label:** AD **User Program:** Yes.
- **Function Number:** 129. **Default Softkey:** No. **9040:** No.

Abbreviated Dial Pause

Not supported. Allows a user to enter a pause character when programming an abbreviated dial.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Abbreviated Dial Pause.
- **Label:** Pause. **User Program:** No.
- **Function Number:** 130. **Default Softkey:** No. **9040:** No.

Abbreviated Dial Program
Allows a user to program abbreviated dialing numbers against other DSS keys.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Abbreviated Dial Program.
- **Label:** Prog. **User Program:** Yes.
- **Function Number:** 7. **Default Softkey:** No. **9040:** No.

Abbreviated Dial Stop
Not supported. Allows a user to enter a stop character when programming an abbreviated dial.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Abbreviated Dial Stop**.**
- **Label:** Stop. **User Program:** No.
- **Function Number:** 148. **Default Softkey:** No. **9040:** No.

Appearance
Allows a user to have a visual appearance of calls that are made and received.

- **Telephone Number:** Optional. Text entered appears on the call appearance display line of 2420 and 4620 when idle.
- **Button Programming:** Emulation | Appearance.
- **Label:** Appear. **User Program:** Yes.
- **Function Number:** –. **Default Softkey:** No. **9040:** Yes.

Account Code Entry
Enter an account code for a call.

- **Telephone Number:** Optional. If an code is entered, it must match an account code set in the account codes list. If no account code is entered, the phone display will request entry of a valid code.
- **Button Programming:** Emulation | Account Code Entry.
- **Label:** Acct. **User Program:** Yes.
- **Function Number:** 128. **Default Softkey:** No. **9040:** No.

ACD Agent Statistics
Not supported.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | ACD Agent Statistics.
- **Label:** Stats. **User Program:** No.
- **Function Number:** 147. **Default Softkey:** No. **9040:** No.

ACD Stroke Count
Not supported.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | ACD Stroke Count.
- **Label:** Count. **User Program:** No.
- **Function Number:** 135. **Default Softkey:** No. **9040:** No.

AD Special Function Mark
Not supported. Allows a user to enter a mark character when programming abbreviated dial.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | AD Special Function Mark.
- **Label:** Mark. **User Program:** No.
- **Function Number:** 142. **Default Softkey:** No. **9040:** No.

AD Special Function Wait
Not supported. Allows a user to enter a Wait for Dial Tone character when programming an abbreviated dial.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | AD Special Function Wait.
- **Label:** Wait. **User Program:** No.
- **Function Number:** 149. **Default Softkey:** No. **9040:** No.

AD Special Functions
Not supported. Allows a user to enter a special character (mark, pause suppress, wait) when entering an abbreviated dial.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | AD Special Functions.
- **Label:** Sfunc. **User Program:** No.
- **Function Number:** 145. **Default Softkey:** No. **9040:** No.

AD Suppress
Suppresses the display of dialed digits on the telephone display. Dialed digits are replaced with an **s** character.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | AD Suppress.
- **Label:** Spres. **User Program:** Yes. **Toggles:** Yes.
- **Function Number:** 146. **Default Softkey:** No. **9040:** Yes.

Automatic Callback
Initiates a call to an extension automatically when that extension becomes free.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Automatic Callback.
- **Label:** AutCB. **User Program:** Yes. **Toggles:** Yes.
- **Function Number:** 6. **Default Softkey:** Yes. **9040:** No.

Automatic Intercom
Call an extension and have the call answered on speakerphone. Handsfree auto-answer must be supported by the called extension.

- **Telephone Number:** Extension number.
- **Button Programming:** Emulation | Automatic Intercom.
- **Label:** Iauto. **User Program:** No.
- **Function Number:** 139. **Default Softkey:** No. **9040:** Yes.

Call Forwarding All
Forward all calls to a number entered. Alters the users forward unconditional number and forward on busy number.

- **Telephone Number:** Telephone number (optional). If blank, phone will display current setting and allow change.
- **Button Programming:** Emulation | Call Forwarding All.
- **Label:** CFrwd. **User Program:**
- **Toggles:** Yes.
- **Function Number:** 8. **Default Softkey:** Yes. **9040:** No.

Call Park
Allows the user to park their current call.

- **Telephone Number:** Park slot number or blank (park slot number assigned based on parking extension number).
- **Button Programming:** Emulation | Call Park.
- **Label:** CPark. **User Program:** Yes. **Toggles:** Yes.
- **Function Number:** 9. **Default Softkey:** Yes. **9040:** Yes.

Call Park To Other Extension
Allows the user to place their current call against another extension. The parked call indication on that extension is then activated (this varies according to the telephone. The park slot number assigned to the parked call is based on the number of the extension parking the call.

- **Telephone Number:** Extension number.
- **Button Programming:** Emulation | Call Park to Other Extension.
- **Label:** Park. **User Program:** Yes.
- **Function Number:** 143. **Default Softkey:** No. **9040:** No.

Call Pickup
Answer an alerting call in the system.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Call Pickup.
- **Label:** CpkUp. **User Program:** Yes.
- **Function Number:** 132. **Default Softkey:** No. **9040:** No.

Cancel Leave Word Calling
Not supported. Cancels the last Leave Word Calling message originated by the user.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Cancel Leave Word Calling.
- **Label:** CnLWC. **User Program:** No.
- **Function Number:** 133. **Default Softkey:** No. **9040:** No.

Consult
Not supported.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Consult.
- **Label:** Cnslt. **User Program:** No.
- **Function Number:** 134. **Default Softkey:** No. **9040:** No.

Dial Intercom
Call an extension and have the call answered on speakerphone. Handsfree auto-answer must be supported by the called extension.

- **Telephone Number:** Extension number.
- **Button Programming:** Emulation | Dial Intercom.
- **Label:** Idial. **User Program:** No.
- **Function Number:** 140. **Default Softkey:** No. **9040:** No.

Directed Call Pickup
Pickup a call ringing at a specific extension or hunt group.

- **Telephone Number:** Ringing extension or group number.
- **Button Programming:** Emulation | Directed Pickup.
- **Label:** DpkUp. **User Program:** Yes.
- **Function Number:** 136. **Default Softkey:** Yes. **9040:** No.

Directory
Provides access to the system directories of telephone numbers.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Directory.
- **Label:** Dir. **User Program:** Yes.
- **Function Number:** 1. **Default Softkey:** Yes. **9040:** No.

Drop
For alerting calls, pressing the button removes the call from the set. This allows the user to perform other operations at their set. After a few seconds, the call attempts to re-alert the station. For active calls, pressing this button disconnects and clears the call.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Drop.
- **Label:** Drop. **User Program:** Yes.
- **Function Number:** 2. **Default Softkey:** Yes. **9040:** No.

Group Paging
Allows a user to make announcements to a group of extensions. The extensions must support handsfree auto-answer.

- **Telephone Number:** Group number.
- **Button Programming:** Emulation | Group Paging.
- **Label:** GrpPg. **User Program:** Yes.
- **Function Number:** 138. **Default Softkey:** No. **9040:** No.

Inspect
Not supported. Allows users on display phones to determine the identification of held calls. Allows users on an active call to display the identification of incoming calls.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Inspect.
- **Label:** Inspt. **User Program:** No.
- **Function Number:** 141. **Default Softkey:** No. **9040:** No.

Internal Auto-Answer
Sets the user's extension to automatically connect internal calls after a single ring.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Internal Auto-Answer.
- **Label:** HfAns. **User Program:** Yes. **Toggles:** Yes.
- **Function Number:** 3. **Default Softkey:** Yes. **9040:** No.

Leave Word Calling

Not supported. Leaves a message for the user associated with the last number dialed to call the originator.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Leave Word Calling.
- **Label:** LWC. **User Program:** No.
- **Function Number:** 131. **Default Softkey:** No. **9040:** No.

Manual Exclusion

Not supported.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Manual Exclusion.
- **Label:** Excl. **User Program:** No.
- **Function Number:** 137. **Default Softkey:** No. **9040:** No.

Priority Calling

Not supported.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Priority Calling.
- **Label:** Pcall. **User Program:** No.
- **Function Number:** 5. **Default Softkey:** No. **9040:** No.

Ringer Off

Switches the call alerting ring on/off at the user's extension.

- **Telephone Number:** *None*.
- **Button Programming:** Emulation | Ringer Off.
- **Label:** RngOf. **User Program:** Yes. **Toggles:** Yes.
- **Function Number:** 144. **Default Softkey:** No. **9040:** No.

Self-Administer

Allows a user to program features against the DSS buttons on their phone.

- **Telephone Number:** *None or 1.*
  - If no value is set for the telephone number, allows user programming of those Emulation functions marked as **User Program:** Yes.
  - If ***1*** is entered as the telephone number, allows user programming of Dial, Group, Park, User and Hook Flash functions against DSS keys.
- **Button Programming:** Emulation | Self-Administer.
- **Label:** Admin. **User Program:** Yes.
- **Function Number:** 12. **Default Softkey:** Yes. **9040:** No.

Send All Calls
Sets the user's extension into 'Do Not Disturb' mode.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Send All Call.
- **Label:** SAC. **User Program:** Yes. **Toggles:** Yes.
- **Function Number:** 10. **Default Softkey:** Yes. **9040:** Yes.

Stored Number View
Not supported. Allows a user to view on the phone's display the contents of any programmed feature button.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Stored Number View.
- **Label:** BtnVu. **User Program:** No.
- **Function Number:** 150. **Default Softkey:** No. **9040:** No.

Time of Day
Displays the time and date on the user's telephone.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Time of Day.
- **Label:** TmDay. **User Program:** Yes. **Toggles:** Yes.
- **Function Number:** 11. **Default Softkey:** Yes. **9040:** Yes.

Timer
Starts a timer running on the display of the user's extension. Note: The timer disappears when the user end a call.

- **Telephone Number:** *None.*
- **Button Programming:** Emulation | Timer.
- **Label:** Timer. **User Program:** yes. **Toggles:** Yes.
- **Function Number:** 4. **Default Softkey:** Yes. **9040:** No.

Button Numbering Layout

On 4400, 4600 and 6400 Series telephones, the default button layout assigns Call Appearance to the first 3 buttons.

The following tables indicate the button numbered assumed by the IP Office for different telephones. In some cases, this numbering differs from that used for the same sets on other Avaya telephone systems.

As a general rule: Button 1 is the top button on the left-hand column. Buttons numbers then go down the column and then continue at the top of the next column.

4406/4406D+

The following is the button layout for a 4406D+ set.

1	4
2	5
3	6

4412D+/4424D+

The following is the button layout for a 4412D+ or 4424D+ telephone.

1	7	13	19
2	8	14	20
3	9	15	21
4	10	16	22
5	11	17	23
6	12	18	24

4450

The following is the button layout for a 4450.

25	35	45	55	65
26	36	46	56	66
27	37	47	57	67
28	38	48	58	68
29	39	49	59	69
30	40	50	60	70
31	41	51	61	71
32	42	52	62	72
33	43	53	63	73
34	44	54	64	74

75	77	79	81	83
76	78	80	82	84

6400 Sets

6408 = Column 1 only.

6416 = Column 1 and 2 only.

6424 = Whole table.

1	9	17
2	10	18
3	11	19
4	12	20
5	13	21
6	14	22
7	15	23
8	16	24

Hunt Group Form

Hunt Group Overview

A Hunt Group is a collection of users, eg. Sales - a group to handle all sales related calls

An incoming caller wishing to speak to Sales can ring one number but the call can be answered by any number of extensions that are members of the Sales Hunt Group.

Changing the name of a hunt group has the following effects:

- A new empty mailbox is created on voicemail with the new hunt group name.
- Entries in other groups' **Overflow** lists will be updated.
- **Out-of-Service** and **Night-Service** fallback references are updated.

Modifying the extension number of a hunt group updates the following:

- DSS queue monitoring configurations.
- Incoming call routing entries.
- Transfer-target in auto-attendant.

When a hunt group is deleted:

When a hunt group is deleted, all references to the deleted group will be removed including:

- Entry in Incoming call routing table.
- Transfer target in internal auto-attendant.
- Overflow, Night-Service or Fallback-Service on other groups.
- DSS keys monitoring group status.

Note that a group will not be deleted until all calls that were established through calling the hunt group are cleared. In the meanwhile, the group is set to **Out of Service** and any new calls to that group will not be processed. The group is now set in a *Deleting* state. While in this state, updating any setting on the group using Manager or the Installation Wizard will reinstate the group, that is, the *Deleting* state is lost and the group will not be deleted.

For a full overview of hunt groups, see Overview of Hunt Groups.

Hunt Group

The following fields are available for configuration within the **Hunt Group** tab:

- **Name:**
  The name to identify this Hunt Group. It is recommended that only alphanumeric characters with no spaces be used. This field is case sensitive and must be unique.
    - **Voicemail uses the name to match a group and its mailbox. Changing a group's name will route its voicemail calls to a new mailbox.**
- **Extension:**
  The extension number to be used by the Hunt Group. This can be left blank, however, many useful features will not be available, for example, it will not be possible to transfer a call to the Hunt Group or collect Voicemail messages remotely.
- **No Answer Time (secs):** *Default = Blank*
  The number of seconds an extension rings before the call is passed to another extension in the list. This applies to all telephones in this group and the Overflow Groups (if used). If left blank the **System** Default **No Answer Time** will be used.
- **Overflow Time:** *Default = Blank*
  The Overflow Time is the amount of time (in seconds) a call will ring round the Extension List before being passed to the Overflow Group. If all the members in the extension list are busy, this is the amount of time the caller is held in the group queue before being passed to the Overflow Group. See Using Queuing .
- **Call Waiting On:** *Default = Off*
  Only supported by group's set to the **Ring Type** of ***Group***. When on, user's in the group already on a call, receive call waiting indication when a new call rings the group. The user's must also have their own **Call Waiting** setting set to **On**.
- **Hunt Type:** *Default = Group*
  Sets the order in which each extension in a Hunt Group is rung.
    - **Group:** All telephones in the Extension List ring simultaneously.
    - **Hunt:** Each extension is rung in order, one after the other, starting from the first extension in the list each time.
    - **Rotary:** Each extension is rung in order, one after the other. However, the last extension used is remembered. The next call received rings the next extension in the list.
    - **Idle:** The extension that has been unused for the longest period rings first, then the extension that has been idle second longest rings, etc.
- **Extension List:**
  An ordered list of telephone extensions that form the Hunt Group. These telephones ring when the Group is In Service (See the Fallback tab). Repeated numbers can be used, eg. 201, 202, 201, 203 etc. Each extension will ring for the number of seconds defined by the **No Answer Time** before moving to the next extension in the list, dependent on the Ring Mode chosen.
    - **To alter entries:**
      Right-click in the Extension List box and select **Add** from the menu and select the User to be a member of the Hunt Group. CTRL or SHIFT can be used to select multiple entries. Repeated users can be added, eg. 201, 202, 201, 203 etc.
    - To change the order of the Extensions, drag and drop the extension to the required position.
        - To delete an entry, right-click on the required User and select **Delete**.
        - It is also possible to disable a User's membership to a Hunt Group temporarily. Right-click on the User and select Disable. An asterisk appears to the left of the User's name. To reverse this option right-click on the User and select Enable.

- This facility can also be activated via short codes - see Enable/Disable Membership .

- **Overflow Group List:**
  If a call cannot be answered by the extensions shown in the Extension List, the call can be passed to another Hunt Group called an Overflow Group. The Overflow Group acts as a single extension in the Hunt Group. Overflow/Fallback settings relevant to the Hunt Group acting as an Overflow Group will be ignored. Multiple Overflow Groups can be used and a Hunt Group may be added more than once to the Overflow Groups list. To alter entries right-click on the list.

Voicemail

If a Voicemail Server is being used on your system, each Hunt Group can have its own voicemail box. You can use this form to enable this facility (default) and control various hunt group voicemail settings.

- **Voicemail Code:** *Default = Blank*
  A security code (1-15 digits) used by the Voicemail Server. This is required when users retrieve Voicemail messages for this Hunt Group remotely, ie. from an extension not a member of the Hunt Group or from an external telephone, eg. a cell phone.
- **Confirm Password:**
  The Voicemail Code must be retyped to ensure it has been correctly entered.
- **Voicemail Email:** *Default = Blank*
  Messages for this Hunt Group can be sent to an email account. Enter the email address, eg. jbloggs@bloggs.com. Select the required Voicemail Email mode below. The Voicemail message is received by the email application as a .wav file and played through the speakers of the PC. Refer to the Voicemail Installation & Administration Manual for full details. This entry is not used by IMS.
- **Voicemail On:** *Default = On*
  Each Hunt Group can use Voicemail to collect group related messages. Use this option to turn this feature on or off.
- **Voicemail Help:** *Default = Off*
  When retrieving Voicemail messages users can be given a recorded message helping them to use the Voicemail facility - "For help at any time press 8." This option turns this facility on or off.
- **Voicemail Email mode:** *Default = Off*
  If a Voicemail Email address has been entered above, select one of the following modes:
  - **Off:** Voicemail messages or notifications are not sent to the email account automatically.
  - **Copy:** A copy of the Voicemail message is sent to the email account.
  - **Forward:** Voicemail messages are sent to the email account and deleted from the Voicemail server.
  - **Alert:** Notification that a new Voicemail message has been received is sent to the email account.

Fallback

The Fallback Tab allows you to configure what happens to group calls at times when the extensions in the Extension List are not manned, for example, outside of office hours or during a holiday period.

See Using the Fallback Tab .

The following fields are configurable within the **Fallback** tab:

- **Time Profile:** *Default = Blank*
  This field allows selection of a previously created Time Profile (See Time Profile Form). That time profile then specifies the time period within which the Hunt Group is operational. Outside of these hours the group behaves as if in Night Service mode. Please note:
  - The Time Profile does not change the groups Service Mode setting.
  - Short codes cannot be used to override the time profile action.
- **Out of Service Fallback Group:** *Default = Blank*
  Select from the list box a Hunt Group previously created. The Out of Service Fallback Group is used to provide cover when the Hunt Group is in Out of Service mode.
- **Night Service Fallback Group:** *Default = Blank*
  Select from the list box a Hunt Group previously created. The Night Service Fallback group is used to provide cover when the Hunt Group is in Night Service mode.

- **Service Mode:** *Default = In Service*
  Indicates the service mode that the group is currently providing:
  - **Out of Service**
    When selected callers to the group hear busy tone or are passed to voicemail if operational and played the Out of Hours greeting. Alternatively an **Out of Service Fallback Group** can be set to provide cover.
  - **In Service** 
    When selected the Hunt Group is enabled.
  - **Night Service** 
    When selected callers to the group hear busy tone or are passed to voicemail if operational and played the Out of Hours greeting. Alternatively a Night Service Fallback Group can be set to provide cover.

Using Short Codes to Change Group Service Mode
Short code features exist to set and clear night service mode and to set and clear out of service mode. Note that the night service short code features cannot override when the time profile puts the group into night service, they are meant for putting a group in or out of night service mode at times outside its time profile.

The following default short codes can be used for night service mode. No default short codes exist for out of service mode:

- ***20*N#** - Put group ***N*** in Night Service mode.
- ***21*N#** - Take group ***N*** out of Night Service mode.

Queuing

The Queuing feature allows calls to the Hunt Group to be held in a queue when all extensions in the Extension List are busy. When an extension becomes free a queued call is then presented to that extension.

If the system has voicemail operational then queued callers are played queue messages at set intervals.

See Using Queuing .

- **Queuing On** : *Default = On*
  If selected (default) queuing is available for this Hunt Group.
- **Queue Limit:** *Default = Blank*
  This features sets the number of calls that is held in the queue at any one time. If this number is exceeded the caller will hear busy tone or be passed to Voicemail (if operational).
- **Queue Ring Time (secs):** *Default = 10 seconds*
  This facility defines the time (in seconds) before the caller is placed in the queue.

Voice Recording

This tab is used to activate the automatic recording of external hunt group calls. The recordings are placed in the hunt group mailbox. This requires Voicemail Pro to be installed and running.

- **Record Inbound:** *Default = None*
  Select whether inbound calls by group members should be recorded. Options are **On**, **Mandatory** and then various percentages of calls made by the group.
  - **On:** Record the call if possible.
  - **Mandatory:** If not possible to record, return busy tone to the caller.
- **Record Time Profile:** *Default = Blank*
  Used to select a time profile during which calls are recorded.

Short Code Form

Short Code Form

This form is used to create System Short Codes. System short codes allow access to certain phone features by all users on the system. A list of default short codes are provided, but they can be amended and new ones added by the system administrator. Because short codes are very involved and their rules/restrictions apply across several configuration forms, please see Understanding Short Codes and its related topics before creating a short code.

In the panel to the right of the Configuration Tree panel, right-click to add a new short code or select a existing short code and right-click to view, edit, delete or copy one. For each short code, the following fields are available for configuration:

- **Short Code:** The dialing digits used to trigger the short code. Maximum length is 33 characters. See Short Code Characters for a list of valid characters.
- **Telephone Number:** The number dialed by the short code or parameters for the short code feature. This field can contain numbers and characters. For example, it can contain Voicemail Pro start point names, user names, hunt group names and telephone numbers (including those with special characters). Maximum length 33 characters. See Telephone Number Characters for a list of valid characters.
- **Line Group ID:** *Default = 0*
  Enter the identity of the Line that this Short Code will use to make a call.
- **Feature:**
  Select the feature used by the Short Code.
- **Locale:** *Default = Blank*
  This option sets country variations if applicable, eg. Voicemail server prompts. For a list of the locales supported, see Supported Country and Locale Settings.
- **Force Account Code:** When creating a short code that specifies how an outgoing call will be handled, having **Force Account Code** ticked will assert that the dialed number requires an account code before the call is put through. Any existing account code can be used by the user to put the call through. See Force Account Code for more information.

Service Form

Service Form Overview

A Service is configured to provide remote data access for local users. A Service is needed when configuring, for example, connection to an ISP for Internet access or connection to a remote Control Unit via ISDN or via a WAN link.

When creating a new Service, you are given several options:

- A **Normal Service** should be selected when configuring, for example, a connection to an ISP. If this type of service is selected, the following tabs are available:
  - Service
  - Bandwidth
  - IP
  - AutoConnect
  - Quota
  - Fallback
  - PPP
- A **WAN Service** can be selected when creating a WAN link. A User and RAS Service will also be created with the same name. These three entries are automatically linked and each open the same form. Note however, that this type of Service cannot be used if the Encrypted Password option is checked. In this case the RAS Service name must match the Account Name. Therefore either create each entry manually or create an Intranet Service. If a Wan Service is selected, the DialIn configuration tab is available along with the Normal Service's configuration tabs above.
- An **Intranet Service** can be selected to automatically create a User with the same name at the same time. These two entries are linked and will each open the same form. Note that the Dial In tab is now added to the Service configuration form and the Dial In On option is assumed. The User's password is entered in the Incoming Password field at the bottom on the Service tab. An Intranet Services shares the same configuration tabs as those available to the WAN Service.

