IP Office 4.2

H323 IP Telephone Installation

15-601046 Issue 14j - (10 March 2009)

© 2009 AVAYA All Rights Reserved.

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

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

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

License
USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.
Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.
License Type(s): Designated System(s) License (DS).
End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
Copyright
Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

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

Avaya Fraud Intervention
If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. Suspected security vulnerabilities with Avaya Products should be reported to Avaya by sending mail to: securityalerts@avaya.com.
For additional support telephone numbers, see the Avaya Support web site (http://www.avaya.com/support).

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

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

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

Contents

1. IP Office IP Phones

1.1 What is New 8
1.2 Supported Phones 9
1.3 System Capacity 10
1.4 Phone Firmware 11
1.5 Simple Installation 12
1.6 Complex Installation 13
1.7 Installation Requirements 14
1.8 Network Assessment 15
1.9 Voice Compression 16
1.10 QoS 18
1.11 Potential VoIP Problems 18
1.12 User PC Connection 19
1.13 Power Supply Options 20
1.14 File Server Options 22
1.15 Control Unit Memory Card 23

2. Installation

2.1 Creating/Editing the Settings File 28
2.2 Manually Creating Extensions 29
2.3 Phone Connection 30
2.4 Static Address Installation 31
2.5 Phone Registration 32
2.6 Extension & User Setup 33
2.7 Phone Security 33
2.8 Backup Restore 34
2.9 Listing Registered Phones 37
2.10 Error Messages 38

3. Other Installation Options

3.1 VPN Remote Phones 40
3.2 VLAN and IP Phones 43

4. Static Administration Options

4.1 QOS Option Settings 51
4.2 Secondary Ethernet (Hub)/IR Interface Enable/Disable 51
4.3 View Details 52
4.4 Self-Test Procedure 53
4.5 Resetting a Phone 54
4.6 Site Specific Option Number 55
4.7 Automatic Gain Control 56

5. Restart Scenarios

5.1 Boot File Needs Upgrading 59
5.2 No Application File or Application File Needs Upgrading 59
5.3 Correct Boot File and Application File Already Loaded 59

6. Infrared Dialling

6.1 Enabling the IR Port 63
6.2 Dialling Phone Numbers 63
6.3 Beaming Files During a Call 64

7. Alternate DHCP Server Setup

7.1 Using a Windows DHCP Server 67
7.2 Alternate Options 70

8. WML Server Setup

8.1 Testing 4620 WML Browsing Using Xitami 73
8.2 Setting the Home Page 75
8.3 Apache Web Server WML Configuration 76
8.4 Microsoft IIS Web Server WML Configuration 76
8.5 Open URL Entry 77
Index 79

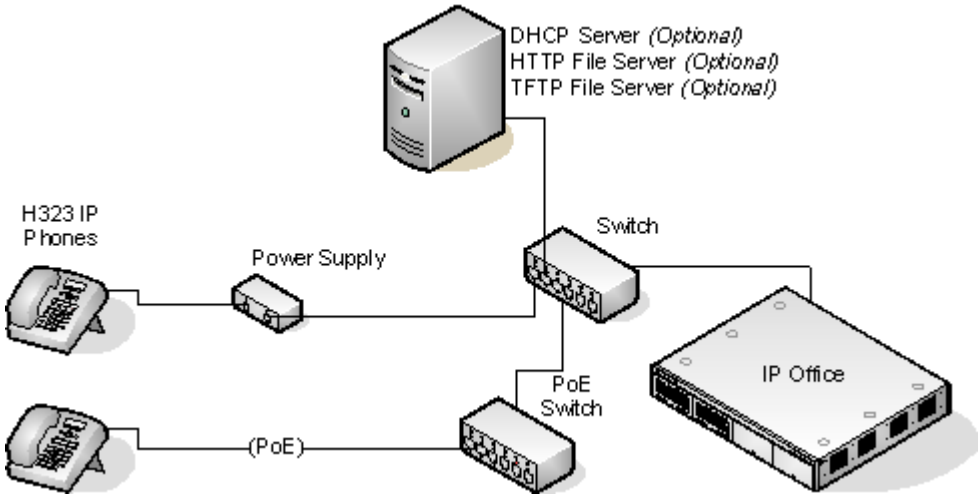
Chapter 1.
IP Office IP Phones

1. IP Office IP Phones

This documentation provides notes for the installation of supported Avaya 1600, 4600 and 5600 IP 9 phones onto IP Office phone systems. It should be used in conjunction with the existing installation documentation for those series of phones, especially the following:

- **4600 Series IP Telephone LAN Administrator Guide** *(555-233-507)*.
- **1600 Series IP Telephones Administrators Guide** *(16-601443)*.

Avaya 3600 Series IP telephones, Avaya IP DECT telephones and Phone Manager Pro PC Softphone are covered by their own separate installation documentation.



- **DHCP versus Static IP Installation**
  Though static IP installation of H323 IP phones is possible, installation using DHCP is strongly recommended. The use of DHCP eases both the installation process and future maintenance and administration. For static installations, following a boot file upgrade, all static address settings are lost and must be re-entered.
- **Network Assessment**
  High quality voice transmission across an IP network requires careful assessment of many factors. Therefore:
  - We strongly recommend that IP phone installation is only done by installers with VoIP experience.
  - The whole customer network must be assessed for its suitability for VoIP, before installation. Avaya may refuse to support any installation where the results of a network assessment cannot be supplied. See Network Assessment 15 for further details.

1.1 What is New

IP Office 4.2

The following changes specific to IP phone support have been made as part of the IP Office 4.2 release.

- **Support for 1600 Series Phones**
  IP Office 4.2 Q4 2008+ supports the 1603, 1608, 1616 IP phones.
- **HTTP Server Support**
  For Avaya IP phones using IP Office DHCP, the address of the HTTP server from which those phones should download their software and settings files can now be specified in the IP Office configuration. 4600 Series and 5600 Series phones attempt to load files via HTTPS and then HTTP before falling back to TFTP. 1600 Series IP phones only support HTTPS or HTTP.
  - **HTTP-TFTP Relay**
    The IP Office control unit supports HTTP-TFTP relay for HTTP file requests from phones.
    - **HTTP-TFTP Using an Embedded Memory Card**
      For IP Office 4.2, using the Embedded Voicemail memory card is also supported for HTTP file requests for up to 50 IP phones. This is done by setting the **TFTP Server IP Address** and **HTTP Server IP Address** to the control unit IP address. This method is supported for up to 50 IP phones.
    - **HTTP-TFTP Using IP Office Manager**
      For the IP Office 4.2 Q4 2008 maintenance release, HTTP-TFTP Relay is support using IP Office Manager as the TFTP server. This is done by setting the **TFTP Server IP Address** to the address of the Manager PC and the **HTTP Server IP Address** to the control unit IP address. This method is supported for up to 5 IP phones.
  - **HTTP User Backup and Restore**
    The HTTP file support methods detailed in this manual are for the download of phone firmware, settings and language files to phones. HTTP support for phone user settings backup and restore requires a separate HTTP server, the address of which is defined with the phone settings files rather than through the DHCP server configuration settings.
- **Secondary Site Specific Options Number**
  A Site Specific Option Number (SSON) is used by Avaya IP phones when requesting phone specific settings from a DHCP server. When the IP Office is acting as the DHCP server, the matching number must be set in the IP Office configuration. IP Office 4.2 now provides two fields for settings SSON numbers in order to support Avaya 4600 and 5600 Series IP Phones (which use a default SSON of 176) and Avaya 1600 Series phones (which use a default SSON of 242).
- **IP Phone Restart using System Status Application**
  Individual Avaya IP phones or groups of phones can be selected and then restarted remotely using the System Status Application. This allows individual phones or groups of phones to be restarted in order to upgrade their firmware.
- **IP500 DHCP Enhancements**
  The scope of DHCP support on IP500 has been enhanced in a number of areas.
  - **Full Avaya IP Phone Support**
    Previous only a maximum of 5 IP phones have been supported if using the IP Office for DHCP and TFTP functions. An external DHCP server is required to support more than 5 Avaya IP Phones. For IP Office 4.2+, the IP500 supports up to 272 Avaya IP phones, the maximum extension capacity of the IP500 control unit.
  - **Multiple DHCP IP Address Pools**
    On each IP Office LAN interface, up to 8 DHCP address ranges (called 'pools') can be specified. These pools do not have to be on the same subnet as the IP Office itself. This allows devices being supported by IP Office DHCP to be given addresses on a different subnet than the IP Office.
  - **DHCP for Avaya IP Phones Only**
    The DHCP pools provided by the IP Office can be restricted for use by Avaya IP phones only. The IP Office will then not respond to DHCP request from other devices.
- **Embedded Card File Management**
  For systems with a compact flash memory card installed, the contents of the card can be viewed through Manager. This mode is accessed through the **File | Advanced | Embedded File Management** option. This view can also be used to add and remove files from the card. This may be useful when the memory card is being used to store music on hold files and or phone firmware files.
- **IP500 VCM Controls**
  For IP Office 4.2+, the VCM controls for echo and comfort noise supported in the IP Office configuration (**System | VCM**) are now also applied to IP500 VCM cards.