Service

Fields within this tab enable you to create a service. the following field are available for configuration:

- **Name:**
  The name of the service, eg. Holmdel, Internet etc. It is recommended that only alphanumeric characters be used.
- **Account Name:**
  The User Name that is used to authenticate the connection. This is provided by the ISP or remote system.
- **Password:** *Default = Blank*
  Enter the password that is used to authenticate the connection. This is provided by the ISP or remote system.
    - **Confirm Password:**
      Reenter the password to ensure it has been entered correctly.
- **Telephone Number:** *Default = Blank*
  If the connection is to be made via ISDN enter the telephone number to be dialed. This is provided by the ISP or remote system.
- **Firewall Profile:** *Default = Blank*
  From the list box select the Firewall Profile that is used to allow/disallow protocols through this Service.
- **Encrypted Password:** *Default = Off*
  When enabled the password is authenticated via CHAP (this must also be supported at the remote end). If disabled, PAP is used as the authentication method.
- **Default Route:** *Default = Off*
  When enabled this Service is the default route for data packets (unless a specific route has been created under IP Route). A green arrow appears to the left of the Service in the Configuration Tree. Only one Service can be the default route. If disabled, a route must be created under IP Route.

If you have created a WAN or Intranet Service, the following fields are available:

- **Incoming Password:** *Default = Blank*
  Enter the password that will be used to authenticate the connection from the remote Control Unit. (If this field has appeared because you have created a Service and User of the same name, this is the password you entered in the User's Password field).
- **Confirm Password:**
  Reenter the password to ensure it has been entered correctly.

Bandwidth

These options give the ability to make ISDN calls between sites only when there is data to be sent or sufficient data to warrant an additional call. The calls are made automatically without the users being aware of when calls begin or end. Using ISDN it is possible to establish a data call and be passing data in less that a second. Note: the system will check Minimum Call Time first, then Idle Period then Active Idle Period.

The following bandwidth related configuration fields are available:

- **Minimum No of Channels:** *Default = Blank (1 channel)*
  Defines the number of channels used to connect for an outgoing connection. The initial channel must be established and stable, before further calls are made.
- **Maximum No of Channels:** *Default = Blank*
  Defines the maximum number of channels to can be used. If blank then the number is the same as set in the Minimum Channels field. This field should be blank or contain a value greater than the Minimum Channels field.
- **Extra BW Threshold:** *Default = 50%*
  Defines the utilization threshold at which extra channels are connected. The value entered is a %. The % utilization is calculated over the total number of channels in use at any time, which may be one, two etc.
    - For example, if Minimum Channels set to 1, Maximum Channels set to 2 and Extra Bandwidth set to 50 - once 50% of first channel has been used the second channel are connected.
- **Reduce BW Threshold:** *Default = 10%*
  Defines the utilization threshold at which additional channels are disconnected. The value entered is a %. Additional calls are only dropped when the % utilization, calculated over the total number of channels in use at the time, falls below the % value set, for a time period defined by the Service-Idle Time. The last call (calls - if Minimum Calls is greater than 1) to the Service is only dropped if the % utilization falls to 0, for a time period defined by the Service-Idle Time. Only used when 2 or more channels are set above.
    - For example, if Minimum Channels set to 1, Maximum Channels set to 2 and Reduce Bandwidth is set to 10 - once the usage of the 2 channels drops to 10% the number of channels used is 1.
- **Callback Telephone Number:** *Default = Blank*
  The number that is given to the remote service, via BAP, which the remote Control Unit then dials to allow the bandwidth to be increased. Incoming Call routing and RAS Services must be appropriately configured.
- **Idle Period (secs):** *Default = 10 seconds*
  The time period, in seconds, required to expire after the line has gone idle (ie. no real data has passed during this time period). At this point the call is considered inactive and is completely closed.
    - For example, the 'Idle Period' is set to X seconds. X seconds before the 'Active Idle Period' timeouts the Control Unit checks the packets being transmitted/received, if there is nothing then at the end of the 'Active Idle Period' the session is closed & the line is dropped. If there are some packets being transmitted/received then the line stays up. After the 'Active Idle Period' has timed out the system performs the same check every X seconds, until there are no packets being transferred and the session is closed and the line dropped.
    - **Active Idle Period (secs):** *Default = 180 seconds*
      Sets the time period during which time the line has gone idle (ie. no real data has passed) but there are still active sessions in progress (eg an FTP is in process, but not actually passing data at the moment). Only after this timeout will call be dropped.
        - For example, you are downloading a file from your PC and for some reason the other end has stopped responding, (the remote site may have a problem etc.) the

line is idle, not down, no data is being transmitted/ received but the file download session is still active. After the set time period of being in this state the line will drop and the sessions close. You may receive a remote server timeout error on your PC in the Browser/FTP client you were using.

- **Min Call Time (secs):** *Default = 60 seconds*
  Sets the minimum time that a call is held up after initial connection. This is useful if you pay a minimum call charge every time a call is made, no matter the actual length of the call. The minimum call time should be set to match that provided by the line provider.
- **Extra BW Mode:** *Default = Incoming Outgoing*
  Defines the mode of operation used to increases bandwidth to the initial call(s) to the remote Service.
- **Outgoing Only:** Bandwidth is added by making outgoing calls.
- **Incoming Only:** Bandwidth is added by the remote service calling back on the BACP number (assuming that BACP is successfully negotiated).
- **Outgoing Incoming:** Uses both methods but bandwidth is first added using outgoing calls.
- **Incoming Outgoing:** Uses both methods but bandwidth is first added using incoming BACP calls.

DialIn

Only available for WAN and Intranet Services. This tab is used to define a WAN connection.

To define a WAN connection:

1. Right-click within the **DialIn** window and select **Add**.
2. Enter **WAN** if the service is being routed via a WAN port on a WAN3 expansion module.

IP

The fields in this tab are used to configure network addressing for the services you are running. Depending on how your network is configured, the use of Network Address Translation (NAT) may be required.

The following fields are configurable within the **IP** tab:

- **IP Address:** *Default = Blank (address assigned by ISP)*
  A value should only be entered here if a specific IP Address (and appropriate mask as below) is required. Note that if the address is in a different domain from the Control Units IP address then NAT is automatically enabled.
  - Note: IP412 Control Units include an **Enable NAT** checkbox on their System LAN1 and LAN2 tabs.
- **IP Mask:** *Default = Blank (use NAT)*
  Enter the IP Mask associated with the required IP Address if an address is entered.
- **Primary Trans IP Address:** *Default = Blank*
  This address acts as a primary address for incoming IP traffic. All incoming IP packets without a session are translated to this address. This would normally be set to the local Mail/Web Server's IP Address.
  - On systems using an IP412 Control Unit, primary transfer IP addresses for each LAN can also be set through the **System | LAN1** and **System | LAN2** tabs. See LAN1 .
- **Request DNS:** *Default = Off*
  By selecting this option DNS information is automatically obtained - typically from your ISP. You should also leave the DNS Server IP Address box in the DNS tab of the System configuration form blank. The PC making the DNS request should point to the Control Unit as the DNS Server, this happens automatically if you are using DHCP. Use ***winipcfg*** or ***ipconfig*** to check the PC's DNS Server setting.
- **Forward Multicast Messages:** *Default = On*
  By default this option is on. Multicasting allows WAN bandwidth to be maximized through the reduction of traffic that needs to be passed between sites.
- **RIP Mode :** *Default = None*
  Routing Information Protocol (RIP) is a method by which network routers can exchange information about device locations and routes. RIP can be used within small networks to allow dynamic route configuration as opposed to static configuration using.
  - **None:** The LAN does not listen to or send RIP messages.
  - **Listen Only (Passive):** Listen to RIP-1 and RIP-2 messages in order to learn RIP routes on the network.
  - **RIP1:** As above plus send RIP-1 responses as a sub-network broadcast.
  - **RIP2 Broadcast (RIP1 Compatibility):** As above but send RIP-2 responses as a sub-network broadcast.
  - **RIP2 Multicast:** As above but send RIP-2 responses to the RIP-2 multicast address.

Autoconnect

Fields in this tab enable you to set up automatic connections to the specified Service.

- **Auto Connect Interval (mins):** *Default = Blank (AutoConnect is disabled)*
  This field defines how often this Service will automatically be called ("polled"), eg. 60 means the system will call this Service every hour in the absence of any normally generated call (this timer is reset for every call; therefore if the service is already connected, then no additional calls are made). This is ideal for SMTP Mail polling from Internet Service Providers.
- **Auto Connect Time Profile:** *Default = Blank*
  Allows the selection of any configured Time Profiles. (The Time Profile must first be configured within the Time Profile Form configuration form.) The selected profile controls the time period during which automatic connections to the service are made. It does NOT mean that connection to that service is barred outside of these hours. For example, if a time profile called "Working Hours" is selected, where the profile is defined to be 9:00AM to 6:00PM Monday to Friday, then automatic connection to the service will not be made unless its within the defined profile. If there is an existing connection to the service at 9:00AM, then the connection will continue. If there is no connection, then an automatic connection will be made at 9:00AM.

Quota

Quotas are associated with outgoing calls, they place a time limit on calls to a particular IP Service. This avoids excessive call charges when perhaps something changes on your network and call frequency increases unintentionally.

The following fields are configurable:

- **Quota Time (mins):** *Default = 240 minutes*
  Defines the number of minutes used in the Quota. When the Quota Time is used up no further data can be passed to this Service. This feature is useful to catch/stop things like an Internet game keeping a call to your ISP open for 3 months.
  - **Warning:** Setting a value here without selecting Daily/Weekly/Monthly refresh will stop all further calls after this period has expired.
- **Quota:** *Default = Daily*
  Sets the period of quota operation (None, Daily, Weekly or Monthly). For example, if the Quota Time is 60 and Quota is set to Daily then the maximum allowed total connect time during any one calendar day is 60 minutes. Any time beyond this will cause the system to close the Service and prevent any further calls to this Service. To disable quotas select none AND set a quota time of zero/blank.
  - Note: The **ClearQuota** feature can be used to create Short Codes to refresh the quota time.

Fallback

These options allow you to set up a fallback for the Service. For example, you may wish to connect to your ISP during working hours and at other times take advantage of varying call charges from an alternative carrier. You could therefore set up one Service to connect during peak times and another to act as fallback during the cheaper period.

See Using a Fallback Service .

The following fields are configurable within the **Fallback** tab:

- **In Fallback:** *Default = Off*
  This option indicates whether the Service is in Fallback or not. This can be set manually, via a Time Profile or via a Short Code.
- **Time profile:**
  Select the Time Profile you wish to use for this Service. The time profile should be set up for the hours that you wish this service to be operational, out of these hours the Fallback Service is used.
- **Fallback Service:**
  Select the Service that is used when this Service is in fallback.

PPP

Fields in this tab enable you to configure Point to Point Protocol (PPP) in relation to this particular service. PPP is a protocol for communication between two computers using a Serial interface. For an overview of PPP, see Point to Point Protocol (PPP) .

The following fields are configurable within the **PPP** tab:

- **Chap Challenge Interval (secs):** *Default = Blank*
  The period between CHAP challenges. Blank or 0 disables repeated challenges. Some software such as Windows 95 DUN does not support repeated CHAP challenges.
- **Header Compression Mode:** *Default = None selected*
  Enables the negotiation and use of IP Header Compression. Supported modes are ***IPHC*** and ***VJ***. ***IPHC*** should be used on WAN links.
- **BACP:** *Default = Off*
  Enables the negotiation and use of BACP/BCP protocols. These are used to control the addition of B channels to increase bandwidth.
- **Incoming traffic does not keep link up:** *Default = On*
  When enabled, the link is not kept up for incoming traffic only.
- **Multilink/QoS:** *Default = Off*
  Enables the negotiate and use of the Multilink protocol (MPPC) on the link(s) into this Service. Multilink must be enabled if there is more than one channel that is allowed to be Bundled/Multilinked to this RAS Service.
- **Compression Mode:** *Default = MPPC*
  Enables the negotiate and use of compression. Do not use on VoIP WAN links.
  - **Disable:** Do not use or attempt to use compression.
  - **StacLZS:** Attempt to use STAC compression (Mode 3, sequence check mode).
  - **MPPC:** Attempt to use MPPC compression. Useful for NT Servers.
- **Callback Mode:** *Default = Disable*
  - **Disable:** Callback is not enabled
  - **LCP:** (Link Control Protocol) After authentication the incoming call is dropped and an outgoing call to the number configured in the Service is made to re-establish the link.

- **Callback CP:** (Microsoft's Callback Control Protocol) After acceptance from both ends the incoming call is dropped and an outgoing call to the number configured in the Service is made to re-establish the link.
- **Extended CBCP:** (Extended Callback Control Protocol) Similar to Callback CP except the Microsoft application at the remote end prompts for a telephone number. An outgoing call is then made to that number to re-establish the link.

- **Access Mode:** *Default = Digital64*
  Sets the protocol, line speed and connection request type used when making outgoing calls. Incoming calls are automatically handled (see RAS services).
  - **Digital64:** Protocol set to Sync PPP, rate 64000 bps, call presented to local exchange as a "Data Call".
  - **Digital56:** As above but rate 56000 bps.
  - **Voice56:** As above but call is presented to local exchange as a "Voice Call".
  - **V120:** Protocol set to Async PPP, rate V.120, call presented to local exchange as a "Data Call". This mode runs at up to 64K per channel but has a higher Protocol overhead than pure 64K operation. Used for some bulletin board systems as it allows the destination end to run at a different asynchronous speed to the calling end.
  - **V110:** Protocol is set to Async PPP, rate V.110. This runs at 9600 bps, call is presented to local exchange as a "Data Call". It is ideal for some bulletin boards.
  - **Modem:** Allows Asynchronous PPP to run over an auto-adapting Modem to a service provider (requires a Modem2 card in the main unit)
- **Data Pkt. Size:** *Default = 0*
  Sets the size limit for the Maximum Transmissible Unit.

RAS Form

RAS Form Overview

Remote Access Server (RAS) is a piece of computer hardware which sits on a corporate LAN and into which employees dial on the public switched telephone network to get access to their email and to software and data on the corporate LAN.

This form is used to create a RAS service that the system offers Dial In users. A RAS service is needed when configuring modem dial in access, digital (ISDN) dial in access and a WAN link. Some systems may only require one RAS service since the incoming call type can be automatically sensed.

The following tabs contain configurable information for this form:

- RAS
- PPP

RAS

Remote Access Server (RAS) is a piece of computer hardware which sits on a corporate LAN and into which employees dial on the public switched telephone network to get access to their email and to software and data on the corporate LAN.

- **Name:**
  A textual name for this service, eg. DialIn. If Encrypted Password (see below) is used this name must match the Account Name entered in the Service Form .
- **Extension:**
  Enter an Extension Number if this service is to be accessed internally, eg. via a modem.
- **COM Port:**
  For future use.
- **TA Enable:** *Default = Off*
  Select to enable or disable - if enabled RAS will pass the call onto a TA port for external handling, eg. HyperTerminal, NT RAS etc.
- **Encrypted Password:** *Default = Off*
  This option is used to define whether Dial In users are asked to use PAP or CHAP during their initial logon to the RAS Service. If the Encrypted Password box is checked then Dial In users are sent a CHAP challenge, if the box is unchecked PAP is used as the Dial In Authorization method.

PPP

PPP (Point-to-Point Protocol) is a Protocol for communication between two computers using a Serial interface, typically a personal computer connected by phone line to a server. See Point to Point Protocol (PPP) for a more detailed overview of PPP.

- **CHAP Challenge Interval (secs):** *Default = Blank*
  The period between successive CHAP challenges. Blank/0 disables repeated challenges. Some software, eg. Windows 95 DUN does not support repeated CHAP challenges.
- **IP Header Compression:** *Default = Off*
  Enables the negotiation and use of IP Header Compression as per RFC2507, RFC2508 and RFC2509.
- **Multilink:** *Default = Off*
  Enable/Disable – When enabled the system attempts to negotiate the use of the Multilink protocol (MPPC) on the link(s) into this Service. Multilink must be enabled if the more than one channel is allowed to be Bundled/Multilinked to this RAS Service.
- **BACP:** *Default = Off*
  Enable/Disable - Allows negotiation of the BACP/BCP protocols. These are used to control the addition of additional B channels to simultaneously improve data throughput.
- **Incoming traffic does not keep link up:** *Default = On*
  When enabled, the link is not kept up for incoming traffic only.
- **Compression Mode:** *Default = MPPC*
  This option is used to negotiate compression (or not) using CCP. If set to MPPC or StacLZS the system will try to negotiate this mode with the remote Control Unit. If set to Disable CCP is not negotiated.
  - **Disable:** Do not use or attempt to use compression.
  - **StacLZS:** Attempt to use and negotiate STAC compression (the standard, Mode 3)
  - **MPPC:** Attempt to use and negotiate MPPC (Microsoft) compression. Useful for dialing into NT Servers.
- **Callback Mode:** *Default = Disable*
  - **Disable:** Callback is not enabled
  - **LCP:** (Link Control Protocol) After authentication the incoming call is dropped and an outgoing call to the number configured in the Service will be made to reestablish the link.
  - **Callback CP:** (Microsoft's Callback Control Protocol) After acceptance from both ends the incoming call is dropped and an outgoing call to the number configured in the Service is made to reestablish the link.
  - **Extended CBCP:** (Extended Callback Control Protocol) Similar to Callback CP however the Microsoft application at the remote end will prompt for a telephone number. An outgoing call will then be made to that number to reestablish the link.
- **Data Pkt. Size:** *Default = 0*
  This is the number of data bytes contained in a Data Packet.

Incoming Call Route Form

Incoming Call Route Form

The **Incoming Call Route** form allows entries to be created to route incoming calls to different groups, extensions, RAS services or voicemail. These routes can be based on the incoming line group, the type of call, incoming digits or the caller's CLI. See Incoming Call Routing . If a range of MSN numbers has been issued, this form can be populated using the MSN Configuration tool (see MSN Configuration).

The following fields are available for configuration:

- **Line Group ID:** *Default = 0*
  The identity of the Line Group. Only calls received on this Line Group use this route. This entry only applies to Lines with the same Line Group ID.
- **Incoming Number:**
  This is the number presented by the ISDN provider. A blank entry collects all calls that do not match other entries. For PRI, the administrator must add to the Incoming Call Route table one entry for each subscribed digit-string the service provider will send to IP Office, and must add one entry for unassigned numbers. Entries that are intended to match the subscribed digit-strings must specify the digit-strings as the rightmost digits in the Incoming Number field, because, with PRI, IP Office matches from right to left. See Incoming Call Route Examples.
  - Use a **-** in front of the number forces a left-to-right match (the default is right-to-left).
  - Use a ***** to match any number for which a specific matching route does not exist.
  - Use **X**'s to enter a single digit wildcard character.
- **Incoming Sub Address:** *Default = Blank*
  The sub address component of the incoming call request. If this field is left blank it means all calls with the sub addresses field set is routed to the entry specified in the Destination field.
- **Incoming Caller ID:**
  Enter the number to match the caller's incoming telephone number. This can be: -
  - full telephone number, eg. 7325551234
  - partial telephone number area code, eg. 7321 for New Jersey calls.
  - **!** for number withheld.
  - **?** for number unavailable.
  - blank for all.
  - Note: Calls are matched on the Incoming Number field before they are matched on the **Incoming Caller ID**, thus if you want to send all callers who withhold their number to Voicemail you may need several entries.
- **Destination:**
  Select the destination for the call from the list box which contains all available extensions, users, groups, RAS services and voicemail. System short codes and dialing numbers can be entered manually. Once the incoming call is matched (to the appropriate Line Group ID, Incoming Number, Incoming Caller ID etc.) the call is passed to that destination. For additional methods for routing calls directly to a specific Voicemail Pro module or short code start point see Directing Incoming Calls to Voicemail Pro.
  - **Drop-Down List Options**
    The following options appear in the Destination drop-down
    - **Hunt Group** and **User Names**.

- **Voicemail:** Allows remote mailbox access (Voicemail Lite and Voicemail Pro). Callers are asked to enter the extension ID of the mailbox required and then the mailbox access code.
- **AA:*Name*** Directs calls to an Embedded Voicemail auto-attendant service (Small Office Edition systems only). See Auto Attendant.

- **Manually Entered Options**
  The following options can be entered manually into the Destination field.
  - **VM:*Name*** Directs calls to the matching start point in Voicemail Pro.
  - A **.** matches the incoming number field. This can be used even when a ***** (match all) or **X** wildcards are being used in the Incoming Number field.
  - A **#** matches all **X** wildcards in the Incoming Number field.
  - Text and number strings entered here are passed through the System Short Code table.

- **Locale:**
  This option sets country variations.
- **Priority:** *Default = 1*
  Allows calls to be assigned a priority between 1 (lowest) and 3 (highest). In situations where calls are queued, high priority calls are placed before calls of a lower priority.
- **Fallback Extension:** *Default = Blank*
  Defines an alternate destination which should be used when the current primary destination (set in the Destination or Night Service Destination field) cannot be obtained. For example if the primary destination is a hunt group returning busy and without queuing or voicemail.
- **Night Service Profile:** *Default = Blank*
  A time profile during which the **Night Service Destination** should be used rather than the **Destination**.
- **Night Service Destination:** *Default = Blank*
  Set the destination to be used during periods defined by the **Night Service Profile**.
- **Bearer Capability:**
  The type of call selected from the list of standard bearer capabilities.
  - **AnyVoice** - all calls designated as being used for Speech services - a Speech or Audio3K1 call will meet these criteria.
  - **Speech** - normal speech call.
  - **Audio3K1** - speech call requesting a guaranteed bandwidth of 3,100 Hz.
  - **AnyData** - all calls designated as containing data - a Data64K, Data56K, DataV110, DataV120 or Video call will meet this classification.
  - **Data64K** - data call with 64000 bps throughput capability.
  - **Data56K** - data call with 56000 bps throughput capability.
  - **DataV110** - data call that supports the V.110 sub-rate multiplexing scheme.
  - **DataV120** - data call that supports the V.120 sub-rate multiplexing scheme.
  - **Video** - calls from equipment, which support Video conferencing.
  - **Any** - any call type is accepted and route (this may be useful for the S0 module).

Incoming Call Route Examples

For PRI, the administrator must add to the Incoming Call Route table one entry for each subscribed digit-string the service provider will send to IP Office, and must add one entry for unassigned numbers.

The entries that are intended to match the subscribed digit-strings must specify the digit-strings as the rightmost digits in the Incoming Number field, because, with PRI, IP Office matches from right to left.