1.2 Supported Phones

This documentation provides installation notes for the following Avaya IP phone supported by IP Office.

H323 IP Phones	Supported Models	IP Office Core Software	Note
1600 Series	**1603**	Supported on IP Office 4.2 Q4 2008+.	
	1608		
	1616		
3600 Series	**3616**	Supported on IP Office 2.1+.	Also known as Spectralink phones, these IP phones connect via a WiFi network and additional equipment. They are covered by their own separate IP Office installation documentation.
	3626		
	3620	Supported on IP Office 3.2+.	
	3641	Supported on IP Office 4.1+.	
	3645		
4600 Series	**4601**	Supported on IP Office 3.0+	These phones are supported on a range of Avaya phone systems including IP Office. However when used with IP Office the firmware installed on the phones must be that supplied with the IP Office administration software.
	4602	Supported on IP Office 2.1+.	
	4602SW		
	4606	Only supported up to IP Office 3.2.	
	4610SW*	Supported on IP Office 3.0+.	
	4612	Only supported up to IP Office 3.2.	
	4620	Supported on IP Office 2.0+.	
	4620SW		
	4624	Only supported up to IP Office 3.2.	
	4621SW*	Supported on IP Office 3.0+.	
	4625	Supported on IP Office 3.2+	
5600 Series	**5601**	Supported on IP Office 3.0+.	These phones are supported on IP Office only. They cannot be used with other phone systems.
	5602		
	5602SW		
	5610SW*		
	5620		
	5620SW		
	5621SW*	Supported on IP Office 3.2+.	

*These phones can also be used with VPNremote firmware.

- **Other H323 IP Phones**
  Other H323 IP telephony devices are supported through the entry of an IP Office ***IP Endpoint license*** into the IP Office configuration. However, no functionality on these devices beyond basic call answering and making is guaranteed by Avaya. Therefore, installation of these devices should be thoroughly tested before any customer deployment.

1.3 System Capacity

System capacity can be separated into two aspects; the number of configurable phone extensions and the number of simultaneous IP phone calls.

Extension Capacity

The maximum number of H323 IP phones supported by an IP Office system is based on that system's maximum capacity for extensions of any type as listed in the table below. To find the capacity for IP phones remove the number of physical non-IP extensions installed on the system, ie. extension ports on the IP Office control unit and any external expansion modules.

IP Office Unit	Maximum Extensions	Maximum VCM Channels
Small Office Edition	28 Total/16 IP[1]	3[2] or 16[2]
IP406 V2	190	30
IP412	360	60
IP Office 500	272	128

1. The maximum extension capacity is 28 for all phone types but only 16 may be IP phones.
2. Fixed non-adjustable capacity.

Call Capacity

There are a number of situations where the IP Office system needs to provide a voice compression channel in order for an IP phone to make calls. These channels are provided by Voice Compression Modules (VCMs) installed in the IP Office system. The number of VCM channels required and how long the channel is required will depend on a number of factors. For further details see Voice Compression 16.

A simple summary is:

- A VCM channel is required during call setup.
- The VCM channel is released if the call is to/from another IP device using the same compression codec (the supported VCM codecs are G711, G729 and G723a).
- The VCM channel is used for the duration of the call when the call is to/from/via a non-IP device (extension or trunk line).
- It should be remembered that VCM channels are also used for calls from non-IP devices to IP lines if those are configured in the IP Office system (IP, SIP and SES lines).
- Calls from IP phones to the IP Office voicemail server use a VCM channel.
    - Note that on Small Office Edition systems with Embedded Voicemail, an additional channel is used for every call to voicemail.

1.4 Phone Firmware

The firmware in Avaya IP phones is upgradeable and different releases of firmware are made available via the Avaya support website. However H323 IP phones used on an IP Office system must only use the IP Phone software supplied with the IP Office Manager application. Other versions of IP Phone software may not have been tested with IP Office and so should not be used unless IP Office support is specifically mentioned in their accompanying documentation.

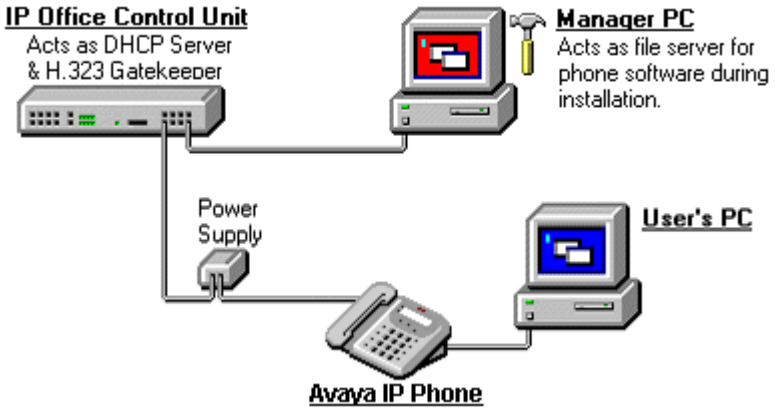
The phone firmware files are installed as part of the IP Office Manager application and are found in the applications installation directory. By default this is **c:\Program Files\Avaya\IP Office\Manager**.

For IP Office 4.2+, they firmware files are also available on the IP Office Administrator Applications CD from which IP Office Manager is installed. The files are located in the **program files\Avaya\IP Office\Manager** folder of the installation files. This makes it easier to locate all the files needed for IP phone installation though it also includes the .bin files used for IP Office control and external expansion units.

1.5 Simple Installation

The diagram below shows the simplest installation scenario.

- For IP Office control units other than the IP500, and for IP500 units running IP Office 4.0/4.1 software, this type of installation is only supported for up to 5 IP phones.
- For IP500 control units running IP Office 4.2+, this type of installation can be used for DHCP support of up to 272 IP phones (the maximum extension capacity of IP500 systems). The IP Office control unit can also act as the file server to up to 50 phones.

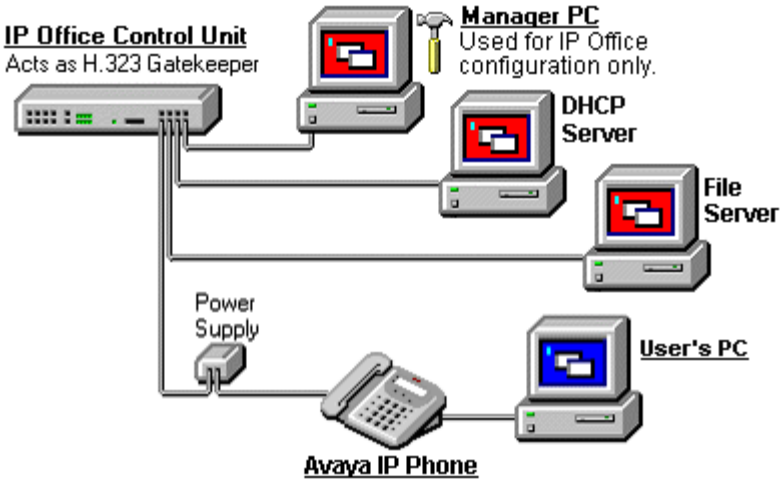


- **DHCP Server**
  The IP Office unit is acting as the DHCP server for the Avaya IP phones. Key settings such as the file server address are entered into the IP Office configuration and then provided to the phones in addition to their IP address.
  - For IP Office 4.2+, the IP Office DHCP server can be configured to provide DHCP addresses only in response to requests from Avaya IP phones. This allows an alternate DHCP server to be used for other devices that use DHCP.
- **H323 Gatekeeper**
  IP phones require an H323 gatekeeper to which they register. The gatekeeper then controls connecting calls to the phone. In this scenario the IP Office control unit acts as the H323 Gatekeeper.
- **File Server**
  During installation, and occasionally for maintenance, the IP phones need to download software and settings files. They can download the files from an HTTP server or TFTP server. The phones will try HTTP first and then TFTP. There are a number of options for the file server role:
  - **TFTP Server**
    For all IP Office releases, for phones being supported by IP Office DHCP, the address of the TFTP server is set as part of the IP Office configuration. If otherwise the only way to specify the TFTP server is via a separate DHCP server or via static installation settings.
    - **IP Office Control Unit**
      For IP Office control units fitted with an additional memory card (Small Office Edition, IP406 V2 and IP500), the IP Office itself can be used as the TFTP server. This requires the IP phone firmware files to be transferred onto the memory card.
  - **HTTP Server**
    or IP Office 4.2+, phones being supported via IP Office DHCP, the address of the HTTP server is set as part of the IP Office configuration. If otherwise the only way to specify the HTTP server is via a separate DHCP server or via static installation settings.
    - For IP Office 4.2, using an Embedded Voicemail memory card is supported for HTTP file requests for up to 50 IP phones. This is done by setting the **TFTP Server IP Address** and **HTTP Server IP Address** to the control unit IP address. This is supported for up to 50 IP phones.
    - For IP Office 4.2 Q4 2008 maintenance, using the IP Office Manager application is supported for HTTP file requests for up to 5 IP phones. This is done by setting the **TFTP Server IP** address to that of the IP Office Manager PC and the **HTTP Server IP Address** to the control unit IP address. This is supported for up to 5 IP phones.
- **Power Supply**
  The IP phones require a power supply. This is not provided by the IP Office.
  - **Individual Power Supply Units**
    An individual power supply unit can be used with each phone. This will require a power supply socket at each phone location. Note that for phones using a button add-on, for example a EU24 or BM32 an individual power supply unit is a requirement.
  - **Power over Ethernet Supply**
    Most Avaya IP phones can be powered from an 802.3af Power over Ethernet (PoE) power supply. The IP Office system does not provide PoE ports so a separate PoE switch will be required.

1.6 Complex Installation

The diagram below shows a scenario where more than 5 IP phones are being supported. The key difference is that the file server and DHCP support must be done using 3rd-party applications.

- For IP Office 4.2+ running on an IP500 IP Office system, the full capacity of up to 272 extensions is supported using the IP Office for DHCP. Control units with an Embedded Voicemail memory card installed can be used as the HTTP file server for up to 50 IP phones.



- **DHCP Server**
  In this scenario, the IP Office role as DHCP server must be replaced by an alternate DHCP server. This requires that the DHCP function of the IP Office unit is switched off. Therefore the IP Office unit must be given a fixed IP address (or act as a DHCP client).
- **File Server**
  In this instance an alternative file server application must be used.

1.7 Installation Requirements

To install an IP phone on IP Office, the following items are required:

- ☐ **Extension Number and User Details**
  A full listing of the planned extension number and user name details is required. The planned extension number must be unused and is requested by the phone during installation.
- ☐ **Power Supplies**
  Each phone requires a power supply. Avaya IP phones do not draw power from the IP Office. A number of options exist for how power is supplied to the phones. See Power Supply Options 20.
- ☐ **LAN Socket**
  An RJ45 Ethernet LAN connection point is required for each phone.
- ☐ **Category 5 Cabling**
  All LAN cables and LAN cable infrastructure used with H323 IP phones should use CAT5 cabling. Existing CAT3 cabling may be used but will be limited to 10Mbps (maximum).
- ☐ **LAN Cables**
  Check that an RJ45 LAN cable has been supplied with the IP phone for connection to the power supply unit. You will also need an additional RJ45 LAN cable for connection from the power unit to the customer LAN.
  - A further RJ45 LAN cable can be used to connect the user's PC to the LAN via the IP phone [not supported on 4601, 4602, 5601 and 5602 H323 IP phones].
- ☐ **Voice Compression Channels**
  The IP Office Unit must have voice compression channels installed. Channels are required during the connection if calls involving IP phones and may also be required during the call. See Voice Compression Channels 16 for full details.
  - For Small Office Edition units, either 3 or 16 voice compression channels are pre-built into the unit.
  - For IP400 control units, voice compression channels are provided by fitting a Voice Compression Module 16.
  - For IP500 control units, channels are installed using a IP500 VCM base card and licenses or using IP400 VCM modules on an IP500 Legacy Card.
- ☐ **DHCP Server**
  The IP Office Unit can perform this role for up to 5 IP phone devices. If another DHCP server already exists, this may be able to do DHCP for the H323 IP phones, see Alternate DHCP Servers 66. Static IP addressing can also be used, if required, but is not recommended.
  - For IP500 IP Office 4.2+ systems, up to 272 IP phones are supported using the IP Office Manager.
- ☐ **HTTP or TFTP File Server**
  A PC running the IP Office Manager application can perform this role for up to 5 H323 IP phones. Otherwise an alternate HTTP or TFTP server is required.
- ☐ **H323 Gatekeeper**
  The IP Office Unit performs this role.
- ☐ **IP Office Manager PC**
  A PC running Manager is required for IP Office Unit configuration changes. This PC should have a static IP address.
- ☐ **IP Telephone Software**
  The software for IP phone installation is installed into the IP Office Manager program folder during Manager installation.
- ☐ **Licence Keys**
  IP Office supported H323 IP phones do not need a licence key entered on the system. The only exception are IP phones running Avaya VPN remote software, see VPN Remote Phones 40.