Example 1

For example, if the customer subscribes to two DID numbers for Sales and Service, the administrator must add an entry for Sales and an entry for Service:

Line Group	Incoming Number	Destination
1	77	SalesHuntGrp
1	88	ServiceHuntGrp
1		Extn201

1. Note that the Incoming number could be the full dialed number (7325551177 and 7325551188 respectively) and produce the same results.

Example 2

The right-to-left matching gets complicated when the number of incoming digits is greater than the number of digits specified in the Incoming Number field. Consider a PRI circuit that delivers the digits 77 to the customer. The following tables will route the call to the MatchGrp hunt group.

Line Group	Incoming Number	Destination
1	677	NoMatchGrp1
1	77	MatchGrp
1	7	NoMatchGrp2
1		Extn201

- The first and second entries have the same number of matching digit places and no non-matching places, but the second entry has a shorter Incoming Number, so the second entry is chosen.

Line Group	Incoming Number	Destination
1	677	MatchGrp
1	7	NoMatchGrp2
1		Extn201

- The first entry had more matching digit places, 2 versus 1, and no non-matching digit places.

Example 3

If the PRI circuit delivers the digits 777 to the customer, the following table routes the call to the MatchGrp.

Line Group	Incoming Number	Destination
1	677	NoMatchGrp1
1	7	MatchGrp
1		Extn201

- The first entry had a non-matching digit place, so there was no match. The second had one matching digit place and no non-matching digit places.

WAN Port Form

WAN Port

Use this form to configure the leased line connected to the WAN port on the Control Unit. Important - this connection is automatically detected by the Control Unit therefore please ensure you are editing the correct form. If a WAN Port is not displayed, connect the WAN cable, reboot the Control Unit and receive the configuration. The WANPort configuration form should now be added.

The following fields are available for configuration:

- **Name**
  The physical ID of the Extension port, eg. WAN01. This parameter is not configurable, it is allocated by the system.
- **Speed**
  The operational speed of this port, eg. for a 128K connection enter 128000. This should be set to the actual speed of the leased line as this value is used in the calculation of Bandwidth Utilization. If set incorrectly additional calls may be made to increase Bandwidth erroneously.
- **Mode:** *Default = SyncPPP*
  Select the protocol required:
  - **SyncPPP:** For a data link.
  - **SyncFrameRelay:** For a link supporting Frame Relay.
- **RAS Name**
  If the **Mode** is ***SyncPPP***, selects the RAS service to associate with the port. If the **Mode** is ***SyncFrameRelay***, the RAS Name is set through the **DCLIs** tab.

- Note: If using Frame Relay; temporarily set the **Mode** to ***SyncPPP*** and in the **RAS Name** field select the default RAS service ***DialIn***. Then set the **Mode** back to ***SynchFrameRelay***. This is necessary even though the RAS service actually used for Frame Relay is set through the **DCLIs** tab.

Frame Relay

This tab is only available when SyncFrameRelay is selected in the Mode field of the WANPort configuration form.

- **Frame Management Type:**
  This must match the management type expected by the network provider. Selecting AutoLearn option allows the Control Unit to automatically determine the management type based on the first few management frames received. If a fixed option is required the following are supported: Q933 AnnexA 0393, Ansi AnnexD and FRFLMI.
- **Frame Learn Mode:**
  This parameter allows the DLCIs that exist on the given WAN port to be provisioned in a number of different ways.
  - **None:** No automatic learning of DLCIs. DLCIs must be entered and configured manually.
  - **Mgmt:** Use LMI to learn what DLCIs are available on this WAN.
  - **Network:** Listen for DLCIs arriving at the network. This presumes that a network provider will only send DLCIs that are configured for this particular WAN port.
  - **NetworkMgmt:** Do both management and network listening to perform DLCI learning and creation.
- **Max Frame Length:** Maximum frame size that is allowed to traverse the frame relay network.

Advanced

The following are used for frame relay:

- **Address Length:**
  The address length used by the frame relay network. The network provider will indicate if lengths other than two bytes are to be used.
- **N391:** *Full Status Polling Counter*
  Polling cycles count used by the CPE and the network provider equipment when bi-directional procedures are in operation. This is a count of the number of link integrity verification polls (T391) that are performed (ie. Status Inquiry messages) prior to a Full Status Inquiry message being issued.
- **N393:** *Monitored Events Counte*r
  Events counter measure used by both the CPE and network provider equipment. This counter is used to count the total number of management events that have occurred in order to measure error thresholds and clearing thresholds.
- **T392:** *Polling Verification Timer*
  The polling verification timer only applies to the user equipment when bi-directional procedures are in operation. It is the timeout value within which to receive a Status Inquiry message from the network in response to transmitting a Status message. If the timeout lapses an error is recorded (N392 incremented).
- **T391:** *Link Integrity Verification Polling Timer*
  The link integrity verification polling timer normally applies to the user equipment and to the network equipment when bi-directional procedures are in operation. It is the time between transmissions of Status Inquiry messages.
- **N392:** *Error Threshold Counter*
  Error counter used by both the CPE and network provider equipment. This value is incremented for every LMI error that occurs on the given WAN interface. The DLCIs attached to the given WAN interface are disabled if the number of LMI errors exceed this value when N393 events have occurred. If the given WAN interface is in an error condition then that error condition is cleared when N392 consecutive clear events occur.

DLCIs

Only available if **SyncFrameRelay** is selected in the Mode box of the WANPort configuration form. To add an entry, right-click and select **Add**.

- **Frame Link Type:** *Default = PPP*
  Data transfer encapsulation method. Set to the same value at both ends of the PVC.
  - **None:**
  - **PPP:** Using PPP offers features such as out of sequence traffic reception, compression and link level connection management.
  - **RFC 1490:** RFC 1490 encapsulation offers performance and ease of configuration and more inter-working with third party CPE.
  - **RFC1490 + FRF12:** Alternate encapsulation to PPP for VoIP over Frame Relay. When selected all parameters on the **Service | PPP** tab being used are overridden.
- **DLCI: (**Data Link Connection Identifier) *Default = 100*
  Unique number assigned to a PVC end point that has local significance only. Identifies a particular PVC endpoint within a user's physical access channel in a frame relay.
- **RAS Name:**
  Select the RAS Service you wish to use.
- **Tc:** (Time Constant [ms]) *Default = 10*
  The time interval used for measurement of data traffic rates (CIR and EIR). General a shorter Tc should be used when carrying VoIP traffic. The Tc used by the IP Office can be shorter than that used by the network provider.
- **CIR:** (Committed Information Rate) *Default = 64000 bps*
  The maximum amount of data that the network agrees to transfer during the given time interval (Tc). The number of committted bits can be calculated as Bc = CIR x Tc. When carrying VoIP traffic the Bc figure should be sufficient to carry a fully VoIP packet
- **EIR:** (Excess Information Rate) *Default = 0 bps*
  The maximum amount of data in excess of the CIR that a frame relay network may attempt to transfer during the given time interval (Tc). This traffic is normally marked as DE (discard eligabal). The number of excess bits can be calculated as Be = EIR x Tc. The probability of Be data arriving is lower than the probability of Bc data arriving.

Example:
G.729 VoIP creates 20 byte packets every 20ms. Adding typical WAN PPP overheads results in a 33 byte packet every 20ms.

For a CIR of 14Kbps and a Tc of 10ms, Bc = CIR x Tc = 14,000 x 0.01 = 140 bits = 17.5 bytes. Clearly a full VoIP packets cannot be sent within the Tc without exceeding the Bc. The most likely result is lost packets and jitter.

If the Tc is increased to 20ms, Bc = 14,000x0.02 = 280 bits = 35 bytes. The Bc is now sufficient to carry a VoIP packet within the Bc threshold every 20ms.

Note:

1. Backup over Frame Relay is not supported when the Frame Link Type is set to RFC1490.
2. When multiple DLCIs are configured, the WAN link LED will be switched off in any one of those DLCIs is made inactive, regardless of the state of the other DLCIs. Note also that the WAN link LED is switched on following a reboot even if one of the DLCIs is inactive. Therefore when multiple DLCIs are used the WAN link LED cannot be used to determine the current state of all DLCIs.
3. When the Frame Link Type is set to RFC1490, the WAN link LED is switched on when the WAN cable is attached regardless other whether being connected to a frame relay network. Therefore the WAN link LED cannot be used to determine the state of RFC1490 links.

Directory Form

Directory Entry Form

This configuration form can be used to create an entry in the Directory. See Directory .

- **Name:**
  Enter the text, without spaces, to be used to identify the number.
- **Number:**
  Enter the number, without spaces, to be matched with the above name.

If this Directory Entry is to be used to identify an incoming call enter the part of the incoming telephone number that is to be used as a match as follows:

1. The number is matched against the **right hand side** of the Calling Line ID number, therefore specifying a Directory Number of 1234 will successfully match all the following incoming numbers: -
   - 1234
   - 5551234
   - 7325551234 etc.
2. Partial matches can be used to allow area codes or company location matches to be made, eg
   - Name = Holmdel
   - Number = 732555????
     These area numbers must be padded with question marks to the correct length, ie. Holmdel local numbers are 10 digits long so 4 question marks are required.
   - This entry displays "Holmdel:1234" for a call from 5551234.
3. Brackets can be used around the area code, eg. (732) 5551234, so that if a call is received from both 5551234 and 7325551234 the directory entry is displayed.

Time Profile Form

Time Profile Form

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 a hunt group calls are routed outside of office hours.

- **Name:**
  Enter the Name to identify this Time Profile.
- **Time Entry List:**
  Place the cursor within the Time Entry List. Right-click and select **Add**. Multiple Time Entries can be created so that a Time Profile can be used to stipulate specific hours in the day, eg. 09:00-12:00 and 1:00-5:00.

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.

Data calls are cut off when a time profile goes out of service, then the new service is started immediately if specified.

Time Entry

A Time Entry is used to stipulate the specific hours you wish the time profile to be active, eg. 9 - 12, Monday to Friday.

- **Start Time:**
  The time during the day at which this profile becomes active (useable). Use a colon to separate the hours from the minutes.
- **End Time:**
  The time during the day at which the profile becomes inactive (un-useable). Use a colon to separate the hours from the minutes.
- **Days of Week:**
  The days of the week that the above start and end time applies to.

- **Note:**
  A Time Entry cannot span over two days eg. you cannot have a time profile starting at 6:00 PM and ending 8:00 AM. If this time period is required two Time Entries should be created - one starting at 6:00 PM and ending 11:59 PM and the other starting at 12:00 AM and ending 8:00 AM.

Firewall Profile Form

Firewall Profile Form Overview

You can apply firewall settings to each service that you setup. The system allows you to have a number of firewall profiles, which can be shared between different services. See Firewall for more information on firewalls.

If during the initial configuration from the Administration CD an ISP connection was specified, a default firewall profile called 'internet' is created unless the installer selected otherwise. The 'internet' firewall profile has the standard default firewall settings.

The following tabs contain configurable information for this form:

- Standard
- Custom

Standard

By default, any protocol not listed in the standard firewall list is dropped unless a custom firewall entry is configured for that protocol.

The following fields are available for configuration within the **Standard** tab:

- **Name:**
  Enter the name to identify this profile, eg. "InternetFirewall".
- Select one the following options for each protocol.
  - **Drop:** No sessions via this protocol are allowed through the wall
  - **In:** An incoming session can "punch a hole" in the wall to allow traffic in both directions
  - **Out:** An outgoing session can "punch a hole" in the wall to allow traffic in both directions
  - **In/Out:** Both incoming or outgoing sessions can "punch a hole" in the wall to allow traffic in both directions
- **Protocols:**
  - **TELNET:** Remote terminal login. *Default* = *Out.*
  - **FTP:** File Transfer Protocol. *Default* = *Out*.
  - **SMTP:** Simple Mail Transfer Protocol. *Default* = *Out*.
  - **TIME:** Time update protocol. *Default* = *Out*.
  - **DNS:** Domain Name System. *Default* = *Out*.
  - **GOPHER:** Internet menu system. *Default* = *Drop.*
  - **FINGER:** Remote user information protocol. *Default* = *Drop*.
  - **RSVP:** Resource Reservation Protocol. *Default* = *Drop*.
  - **HTTP:** Hypertext Transfer Protocol. *Default* = *Out*.
  - **POP3:** Post Office Protocol. *Default* = *Out*.
  - **NNTP:** Network News Transfer Protocol. *Default* = *Out*.
  - **SNMP:** Simple Network Management Protocol. *Default* = *Drop*.
  - **IRC:** Internet Relay Chat. *Default* = *Out*.
  - **PPTP:** Point to Point Tunneling Protocol. *Default* = *Drop*.
  - **IGMP:** Internet Group Membership Protocol. *Default* = *Drop*.

Custom

The Custom form gives a list of the filters created for this Firewall. To create a custom entry, right-click within the Firewall Entry List and select **Add**, see Firewall Entries .

See Firewalls .

Firewall Entries

See Firewalls .

- **Notes:**
  For information only - enter text to remind you what this entry is for. When left blank you are prompted.
- **Remote IP Address:**
  The IP address of the system at the far end of the link. Blank allows all IP addresses.
- **Remote IP Mask:**
  The mask to use when checking the Remote IP Address. When left blank then no mask is set, ie. 255.255.255.255 - allows all.
- **Local IP Address:**
  The address of devices local to this network (pre-translated). Blank allows all IP addresses.
- **Local IP Mask:**
  The mask to use when checking the Local IP Address. When left blank then no mask is set, ie. 255.255.255.255 - allows all.
- **IP Protocol:**
  The value entered here corresponds to the IP Protocol which is to be processed by this Firewall profile: 1 for ICMP, 6 for TCP, 17 for UDP or 47 for GRE. This information can be obtained from the "pcol" parameter in a Monitor trace.
- **Match Offset:**
  The offset into the packet (0 = first byte of IP packet) where checking commences for either a specific port number, a range of port numbers, or data.
- **Match Length:**
  The number of bytes to check in the packet, from the Match Offset point, that are checked against the Match Data and Match Mask settings.
- **Match Data:**
  The values the data must equal once masked with the Match Mask. This information can be obtained from "TCP Dst" parameter in a Monitor trace (the firewall uses hex so a port number of 80 is 50 in hex)
- **Match Mask:**
  This is the byte pattern, which is logically ANDed with the data in the packet from the offset point. The result of this process is then compared against the contents of the "Match Data" field.
- **Direction:**
  The direction that data may take if matching this filter.
  - **Drop:** No packets matching this may pass.
  - **In:** Allow new sessions into the private network.
  - **Out:** Allow sessions out to the Internet.
  - **Bothway:** Do both "In" and "Out".

IP Route Form

IP Route Form

Use this configuration form to specify where packets destined for a specific network are to be sent. These are static routes. See Understanding IP Routing via ISDN .

The following fields are available for configuration:

- **IP Address:**
  The IP address to match for ongoing routing, eg. 192.168.131.0. Any packets meeting the IP Address and IP Mask settings are routed to the entry configured in the Destination field. When left blank then an IP Address of 255.255.255.255 (all) is used.
- **IP Mask:**
  The Subnet Mask used to mask the IP Address for ongoing route matching, eg. 255.255.255.0. If blank the mask used is 255.255.255.255 (all).
    - **Note:** A blank entry in the IP Address and IP Mask fields means route all packets where the destination IP address is not on the local LAN or where a specific IP Route is not available. The Default Route option in the Service Form achieves the same goal.
- **Gateway IP Address:** *Default = Blank*
  The address of the gateway where packets for the above address are to be sent. If this field is set to 0.0.0.0 or is left blank then all packets are just sent down to the Destination specified, not to a specific IP Address. This is normally only used to forward packets onto another Router on the local LAN.
- **Destination:**
  The name of the Service to send these packets to. Note: Only those Services configured are shown and can be selected.
- **Metric:** *Default = 1*
  The number of "hops" this route counts as.
- **ProxyARP:** *Default = Off*
  This allows the Control Unit to respond on behalf of this IP address when receiving an ARP request.

Least Cost Route Form

Least Cost Route Form Overview

Least cost routing (LCR) allows calls to be routed making the best use of system resources. Time profiles can also be used to allow you to take advantage of cheaper rates at specific times.

Note: The LCR menu is not compatible with short codes using the **;** (semi-colon) character (used for T1/PRi line) and secondary dial tone features. To achieve least cost routing on those lines, refer to Alternate LCR.

Least cost routing uses the following standard elements of IP Office Configuration:

- **Short Codes:**
  Short codes are used to match the dialed number. When a match occurs, the matching short code indicates the number that should be output and which line group to use.
  - Short Codes can be configured in the Least Cost Route form. The following are the only kind of features allowed in the feature field: Dial, Dial3K1, Dial56K, Dial64K, DialEmergency, Dial Speech, DialV110, DialV120, DialVideo, Busy.
  - Short codes in a Least Cost Route form are applied after any User or System short code but before Line Short codes.
- **Outgoing Group IDs:**
  Outgoing Group IDs within the Line Form are used to group lines. Typically a separate group ID will be used for lines from different PSTN service providers. Once these lines are grouped, they can be used by Short codes to match which lines can be used to route an outgoing call.

In addition the following elements can also optionally be used:

- **Time Profiles:**
  Time Profiles can be used to set when a particular set of Least Cost Route settings are used.
- **Alternate Routes:**
  If a call is routed by Least Cost Routing to a Outgoing Group ID in which all the lines are busy, then after an adjustable timeout, the IP Office can look for a another short code match in a further set of Short codes.
- **Priority:**
  Each user has an assigned priority between. High priority users can bypass route settings with a lower priority. Low priority user must wait for a busy period to expire before they can try a higher priority route setting. Priority settings for individual users are located in the **User** form on the **User** tab.

To Route Calls via an Alternative Carrier During Specific Hours

1. Create a Time Profile for the required hours.
2. Create a Least Cost Route that uses that Time Profile and with a short code that will route all calls via the required carrier, eg.
   - **Short Code:** ?
   - **Telephone Number:** 1234. (1234 being the carriers required prefix)
   - **Feature:** Dial

To Use Multiple Carriers

If you wish to use multiple carriers, for example, local calls and international calls are to go through one carrier between specific hours, all calls to UK through an alternative carrier and all other calls via a third carrier.

1. Create a Least Cost Route and create short codes for all local dial codes and international calls, eg. short codes for 732n, 609n, etc.
2. All other calls will use the system short code used for dialing out.

2-Stage LCR Set-up (In-band DTMF)

To take advantage of the Least Cost Routing services offered by second-tier carriers/PTOs/Telcos/etc. who utilize older Central Office switches, a second string of digits needs to be presented, in-band to them after the call is initially set-up. To set this up, use the following Short Code features:

- **D** = wait for the connection then send the following DTMF
- **,** = one second pause in between DTMF digit dialing, eg. 18005551234D12345,N This represents the carrier's telephone number, then D, then the digits required by the carrier, eg. an account number, then comma and N representing the number dialed.

Note: A DTMF tone will not be produced if you are running IP Office 401 control unit.

Right-click on the list area or an existing route to select **View, Edit, Delete** or **New**. The following tabs within the LCR form contain fields for configuration:

- LCR
- Main Route
- Alternate Route 1
- Alternate Route 2

LCR

- **Name:**
  The name to identify the Route set.
- **Time Profile:**
  Select the Time Profile to be used with this Least Cost Route. If no profile is selected the route settings apply at all times.

Main Route

The three routing tabs; Main Route, Alternate Route 1 and Alternate Route 2, all contain the same settings.

- **Timeout (secs):** *Default = 30 seconds*
  When a call goes to a line group where all lines are busy, this timeout sets how long the system waits before trying short code options in the next tab.
  - Note: When a user is routed to a short code with the Busy feature, then they remain at busy and do not try any other options.
- **Priority:** *Default = 5, Range 0(lowest) to 5(highest).*
  If the user's priority is higher than that of the tab, routing is applied using the Short codes in the tab and those in the next tab simultaneously. When a short code exists in both tabs, the short code from the next tab is used.
- **Allow Bump:** *Default = Off*
  When the lines indicated by a route are being used by a multilink PPP data call, if this option is selected, the user's call is able to seize a line from the data call.
- **Short Code List:**
  These perform dialed number matching. When a match occurs, the matching short code indicates the telephone number to outdial and the line group in which a line should be seized. To add a short code, right-click on the list and select Add.
  - The only short code features that should be used in a Least Cost Route short code are: Dial, Dial3K1, Dial56K, DialEmergency, DialSpeech, DialV110, DialV120, DialVideo and Busy.
  - The ; character and [n] syntax cannot be used.

Alternate Route 1

Operates similarly to the Main Route tab.

Alternate Route 2

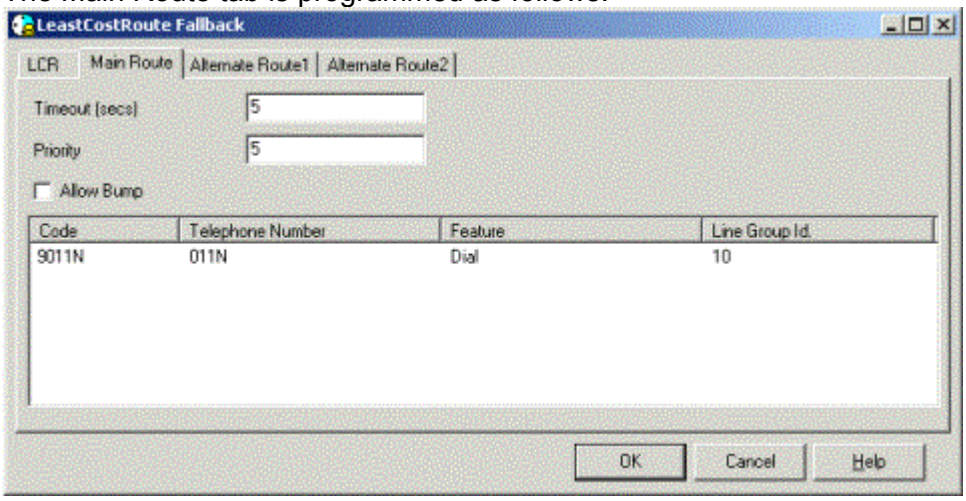
Operates similarly to the Main Route tab.