1.8 Network Assessment

- ⚠ **WARNING: A Network Assessment is Mandatory**
  When installing H323 IP phones on an IP Office system, it is assumed by Avaya that a network assessment has been performed. If a support issue is escalated to Avaya, Avaya may request to see the results of the network assessment and may refuse to provide support if a suitable network assessment was not performed.

Current technology allows optimum network configurations to deliver VoIP with voice quality close to that of the public phone network. However, few networks are optimum and so care should be taken assessing the VoIP quality achievable across a customer network.

Not every network is able to carry voice transmissions. Some data networks have insufficient capacity for voice traffic or have data peaks that will impact voice traffic on occasion. In addition, the usual history of growing and developing networks by integrating products from many vendors makes it necessary to test all the network components for compatibility with VoIP traffic.

A network assessment should include a determination of the following:

- A network audit to review existing equipment and evaluate its capabilities, including its ability to meet both current and planned voice and data needs.
- A determination of network objectives, including the dominant traffic type, choice of technologies and setting voice quality objectives.
- The assessment should leave you confident that the network will have the capacity for the foreseen data and voice traffic, and can support H323, DHCP, TFTP and jitter buffers in H323 applications.

The network assessment targets are:

- **Latency:** *Less than 180ms for good quality. Less than 80ms for toll quality.*
  This is the measurement of packet transfer time in one direction. The range 80ms to 180ms is generally acceptable. Note that the different audio codecs used each impose a fixed delay caused by the codec conversion as follows:
  - **G711:** 20ms.
  - **G723a:** 80ms.
  - **G729:** 40ms.
- **Packet Loss:** *Less than 3% for good quality. Less than 1% for toll quality.*
  Excessive packet loss will be audible as clipped words and may also cause call setup delays.
- **Jitter:** *Less than 20ms.*
  Jitter is a measure of the variance in the time for different packets in the same call to reach their destination. Excessive jitter will become audible as echo.
- **Duration:** *Monitor statistics once every minute for a full week.*
  The network assessment must include normal hours of business operation.

1.9 Voice Compression

Calls to and from IP devices can require conversion to the audio codec format being used by the IP device. In the IP Office this conversion is done by voice compression channels. These support the common IP audio codecs G711, G723 and G729a.

For Small Office Edition control units either 3 or 16 integral channels are included. For IP400 control units channels can be added by fitting IP400 VCM cards. For the IP500 control unit channels can be added using either IP400 VCM cards or licensed IP500 VCM cards.

The voice compression channels are used as follows.

- **IP Device to Non-IP Device**
  These calls require a voice compression channel for the duration of the call. If no channel is available busing indication is returned to the call.
- **IP Device to IP Device**
  - Call progress tones (for example dial tone, secondary dial tone, etc) do not require voice compression channels with the following exceptions:
    - Short code confirmation, ARS camp on and account code entry tones require a voice compression channel.
    - Devices using G723 require a voice compression channel for all tones except call waiting.
  - When a call is connected:
    - If the IP devices use the same audio codec no voice compression channel is used.
    - If the devices use differing audio codecs, a voice compression channel is required for each.
- **Non-IP Device to Non-IP Device**
  No voice compression channels are required except for Small Office Edition Embedded Voicemail access.
- **Music on Hold**
  This is provided from the IP Office's TDM bus and therefore requires a voice compression channel when played to an IP device.
- **Conference Resources and IP Devices**
  Conferencing resources are managed by the conference chip which is on the IP Office's TDM bus. Therefore, a voice compression channel is required for each IP device involved in a conference. This includes services that use conference resources such as call listen, intrusion, call recording and silent monitoring.
- **Page Calls to IP Device**
  Page calls require 1 voice compression channel per audio codec being used by any IP devices involved. IP Office 4.0 and higher only uses G729a for page calls, therefore only requiring one channel but also only supporting pages to G729a capable devices.
- **Voicemail Services and IP Devices**
  Calls to the IP Office voicemail servers (Voice Mail Pro, Voicemail Lite and Embedded Voicemail) are treated as data calls from the TDM bus. Therefore calls from an IP device to voicemail require a voice compression channel.
  - On the Small Office Edition, embedded voicemail uses voice compression channels for audio conversion. Therefore all calls to SOE embedded voicemail require a voice compression channel and calls from IP devices require two voice compression channels.
- **Fax Calls**
  These are voice calls but with a slightly wider frequency range than spoken voice calls. IP Office only supports fax across IP between IP Office systems with the Fax Transport option selected. It does not currently support T38.
- **SIP Calls**
  - **SIP Line Call to/from Non-IP Devices**
    Voice compression channel required.
  - **Outgoing SIP Line Call from IP Device**
    No voice compression channel required.
  - **Incoming SIP Line Call to IP Device**
    Voice compression channel reserved until call connected.

Installing VCM Cards

Refer to the IP Office Installation manual.

IP400 VCM Cards

The following IP400 VCM cards are available.

IP400 VCM Cards		SAP Code	Small Office Edition	IP406 V2	IP412	IP500
25ms echo cancellation.	IP400 VCM5[1]	700185119	✗	✓	✓	✗
	IP400 VCM10[1]	700185127	✗	✓	✓	✗
	IP400 VCM20[1]	700185135	✗	✓	✓	✗
	IP400 VCM30	700293939	✗	✓	✓	✓
64ms echo cancellation.	IP400 VCM4	700359854	✗	✓	✓	✓
	IP400 VCM8	700359862	✗	✓	✓	✓
	IP400 VCM16	700359870	✗	✓	✓	✓
	IP400 VCM24	700359888	✗	✓	✓	✓
Number of IP400 VCM cards.			0	1	2	2[2]
Maximum number of channels.			3/16[3]	30	60	128

1. These modules are still supported but are no longer available from Avaya.
2. Requires a IP500 Legacy Card Carrier for installation into an IP500 control unit.
3. The VCM channels in Small Office Edition control units are fixed at either 3 or 16 depending on the model.

IP500 VCM cards

The following IP500 VCM cards are available. Each card provides 4 unlicensed channels with the addition capacity of the card requiring licenses within the IP Office configuration. Up to 2 IP500 VCM cards are supported in a system.

Name	Description	SAP Code
IPO 500 MC VCM 32	IP Office 500 Media Card Voice Coding Module 32	700417389
IPO 500 MC VCM 64	IP Office 500 Media Card Voice Coding Module 64	700417397
IPO LIC IP500 VCM LIC 4 CH	IP500 Addition VCM Channels License: 4 Channels	202961
IPO LIC IP500 VCM LIC 8 CH	IP500 Addition VCM Channels License: 8 Channels	202962
IPO LIC IP500 VCM LIC 16 CH	IP500 Addition VCM Channels License: 16 Channels	202963
IPO LIC IP500 VCM LIC 28 CH	IP500 Addition VCM Channels License: 28 Channels	202964
IPO LIC IP500 VCM LIC 60 CH	IP500 Addition VCM Channels License: 60 Channels	202965

- The maximum number of simultaneous channels useable on an IP500 VCM base card is affected by the codec being used. The following table assumes that all calls using the VCM use the same codec.

Codec	IP500 VCM32	IP500 VCM64
G.711	32	64
G.729a	30	60
G.723	22	44

1.10 QoS

When transporting voice over low speed links it is possible for normal data packets (1500 byte packets) to prevent or delay voice packets (typically 67 or 31 bytes) from getting across the link. This can cause unacceptable speech quality.

Therefore, it is vital that all traffic routers and switches in the network to have some form of Quality of Service (QoS) mechanism. QoS routers are essential to ensure low speech latency and to maintain sufficient audible quality.

IP Office supports the DiffServ (RFC2474) QoS mechanism. This is based upon using a Type of Service (ToS) field in the IP packet header. On its WAN interfaces, IP Office uses this to prioritize voice and voice signalling packets. It also fragments large data packets and, where supported, provides VoIP header compression to minimize the WAN overhead.

Note

- IP Office does not perform QoS for its Ethernet ports including the WAN Ethernet port on the Small Office Edition.

1.11 Potential VoIP Problems

It is likely that any fault on a network, regardless of its cause, will initially show up as a degradation in the quality of VoIP operation. This is regardless of whether the fault is with the VoIP telephony equipment. Therefore, by installing a VoIP solution, you must be aware that you will become the first point of call for diagnosing and assessing all potential customer network issues.

Potential Problems

- **End-to-End Matching Standards**
  VoIP depends upon the support and selection of the same voice compression, header compression and QoS standards throughout all stages of the calls routing. The start and end points must be using the same compression methods. All intermediate points must support DiffServ QoS.
- **Avoid Hubs**
  Hubs introduce echo and congestion points. If the customer network requires LAN connections beyond the capacity of the IP Office Unit itself, Ethernet switches should be used. Even if this is not the case, Ethernet switches are recommended as they allow traffic prioritization to be implemented for VoIP devices and for other device such as the Voicemail Server PC.
- **Power Supply Conditioning, Protection and Backup**
  Traditional phone systems provide power to all their attached phone devices from a single source. In a VoIP installation, the same care and concern that goes into providing power conditioning, protection and backup to the central phone system, must now be applied to all devices on the IP network.
- **Multicasting**
  In a data only network, it is possible for an incorrectly installed printer or hub card to multicast traffic without that fault being immediately identified. On a VoIP network incorrect multicasting will quickly affect VoIP calls and features.
- **Duplicate IP Addressing**
  Duplicate addresses is a frequent issue.
- **Excessive Utilization**
  A workstation that constantly transmits high traffic levels can flood a network, causing VoIP service to disappear.
- **Network Access**
  An IP network is much more open to users connecting a new device or installing software on existing devices that then impacts on VoIP.
- **Cabling Connections**
  Technically VoIP can (bandwidth allowing) be run across any IP network connection. In practice, Cat5 cabling is essential.

1.12 User PC Connection

To simplify the number of LAN connections from the user's desk, it is possible to route their PC Ethernet LAN cable via some H323 IP phones. The LAN cable should be connected from the PC to the socket with a PC symbol (🖳) at the back of the IP phone. This port supports 10/100Mbps ethernet connections. The PC's network configuration does not need to be altered from that which it previously used for direct connection to the LAN.

Those phones that include a PC pass-through port and also provide priority to phone voice traffic over PC data traffic are normally indicated by an SW suffix in the phone name. However some phones have a PC pass-through port but do not provide switching priority.

The table below summarizes the phones:

H.232 IP Phone	PC Port	With Voice Priority	Supports Gigabit Adaptor		H.232 IP Phone	PC Port	With Voice Priority	Supports Gigabit Adaptor
1603	✗	✗	✗		4620SW	✓	✓	✓
1608	✓	✓	✗		4621	✓	✓	✓
1616	✓	✓	✗		4624	✓	✗*	✗
4601	✗	✗	✗		5601	✗	✗	✗
4602	✗	✗	✗		5602	✗	✗	✗
4602SW	✓	✓	✓		5602SW	✓	✓	✓
4606	✓	✗*	✗		5610SW	✓	✓	✓
4610SW	✓	✓	✓		5620	✓	✗	✓
4612	✓	✗*	✗		5620SW	✓	✓	✓
4620IP	✗	✗	✗					

- *The 4606, 4612 and 4624 phones can be upgraded to provide voice priority switching by fitting an Avaya 30A Switch Upgrade Base to the phone. In addition, this base also allows the phone to be powered from a IEEE 802.3af Power over Ethernet source.

- **Gigabit Ethernet**
  If a 1000mbps ethernet connection is being used then a separate Gigabit Adapter (SAP 700416985) must be used. This device splits the data and voice traffic before it reaches the phone, providing a 10/100Mbps output for the phone and a 10/100/1000Bbps output for the PC. The adapter is powered from the phone's existing PoE supply or 1151 type power supply unit. Refer to the "Gigabit Ethernet Adapter Installation and Safety Instructions" (16-601543).

1.13 Power Supply Options

Each H323 IP phone requires a power supply. They do not draw power from the IP Office phone system. Listed below are the power supply options that can be used.

Spare Wire Power Options

The following power supplies use the normally unused pin 7 & 8 connections in the CAT3 or CAT5 network cable. This is referred to as "spare wire" or "mid-span" power supply units. They can be used with 4600 Series and 5600 Series IP phones.

- **Avaya 1151D1 Power Supply Unit (PSU)**
  A power supply unit for a single IP phone. Has a LINE port for the LAN cable from the IP Office, and a PHONE port for the LAN cable to the IP phone. Power into the PSU requires a 90 to 264V AC, 47 to 63HZ mains supply. A green LED indicates when power is available.

- **Avaya 1151D2 Power Supply Unit**
  Same as the 1151C1 above but with integral battery backup. When AC mains supply is removed, the battery will power the IP phone for between 8 hours at light load (2 Watts) and 15 minutes at full load (20 Watts). A green LED indicates when power is available. A yellow LED indicates when the backup is charging. The green LED flashes when the phone is running from the backup battery.

Dedicated Plug-Top Power Supply Units

1600 Series IP phones can be powered using plug-top PSU's. Different models of PSU exist for various power outlet sockets. These connect to the phone using a barrel connector.

802.3af Power over Ethernet (PoE) Options

IEEE 802.3af is a standard commonly known as Power over Ethernet (PoE). It allows network devices to receive power via the network cable using the same wires as the data signals. All the H323 IP phones supported on IP Office also support this standard. Note that for phones being used with an add-on unit such as an EU24, EU24BL or BM32, an individual power supply must be used rather than PoE.

- Exceeding the Class limit of a PoE port or the total Class support of a PoE switch may cause incorrect operation.

Phone	802.3af Class		Phone	802.3af Class
1603[1]	Class 2		4606, 4612, 4624 Gen2[2]	Class 0
1608	Class 2		4610SW, 5610	Class 2
1616	Class 2		4620	Class 3
4601, 5601	Class 2		4620SW	Class 2
4602	Class 1		4621SW[3]	Class 2
4602SW, 5602SW	Class 2		4625SW	Class 3

1. Requires the addition of a 1603 PoE Splitter (SAP 700415607).
2. GEN1 versions of these phones cannot use PoE. The GEN of a phone can be determined from the label on the base of the phone. The label text giving the phone's type, for example 4624D, is followed by two digits which give its generation (GEN) number, for example 4624D01. GEN1 4612 and 4624 phones can be Ethernet powered using a 30A Switch Upgrade Base unit.
3. 4621SW with a Gigabit Adapter is Class 3.