Examples

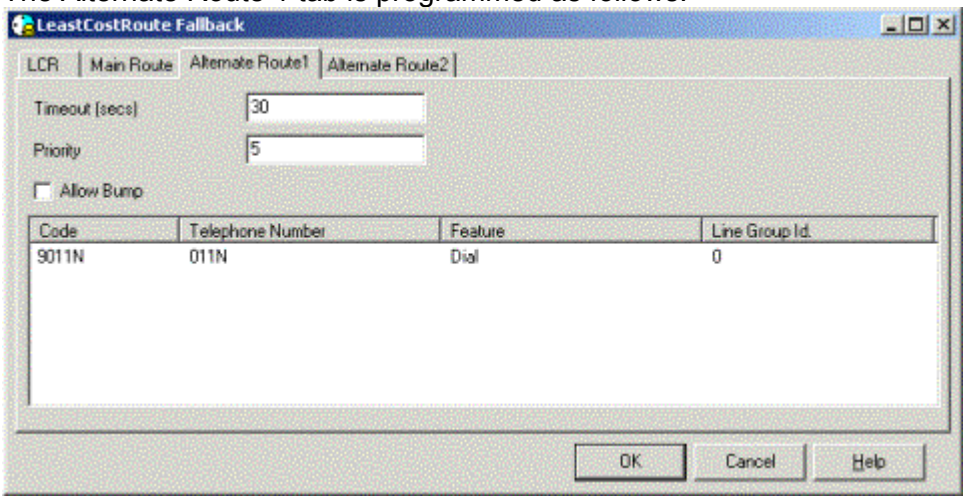
Example: Fallback Carrier Routing

In this example, the customer has lines from two separate providers.

- The required routing is:
  - Local and national calls should go via the standard provider's lines.
  - International calls should go via the alternate provider's lines.
  - If all lines to the alternate provider are busy, users should be able to use the standard providers lines
- To achieve this the following configuration changes were made:
  - Lines to the standard provider were given the Outgoing Group ID 0.
  - Lines to the alternate provider were given the Outgoing Group ID 10.
  - In Least Cost Route, a new route called "Fallback" was added.
  - The Main Route tab is programmed as follows:



    - **9011N:** This short code matches any dialing beginning with 9011, ie. an international call. It strips the 9 and then tries to seize a line in group 10 to dial the number.
    - The timeout is 5 seconds. This means that if after 5 seconds the system is still unable to seize a line from Line Group 10, it should look for an alternate short code match (against the original dialed digits) in the Alternate Route 1 tab.
  - The Alternate Route 1 tab is programmed as follows:



    - **9011:** The short code again matches any international dialing. This time however, it tries to seize a line in Line Group 0.

Example: Using an Alternate Carrier

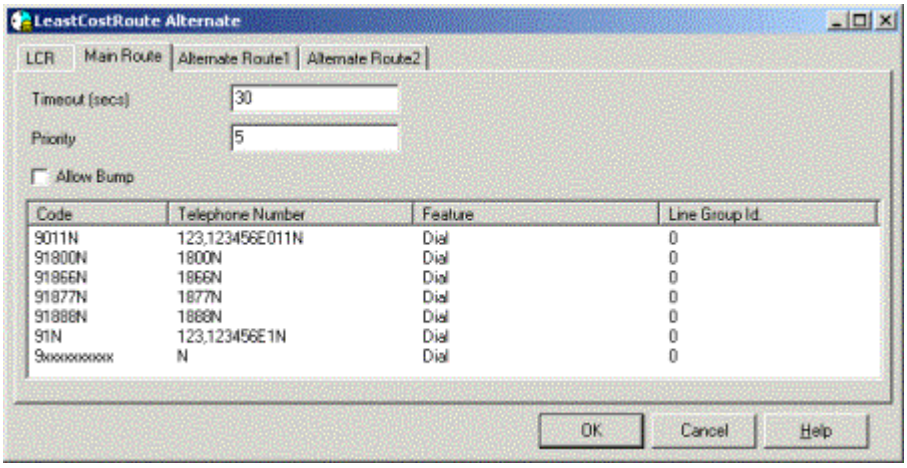
In this example, the customer's lines are all from the same provider. However,the customer wants any calls other than local calls to go via an alternate carrier.

The required routing is:

- All calls go via the same set of lines.
- Any national or international calls should be prefixed with the alternate carrier's access code (123), a short pause and a customer ID number (123456).
- The alternate carrier also provides billing by extension number, so insertion of the dialing extension number is desired.
- Local numbers dialed in full (ie. with the local area code) should not go via the alternate carrier.
- Toll free numbers provided by the line provide should not go via the alternate carrier.

To achieve this routing, the following configuration changes were made:

- All the PSTN providers' lines have been left in **Outgoing Group ID** 0.
- In Least Cost Route, a new route called "Alternate" was added. The following settings were added to the Main Route tab:



  - **9011N:** This short code matches anyone dialing an international number. Before trying to seize a line, it inserts the information required by the alternate call carrier. The **,** (comma) adds a pause, the **E** sends the dialing extension number.
  - **91N:** This short code matches anyone dialing an national number and again inserts the information required to route the call via the alternate call carrier.
  - **91800N**, **91866N**, **91877N**, **91888N:** These short codes match national numbers that are toll free and so do not need to be routed via the alternate call carrier.
  - **9xxxxxxxxxx:** This short code matches any local dialing. These calls are not routed via the alternate call carrier.

Example: International Call Restriction

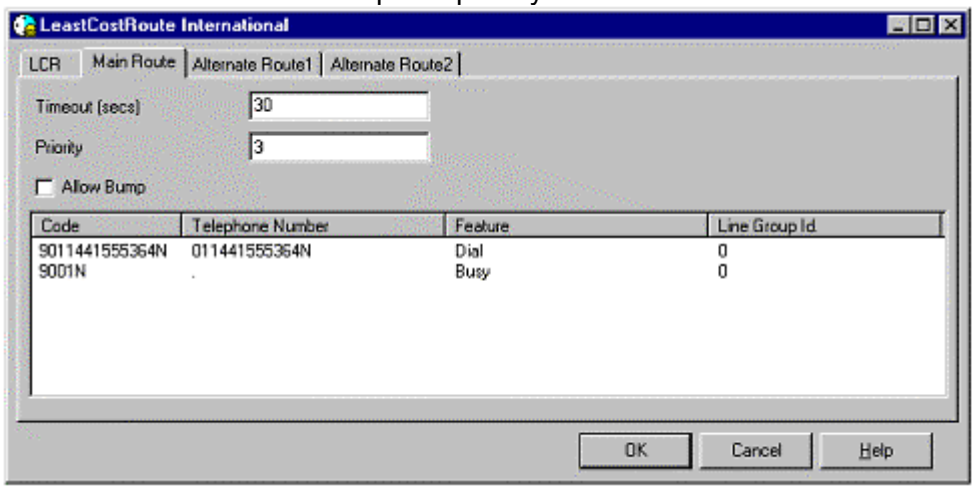
In this example, we want to restrict who makes international calls.

The required routing is:

- Users with a priority of 3 or lower should not make international calls.
- Users with a higher priority can make international calls.
- The customer has an overseas office to which all users should be able to make calls.

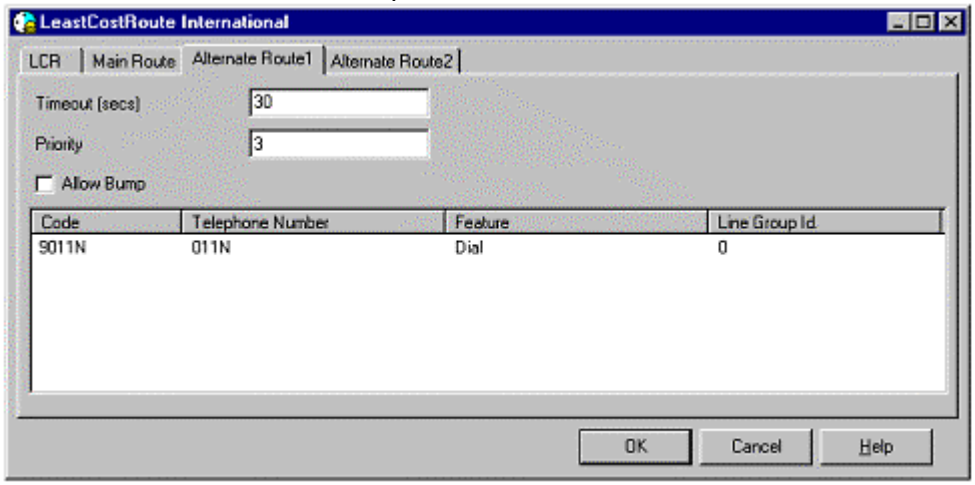
To achieve this routing, the following configuration changes were made:

- Those extension users cannot to make international calls had their Priority set to 3. This is done through the User tab of the User form.
- In Least Cost Route, a new route called "International" was added.
- In the Main Route tab the required priority was left as 5.



  - **901141555364N**: This short code matches DID numbers at the overseas office and allows any user to dial those numbers.
  - **9011N**: This short code matches the dialing of any other international numbers and returns busy tone to the dialer.

- For users with Priority higher than 3, the IP Office immediately looks for a short code match in the Alternate Route 1 tab as well as the Main Route tab. When identical short codes exist, the one in the Alternate Route tab takes precedence.



  - **9011N:** Again this short code matches international number dialing but this time it allows such calls rather than returning busy tone.

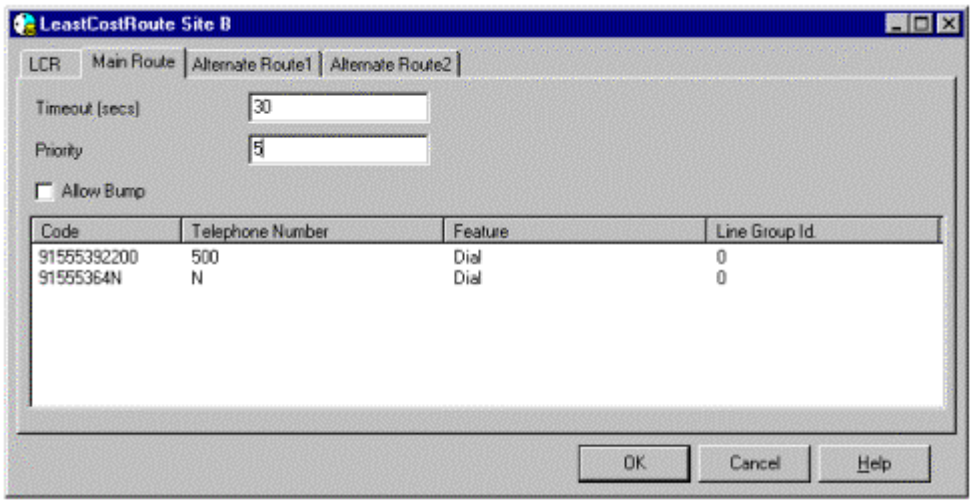
Example: Small Community Network VoIP Routing

In this example, the customer has two IP Office systems. In addition to their own external lines, the two sites are linked by a data link. The data link has to be configure as a VoIP VPN link and use IP Office Small Community Networking.

- System A has extensions and groups numbered from 200 upwards.
- System B has its extensions and groups numbered from 500 upwards.
- The customer wants anyone at Site A dialing the external number of Site B or a DID at Site B to have the call re-routed via the VoIP link.

To achieve this, the following changes were made on System A.

- The VoIP lines from System A to System B were put into Outgoing Group ID 5.
- In Least Cost Route a new route called "SiteB" was added.



- In the Main Route tab the following Short codes were added:
  - **91555392200:** This short code matches the main reception number at Site B. The short code changes the number to the main group at Site B and re-routes the call to the VoIP Link.
  - **91555364N:** This short code matches the dialing of DID numbers of extensions and groups on System B. It removes everything apart from the extension /group number and route the call to the VoIP link.

Similar changes would also be implemented on System B to reroute return calls.

LCR Using T1/PRI Lines or Secondary Dial Tone

Alternate LCR Overview

Least Cost Routing allows calls to be routed making the best use of system resources. The examples in this section demonstrate how to achieve Least Cost Routing when using T1/PRI lines or secondary dial tone.

- If using T1/PRI lines, you must include the **;** (semi-colon) at the end of the Short code entry.
- If you want to provide a secondary dial tone to users, the dial access number must be surrounded by **[ ]** (brackets).

These characters are not supported in the short codes entered in IP Office Least Cost Route forms. Least cost routing functionality instead is achieved through system short codes. This section gives various examples. In all the examples, the number “9” is used to get access to outside lines.

- Note: When not using the **;** or **[ ]** in short codes, least cost routing can be done through the Least Cost Route form in the IP Office configuration.

Example: Fallback Carrier Routing

In this example, the customer has lines from two separate providers.

The required routing is:

- Local and national calls should go via the standard provider's lines.
- International calls should go via the alternate provider's lines.
- “900” calls should be blocked
- The dial access code must be the same for both national and international lines

The first thing to do is to change the **Outgoing Line Group ID** (on the Line Form). Put all the lines that will be used for local and national calls in one group (10 for this example). The lines that are going to be used for international dialing should be in a second group (20 for this example).

Configure the following Short codes on the **Short code** Form.

T1 or PRI Short code	Secondary Dialtone Short code	Explanation
	Short code: 9 **Telephone Number:** . **Line Group ID:** 0 **Feature:** SecondaryDialTone	Secondary Dial Tone
Short code: 9001N; **TelephoneNumber:** 001N **Line Group ID:** 10 **Feature:** Dial	**Short code:** [9]001N **Telephone Number:** 001N **Line Group ID:** 10 **Feature:** Dial	Matches international number
Short code: 91N; **Telephone Number:** N **Line Group ID:** 20 **Feature:** Dial	**Short code:** [9]1N **Telephone Number:** N **Line Group ID:** 20 **Feature:** Dial	Matches Long Distance (national) number
Short code:9xxxxxxxxxx; **Telephone Number:** N **Line Group ID:** 20 **Feature:** Dial	**Short code:** [9]xxxxxxxxxx **Telephone Number:** N **Line Group ID:** 20 **Feature:** Dial	Matches local number
Short code: 91900N; **Telephone Number:** **Line Group ID:** **Feature:** Busy	**Short code:** [9]1900N **Telephone Number:** **Line Group ID:** **Feature:** Busy	Matches 900 numbers

Example: Using an Alternate Carrier

In this example, the customer's lines are all from the same provider. However, they want calls other than local calls to go via an alternate carrier.

The required routing is:

- All calls go via the same set of lines.
- Any national or international calls should be prefixed with the alternate carrier's access code (123), a pause and a customer ID number (123456).
- The alternate carrier also provides billing by extension number, so insertion of the dialing extension number is desired.
- Local numbers dialed in full (ie. with the local area code) should not go via the alternate carrier.
- Toll free numbers provided by the line provide should not go via the alternate carrier.

Configure the following Short codes on the **Short code Form**.

T1 or PRI Short code	Secondary Dialtone Short code	Explanation
	Short code: 9 **Telephone Number:** . **Line Group ID:** 0 **Feature:** SecondaryDialTone	Provides secondary dial tone after dialing 9.
Short code: 91N; **Telephone Number:** 123,123456E1N **Line Group ID:** 10 **Feature:** Dial	**Short code:** [9]1N **Telephone Number:** 123,123456E1N **Line Group ID:** 10 **Feature:** Dial	Matches national number
Short code: 9001N; **Telephone Number:** 123,123456E1N **Line Group ID:** 10 **Feature:** Dial	**Short code:** [9]001N **Telephone Number:** 123,123456E1N **Line Group ID:** 10 **Feature:** Dial	Matches International number
Short code: 91800N; **Telephone Number:** 1800N **Line Group ID:** 10 **Feature:** Dial	**Short code:** [9]1800N **Telephone Number:** 1800N **Line Group ID:** 10 **Feature:** Dial	Matches toll free number
Short code: 91888N; **Telephone Number:** 1888N **Line Group ID:** 10 **Feature:** Dial	**Short code:** [9]1888N **Telephone Number:** 1888N **Line Group ID:** 10 **Feature:** Dial	Matches toll free number
Short code: 91866N; **Telephone Number:** 1866N **Line Group ID:** 10 **Feature:** Dial	**Short code:** [9]1866N **Telephone Number:** 1866N **Line Group ID:** 10 **Feature:** Dial	Matches toll free number
Short code: 91877N; **Telephone Number:** 1877N **Line Group ID:** 10 **Feature:** Dial	**Short code:** [9]1877N **Telephone Number:** 1877N **Line Group ID:** 10 **Feature:** Dial	Matches toll free number
Short code: 9xxxxxxxxx; **Telephone Number:** N **Line Group ID:** 1 **Feature:** Dial	**Short code:**[9]xxxxxxxxx **Telephone Number:** N **Line Group ID:** 10 **Feature:** Dial	Matches local number
Short code: 91900N;	**Short code:** [9]1900N;	Matches 900

Telephone Number: **Line Group ID:** **Feature:** Busy	**Telephone Number:** **Line Group ID:** **Feature:** Busy	numbers

In the above table, the short codes 9001N and 91N match long distance and international dialing. The alternate carrier's access code (123), a pause (",") and the customer's identification number (123456) followed by the user dialing (E), followed by the dialed number (1N) are sent out to the line.

Example: International Call Restriction

In this example, the customer wants to restrict who can make international calls.

The required routing is:

- The customer has an overseas office to which all users should be able to make calls.
- Certain users can make international calls.

To achieve this the following configuration changes are done in the System Short code form:

T1 or PRI Short code	Secondary Dialtone Short code	Explanation
	Short code: 9 **Telephone Number:** . **Line Group ID:** 0 **Feature:** SecondaryDialTone	Provides secondary dial tone after dialing 9.
Short code: 9011441707364N; **Telephone Number:** 0014417017369N **Line Group ID:** 10 **Feature:** Dial	**Short code:** [9]011441707364N **Telephone Number:** 011441707364N **Line Group ID:** 10 **Feature:** Dial	Matches DID numbers to the overseas office
Short code: 9011N; **Telephone Number:** **Line Group ID:** **Feature:** Busy	**Short code:** [9]011N **Telephone Number:** **Line Group ID:** **Feature:** Busy	Matches international calls and returns busy to the user.
Short code: *80 **Telephone Number:** 00144392200 **Line Group ID:** 10 **Feature:** Dial	**Short code:** *80 **Telephone Number:** 00144392200 **Line Group ID:** 10 **Feature:** Dial	Allows users to call main overseas number

To achieve this the following configuration changes are done in the Short code Tab of the User Form. This needs to be done for each user that can override the international call restriction.

T1 or PRI Short code	Secondary Dialtone Short code	Explanation
Short code: 9011N; **Telephone Number:** 01N **Line Group ID:** 10 **Feature:** Dial	**Short code:** [9]011N **Telephone Number:** 01N **Line Group ID:** 10 **Feature:** Dial	Matches international calls and allows the call.

Example: Small Community Network Routing

In this example, the customer has two IP Office systems. These are linked by a VoIP connection and use IP Office Small Community Networking.

System A has extensions and groups numbered from 200 upwards. System B has its extensions and groups numbered from 500 upwards.

- The customer wants anyone dialing the external DID of an extension on the remote system to have the call routed via the VoIP connection.

To achieve this, the following configuration changes were made on System A. Similar changes would also be implemented on System B.

- The VoIP VPN lines from System A to System B were put into Outgoing Group ID 5.

The following System Short codes are added:

Short code	Explanation
Short code: 9011441707392200 **Telephone Number:** 500 **Line Group ID:** 5 **Feature:** Dial	Routes the call via VoIP to Site B's reception group (500).
Short code: 9011441707364N; **Telephone Number:** N **Line Group ID:** 5 **Feature:** Dial	Matches users dialing the DID of a Site B user. It routes the call via VoIP directly to the remote extension.
Short code: 5N **Telephone Number:** 5N **Line Group ID:** 5 **Feature:** Dial	Matches any user dialing a Site B extension or group number.

License Form

License Form

This form is used to display the function, value and status of License keys entered into the system. License keys are unique and are 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 LAN1 form, see LAN1 .

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

Refer to the Feature & License Key Manual for full details.

Account Code Form

Account Code Overview

Account codes are commonly used to control cost allocation and out-going call restriction. Once a successful call has been completed using a certain account code, that account code information will be removed from the internal call information. This means that using the redial button will not re-activate the account code; the user must re-enter the account code each time the restricted number is dialed.

The method for entering account codes depends on the type of phone used. An account code can be entered before the number is dialed if the user knows the number to be dialed is restricted. If the account code is entered before the number is dialed, a dial tone is supplied to indicate the line is ready to accept the phone number. If the phone number is dialed first, a re-occurring beeb will wound to indicate the request for an account code

The account code used on a call is included in the call information output by the system's call log. Incoming calls can also trigger account codes automatically by matching the Caller ID stored with the account code.

- To create an account code:
  1. Click **Account Code** to display a list of existing account codes.
  2. Double-click on an existing account code to edit it or right-click on the displayed list and select **New**.
  3. In the **Account Code** field, enter the code to be used to track specific calls.
     - Alphabetic characters can be used in account codes for users dialing from Phone Manager.
     - Wildcards can be used within the account code. The wildcard ***?*** matches a single character, for example 123??? matches any 6 digit account code starting 123. The wildcard ***** matches any digits, for example 456* matches any account code beginning with 456.
  4. In the **CLI** field (optional), entering a Caller ID means that the account code is automatically assigned to incoming or outgoing calls with the same Caller ID.
  5. Send the configuration changes to the Control Unit via Merge.

Once the account code is created, it can be used in the following ways:

- For controlling cost allocation
- For out-going call restriction

If you have IP Office Phone Manager, the list of account codes can be made available to Phone Manager users. See Account Codes and Phone Manager.

Account Code

- **Account Code:**
  Enter the account code required. The code can include alphabetic characters for users dialing via Phone Manager. It can also include wildcards; **?** matches a single digit and ***** matches any digits.
- **Caller ID:**
  Enter the number to be matched to incoming or outgoing Caller ID to automatically assign an Account Code.

Voice Recording

This tab is used to activate the automatic recording of external calls to or from a recognized **Account Code**. The recordings are placed in the IP Office user's mailbox. This requires Voicemail Pro to be installed and running.

The following field are configurable:

- **Record Outbound:** *Default = None*
  Select whether outbound calls are recorded. Options are **On**, **Mandatory** and then various percentages of calls made by the user.
  - **On:** Record the call if possible.
  - **Mandatory:** If not possible to record, return busy tone to the caller.
- **Record Inbound:** *Default = None*
  The same as Record Outbound but applied to call to the user.
- **Record Time Profile:** *Default = Blank*
  Used to select a time profile during which calls are recorded.

E911 System

E911 System

IP Office supports Enhanced 911 (E911) service that allows the recipient of 911 calls to accurately identify the telephone number and physical location of the calling party. Emergency personnel cross-check the incoming Automatic Number Identification (ANI) with the Automatic Line Identification (ALI) or billing information (in other words, the billing address) associated with the telephone number. If the caller is in a multi-floor office or multi-billing campus, emergency operators have little idea of the exact location of the caller since the information presented is often just the main billing address of the company. You can use the E911 zones in combination with E911 adjuncts to provide more specific ALI about the caller's location.

As a building can be partitioned into different floors or different areas on one floor, the extensions in IP Office can be grouped ("zoned") according to their locations. For example you can place all the extensions in the Northeast Corner of the building in one zone and the extensions in the Northwest Corner in another zone. You can then assign some trunks with ALI of the Northeast Corner to the first zone and trunks with ALI of the Northwest Corner to the second zone. When a caller dials "911", the ALI information shows the emergency response team exactly where the caller is located.

If your states requires that dialing the access code (ie. "9") in front of "911" also allow the call to go out, add the following System Short Code:

- **Short Code:** 9911
- **Telephone Number:** 911
- **Line Group ID:** 0
- **Feature:** Dial

The following options are only available in regions where E911 is supported (it is available in the United States). The configuration consists of an E911 System entry (shown by the icon) and ten E911 partitions (shown by icons). The IP Office E911 solution requires that Analog Loop Start lines be used for all trunks that are used for Adjuncts (see System Parameters) and Zones (see E911 Zone Configuration).

More:

- E911 System Configuration
- E911 Zone Configuration
- E911 Warning Screen
- E911 Configuration Steps

E911 System Configuration

Clicking on the icon in the configuration tree and then double-clicking on the entry in the right-hand panel displays the E911 System Configuration form.

The form contains two tabs.

System Parameters

- **Enable E911 System:***Default = Off (Not Selected)*
  This is the parameter that indicates whether Enhanced 911 service will be used on the system. By default this is off. If your state requires E911 service, check this. When selected, the functionality provided by the other administration items in the E911 System form are used when "911" calls are dialed.
- **Alarm Station:** *Default = Blank*
  When the E911 Adjunct detects an error condition (such as the disconnection of the trunk cable between the adjunct and the PSTN) the alarm station (which is a connection from the adjunct to a Tip/Ring port) is notified. A station in the system should be configured for a **User** DSS button (See Button Programming section for more details). When the alarm station is notified, the DSS button is lit. This indicates that there is a problem with the lines or the adjunct device. When this situation occurs, the lines for the adjunct are NOT used and all "911" calls are routed over local lines. That means that they go out a non-adjunct line without the extra information. Once the lines are back in service, the alarm extension is notified and the User LED is extinguished and normal adjunct E911 operation resumes.
- **Adjuncts:**
  If your State requires detailed information about a caller (i.e. office number), an adjunct can be used to provide that information. The adjunct box sits between the IP Office and Central Office and is connected via Loop Start lines to the IP Office and Centralized Automatic Message Accounting (CAMA) trunks to the Central Office. When this is administered, "911 calls" that are routed over these lines send out additional information about the caller (Extension ID). This information is used by the adjunct to provide detailed caller location. Right-click the mouse to add or remove entries. Use the standard Window Key to select a continuous group (Shift Key) or Individual Channels (Control Key). There can be five Analog Loop Start trunks (either on the Control Unit or those on the ATM 16 module) administered to an E911 adjunct.

E911 Zone Configuration

Zones allow stations to be grouped together that have a similar physical location. Lines are then assigned to the partition. This billing address associated with the lines can be used to locate the caller. For E911, what needs to get out is the actual phone that a person is calling from. In the case of IP Office, Hot Desking allows multiple users to use a single phone (at different times – See Extension versus User). For that reason, it is important to understand that it is the default User ID that gets sent out, no matter what user is currently "logged in" to that extension. This allows the physical extension number to be associated (via an external database) to a specific address (i.e. room number). The Extension form will provide the information about default users for each extension. In an IP403, the following is the default for the extensions on the Control Unit:

Extension ID	User
74	201
78	202
67	203
71	204
75	205
79	206
83	207
87	208
91	209
95	210

With the above numbering, when a person was using the phone connected to Extension ID 67, "203" would be sent out regardless of the extension number associated with the user currently logged into that station. A person would be able to dial the phone by using either of the following short codes (these are the defaults).

- **DialPhysicalExtnByNumber** (default short code *70*N# – where "N" is the default User ID for the extension). This allows the user to call the default user id no matter who is currently using that station. Using the numbers from the table above, if a user with an extension number 505 was currently logged into physical extension 67, they could always be called by dialing "*70*203#".
- **DialPhysicalExtnByID** (default short code *71*N# – where "N" is the default extension ID for the extension). This allows the user to call the default user id no matter who is currently using that station. Using the numbers from the table above, if a user with an extension number 505 was currently logged into physical extension 67, they could always be called by dialing "*71*67#".

It is expected that the first short code will be used more often due to the fact that the number that gets sent out will be the extension number not the physical ID.

Double-clicking on the icon expands and collapses the display of E911 zones (icons). Click on any icon to display details of the partitions in the right-hand panel.

Double-click on the icon to edit the zone settings. Alternatively, in the right-hand panel, right-click and select the option required (**View**, **Edit**, **New** or **Delete**).

- **Name:** *Default = Default*
  Allows a unique name to be assigned to each zone.
- **Stations:** *Default = Contains all Extension ID's*
  Lists the extensions id's within the partition. Right-click on the list to add or delete

entries. An extension can only be in one zone, so when you add an extension it is automatically removed from it previous assignment. When adding stations, the **Selecting E911 Stations** form appears listing available stations and the partition to which they are currently assigned.

- **Trunks:** *Default = Blank*
  List the Analog Loop Start trunks within the partition. Right-click on the list to add or delete entries. When adding trunks, the **Selecting E911 Trunks** form appears listing all available trunks and the partition to which they are currently assigned. Only reliable Analog Loop Start trunks should be used.

E911 Warning Screen

The following warning screen appears when new extensions (eg. IP Phones) or expansion modules have been added to the system. This message indicates that the zones may not contain all the extensions in the system.

When this appears, hit the "OK" button. Verify that the new extensions are in a zone (Note that they may belong in the default, or one that you have created).

E911 Configuration Steps

If you are using E911 without an adjunct box, the following needs to be administered:

1. Set up zones that you require. Make sure that you add both lines and extensions.

If you are using E911 with an adjunct box:

1. Administer an alarm extension.
2. Program a "User" button for that alarm extension.
3. Administer Analog Loop Start Lines as Adjunct lines.
4. Set up zones.

Wireless 802.11b

Wireless 802.11b

The Avaya IP Office - Small Office Edition can act as an 802.11b wireless access point. To do this requires the insertion of an Agere wireless card into one of the Avaya IP Office - Small Office Edition's PCMCIA slots and entry of a Avaya IP Office - Small Office Edition WiFi licence.

This allow 802.11b wireless devices to connect to the Avaya IP Office - Small Office Edition LAN including VoIP devices.

In order to connect to the wireless LAN, the wireless device must be configure for the same wireless network name and encryption key as the Avaya IP Office - Small Office Edition. Additionally the wireless device must match the Avaya IP Office - Small Office Edition's LAN1 or LAN2 network settings unless using DHCP.

More:

- SSID
- Security

SSID

The Service Set Identifier (SSID) tab.

- **Network Name:** *Default = IP Office Wireless.Net*
  A unique name used to identify and distinguish the Avaya IP Office - Small Office Edition wireless LAN from other wireless LANs.
- **Wireless Mac Address:**
  Displays a list of the MAC addresses of the devices currently connected to the wireless LAN.
- **Frequency/Channel:** *Default = 6*
  The 802.11b wireless frequency band is sub-divided into a number of channels. In locations where there are multiple wireless LANs or multiple access points to the same wireless LAN, each access point should use a separate channel. Devices connecting to a wireless LAN will automatically connect to the channel providing the strongest signal.
  - The number of channels available is country specific. In the US channels 1 to 11 are available. In most of Europe, channels 1 to 13 are available. In Japan only channel 14 is available.
  - The channel frequencies overlap. For instance, channel 2 shares part of the same frequency band as channels 1 and 3. In areas with mulitple access points, use widely spaced channels, for example 1, 6 and 11, on the different access point.
- **Accept Any:** *Default = Off*
  If on, allows any wireless device to connect to the wireless LAN without having to have a matching wireless network name (SSID) set. When off, only devices configured with a matching wireless network name can connect to the wireless LAN.

Security

This tab allows for additional security through the use of wireless encryption keys. If enabled, in addition to encrypting the wireless traffic, only devices using a matching encryption key can connect to the wireless LAN.

- **Encryption:** *Default = Disabled*
  Allows selection of 50/64 bit or 128 bit security. Note: 50/64 bit encryption is also know as 40/64 encryption.
- **Alpha/Hex:** *Default = Hex*
  Switch key entry between hexadecimal and alphabetic entry modes.
- **Key 1/4:**
  Allows entry of the security key and selection of which key is the current key to use.
    - Key entries are only viewable by Manager users using an Operator with the **Wireless** form ***Advanced*** setting ticked.

User Restrictions

User Restrictions Overview

User restrictions can be used to apply the same set of dialing rules to multiple users. The restrictions are applied to individual users through the **Restrictions** field in each individual user's **User** settings.

The following tabs contain configurable information for this form:

- Restrictions
- Short Codes

Restrictions

- **Name:** *Default = Blank*
  A name used to identify the set of user restrictions and allow its selection through the **Restrictions** field in each individual user's **User** settings.
- **Priority:** *Default = 5 (low), Range 0 to 5*
  The priority that should be applied to user calls if routed via a Least Cost Route. This overrides the priority of the individual user.
- **Outgoing Call Bar:** *Default = Off.*
  When on, bars users making external calls.

Short Codes

Allows entry of short codes for dialing by associated users. These short codes override any match system short codes but not individual user short codes.

Logical LAN

Logical LAN

A logical LAN carries traffic between two IP Office LANs via an intermediate network such as an ADSL network.

- **Name:** *Default = Blank.*
  A unique name for the logical LAN. This name will then be selectable as a destination in the IP Route table.
- **IP Address:** *Default = Blank*
  The IP address provided by the internet service provider.
- **IP Mask:** *Default = Blank*
  The IP address mask provided by the internet service provider.
- **Gateway IP Address:** *Default = Blank*
  The IP address of the router.
- **Gateway Mac Address:** *Default = Blank*
  The MAC address of the router.
- **Firewall Profile:** *Default = Blank*
  The firewall profile that should applied to traffic.
- **Enable NAT:** *Default = Off.*
  Enable NAT for traffic across the logical LAN.

Tunnel

Tunnel

Tunneling improves the security of data exchange between sites where that data crosses an unsecure network such as the public internet. The IP Office supports two methods of tunneling, L2TP and IPSec.

- **L2TP - Layer 2 Tunneling Protocol**
  PPP authentication using PAP or CHAP normally takes place between directly connected routers. When connecting to the internet, authentication is between the customer router and the internet service providers. L2TP allows additional authentication to be performed between the routers at each end of the connection despite the intermediate network routers.
- **IPsec**
  IPsec allows data between two locations to be secured using sender authentication and encryption of the data. The use of IPsec requires entry of an IPsec Tunnelling licence.

To create a tunnel, right-click the cursor on the list of existing tunnels and select **New**. The **Tunnel Selection** window will appear for you to select the type of tunnel (L2TP or IPsec) to create. Depending which tunnel you choose to create, different configurations will be available to you.

L2TP Tunnel

Tunnel

- **Name:** *Default = Blank*.
  A unique name for the tunnel. Once the tunnel is created, the name can be selected as a destination in the IP Route table.
- **Local Account Name:**
  The local user name.
- **Local Account Password:**
  The local user password. Used during authentication.
- **Remote Account Name:**
  The remote user name.
- **Remote Account Password:**
  The password for the remote user. Used during authentication.
- **Remote IP Address:**
  The IP address of the remote IP Office or the local VPN line IP address or the WAN IP address.
- **Minimum Call Time (Mins):** *Default = 60*
  The minimum time that the tunnel will remain active.
- **Forward Multicast Messages:** *Default = On*
  Allow the tunnel to carry multicast messages.
- **Encrypted Password:** *Default = Off*
  Use the CHAP challenge protocol to authenticate users.

L2TP

- **Shared Secret:**
  User setting used for authentication. Must be matched at both ends of the tunnel.
- **Total Control Retransmission Interval:** *Default = 0*
  Time delay before retransmission.
- **Receive Window Size:** *Default = 4*
  The number of unacknowledged packets allowed.
- **Sequence numbers on Data Channel:** *Default = On*
  When on, adds sequence numbers to L2TP packets.
- **Add checksum on UDP packets:** *Default = On.*
  Use checksums to verify L2TP packets.
- **Use Hiding:** *Default = Off*
  When on, encrypts the tunnels control channel.

PPP

- **CHAP Challenge Interval (secs):** *Default = Blank*
  Sets the period between CHAP challenges. Blank or 0 disables repeated challenges. Some software (such as Windows 95 DUN) does not support repeated challenges.
- **Header Compression:** *Default = None*
  Select header compression. Options are: ***IPHC*** and/or ***VJ***.
- **Compression Mode:** *Default = MPPC*
  Select the compression mode for the tunnel connection. Options are: ***Disable***, ***StacLZS*** or ***MPPC***.
- **Multilink / QoS:** *Default = Off*
  Enable the use of Multilink protocol (MPPC) on the link.
- **Incoming traffic does not keep link up:** *Default = On*
  When enabled, the link is not kept up when the only traffic is incoming traffic.

IP Security Tunnel

Main

- **Name:** *Default = Blank*.
  A unique name for the tunnel. Once the tunnel is created, the name can be selected as a destination in the IP Route table.
- **Local IP Address:**
  The IP address or sub-net for the start of the tunnel.
- **Local IP Mask:**
  The IP mask for the above address.
- **Remote IP Address:**
  The IP address or sub-net for the end of the tunnel.
- **Remote IP Mask:**
  The IP mask for the above address.
- **Remote Gateway:**
  The IP address of the remote IP Office or the local VPN line IP address or the WAN IP address.

IKE Policies

- **Shared Secret:**
  The password used for authentication. This must be matched at both ends of the tunnel.
- **Exchange Type:** *Default = ID Prot*
  Aggressive provides faster security setup but does not hide the ID's of the communicating devices. **ID Prot** is slower but hides the ID's of the communicating devices.
- **Encryption:** *Default = DES CBC*
  Select the encryption method used by the tunnel. The options are: ***DES CBC***, ***3DES*** or ***Any***. Note: Use of 3DES requires entry of an IP Office licence.
- **Authentication:** *Default = MD5*
  The method of password authentication. Options are: ***MD5***, ***SHA*** or ***Any***.
- **DH Group:** *Default = Group 1*
- **Life Type:** *Default = KBytes*
  Sets whether **Life** (below) is measured in seconds or kilobytes.
- **Life:**
  Enter the duration before reauthentication is required.
- **Remote Gateway:**
  The IP address of the remote IP Office or the local VPN line IP address or the WAN IP address.

IPSec Policies

- **Protocol:** *Default = ESP*
  ESP (Encapsulated Security Payload) or AH (Authentication Header, ie. no encryption).
- **Encryption:** *Default = DES*
  Select the encryption method used by the tunnel. The options are: ***DES CBC***, ***3DES*** or ***Any***. Note: Use of 3DES requires entry of an IP Office licence.
- **Authentication:** *Default = HMAC MD5*
  The method of password authentication. Options are: ***HMAC MD5***, ***HMAC SHA*** or ***Any***.

Auto Attendant

Auto Attendant

The IP Office 401 and Avaya IP Office - Small Office Edition control units support voicemail using a integral memory card. In addition, IP401 systems also require a VCM card.

On the Small Office Edition, the integral voicemail can provide auto-attendant services in addition to basic user mailbox services.

- **Name:**
  A name for the auto-attendant service. Maximum length 12 characters. External calls can be routed to the service by entering **AA:*Name*** in the Incoming Call Route's Destination field.
- **Morning/Afternoon/Evening:**
  Each auto-attendant can consist of three distinct time periods, defined by associated time profiles.
- **Time Profile:**
  The time profile that defines each period of auto-attendant operation. When there is an overlap between time profiles, precedence is given in the order morning, afternoon and then evening.
- **Short code:**
  The short code that can be dialed to access the morning greeting for the auto-attendant service. The short code is generated automatically and added to the short codes table.
- **Menu Options:**
  The short code that can be dialed to access the menu options prompt for the auto-attendant service.

Actions

The actions tab defines the actions available to callers dependant on which key they press.

- **Key:**
  The standard telephone dial pad keys, 0 to 9 plus * and #.
- **Action:**
  The following actions can be assigned to each key.
  - **Not Defined:**
    The corresponding key takes no action.
  - **Transfer to Operator:**
    Transfer the caller to the set Destination number. This is a supervised transfer, if the caller is not answered they will recall to the auto-attendant.
  - **Normal Transfer:**
    Transfer the caller to the set Destination number. This is an unsupervised transfer, if the caller is not answered they will be handled as per a direct call to that number.
  - **Replay Greeting:**
    Replay the auto-attendant greetings again.
- **Destination:**
  For Transfer to Operator and Normal Transfer actions sets the destination extension or group numbers.

Manager Commands

Toolbar

Clicking one of the Toolbar buttons is a quick alternative to choosing a command from the menu. Buttons on the toolbar activate and deactivate according to the state of the application. The toolbar itself may be moved with the mouse and left as a floating palette, or docked to any edge of the main window.

Button	Action	Menu Equivalent
	Locate and open a file.	File / Open
	Save the file in the active window.	File / Save

File Menu

Open

The **File | Open** command reads and opens the current configuration from the Control Unit selected.

You are prompted for the System Password (if you are using the default password this does not need to be entered)

A copy of the configuration file is also saved in the Manager's Working Directory. The System name is used for the file name if available, otherwise it is named as ***nabranch.cfg***.

See Receiving a Configuration .

Close

This command closes the configuration currently open.

Save

The **File | Save** command saves the amended configuration.

If the configuration has been opened "online", the **Sending Config To** dialog box appears in order to select the Reboot mode required. If you choose to Cancel the file is only saved to disk.

If the configuration file has been opened "offline", the file is saved to disk only.

See Sending a Configuration .

IP Office Manager 2.1

Save As

The **File | Save As** command allows you to save a configuration file under an new name, or in a new location. The command displays the **Save File As** dialog box. You can enter the new file name, including the drive and directory.

Version 15c

(File: saveas.htm)

Change Working Directory

The **File | Change Working Directory** option allows you to set where Manager should save and look for different files.

The normal default in all cases is the Manager application folder (***C:\Program Files\Avaya\IP Office\Manager***). This ensure that whenever Manager is upgraded by deinstalling the existing copy and installing the new Manager, all associated admin files are also upgraded.

If any of the directories is changed, you must ensure that the correct files are present in the new directory and that these files are manually updated whenever Manager is upgraded.

- **Working Directory (.cfg files):**
  The location to which copies of control unit configuration files should be saved.
- **Binary Directory (.bin files):**
  The directory that contains the .bin files for IP Office modules and control units. Also the directory that contains any .bin and other files for 4600 Series IP telephones. This directory is used as the root directory for Manager's BOOTP/TFTP services.
- **Upgrade Directory (UpgradeWiz.exe):**
  The directory that contains the Upgrade Wizard application. This directory should include the files ***UgradeWiz.exe*** and ***bin.cfg*** (which details which units use which bin files).

Change Password

See Operators .

The **File | Change Password** command allows the Operator that is currently logged on to change their password. This setting is held on the Manager PC and so does not require a send to the Control Unit or reboot.

(File: changepassword.htm)

Preferences

This command allows you to specify the IP address of the Control Unit you wish to manage. By default, the broadcast address (255.255.255.255) is used and all Control Units found are then shown. Specifying individual addresses (maximum 10) allows quicker selection of the Control Unit required.

To create a new entry, from the **Preferences** menu, select **Edit**

- **Enter broadcast IP address:**
  The IP address for the Control Unit you wish to manage or a more general broadcast address. If you wish to manage a remote Control Unit then you must enter its IP address here. If it is set as 255.255.255.255 (default) then the Manager will be able to talk to all Control Units on the local LAN. If the PC has two LAN connections then it is necessary to set this for the broadcast address of the LAN, eg. 192.168.42.255 you have connected your Control Unit to.
- **Enable port for serial communication:** *Default = Off*
  When off, the Manager application does not check for a serial port when started.
- **Enter port number to be used for serial communication:**
  Not used. This is a legacy feature for older units that were managed via the serial rather than

LAN port. Setting this to 0 the Manager does not use the serial port, leaving it free for use by programs such as Hyper Terminal.

- **Load Last File:**
  If this option is selected, the last configuration file you were working on will automatically open when launching the Manager application.
- **Close Configuration after send:** *Default = On*
  Automatically closes the configuration file open in Manager when it has been sent to the control unit. This helps ensure that configuration being edited is a recent copy received from the control unit and thus contains any user changes.
- **Save configuration file before send:** *Default = On*
  Save a copy of the configuration file on the Manager PC whenever the configuration is sent to the control unit.
- **Backup files on save:** *Default = On*
  If on, whenever a copy of a configuration is saved on the Manager PC, any existing saved copy is renamed with the backup file extension name (see below).
- **Backup file extension:** *Default = .BAK*
  The file extension used for backup configuration files.

I Cannot Send/Read an Existing Config?

You need to make sure that the manager's preferences are pointing at the correct IP address, which should be either a broadcast address of 255.255.255.255 or the specific address of a Control Unit. You should also check that you are using the correct password.

IP Office Manager 2.1

Open File

The **File | Offline | Open** command displays the Open dialog box so you can select a configuration file to edit from those stored on the PC.

Version 15c

(File: openfile.htm)

IP Office Manager 2.1

Receive Config

This enables you to receive a copy of the current operational configuration from a system. This is saved in the Manager's Working Directory as a file, which can be modified without being connected to the system and then sent back to the Control Unit to become operational when the system is rebooted.

By default, the name given is the System Name as set in the System Form .

Note: The suggested file name is the same for each download from the Control Unit, make sure you have a backup of the file before downloading over an existing file.

Note: Failing to supply the correct password results in an empty file.

See Receiving a Configuration .

Version 15c

(File: receiveconfig.htm)

Send Config

The SendConfig function instructs Manager to save the amended configuration to the Working Directory and send it to the Flash memory. To activate the new configuration the system must be rebooted to pass the configuration from Flash to the RAM. See Sending a Configuration .

Select the type of reboot required as follows:

Reboot Mode:

- **Immediately:** When selected the reboot occurs immediately regardless of the number of calls on the system.
- **When Free:** When this option is selected the Control Unit waits until all calls have cleared before rebooting.
- **Merge Config:** When this option is selected the amendments are merged with the configuration currently stored in the RAM. This means that new features can be active without rebooting the system. See Merging a Configuration .
- **None:** When selected the configuration is sent to the Flash only.
- **Bar Incoming Calls:** When selected this option is checked with the When Free option above the System will bar all new incoming calls until after the reboot
- **Bar Outgoing Calls:** When selected this option is checked with the When Free option above the System prevents all new outgoing calls until after the reboot
- **Reboot Time (hh:mm):** The system waits until this time before attempting to reboot. This option is only available when **When Free** is selected under **Reboot Mode**. The instruction is stored in the Control Unit, not in Manager.
- **Please Enter Password:** Enter the System Password, this is required to authorize a reboot. If you entered the password when you received the configuration this box does not appear.