- **Avaya 1152A1 Power Distribution Unit (Mid-Span Power Unit)**
  This is a 1U high 19-inch rack mountable unit. It is available in models to support 6, 12 or 24 PoE devices including H323 IP phones. For each device, it provides a RJ45 data in ports and a matching RJ45 data and power out port. It can support a maximum of 200 Watts or a peak of 16.8 Watts per port.

- **Power of Ethernet (POE) Switch**
  The Avaya P333T-PWR Switch is a Ethernet LAN switch which also provides PoE input for up to 24 devices including H323 IP phones.

- **IP Phone Inline Adaptor**
  This adaptor allows 4602, 4602SW, 4620, 4621 and 4625 H323 IP phones and 5600 Series equivalents to be powered from a Cisco Catalyst power blade. Using these adaptors, up to 24 H323 IP phones can be supported on a single power blade. The phones do not provide the Catalyst switch with information on their power requirements and future changes to Catalyst switch software may affect operation.

1.14 File Server Options

During installation and maintenance the phones download software and settings files. In order to do this the phone first request files for an HTTPS server. If it gets no response it then tries to obtain the files from an HTTP server and finally from a TFTP server. The address of the server to use is provided through DHCP or entered during static phone installation.

- The phones will check the file server every time they are restarted. However if they do not find it they will continue by using the existing files they have. Therefore there is no requirement for the file sever to be permanently available. The file server is only required during phone installation and maintenance.

For Avaya IP phones using IP Office DHCP, IP Office 4.2+ allows the address of the HTTP server from which those phones should download their software and settings files to be specified in the IP Office configuration. Previously only a TFTP server IP address could be specified. 4600 Series and 5600 Series phones attempt to load files via HTTPS and then HTTP before falling back to TFTP. 1600 Series IP phones only support HTTPS or HTTP.

The following options are available for the file server for IP phones being installed on an IP Office system.

1. **IP Office Manager**
   When running, the IP Office Manager acts as a TFTP server. For systems other than an IP500 running IP Office 4.2+ this option is only supported for up to 5 IP phones.
   - For IP Office 4.2 Q4 2008 maintenance, using the IP Office Manager application is supported for HTTP file requests for up to 5 IP phones. This is done by setting the **TFTP Server IP** address to that of the IP Office Manager PC and the **HTTP Server IP Address** to the control unit IP address. This is supported for up to 5 IP phones.
2. **IP Office Unit Memory Card**
   On Small Office Edition, IP406 V2 and IP500 control units fitted with an additional memory card that card can be used to store the software files. The control unit can then act as the TFTP server.
   - For IP Office 4.2, using an Embedded Voicemail memory card is supported for HTTP file requests for up to 50 IP phones. This is done by setting the **TFTP Server IP Address** and **HTTP Server IP Address** to the control unit IP address. This is supported for up to 50 IP phones.
3. **3rd Party Software**
   TFTP and HTTP server software is available from many sources including Avaya.

1.15 Control Unit Memory Card

The memory card used with the Small Office Edition and IP406 V2 systems can be used to store files other than those used for embedded voicemail.

- Non-Avaya supplied Compact Flash memory cards can be used for this type of file storage. However, they will not support embedded voicemail.
- If an Avaya supplied memory card is used, any files stored in this way will reduce the message storage capacity of the Compact Flash memory card.

Transferring Files to the Card Using TFTP

This process allows a specified PC to send files to the memory card and tells the IP Office system to use the memory card. The location of the bin files should be the top level folder of the card.

1. Using Manager, receive the IP Office system's configuration.
2. On the **System** tab of the System form, set the **File Writer IP Address** to the IP address of the PC from which sending files to the memory card will be allowed.
3. Send this configuration back to the IP Office unit and allow it to reboot.
4. Within Windows, select **Start | Run**.
5. Enter **cmd** and then click **OK**.
6. Within the command window, you can use TFTP to upload files to the memory card. For example:

   ```
   c:\tftp -i 192.168.42.1 put d:\IPSets Firmware\4601dbtel1_82.bin
   ```

7. The above command will send the file **d:\IPSets Firmware\4601dbtel1_82.bin** to the IP Office units LAN1 IP address. For additional information about the TFTP command, enter ***TFTP***. If a destination needs specifying, the memory card is treated as the IP Office's drive ***a:***.
8. Receive the IP Office system's configuration again.
9. On the **System** tab of the **System** form, set the **TFTP Server IP Address** to the unit's own LAN1 IP address.
10. Send this configuration back to the IP Office unit and allow it to reboot. The IP Office system will now look on the memory card for any files it needs to download following a reboot.
11. If in future an upgrade or file transfer from the Manager PC is required, the TFTP Server IP Address will first need to be changed back to the Manager PC's IP address.

Transferring Files to the Card Using File Management

IP Office 4.2+ allows the contents of the memory card in a system to be viewed and updated. This is done using IP Office Manager and requires the same user name and password access as used for configuration changes.

1. Within IP Office Manager, select **File | Advanced | Embedded File Management**.
2. The **Select IP Office** discovery menu is shown. Select the IP Office systems whose memory card you want to view and click **OK**.
3. Enter a user name and password for configuration access to that system.
   - **`TFTP: Received TFTP Error "Not Found"`** in the Manager status bar indicates that no card was detected in the selected system. To select another system use **File | Open File Settings**. To return Manager to normal configuration mode select **File | Configuration**.
4. The contents of the card are shown in Manager.
   - New files can be drag and dropped to the Files section of the currently selected folder or transferred using **File | Upload File...**.
     - The transfer is serial and can be interrupted by other activities on the IP Office system. Therefore it is recommended that files are transferred in small batches.
   - Existing files can be deleted by right-clicking on the file and selecting **Delete**.
   - Files can be downloaded from the card by right-clicking on the file and selecting **Download**. The file is downloaded to the Manager applications working directory.
5. When transfers have been completed, to select another system use **File | Open File Settings**. To return Manager to normal configuration mode select **File | Configuration**.

Chapter 2. Installation

2. Installation

Check the following before beginning installation:

1. ☐ **IP Office Manager PC**
   Check that the applications for configuring and monitoring an IP Office system are available and able to connect to that system.
   - ☐ Check that IP Office Manager and IP Office System Status Application (SSA) or System Monitor are installed and can be used to connect to the IP Office system.
   - ☐ Verify that you can receive the configuration from the system and send it back to the IP Office.
   - ☐ Ensure that the Manager PC has been given a static IP address.
2. ☐ **Voice Compression Channels**
   The IP Office Unit must be fitted with a voice compression channels 16. Use either SSA or System Monitor application to verify that the voice compression channels are available. SSA list the VCM channels on the Resource screen. The initial lines of Monitor output include the item ***VCOMP=*** which will state the number of channels installed in the control unit.
3. ☐ **File Server Settings**
   Using Manager, receive the configuration from the IP Office. Select **System** and then select the **System** tab. Check the following:
   - ☐ **System Name**
     On the **System** tab ensure that a **Name** for the IP Office Unit has been entered.
   - ☐ **TFTP Server IP Address**
     If using TFTP to download software file to the phones, enter the TFTP server address here. This address is used by the IP phones (excluding 1600 Series) being supported by IP Office DHCP. If another DHCP server is being used, that address must be set via the DHCP settings on that server, see Alternate DHCP Setup 66.
     - The default ***0.0.0.0*** will cause the phones to broadcast for any TFTP server available on the same subnet as themselves.
     - To use the memory card installed in the system, enter the LAN1 IP address of the IP Office system (the address is shown on the LAN1 tab). To use this option the card must be loaded with the IP phone software files, see Control Unit Memory Card 23.
     - If a 3rd-party TFTP server is being used, set the IP address to the address of the PC running that software.
   - ☐ **HTTP Server IP Address**
     IP Office 4.2+ supports the use of HTTP for file requests from IP phones. This is necessary for 1600 Series phones and is supported by all other Avaya IP phones. This address is used by the IP phones being supported by IP Office DHCP. If another DHCP server is being used, that address must be set via the DHCP settings on that server, see Alternate DHCP Setup 66.
     - The default ***0.0.0.0*** disables HTTP support.
     - For IP Office 4.2, using the Embedded Voicemail memory card is also supported for HTTP file requests for up to 50 IP phones. This is done by setting the **TFTP Server IP Address** and **HTTP Server IP Address** to match the control units IP address. This is supported for up to 50 IP phones.
     - If a 3rd-party HTTP server is being used, set the IP address to the address of the PC running that software.
4. ☐ **H323 Gatekeeper Settings**
   Select **System** and then select the **LAN1** tab. Select the **Gatekeeper** sub tab. Check the following settings:
   - ☐ **H323 Gatekeeper Enabled**
     Ensure that this option is enabled.
   - ☐ **H323 Auto-created Extn**
     This installation process assumes that this option is enabled until after installation of the phones has been completed. If not enabled the you must manually add extensions to the IP Office configuration before installation. See Manually Creating Extensions 29.
   - ☐ **H323 Auto-create User**
     This installation process assumes that this option is enabled until after installation of the phones has been completed. If not enabled the you must manually add users to the IP Office configuration before installation.
   - ☐ **Primary Site Specific Option Number**
     Devices being supported by DHCP can request device specific information using a site specific option number (SSON). This method is used for Avaya IP phones to request phone specific information from a DHCP server. For IP phones beign supported by IP Office DHCP, the SSON set here should match that being used by the phones. By default Avaya 4600 and 5600 Series IP phones use the 176 as their SSON.
   - **Secondary Site Specific Option Number** *(IP Office 4.2+)*
     This field allows a second SSON to be specified for use by IP phones. By default Avaya 1600 Series IP phones use 242 as their SSON.

5.☐ DHCP Server

If not using the IP Office for DHCP, check that the alternate DHCP server has been configured for the IP phones. It will need to include details of the files server and gateway settings. See Alternate DHCP Setup 66. If using the IP Office for DHCP, select System and then the LAN1 or LAN2 tab.

- **☐ DHCP Mode**
  Check that the IP Office is set as ***Server***. This allows it to respond to DHCP requests on its subnet.
- **☐ Number of DHCP IP Addresses**
  Set this to a number sufficient for all the IP devices, including phones, that will be supported by the IP Office DHCP.
- **☐ Advanced/DHCP Pools** (IP500 4.2+)
  For IP Office 4.2+ on IP500 systems, multiple ranges of IP addresses can be configured for use by IP Office DHCP. In addition, the IP Office DHCP can be restricted to Avaya IP phones only by selecting ***Apply to Avaya IP Phones Only***.

6.☐ IP Phone Software and Settings Files

The software for IP phone installation is supplied on the IP Office Administrator Applications CD. Those files must be placed on the file server. The files are automatically installed as part of the IP Office Manager application and so are already present if IP Office Manager is used as the file server.

- If another source is used as the file server, the software and settings files must be copied to that server. For pre-IP Office 4.2 system the files must be copied from the Manager application folder. For IP Office 4.2+ the files can be copied from the location program files\Avaya\IP Office\Manager on the installation CD.
- If it does not exist already an additional file, ***46xxsettings.txt***, is also required. See Creating a 46xxsettings.txt File 28.

7.☐ Extension Number and User Name Details

A full listing of the planned extension number and user name details is required. The planned extension number must be unused and is requested by the phone during installation.

2.1 Creating/Editing the Settings File

During installation, the H323 IP phones request software by downloading and following instructions within the **46xxupgrade.scr** file. This file is provided as part of the IP Office Manager software and should not normally be changed.

The last lines of the **46xxupgrade.scr** file instruct the phone to request the file **46xxsettings.scr** or **46xxsettings.txt**. If present, that file is downloaded and used to set customer site specific options for the H323 IP phones. It is this 46xxsettings file that is used to contain site specific options for phones and should be edited to meet the customer requirements before installation of the phones.

1. Using Windows Notepad or any other plain text editing tool, open the ***46xxsettings.txt*** file.
2. Edit the file as required. The file contains numerous comments and notes. Further details of the various settings are contained in the 4600 Series IP Telephone LAN Administrator Guide. For some specific options see the notes below.
   - A **#** character at the start of a line comments out the command on that line. Note however that for some options the phones will assume a default value if the option in the **46xxsettings.txt** file is commented out. For example if **SET PHNOL** is commented out, the phones will assume the addition of a dial 9 prefix to numbers.
3. Place this file in the same folder as the 4600 Series IP Phone software files including the **46xxupgrade.scr** file. Normally this is the same folder as the Manager application.
4. Ensure that you have a copy of the edited file.

Dialing Prefix

For IP Office systems the addition or removal of dialing prefixes is normally done by the IP Office system rather than individual phones or applications. For IP Office operation the following changes are recommended in the **ENHANCED LOCAL DIALING RULES** section of the **46xxsettings.txt** file.

- Change ## **SET ENHDIALSTAT 0** to **ENDIALSTAT 0**.
- Change ## **SET PHNOL 9** to **SET PHNOL ""**.

802.1Q Tagging

Unless specifically required for the customer network, for IP Office operation it is recommended that ## **SET L2Q 0** is changed to **SET L2Q 2**.

WML Web Server Setup

If a WML web site has been setup for viewing by phone users, see WML Server Setup 72, the site address is set through the **46xxsettings file**. Change ## **WMLHOME http://....** to **WMLHOME** followed by the required address.

1600 Series Phone Languages

In addition to English, the 1600 phones can support up to 4 language other languages. This is done by the phones downloading languages files specified in the 46xxsettings.txt file. Currently 9 non-English language files are provided as part of the IP Office Manager installation.

Language	File	Language	File
Dutch	mlf_S1_v8_dutch.txt	**Latin Spanish**	mlf_S1_v8_spanish_latin.txt
French Canadian	mlf_S1_v8_french_can.txt	**Portuguese**	mlf_S1_v8_portuguese.txt
French	mlf_S1_v8_french_paris.txt	**Russian**	mlf_S1_v8_russian.txt
German	mlf_S1_v8_german.txt	**Spanish**	mlf_S1_v8_spanish.txt
Italian	mlf_S1_v8_italian.txt		

The files to download to the phones are defined in the # **SETTINGS1603**, # **SETTINGS1608** and # **SETTINGS1616** sections of the **46xxsettings.txt** file. To have the phone download a language file, remove the ## in front of one of the **SET** options and change the file name to match the required language.

Backup/Restore

Phones can use an HTTP server as a location to which the user's phone settings are backed up and restore when they log on or off the phone. See Backup Restore 34 for full details.

2.2 Manually Creating Extensions

If installing without auto-create extensions enabled, then VoIP extensions and associated users must first be created in IP Office Manager.