Erase Config

The **Erase Config** command removes the active configuration from the Control Unit and restores it to the factory default.

Select **Advanced** from the **File** menu and then **Erase Config (factory default)**.

In order to complete this operation you must enter the System Password.

Version 15c

(File: eraseconfig.htm)

Reboot

This command instructs the System to reboot. This sends the configuration currently stored in the Flash memory to the RAM.

Select Advanced from the File menu then Reboot and select the type of reboot required as follows:

- **Reboot Mode:**
  - **Immediately:** When selected the reboot occurs immediately regardless of the number of calls on the system.
  - **When Free:** When this option is selected the Control Unit waits until all calls have cleared before rebooting.
  - **Merge Config:** When this option is selected the amendments are merged with the configuration currently stored in the RAM. This means that new features can be active without rebooting the system. See Merging a Configuration.
- **Bar Incoming Calls:** When selected this option is checked with the When Free option above the System will bar all new incoming calls until after the reboot
- **Bar Outgoing Calls:** When selected this option with the When Free option above the System prevents all new outgoing calls until after the reboot
  - **Reboot Time (hh:mm):** The system waits until this time before attempting to reboot. This option is only available with When Free is selected under Reboot Mode. The instruction is stored in the Control Unit not in the Manager.
- **Please Enter Password:** Enter the System Password, this is required to authorize a reboot.

Upgrade

This command starts the Upgrade Wizard. This application is installed with the Manager application from the Administration CD and allows you to follow the progress of upgrading your system.

- **WARNING: Upgrading from IP Office 1.4 and earlier**
  If upgrading from a previous version of Manager please refer to the Job Aid 046 Upgrades. This is especially important for IP403 systems which require a two-stage upgrade process.

- **WARNING:**
  Incorrect use of the Upgrade command can halt Control Unit operation. If an upgrade is performed from a Manager PC that is not on the same LAN segment as the IP Office Control Unit, the Validate box on the Upgrade Wizard screen must be ticked (default) to invoke a remote upgrade. ONLY untick the Validate box if the Manager PC is on the same LAN segment as the IP Office and running on a PC with a fixed IP address. For full details, refer to the IP Office Job Aid 046 Upgrading IP Office Software.

IP Office Manager 2.1

Backup

The Backup feature creates a copy of all configuration files (***.cfg***) and software files (***.bin***) stored in the Manager's Working Directory to a folder of your choice.

Use this dialogue box to select the folder where you wish the files to be copied. Double-click to expand or collapse a folder.

Version 15c

(File: backup.htm)

Restore

The Restore feature copies all configuration files (***.cfg***) and software files (***.bin***) stored in the selected folder to the Working Directory.

Use this dialogue box to select the folder the files are to be retrieved from. Double-click to expand or collapse a folder.

Version 15c

(File: restore.htm)

Import Directory

This command allows you to import a ***.cvs*** or ***.tab*** file into the Directory stored in the configuration.

Directory Format

Use this dialogue box to select the format in which the Directory Entries are to be saved or imported.

- **Export To/Import From:** The box displays the path selected in the previous dialogue box. This is the location and file name that is used to save or retrieve the directory entries.
- **Format:** Select the format in which the directory entries are retrieved or saved
- **Comma Separated:** Each field is separated by a comma
- **Tab Separated:** Each field is separated by a tab
- **Name/Number** or **Number/Name:** Select the order of the fields
- **Add Entries:** Select if the current Directory Entries are to be added to existing entries
- **Replace Entries:** Select if the current Directory Entries are to replace existing entries
- **Maximum Directory Name Length:** Specify the length of the name field

Export Directory

This option allows you to export the contents of the Directory stored in the configuration into a ***.csv*** or ***.tab*** file.

Version 15c

(File: exportdirectory.htm)

IP Office Manager 2.1

Import Configuration Entities

You may wish to copy entries, eg. Short Codes, services, from another configuration file into the current configuration. To do this you must first export the entries from the other configuration - see Export Configuration Entities .

Once you have exported the relevant entries, select Import Configuration Entities from the **File | Import | Export** menu. From the **Open** dialog box, select the export file and choose **Open**. The entries are imported into the current configuration file.

Version 15c

(File: importconfigurationentities.htm)

IP Office Manager 2.1

Export Configuration Entities

You may wish to copy entries, eg. Short Codes, Services, to another configuration file to save you time recreating them again.

To do this select the **Export Configuration Entities** option in the **File | Import | Export** menu.

Select the entries you wish to export and enter the path for the new file. This will default to *config.exp* in the Working Directory.

See Import Configuration Entities .

Version 15c

(File: exportconfigurationentities.htm)

IP Office Manager 2.1

Export as Text

This command creates a .csv text file from the open configuration. The name of the file defaults to the system name but this can be changed.

Version 15c

(File: exportastext.htm)

IP Office Manager 2.1

Import as Text

Overwrite the configuration in Manager with an imported .csv file.

Version 15c
©Avaya - May 6, 2004

(File: importastext.htm)

IP Office Manager 2.1

Logoff

Once an Operator has logged on, this menu option becomes available to allow the current Operator to log off and the Manager application waits for another Operator to log on.

Version 15c
©Avaya - May 6, 2004

(File: logoff.htm)

IP Office Manager 2.1

Exit

The **File | Exit** command exits the Manager application. If you have modified a configuration without saving, you'll be prompted to save before exiting.

Version 15c
©Avaya - May 6, 2004

(File: exit.htm)

Tools Menu

MSN Configuration

This form can be used to populate the Incoming Call Route table.

- **MSN:**
  The first number in the set of MSN numbers for which you have subscribed.
  Note: If you require to find an exact match between the MSN numbers and the destination numbers, enter a minus (-) sign before the first MSN number.
- **Destination:**
  Where incoming calls with matching digits should be routed. The drop-down list contains the extensions and groups on the system.
- **Presentation Digits:**
  Set to match the number of digits from the MSN number that the PSTN will actually present to the system.
- **Range:**
  How many MSN numbers were subscribed for. This assumes that all the numbers are in series from the MSN entry above.
- **Add:**
  Adds the appropriate entries to the Incoming Call Route table using the value entered above.
- **Delete:**
  Removes a specific entry.

Edit Menu

This menu allows objects in the configuration to be cut, copied, pasted and deleted.

View Menu

- **TFTP Log:**
  Open a log of all file transfers - this can be used to follow the process of an upgrade or when receiving or sending a configuration.

Window Menu

The Window menu provides commands to control the position and layout of application windows.

- **Tile:**
  Resize and position all windows side-by-side in an non overlapping pattern.
- **Cascade:**
  Resize and position all windows in an overlapping pattern from the top-left hand corner of the application's main window so that the title bar of each is visible.
- **Close All:**
  Close all windows.

DTE Port Maintenance

DTE Port Overview

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.

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

In either case, you must ensure that you have a backup copy of the system configuration.

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.

Loader Version

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

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 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. 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.
9. Close the terminal program session.
10. 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. Attach the serial cable between the PC and the DTE port on the IP Office Control Unit.
7. Start the terminal program on your PC. Ensure that it has been setup as listed in "DTE Port Settings".
8. Arrange the program windows so that the Terminal program and Manager TFTP Log are visible at the same time.
9. Switch off power to the IP Office Control Unit.
10. Power on the Control Unit and press the escape key every second until you get a ***Loader*** message.
11. Enter **AT** (note upper case). The Control Unit should respond ***OK***.
12. Enter **AT-X**. The Control Unit should respond ***Multi-Sector Erase***.
13. The Control Unit will now request the .bin file it requires from Manager. This process appears in the TFTPLog.
14. When completed the system will reboot.

Sample TFTPLog of a successful transfer:

```
: Received BOOTP request for 00e007000123 192.168.42.1 napremis.bin
: Sending BOOTP response for 00e007000123 192.168.42.1 napremis.bin
: Sending napremis.bin length 654321 bytes to 192.168.42.1
: Sent 10% of napremis.bin
: Sent 20% of napremis.bin
: Sent 30% of napremis.bin
: Sent 40% of napremis.bin
: Sent 50% of napremis.bin
: Sent 60% of napremis.bin
: Sent 70% of napremis.bin
: Sent 80% of napremis.bin
: Sent 90% of napremis.bin
: Sent 100% of napremis.bin
: Sent napremis.bin length 654321 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 napremis.bin
: Sending BOOTP response for 00e007000123 192.168.42.1 napremis.bin
: Unable to send napremis.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 napremis.bin, unable to
process
```

DTE Port Trace of Defaulted Unit Reboot

This is an example of a defaulted Control Unit booting.

```
Expanding MPPC image ...
Constructor StaticHeap=56 DynamicHeap=8185688
NoCacheStaticHeap=1442036 NoCacheDynamicHeap=3694348 Overflow=0
Factory Test Status 00000001
Product Variation Status ffffffff
NVConfiguration:: No NV Stored default..
found FLASH file: ..\modem\zmbin004.s37, len=790
found FLASH file: ..\modem\mcode.bin, len=40000
found FLASH file: ..\vcomp\48105ak.123, len=d8
found FLASH file: ..\vcomp\48105ae3.123, len=1c158
found FLASH file: ..\nabranch\onehz.bin, len=3e80
DT interface detected
htl 00010000 hth 20400000
SLOT A: PRI24 Module Added
SLOT B: No ISDN/AT Module fitted
SLICOFI2: chip version: V1.3
Dual-Modem fitted
Voice Compression PCB detected
Found voice compressor 0
No voice compressor 1
No voice compressor 2
No voice compressor 3
USS-820 USB Device Controller: rev 1.3
Route 00000000 00000000 Usurped (NOCHANGE) is LAN1
Route::Attempting DHCP...
USS820: USB bus reset detected
USBDevice: state POWERED --> DEFAULT
1: Reset phone due to SendSABM NACKs
2: Reset phone due to SendSABM NACKs
Route::No DHCP defaulting IP Address c0a82a01 ffffff00
RouteSystem::Starting DHCP Server...
RouteSystem::RouteSystem LAN1 ipaddr=c0a82a01 ipmask=ffffff00
Configuration::Attempting to read from FLASH...
FlashConfigIO::Load(0)
Configuration::Using Default...
No System IPADDR using DISCOVERED Values
No System IPADDR 2 using DISCOVERED Values
Platform::Discover TDM Attached Units...
Platform::Discover Possible LAN Attached Units...
Configuration::WARNING Unit IP 403 is not configured - adding
Configuration::WARNING Unit ANALOGUE POTS2 is not configured - adding
Configuration::WARNING Unit DIGITAL DT 8 is not configured - adding
Checking WAN
Firewall Validating LAN1
Adding RemoteManager route to 192.168.99.0
Configuration::AddDeadRoute 0a000000 ff000000 00000000
Configuration::AddDeadRoute e0000000 ff000000 00000000
Configuration::Complete
0: PCM=2648 ALaw=9f
1: PCM=4452 ALaw=9f
2: PCM=0000 ALaw=9f
3: PCM=1068 ALaw=9f
4: PCM=0000 ALaw=ff
5: PCM=0003 ALaw=73
6: PCM=0000 ALaw=18
7: PCM=0000 ALaw=98
CallSystem::NEW LINE Detected 1
CallSystem::StartExtn  No Config for 2.10 Adding
CallSystem::StartExtn  No Config for 2.14 Adding
CallSystem::StartExtn  No Config for 2.3 Adding
CallSystem::StartExtn  No Config for 2.7 Adding
```

```
CallSystem::StartExtn  No Config for 2.11 Adding
CallSystem::StartExtn  No Config for 2.15 Adding
CallSystem::StartExtn  No Config for 2.19 Adding
CallSystem::StartExtn  No Config for 2.23 Adding
RasServer::Starting...
Added ACDQueue to Main
SNMP::Starting SNMP Server...
MIBII::Creating MIBII base...
IGMP::Starting IGMP Module...
Tue 14/8/2001 09:53:47 FreeMem=7646324
Inband Exception Handling Enabled
Initialisation complete starting TA
```

DTE Port Trace of Normal Reboot

This is an example of a Control Unit rebooting and loading an existing configuration.

```
Expanding MPPC image ...
Constructor StaticHeap=56 DynamicHeap=8185688
NoCacheStaticHeap=1442036 NoCacheDynamicHeap=3694348 Overflow=0
Factory Test Status 00000001
Product Variation Status ffffffff
found FLASH file: ..\modem\zmbin004.s37, len=790
found FLASH file: ..\modem\mcode.bin, len=40000
found FLASH file: ..\vcomp\48105ak.123, len=d8
found FLASH file: ..\vcomp\48105ae3.123, len=1c158
found FLASH file: ..\nabranch\onehz.bin, len=3e80
DT interface detected
htl 00010000 hth 20400000
SLOT A: PRI24 Module Added
SLOT B: No ISDN/AT Module fitted
SLICOFI2: chip version: V1.3
Dual-Modem fitted
Voice Compression PCB detected
Found voice compressor 0
No voice compressor 1
No voice compressor 2
No voice compressor 3
USS-820 USB Device Controller: rev 1.3
Route 00000000 00000000 Usurped (NOCHANGE) is LAN1
RouteSystem::Starting DHCP Server...
RouteSystem::RouteSystem LAN1 ipaddr=c0a82a01 ipmask=ffffff00
Configuration::Attempting to read from FLASH...
FlashConfigIO::Load(0)
No System IPADDR 2 using DISCOVERED Values
Platform::Discover TDM Attached Units...
USS820: USB bus reset detected
USBDevice: state POWERED --> DEFAULT
Platform::Discover Possible LAN Attached Units...
DT5ToneGenerator::UpdateOper
DT5DTMFGenerator::UpdateOper
Checking WAN
Firewall Validating LAN1
Configuration::Complete
0: PCM=2648 ALaw=9f
1: PCM=4452 ALaw=9f
2: PCM=0000 ALaw=9f
3: PCM=1068 ALaw=9f
4: PCM=0000 ALaw=ff
5: PCM=0003 ALaw=73
6: PCM=0000 ALaw=18
7: PCM=0000 ALaw=98
8: PCM=0000 ALaw=00
9: PCM=0012 ALaw=00
RasServer::Starting...
Added ACDQueue to Main
SNMP::Starting SNMP Server...
MIBII::Creating MIBII base...
IGMP::Starting IGMP Module...
Tue 14/8/2001 09:49:54 FreeMem=7646752
Inband Exception Handling Enabled
Initialisation complete starting TA
```

Transactional Pad

Connecting a Transactional Pad

A transaction pad (T-PAD, credit card "swipe" terminal) can use the ISDN (B channel) trunks, via the 25-pin D-type connector on the rear of the system Control Unit. This allows for faster transactions then provided by conventional modem connectivity.

The Control Unit supports a single DTE port. This DTE port has an AT command interface. Certain AT commands may be sent to the serial port so that it runs an X.25 TPAD interface.

The ISDN link between the Control Unit and the transaction pad is digital. The transaction pad does not require a modem.

Configuration Parameters

In order to connect to a remote server, the DTE port needs:

- the Phone number of the remote server
- local_nua
- nui
- lower_channel (defaults to 1024)
- upper_channel (defaults to 1279)

AT commands need to be issued to the DTE port to enable the interface. The following AT commands are relevant to transaction pad operation:

- **ATB6** - set connection mode as TPAD
- **AT%A** - set the local nua.
- **AT%I** - set the nui.
- **AT%L** - set the lower channel limit (defaults to 1024).
- **AT%U** - set the upper channel limit (defaults to 1279).
- **AT&A** - set an autodial number.
- **AT&D=1** - dial autodial number whenever DTR is raised (by pad).

Example:

```
ATB6
AT%A=1234
AT%I=test_host
AT%L=1048
AT%U=1052
AT&A 01923111111
AT&D=1
```

Additional information of IP Office DTE port AT commands can be found in the "IP Office AT Commands Manual".

Configuration Auto-Load

Whereas AT commands can be issue to the DTE port through a serial communications program (eg. Hyperterminal), DTE port settings and parameters are not saved in the IP Office Control Unit's flash memory. Thus they are lost during any reboot.

In order to 'permanently' set the parameters they need to be added to the configuration through the IP Office Manager application. This is done through a configured user called **DTEDefault**.

Create a user called **DTEDefault** and add the required initial AT commands into the **SourceNumbers** table. These commands are then automatically reloaded following any reboot.

Tracing

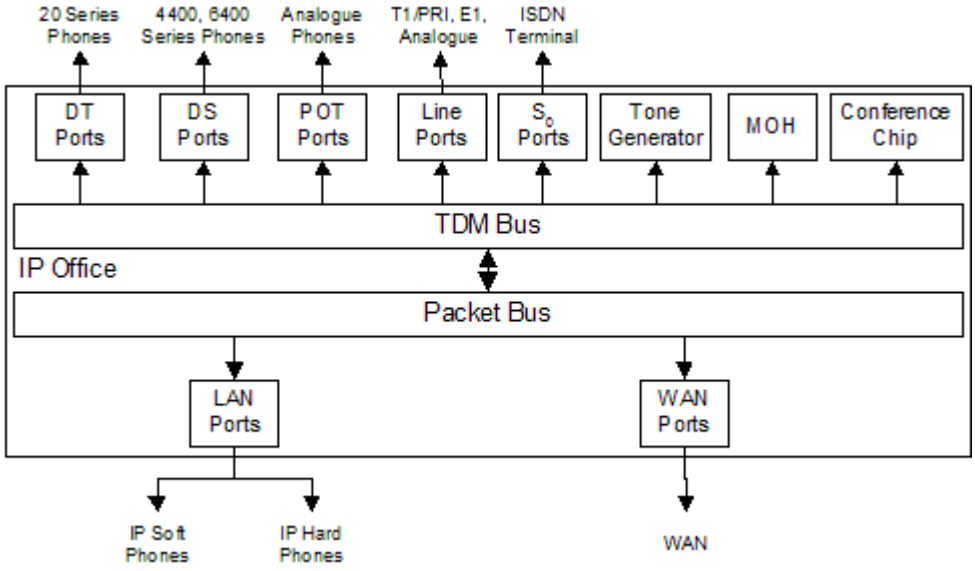
There are a number of locations where the transaction can be traced using the IP Office Monitor application.

- **Options/DTE**
- **DTE Command Tx/Rx**
  This trace information is output when the DTE port is in AT mode
- **DTE Filter Tx/Rx**
  This is trace information of the Serial communication between the DTE port and the pad. Other trace information will appear from time to time.

VCM & Data Channels

Overview of Channels

The IP Office can be treated as having a telephony switching interface (its TDM bus) and a data networking interface (its Packet bus).



- The TDM bus is used by devices attached to the system's DS, DT and POT ports (analog and digital telephones) and by any Line Modules installed in the Control Unit. It is also used by several internal devices, for example the Tone Generator, MOH and Conference Chip.
- The Packet bus Interface is used by devices attached to the system's LAN and WAN ports.

Calls between the two buses will use up the IP Office Control Unit's available data and VCM channel resources as follows:

- When a voice call takes place between a device on the TDM bus and a device on the packet bus, a VCM channel is used. If no VCM channel is available, then busy is indicated to the caller.
- VCM channels are provided by installing a Voice Compression Module into the IP Office Control Unit.
- When any data call takes place between a device on the TDM bus and a device on the packet bus, a data channel is used. If no data channel is available, then the call cannot be initiated.

VCM Examples

In the examples below, IP Phone means both IP Hard Phones and IP Soft Phones. Non-IP Phones mean both analog and digital phones.

- **IP Phone to/from Non-IP Phone:** *1 channel used for duration of call.*
- **IP Phone to/from IP Phone:** *1 channel used during call setup.*
    - Access to the Tone Generator on the TDM bus is required during call setup. Thus a VCM channel is used.
    - Once the call is connected, the VCM channel is no longer used (being IP telephony devices the IP phones perform their own voice compression).
- **Non-IP Phone to/from PSTN:** *No channel used.*
- **IP Phone to/from PSTN Line:** *1 channel used for duration of call.*
- **Conference Calls:** *1 channel per IP phone.*
    - Conference calls are managed on the TDM bus. Therefore, a VCM channel is required for each device on the Packet bus involved in the conference.

Data Channel Examples

The following scenarios all use data channels:

- **Multiple LAN Users dialing the Same ISP:** *1 channel total.*
  The calls are routed via the same digital trunk (assuming sufficient bandwidth) so only one data channel is used between the Packet bus and the TDM bus.
- **Remote Access Users:** *1 channel per user.*
  Each RAS user dialing into the IP Office will use a separate trunk and thus each RAS user requires a data channel.
    - Note: The number of Analog RAS users is also limited by the Modem capacity of the IP Office Control Unit. Currently this is 2 if a Modem 2 module is fitted (not supported on IP401) or 1 if the first analog trunk port is set to Modem operation.
- **Access to Voicemail:** *1 channel per user.*
  Each call to an IP Office Voicemail Server uses a data channel.

VCM & Data Channels Supported

VCM Modules exist in 5, 10, 20 and 30 channel variants. The IP401, IP403 and IP406 Control Units can each support a single VCM as shown below. The IP412 can support two VCM modules.

VCM Channels	IP401	IP403	IP406	IP412
VCM 5	Yes	Yes	Yes	Yes
VCM 10	–	Yes	Yes	Yes
VCM 20	–	Yes	Yes	Yes
VCM 30	–	–	–	Yes
Maximum VCM Channels	2	20	30	60

- **Small Office Edition**
  For these controls units either 3 or 16 VCM channels are pre-installed within the unit. The number is shown by the **VC*x*** item on the label on the unit's base.

Each IP Office Control Unit supports the following number of data channels. Note that the number of those data channels that can be used for voicemail is further restricted

Data Channels	IP401	IP403/Small Office Edition	IP406	IP412
Maximum Data Channels	2	18	24	100
- Usable for Voicemail Lite	2	4	4	4
- Usable for Voicemail Pro	2	10	20	30

Note: The Voicemail Pro also requires licenses for the number of voicemail ports available.

Detecting the VCM Module Fitted

The presence of a VCM module is not shown in the IP Office Control Unit's configuration when opened in the Manager application. However the Monitor application does provide indication of the number of VCM channels installed in a Control Unit.

1. Start Monitor.
    - If necessary, use **File | Select Unit** to indicate the IP Office Control Unit which you want to monitor.
2. Amongst the first lines of monitor output should be two lines similar to the following:

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

3. This line provide information about various aspect of the control unit, as follows:
    - PRI = Number of PRI channels
    - BRI = Number of BRI channels (4=1 card, 8=2 cards).
    - ALOG = Number of Analog Trunks Channels
    - ADSL = Number of ADSL channels.
    - VCOMP = Number of VCM channels installed.
    - MDM = Size of Modem Card Fitted
    - WAN = Number of WAN Ports configured.
    - MODU = Number of TDM units attached (i.e. POTS, DT units etc.)
    - LANM = Number of LAN Modules attached (i.e. WAN3s)
    - CkSRC = Current Clock Source (ISDN port number - 0 = NO Clock Source)
    - VMAIL = 1 if connected, 0 if not (VER is the s/w version of the Vmail Server)
    - CALLS = Number of current calls (TOT - total number of calls made to date since last PBX reboot.)

Voicemail

Access to voicemail and whether this requires VCM or data channels depends upon the type of voicemail system being used. This section only covers dedicated IP Office Voicemail servers.

- **Integral Voicemail** *(IP401 and Small Office Edition only)*
  Integral Voicemail is implemented using a VCM module plus a PCMCIA Smart Media card for prompt and memory storage. VCM channels are used for all calls to the Embedded Voicemail.
  - This means that a call from a VoIP extension to Integral Voicemail will use two VCM channels. A call from a non-IP extension uses just a single VCM channel.
- **Voicemail Lite & Voicemail Pro**
  The Voicemail Server PC is physically attached to the IP Office via a LAN port. However all devices on the system see the Voicemail Server as if it is a device on the TDM bus. This means:
  - For non-IP phones, no VCM channels are used.
  - For each IP phone calling voicemail, a VCM channel is used.
  - Each voicemail user uses a data channel.
- **Centralized Voicemail Pro**
  In this solution the IP Office systems are connected by VoIP trunks.
  - Calls to voicemail from the remote IP Office require a VCM channel on both the remote and central IP Office systems.
  - Calls from remote IP Office IP extensions require a VCM channel on the remote system only during call setup. They require a VCM channel on the central system for the whole call.
- **AUDIX INTUITY Centralized Voicemail**
  This solution can be connected either via a PRI connection or via an H.323 IP connection.
  - If using a PRI connection, the number of available VCM channels limits the number of calls between IP Office IP extensions and the central PBX.
  - If using an H.323 connection, the number of available VCM channels limits the number of simultaneous calls between IP Office non-IP extensions and the central PBX. IP Office IP extensions only require a VCM channel during call setup.

Paging

Paging from IP Office

Paging to and from IP Office phone's is covered by the appropriate telephone user guides. This section covers paging to 3rd-party paging equipment (centrally amplified paging systems or self-amplified speakers).

Typically, 3rd-party paging equipment uses analog connections. The IP Office can provide analog connections via either analog trunks or analog extensions. In terms of flexibility of operation once installed, the use of an analog extension port for paging is the preferred solution.

WARNINGS:

- The Paging Equipment must provide isolation to the IP Office analog port or an additional interface device must be fitted.
- The Paging Equipment (and separate interface device if used) must conform to the local and national telecommunications device regulation:
    - USA: FCC approval.
    - European Union: CE marked indicating compliance with the EMC (EN41003) and Low Voltage (EN60950) directives.
    - All other countries: use equipment that complies with locals and national telecommunication device regulation.
- Failure to observe the notes above could result in damage to the IP Office or the 3rd-party equipment.

Universal Paging Access Module

For the US, the Universal Paging Access Module (UPAM) is recommended as the interface device between the IP Office and the Paging Equipment.

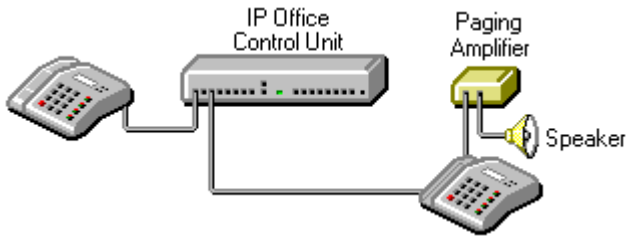
The UPAM:

- Supports analog extension or trunk (loop or ground start) connection.
- Requires a 24V or 48V power supply if used with trunk connections.
- Provides a pre-announce tone heard at the paging extension and over the paging speakers. On/Off selectable.
- Provides a confirmation tone heard by the pager only (not supported for ground start trunks). On/Off selectable.
- Has Paging Time control which sets the maximum page time (6 to 35 seconds) if its other disconnect controls are disabled.
- Supports background music input via an RCA-type jack.

Paging via an Avaya 20 Series Digital Telephone

A page call to any 20 Series digital telephone (2010, 2030, 2050 or 20CC), where the handset is physically off-hook and the telephone is idle (not receiving dial tone), is directed to the handset speaker rather than the 20 Series loudspeaker. This option allows external paging systems to be connected to the 20 Series handset cord socket (marked as **H/SET**).

Though this method of connection requires a 20 Series digital telephone and IP Office DT port. It allows the paging device to be part of a group with other extensions that can be paged simultaneously.



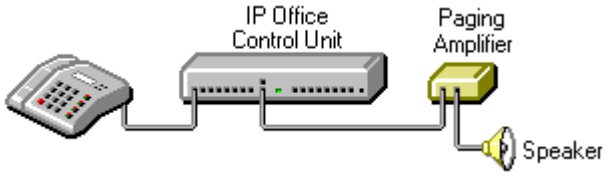
The external loudspeaker system must be CE marked to indicate compliance with the EMC (EN41003) and Low Voltage (EN60950) directives.

- **Loudspeaker Impedance:**
  The matching impedance of the external loudspeaker should be 150 ohms.
- **Voltage Levels :**
  The typical voltage levels on an Avaya 20 Series handset Rx output are:
  - **Minimum volume:** 55mV peak to peak.
  - **Maximum volume:** 555mV peak to peak.
- **Wiring Connection:**
  RJ11 using pins 2 and 3 (the inner pair).

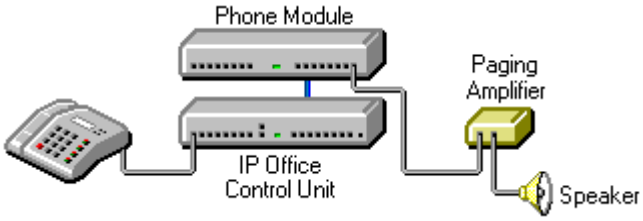
Paging via an Analog Extension Port (POT Port)

IP Office analog extension ports are marked as POT. These can be used for the connection of third-party paging equipment.

The IP Office 401 (not available in North America) and IP Office 403 Control Units have integral POT ports.



POT ports can also be installed by the addition of an IP Office Phone Module to the system.



The Paging Amplifier must provide isolation or an additional isolation device should be fitted.

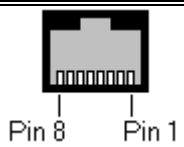
The Paging Amplifier (and separate isolation device if used) must conform to the local and national telecommunications device regulation.

If not done automatically, it may be necessary to set the **Paging Amplifier** to give priority to the VOX input.

Do the following to set up a page via an analog extension port:

1. IP Office POT Port Wiring Connection

   Connections to POT ports should use a twin-pair cable wired as follows:

POT RJ45 Socket	Pin Number	Description
	1 and 3	Do not use.
	2	Bell
	4	A: Ring
	5	B: Tip
	6	Bell
	7 and 8	Do not use.

   - Pins 2 and 6 are connect to pin 5 via a ringing capacitor.

   The POT ports are rated as follows:

   - Off-Hook Current = 25mA.
   - Ring Voltage = 40V rms.
   - REN = 2

2. Configure the Analog Extension

   To configure the analog extension:

1. Start IP Office Manager and receive the configuration from the IP Office.
2. Click the **Extension** icon to display the list of extensions.
3. Double-click on the extension that will be used for the paging equipment connection.
4. In the **Extn** tab, set the following:
   - Set the **Equipment Classification** to ***Paging Speaker***.
   - Set **Caller Display Type** to ***Off***.
5. Click on **OK**.
6. Note that the icon for the extension has changed from to . In this mode the extension connects the speech path imeediately without any ringing.

3. Configure the Analog Extension User

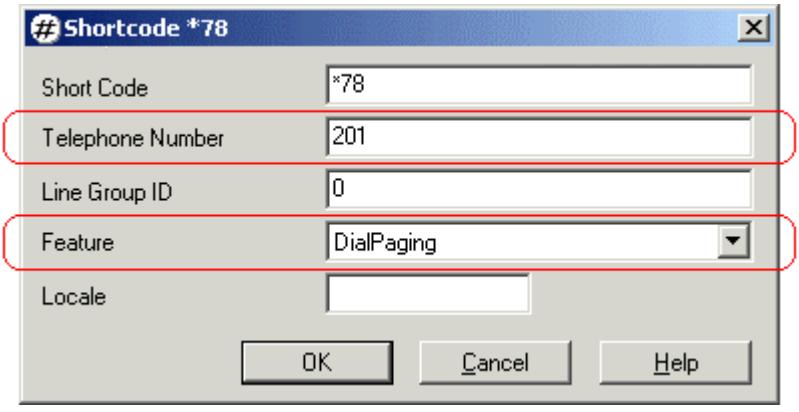
1. Click the **User** icon to display the list of users.
2. Double-click the user currently associated with the extension above.
3. In the **User** tab, set the following set the **Name** to ***Paging*** or similar to indicate the function.
4. In the **Voicemail** tab untick **Voicemail On**.
5. Click **OK**.

4. Create Short code for Paging the Extension

This stage is optional. Since the connection is via a extension with an associated user, page calls can be made using the appropriate user name or number (see "Making Page Calls"). If you skip short code creation, send the new configuration to the IP Office and reboot.

Do the following to create a short code:

1. Click on the **ShortCode** icon to display the list of short codes.
2. Right-click on the list and select **New**.
3. Enter the settings for the short code that users should dial when to make a paging call:



   - **Short Code: *78***
     The numbers users should dial to do a page. *78 is just an example.
   - **Telephone Number:*201***
     The analog extension connected to the paging equipment.
   - **Feature: *DialPaging***
     Note that ***DialPaging*** is used for an analog extension connection. ***Dial*** is used for an analog trunk connection. .
4. Click on **OK**.

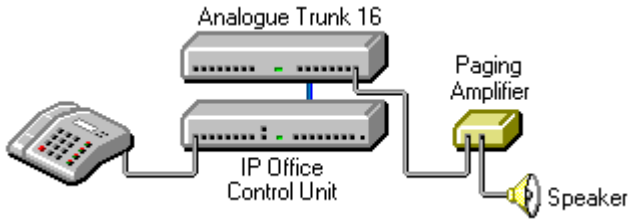
5. Send the new configuration to the IP Office and reboot.

Paging via an Analog Trunk Port

You can use the analog trunk ports provided by the ATM4 or ATM16 modules.

The ATM4 is an internal module installed into the IP Office Control Unit. Note that the ATM4 only provides Loop Start analog trunk ports.

The ATM16 is an external expansion module. It supports both Loop Start and Ground Start analog trunks.



As previously stated the Paging Amplifier must provide isolation or an additional isolation device should be fitted.

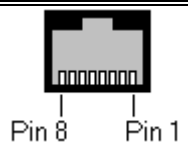
The Paging Amplifier (and separate isolation device if used) must conform to the local and national telecommunications device regulation.

The paging connection must provide power in order to be seen as a real trunk by the IP Office.

Do the following to set up a page via an analog trunk port:

1. Analog Trunk Port Wiring Connection

   The analog trunk ports on IP Office modules are RJ45 sockets. Connections to these should use a single-pair cable wired cable as follows:

RJ45 Socket	Pin Number	Description
	1 to 3	Do not use.
	4	A: Ring
	5	B: Tip
	6 to 8	Do not use.

2. Line Configuration

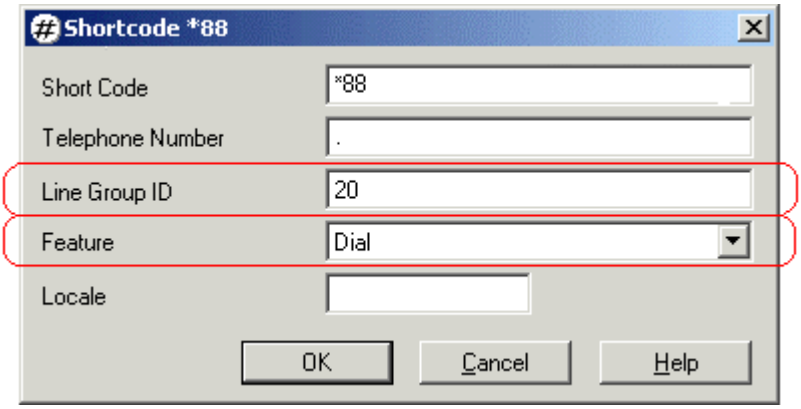
   Configure the line via the Line configuration form in Manager:

   1. Receive the configuration from the IP Office.
   2. Click on the **Line** icon to display the list of installed lines.
   3. Analog lines appear as shown with icons. Double-click on the line that will be used for paging.
   4. In the **Line** tab, set the following:
      - In the **Telephone Number** field enter a note indicating that this is the line to the paging equipment, eg. ***Line to Paging***.

- Set the **Outgoing Group ID** to a unique value, ie. one not used by any other line. This number will be used in a short code that routes page calls to this line.

5. In the **Analog** tab, set the following:
   - Set the **Trunk Type** to ***Loop Start***. Note: This is the only option with ATM4 trunks. With ATM16 trunks ***Ground Start*** can be used if required by the paging equipment.
   - Leave the remaining values at their defaults unless the instructions of the paging equipment manufacturer indicate that other values are required.
6. Click **OK**.

3. Short Code for Paging the Trunk
   1. Click the **ShortCode** icon to display the list of system short codes.
   2. Right-click on the list and select **New**.
   3. Enter the settings for the short code that users should dial when to make a paging call:



   - **Short Code: *88***
     This is the numbers users should dial to do a page. *88 is just an example.
   - **Telephone Number:** .
   - **Line Group ID:*20***
     This must match the Outgoing Group ID set for the analog trunk.
   - **Feature: *Dial***
     Note that ***Dial*** is used for an analog trunk connection. ***DialPaging*** is used for an analog extension connection.
   4. Click **OK**.
   5. Send the new configuration to the IP Office and reboot.

Making Page Calls

Making Page Calls

Having setup and tested the paging equipment, users can begin to use it.

If the paging device has been connected via an analog extension port, then the page call features provided for different phones can also be used to page the extension number. Refer to the appropriate phone user guide. Otherwise users can dial the short code setup for paging.

The following methods can be used to make page calls.

Paging via a DSS Key

For extensions with DSS keys, paging can be assigned to one of those keys. The following method programs the key via the Manager application.

1. Start Manager and load the IP Office configuration.
2. Click **Users** to display the list of Users. In the list, double-click the user whose DSS keys you want to edit.
3. Select the **Button Programming** tab (**Digital Telephony** tab on UK English systems).
4. For the required DSS button, select ***Dial*** as the **Action**. For the Telephone number enter the paging short code or the extension number or the extension name in quotes.
5. Click **OK**.
6. Save the new configuration.

Paging from Phone Manager

You can add a speed dial to Phone Manager in order to make paging calls.

1. Within the users Phone Manager, select the Speed Dials tab.
2. Right-click on the tab area.
    - If paging via a analog extension port, select **Add User** and select the appropriate user.
    - If paging via an analog trunk port, select **New**. Enter a name and enter the paging short code as the number.

Group Paging

If the paging connection is via an extension port, that extension can be included in a group with other pageable extensions. This allows page calls to be heard via the speaker and over pageable telephones.

To set up group paging:

Create a Hunt Group with all the users required as members.

Set the Hunt Group to "Group" ring mode and to turn off the Voicemail and Queuing facilities.

Create a short code to call the Hunt Group using the DialPaging feature,

- **Short Code:** *81
- **Telephone Number:** 305
- **Line Group ID:** 0
- **Feature:** DialPaging

- Note TransTalk 9040 MDW sets do not receive page calls, but may make them.

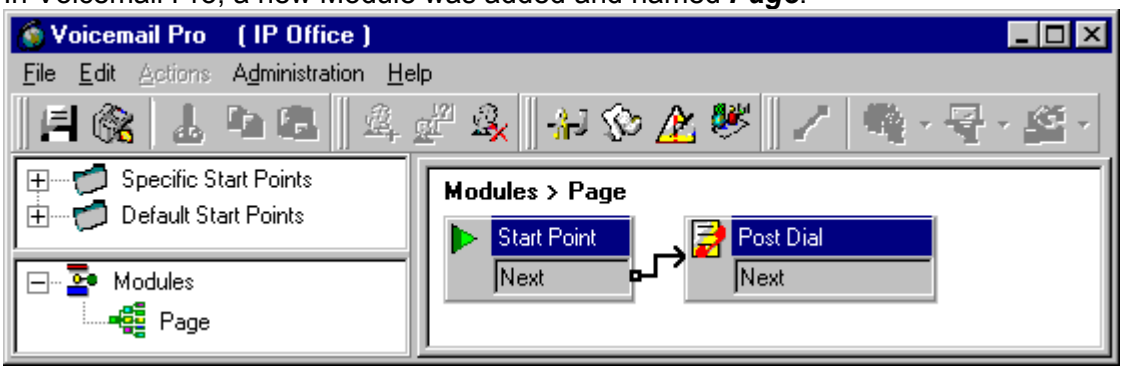
Voicemail Pro

Voicemail Pro can be used to deliver pre-recorded announcements. This can be useful when the same announcement is repeated frequently. This method requires the paging port to be an analog extension.

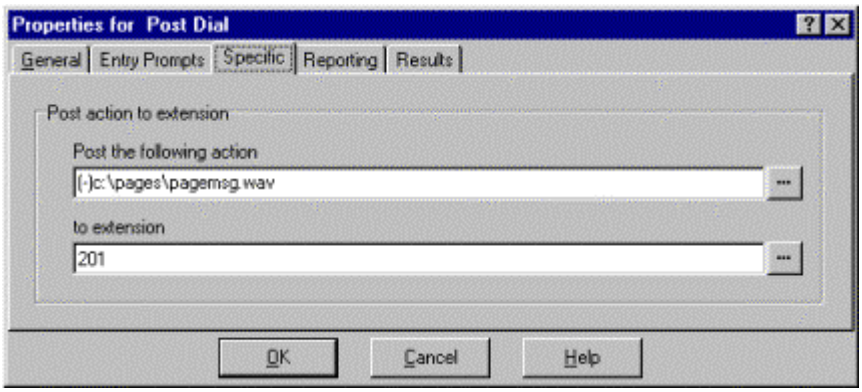
This method also removes the feedback loop that can occur on some sites as the page is first recorded and then played.

Example 1 of a paging method via Voicemail Pro:

1. In Voicemail Pro, a new Module was added and named ***Page***.

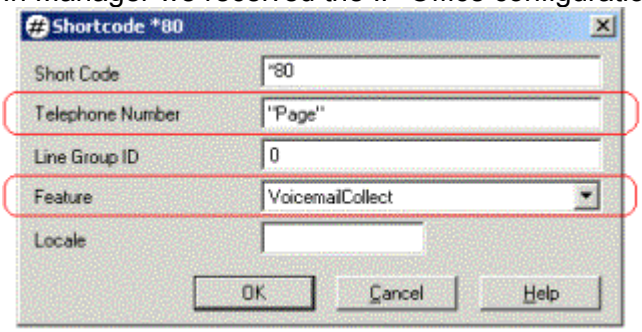


2. A **Post Dial** action was added to the module. The properties of the Specific tab were set as shown:



   - The **Post the following action** field was set to the address of the .wav file we want played. The **(-)** in front indicates play once. In the **to extension** field we put the extension number to which the message should be played, in this case a paging port.

3. We then saved and made live the new Voicemail Pro call flow.
4. In Manager we received the IP Office configuration and created a new short code.

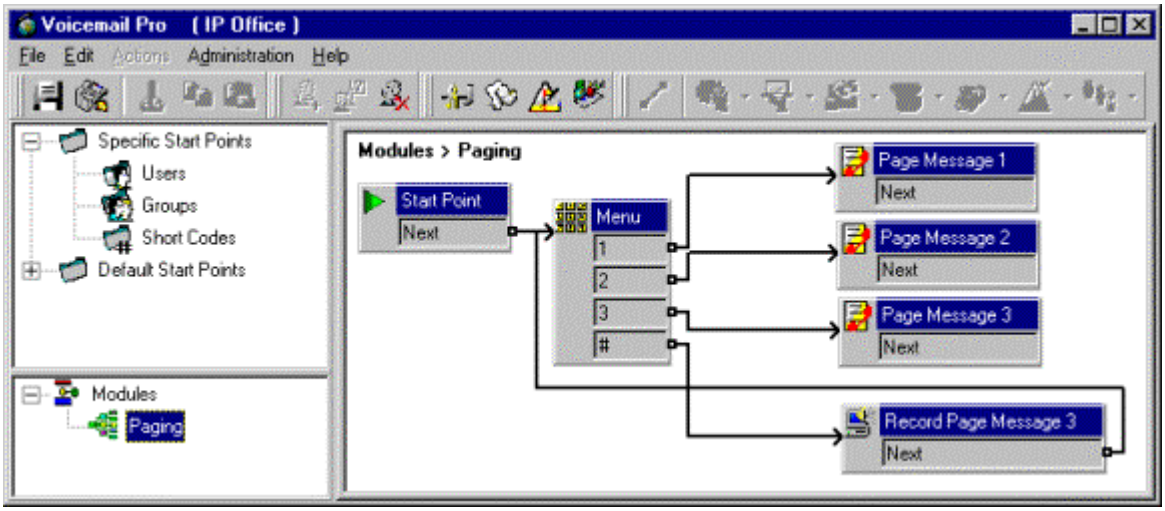


   - The **Telephone Number** matches the name of the Voicemail Pro module in quote marks.
   - The **Feature** is ***VoicemailCollect***.

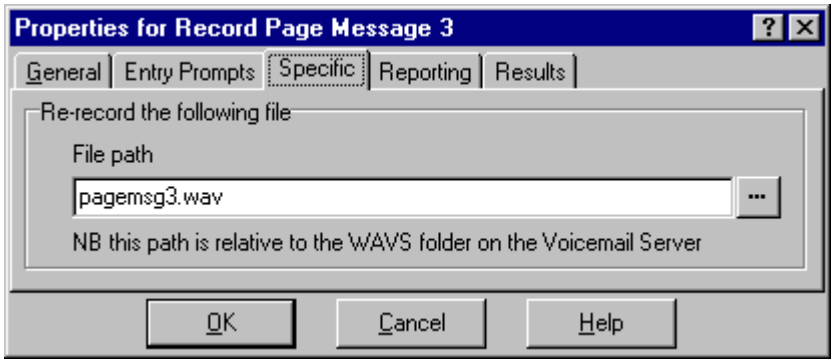
5. The new IP Office configuration was then merged.

Example 2 of a paging method via Voicemail Pro:

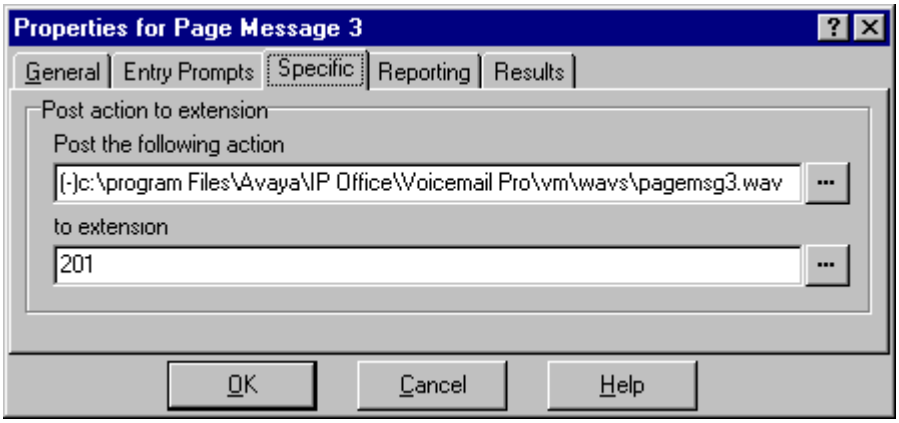
This example builds on example 1 by allowing the user to select which message is played from a menu. In this example the user can press 1, 2 or 3 for different messages. They can also re-record the message associated with option 3 by pressing #.



A **Play List** action was added and in this example set to record ***pagemsg3.wav***. Note that just the file name was specified as this action saves files relative to the Voicemail Server's WAVS folder.



In the **Post Dial** action that plays back ***pagemsg3.wav*** note that the full file path needs to be used.



In IP Office Manager, we then added a short code that triggers the module **"Paging"** using the **VoicemailCollect** feature.

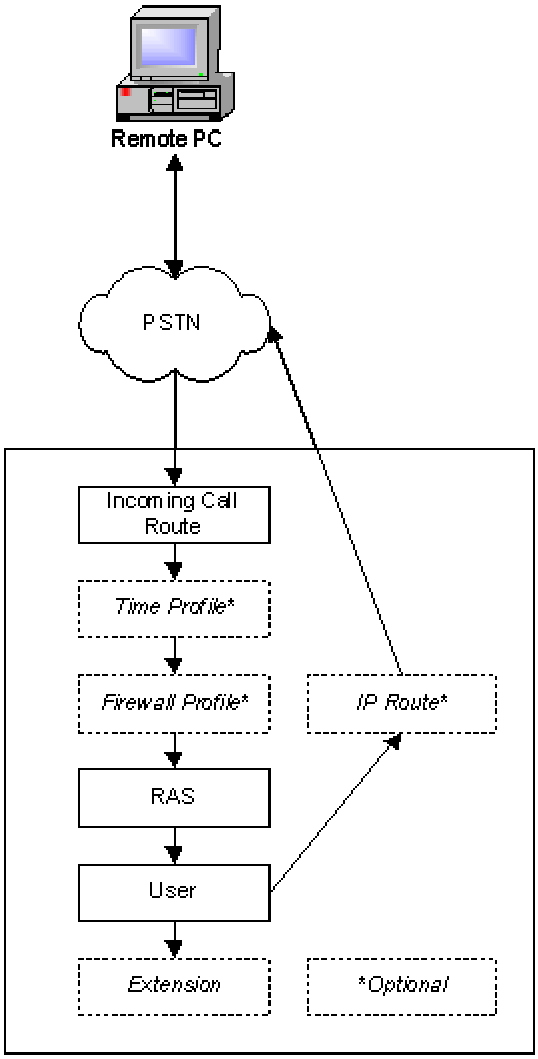
Remote Access

Remote Access

In some cases, there may be a need for connecting a remote PC to an IP Office system. Once connected, the remote PC is part of the IP Office network and can run many of the IP Office applications.

- **WARNING: Do Not Run Upgrade Across RAS Links**
  The Upgrade facility within the IP Office Manager application should not be used over a RAS link of any kind. To do so will result in a 'frozen' Control Unit which will have to be returned to its factory defaults via its DTE port.

The diagram below is a general schematic of RAS.



The need for an IP Route within the IP Office is dependant on the respective IP address domains of the remote PC and the IP Office.

Note: If the connection is via analog, modem or line, the IP Office must also have Modem2 module installed.

IP Office Remote Access Setup

The following process defines a **RAS User** on the IP Office system.

1. **Create a User**
   Click the **User** form within the Configuration Tree to display the list of existing users. Right-click on the list area and select **New**. The required details are:
   - In the **User** tab:
     Enter a **Name** and **Password**. IP Office is case sensitive. Remember to take care with passwords as this is a remote access link into your network.
   - In the **Dial In** tab:
     Ensure that **Dial In On** is ticked.
2. **Create a RAS Entry**
   Click the **RAS** form within the Configuration Tree to display the list of existing remote access services. Right-click on the list area and select **New**.
   - In the **RAS** tab:
     You must enter the same name as the user that you created earlier. Again, remember this is case sensitive.
3. **Create an Incoming Call Route**
   Click the **Incoming Call Route** icon to display the list of existing routes. Right-click on the list area and select **New**.
   - If using an analog modem set the **Bearer Capability** to ***Any Voice***. If using a digital connection set the **Bearer Capability** to ***Any Data***. In the **Destination** drop-down list, select the RAS entry created above.
   - The values that you enter for any of the other fields will depend on whether the remote user will be calling in on a particular line, number or from a set CLID.
4. **Is a Return IP Route Needed ?**
   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.
   - This is not necessary if the remote user has an IP address on same domain as the IP Office. Go to Step 6.
   - 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. Go to Step 6.
5. **Create a IP Route**
   Click on the IP Route icon to display the list of existing routes. Right-click on the list area and select **New**.
   - Enter the IP Address and IP Mask of the remote system.
   - In the **Destination** drop-down list select the RAS entry created above.
6. Send the configuration to the IP Office and reboot.

Remote Access Using Analog Lines

If the remote connection is using an analog line, then the same principles apply except for the following:

- The IP Office must have IP Office Modem2 card installed in order to handle analog data calls.
- To determine if your IP Office Control Unit has a Modem2 card installed, start **Monitor**. One of the first lines shown includes the item MDM= followed by the number of modem circuits.
- Using the **Incoming Call Route** menu, you MUST be able to clearly identify the analog RAS call, either by its incoming number or by the CLI. Create a route entry for this with the **Bearer Capability** set to ***Any*** (there is no D-Channel signal from an analog line so the call is not automatically recognized as data) and the **Destination** set to the RAS entry previously created.

Additional User Controls

Other aspects of system programming that can effect remote access:

- **Time Profiles:**
  A Time Profile can be used to specify when a user can remotely access the system. Once a profile has been created, it is applied to the user through their **User | Dial In** tab.
- **Firewall Profiles:**
  A Firewall Profile can be used to specify what types of traffic can be run across a remote access connection. Once a profile has been created, it is applied to the user through their **User | Dial In** tab.
- **VoIP Extensions:**
  In theory a VoIP call could be run across the remote access connection. However in practice the quality would be reliant on the all parts of the call connection route supporting QoS.
- Note: If a remote access user runs an H.323 IP Softphone, for example an IP Enabled Phone Manager Pro, the H.323 Gateway on the IP Office would create a new extension and user for that Softphone (subject to IP Office licensing). For programming neatness, and to give the remote user a fixed extension number, it may be better to manually create a VoIP Extension and associate it with the RAS User.

Remote Dial-Up PC Setup

These instructions assume that you are using a PC with a Microsoft Windows operating system. However the general principles are applicable to any PC capable of dial-up networking.

1. If the IP Office running **DHCP** is in ***Server*** or ***Dial In*** mode, then set the PC's Network Properties for TCP/IP via the Dial-Up Adapter to **Obtain an IP Address Automatically**. This does not affect the PC's network card settings, which can be running a separate set of IP address settings.
   - You can also alter the TCP/IP settings of individual dial-up connections to either **Server Assigned Address** (DHCP) or to a fixed IP Address (ie. one matching the IP Office's domain).
2. Create a new dial up networking session.
3. Ensure that the **User Name** and **Password** match those created for the RAS User on the IP Office.
4. The telephone number dialed or the CLI from which dialing occurs must match the incoming call route created for remote access.

Remote Domain Browsing and LMHOSTS

Over a basic RAS connection, the remote PC is able to route IP traffic into and out of the IP Office network.

For the remote PC to be able to browse network drives and facilities on the IP Office network requires further setup. This is done via the use of a LMHOST file on the remote PC and requires information from the Network Administrator relating to the network's Domain Controllers and other devices.

Full details of this can be found in Microsoft Knowledge Base Article -Q150800.

Small Community Networking

Small Community Networking

With Small Community Networking (SCN) enabled, the separate IP Office systems 'learn' each others extension numbers. This allow extension calls between systems and support for a range of internal call features.

In IP Office Software Level 1.3, Small Community Networking supports a maximum of 500 extensions across 16 IP Office systems.

Scenario

Within the Small Community Networking section, the linking of two IP Offices are outlined - System A and System B. The routing of data traffic between the two has already been checked and tested. The two systems are configured as follows:

	System A	System B
IP Address:	192.168.42.1	192.168.43.1
Extensions and hunt groups numbered from:	2000	3000

Requirements

To set up a small community network, the following are required:

- A working LAN or WAN link exists between the IP Office systems and that the link has been tested for correct data traffic routing.
- VCM modules are required in the remote and central systems.
- The extension and group numbering on both systems must be unique.
- The extension and group names on both systems must be unique.
- We also recommend that all names and numbers (groups, line, services, etc) on the separate IP Office systems are kept unique. This will reduce potential maintenance confusion.
- All systems should use the same set of **Telephony** timeouts, especially the **Default Allocated Answer Interval** (**System | Telephony**).

For more information on the role of the VCM module in handling VoIP calls, see VCM & Data Channels.

For details on using a single Voicemail Pro server to provide voicemail services in an IP Office Small Community Network, see the **Voicemail Pro Installation & Maintenance Manual**.

Enabling Small Community Networking

Setup the VoIP Line from System A to System B

1. On System A, receive the system configuration.
2. Click the **Line** configuration form to display a list of existing lines.
3. Right-click on the displayed list and select **New**.
4. In the **Line** tab for the VoIP line set the following:
    - Set a unique **Line Number**. Anything over 30 is recommended to avoid clashing with an physical lines that may be added to the system. In this example we will use ***3000***.
    - In the **Telephone Number** field, enter a description of the link, eg. "***System B***".
    - Set the **Outgoing Group ID** to a unique value; ie. one not already used for lines connecting elsewhere. For this example, we will use ***3000*** again.
5. In the **VoIP** tab for the VoIP line, set the following:
    - Ensure that **Voice Networking** is ticked. This enables the exchange of directory and user information between the IP Office systems and is the key enabler of Small Community Networking.
    - For the **Gateway IP Address** enter the IP address of System B.
    - Select the preferred **Compression Mode**. The same mode must be used by all VoIP lines and extensions within the network.
    - Check that the **H450 Support** option is set to ***H450***. This enables various Supplementary Signaling Services across the VoIP connection. QSIG can be used if H450 is not supported across the VoIP connection. However QSIG support fewer supplementary signaling features.
6. Load the configuration and reboot System A. Note: Configuration changes and additions to VoIP line settings cannot be merged.

Setup the VoIP Line from System B to System A

7. On the remote system, repeat the previous steps to create a VoIP VPN link to System A.
    - Ensure that the **Compression Mode** selected in the **VoIP** tab of the VoIP line is the same at both the central and remote system.
    - Load the configuration and reboot the remote IP Office.

Test Small Community Networking

8. Test by making calls between extensions on the different systems.

SCN Programming Tip

The simplest example of a Small Community Network setup is a connection between two IP Offices. In a larger network however, the number of VPN trunk connections on each system may be much larger.

To set up a small community network on a larger network, do the following:

1. In Manager, open the configuration file from one of the systems.
2. Click on **Line** to display the existing lines.
3. Delete the physical lines by right-clicking on each and selecting Delete.
4. Add the VoIP VPN line entries, adding one for each IP Office that will be in the Small Community Network.
    - Remember to enable Voice Networking and H450 on each entry.
5. Select **File | Import/Export | Export Configuration Entities**.
6. In the range of entries, tick **Line** and then click **OK**.
7. All the VPN line entries for the Small Community Network will have now been exported to a separate file (by default a file called ***config.exp*** in the Manager program folder).
8. Close the configuration without saving it (**File | Close**).
9. Load the configuration one of the IP Office systems in the Small Community Network and use **File | Import/Export | Import Configuration Entities** to load the VoIP VPN line settings.
10. Click on **Line** to display the lines.
11. Delete the entry for the line to the site.
12. Save the new configuration back to the IP Office and reboot.

This technique can also be adapted to ensure consistent account codes, firewall profiles, etc. on systems in the same network. A common directory can also be shared between systems using **File | Import/Export | Export Directory and Import Directory**.

Short Code Programming for Small Community Networks

With Small Community Networking enabled, the IP Offices 'learn' each others extension numbers and route extension calls appropriately.

However the same does not apply to dialing group and other numbers meant for the remote IP Office. To allow these to be routed correctly across the VoIP VPN links, short codes can be used.

- **Scenario**
  We want a short code on System A which will correctly route any 3000 range number to System B. This will allow System B group numbers to be dialed from System A.

To achieve the above scenario, we will add a new system short code. By using a system short code it becomes available to all users.

1. Receive the configuration from System A.
2. Click the **Short code** configuration form to display a list of existing system short codes.
3. Right-click on the displayed list and select New.
4. Enter the short code settings as follows:
   - **Short Code: *3XXX***
     This will match any four-digit number beginning with 3.
   - **Telephone Number: .**
     The . indicates that the short code should output the digits as dialed.
   - **Line Group ID: *3000***
     This should match the **Outgoing Group ID** given to the VoIP VPN line connected to System B.
   - **Feature: *Dial***
5. Click **OK**.
6. If the only changes made to the configuration was this short code, load the new configuration using merge, otherwise load the configuration and reboot.
7. A similar system short code can be added to System B's configuration to route 2XXX dialing to System A.

Dial Name

Dial Name

IP Office includes a Dial Name feature for making internal and external calls. It allows users to make calls by dialing the name on their telephone keypad and making a selection from the displayed matches or dialing further characters to improve the match.

When used to make internal calls, the name matches are based on the User Names and Full Names programmed into the system. If a user has a Full Name programmed then that takes precedence over their User Name.

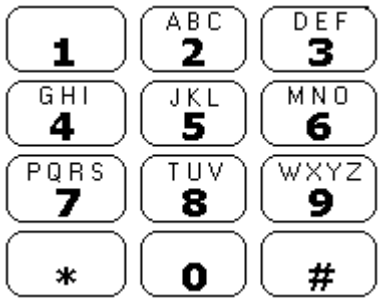
When used to make external calls, the name matches are based on entries in the IP Office Directory.

On supported 4400, 4600 and 6400 series phones Dial Name also supports hunt group names.

Dial Name is supported on the following telephones:

- Avaya 2030, 2050 and 20CC telephones.
- Avaya 4400, 4600 and 6400 Series telephones which have **Menu** and ◀ ▶ keys .

The Dial Name feature uses the ITU key character layout:



Configuration in Manager

Selecting Dial Name Mode:
If **Dial Name** is not selected, the INDeX and Dir features on the telephones operate in their pre-Dial Name capability.

1. In Manager, receive the IP Office's configuration.
2. Double-click **System** to display the **System** form.
3. Select the **Telephony** tab.
4. The **Dial Name** checkbox should be ticked to enable Dial Name mode features.
5. Send the IP Office configuration back to the system and reboot.

Setting User Full Names:
The process below details doing this through Manager. User can also do this through their own telephone *(see Editing the DS User's Full Name and Editing the DT User's Full Name)*.

1. In Manager, receive the IP Office's configuration.
2. Click **User** to display the list of users.
3. Double-click the required user to display their **User** form.
4. In the **Full Name** field enter the name required. Do not use characters other than Aa to Zz and 0 to 9.
5. Click **OK**.
6. Repeat for all users required.
7. Send the IP Office configuration back to the system. If this is the only change made then you can use the merge option.

Adding Directory Entries:
Note that Directory entries are also used for other functions such as name matching against received CLI on incoming calls.

1. In Manager, receive the IP Office's configuration.
2. Click **Directory** to display a list of current entries.
3. Either double-click on an entry to change and right-click on the list and select **New**.
4. Enter the **Name** and **Number** and click **OK**.
5. Repeat for all entries required.
6. Send the IP Office configuration back to the system. If this is the only change made then you can use the merge option.

Dial Name in Small Community Networks

User Names and Full Names are shared within a Small Community Network and thus are available for Dial Name features. This also applies to Group Names.

Directories are not shared within a Small Community Network, so only the Directory of the user's local IP Office is available for Dial Name features.

Use Dial Name with DS Phones

This feature is only supported on phones with a **Menu** and ◀ and ▶ keys. These phones can display a directory of group names, extension names or directory names from which you can select and then dial.

Note: This feature can work in two modes, Classic or Dial Name mode (the default). Contact your System Administrator if unsure which mode your telephone system uses.

To use the directory:

1. Press **Menu** and select **Dir** (this feature can also be set under a DSS key).
    - Alternatively, press **Menu** twice. Press ▶ and then select **Dir**.
2. Select from **INDeX** (internal extension), **Group** (Hunt Groups) or **Extrn** (numbers in the IP Office Directory).
3. The next steps depend on which mode of working your system is using:
    - **Dial Name Mode**
        1. Using the letter keys, start dialing the name that you want, eg. for names starting with ***John*** dial ***5646***. Ignore any spaces in the name.
        2. The display will show the first match to the letters entered so far. Either enter further letters or:
        3. Press the ◀ and ▶ keys on either side of the current name to display the other matches found so far.
        4. If **NO MATCH** is displayed press ◀ to go back to the previous step.
        5. When the name you want is shown select **Call**.
        6. If you cannot find the name you want press **Exit** twice.
    - **Classic Mode**
        1. Press the dial pad button that matches the first letter of the name you want. For example, to select ***L*** press the **5** key three times.
        2. Use the ◀ and ▶ keys to move through the matching entries. You can press another key on the dialing pad to select a different first letter.
        3. When the name you want is shown select **Call**.
        4. If you cannot find the name you want press **Exit** twice.

Accessing the Dir Function via a DSS Key

The **Dir** function can be assigned to a DSS key if required.

Programming a DSS Key from the Terminal:

1. Press **Menu**.
2. Using the ◀ and ▶ keys, display and then select **Admin**.
3. Select **Dir**.
4. Press the DSS key against which you want the function programmed.
    - If the key is already programmed you will see options to **Repla**, **Keep** or **Delete**. Select the option required.
5. **BUTTON PROGRAMMED!** is used to indicate that the DSS key has now been programmed with the **Dir** function. Select **Cont**.
6. Press **Exit**.

Programming a DSS Key via Manager:

1. Start Manager and receive the IP Office's configuration.
2. Click on **User** to display the list of users.
3. Double-click on the required user to display their **User** form.
4. Select the **Button Programming** tab.
5. Locate the DSS button against which you want to program the ***Dir*** function.
6. Click on the **Action** field and select **Emulation | Directory**.
7. Click on **OK**.
8. Send the configuration back to the IP Office. If this is the only change made then you can use the merge option.

Editing the DS User's Full Name

This changes the full name stored by the telephone system. The full name is used within the directory function and by the PhoneManager application. It does not change the name shown when making and receiving calls.

To change your extension name:

1. Press **Menu** twice.
2. Press ▶ and select **ProgA**.
3. Press ▶ and select **Name**.
4. Enter the new name. Use the dialing keys and **Rotat** to enter characters. For example, to enter an L press the 5 key and then press **Rotat** until an ***L*** is displayed. You can use the top-left display key to backspace.
5. When the text is as you require press **Done**.
6. Press **Exit**.

Use with DT Phones

Dial Name is supported on Avaya 2030, 2050 and 20CC telephones.

Your phone can display an index of telephone extension names from which you can select and make calls. It can also display entries in the IP Office directory for external calls.

Note: This feature can work in two modes, Classic or Dial Name mode (the default). Contact your System Administrator if unsure which mode your telephone system uses.

To make a call using the INDeX: (Dial Name Mode)

1. Press ●**INDeX** for an internal call or **SPEED DIAL** and then ●**INDeX** for an external call.
2. Using the letter keys, start dialing the name that you want, eg. for names starting with ***John*** dial ***5646***. Ignore any spaces in the name.
3. The display will show the first match to the letters entered so far. Either enter further letters or:
   - Press the ● keys on either side of the current name to display the other matches found so far.
   - Press ●**CYCLE** to display any alternate set of matches, ie. dialing ***527*** matches names starting with ***JAS*** (ie. Jason) or ***KAR*** (ie. Karl).
   - If **NO MATCH** is displayed press ●**PREVIOUS** to go back a step.
4. When the name required is displayed, press ●**CALL**, otherwise to exit press **ANSWER RELEASE**.

To make a call using the INDeX*: (Classic Mode)*

1. Press ●**INDeX** for an internal call or **SPEED DIAL** and then ●**INDeX** for an external number.
2. Press the key matching the 1st letter of the name you want. For example, to display names beginning with **L**, press the **JKL** key 3 times.
   - To move through the names beginning with L, press the ●-keys on the right and left of the current name.
   - To skip forward 10 names, press ●**SKIP**.
   - To select another letter, press a letter key.
3. To dial the name/number shown, press ●**CALL**, otherwise to exit press **ANSWER RELEASE**.

Editing the DT User's Full Name

1. Press **PROGRAM** and then press **SPEAKER**.
2. To change the name press ●**EDIT**.
   - Enter the current passcode.
   - Use the ● key on the left of the name to delete the last character.
   - Use the ● key on the right of the name to add spaces.
   - To add a character press the matching key on the telephone keypad and the press ●**ROTATE** to change the character to the one required.
   - When you have completed the name press ●**DONE**. Use ●**REFORMAT** to select all upper-case or mixed case letters. Press ●**DONE**.
3. Press **PROGRAM** to return to normal use.

Index

B

C

D

E

F

G

H

M

N

P

Q

R

S

T

U

V

W

X

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