The procedure below covers the minimum required to create a VoIP extension and associated user. Further customization is as per any extension and user.

1. In Manager, receive the system's configuration.
2. To display the list of existing extensions, click **Extension** in the left-hand panel. Right-click on the right-hand panel and select **New**.
3. In the **Extn** tab, set the following:
   - **Extension ID**
     For non-VoIP extension this number is assigned automatically. For a VoIP extension, enter any number so long as it is unique, i.e. not already used by another extension.
   - **Base Extension**
     Enter the extension number to assign to the phone. Again, this must be unique.
4. In the **VoIP** tab, the required IP Address and/or MAC Address can be set if required for additional phone security. See Phone Security 33.
5. To add the new extension, click **OK**.
6. To display the list of existing users, click **User** in the left-hand panel. Right-click on the right-hand panel and select **New**.
7. In the **User** tab set the following:
   - **Name**
     Enter a name for the extension user. The name must be unique. If voicemail is in use, this name will be used as the basis for a new mailbox with matching name.
   - **Extension**
     This must match the extension number set in the VoIP extension created above.
8. Click on the **Button Programming** tab.
9. For the first three buttons, you must click on the **Action** field and select **Appearance | Appearance**.
10. Click on **OK**.
11. When all new IP phone extension being added have been setup, send the new configuration back to the system. Set the **Reboot Mode to Immediate** or **When Free as Extension** changes cannot be merged.

2.3 Phone Connection

In this process the phone is connected to its power source and the ethernet LAN. As soon as the phone is powered up it will start to request information.

1. Follow the steps in Preparation 26. If these steps are not followed, installation will fail. Ensure that the selected file server is running and that the required files are present. Check that the DHCP server is running.
2. Connect the network LAN cable to the data-in socket of the power supply being used for the phone.
   - On 1151 power supply units, the socket is marked **LINE**.
   - On the 1152 power supply units, the lower sockets are data-in.
3. Connect the LAN cable supplied with the IP phone from the power supplies data and power out socket to the socket with a LAN port symbol (⧈) at the back of the IP phone.
   - On 1151 power supply units, the socket is marked **PHONE**.
   - On the 1152 power supply units, the upper sockets are data and power.
4. The phone's message indicator should glow red for a few seconds. The phone will then begin its software loading.
5. After a short delay, the phone displays **Initializing** and then **Loading...**. The loading phase may take a few minutes.
6. If the phone has an existing software boot file (ie. it has been previously installed), it will load that file and then display **Starting...**.
7. If the phone displays **No Ethernet**, check the connection to the LAN.
8. The phone displays **DHCP** and a timer as it attempts to request an IP address and other information from a DHCP server. On 4601 and 5601 phones, initially all lamps will be on as the phone initializes. All lamps on (with the button a lamp flashing) indicates attempting DHCP.
   - **To switch to static address installation**
     Press ***** whilst DHCP is shown if you want to enter static address installation. See Static Address Installation 31. This is not recommended for 4601 and 5601 IP phones.
9. After a few seconds, DHCP negotiation should be completed. If the timer reaches more than 60 seconds, it could indicate an error in either the network or DHCP server configuration.
10. Once DHCP has completed successfully, the phone will display ***HTTP*** or ***TFTP*** as it request files from the file server indicated by the DHCP settings. The first file requested is the ***46xxupgrade.scr*** file. This file contains details of the other files that the phone should load.
    - The phones will go through a sequence of loading files, restarting and loading further files until the files on the phone match those listed for it in the ***46xxupgrade.scr*** file. For phones with some files already installed, the sequence may vary depending on whether the existing files match those specified in the ***46xxupgrade.scr*** file.
    - On 4601 and 5601 phones, all lamps will be on with both the button a and button b lamps flashing whilst file loading is attempted and occurring.
11. The phone now requests additional files according to the instructions it found in the ***46xxupgrade.scr*** file. The phone will go through a cycle of requesting files, loading files and then transferring the files into its flash memory.
12. Following file loading, the phone displays **Ext. =**. See Phone Registration 32.

2.4 Static Address Installation

Static addressing is only necessary when a DHCP server is unavailable or not desired. For ease of maintenance and installation, it is strongly recommended that a DHCP server is installed and that static addressing is avoided. Following a boot file upgrade, static address information must be reinstalled. This process is not supported on 4601 and 5601 phones.

1. Follow the steps in Phone Connection 30 until **DHCP** is shown on the phone display. Press * at this point to switch the phone to static address installation.
   - Existing installed phones can be made to start static address installation using the following key sequence. While the phone is on-hook and idle, press **Hold 2 3 3 7 #** (**Hold A D D R #**).
2. The phone will display a sequence of settings and the existing value for each of those settings. To accept the current value, press # or enter a value and then press #.
3. While entering data in the following actions it may sometimes be necessary to backspace. The method for doing this varies according to the phone type:
   - **4602, 5602:** Speaker key.
   - **4606:** Conference key.
   - **4612 & 4624:** Previous key.
   - **4610, 4620, 4625, 5610, 5620:** Left-most key.
4. The settings shown for static address installation are:
   - **Phone=**
     This is the phone's IP address. To accept the current value, press **#** or enter a value and then press **#**. If entering a new value, press the ***** key to enter a '**.**' character between digits.
   - **CallSv=**
     This is the address of the H323 gatekeeper. For IP Office systems this is the IP address of the IP Office LAN1.
   - **CallSvPort=**
     This is the Gatekeeper transport layer port number. For Avaya IP phones the value used should be ***1719***. To accept the current value, press # or enter a value and then press **#**.
   - **Router=**
     This is the address of the phone's default IP gateway. For IP Office this is typically the IP address of the IP Office LAN1. To accept the current value, press **#** or enter a value and then press #.
   - **Mask=**
     This is the phone's IP Mask (also called the subnet mask). The mask is used with the IP address to indicate the phone's subnet. This should match the IP mask set for the IP Office Unit.
   - **FileSv**=
     This is the address of the file server from which the phone should request software and settings files. Enter the address of the TFTP or HTTP configured with the Avaya IP phone software file set.
   - **802.1Q=**
     To change the setting press ***. P**ress **#** to accept the value.
   - **VLAN ID=**
     For details of VLAN configuration see VLAN and IP Phones 43.
5. If you go through without changing anything the phone displays **No new values**. Press **#**.
   - If the phone displays **Enter command** power off and on again.
6. Once all the values have been entered or the existing values accepted the phone will display **Save new values?**. To save the values press **#**. The phone will save the values and then restart using those values.
   - If a new boot program is downloaded from the TFTP server after you enter static address information, you will need to re-enter your static address information.

2.5 Phone Registration

For new phones and phones that have been reset 54, the phone will request an extension number. If auto-create is enabled the extension number used, if free, will create new extension and user entries in the IP Office configuration. If auto-create is not enabled, the extension number used must match a VoIP extension entry within the IP Office configuration, see Manually Creating Extensions 29.

1. Following file loading the phone will request extension information:
   - **Ext. =**
     Enter the extension number the phone should use and press #. **Wrong Set Type** is displayed if you try to use the extension number of an existing non-IP extension.
     - On 4601 and 5601 phones, this stage is indicated by the lamp at the top of the phone and on the **MESSAGES** button flashing 0.5 seconds on/off.
   - **Password =**
     The password used is as follows:
     - If using auto-create for a new user and extension, just enter any number and press #. Any digits entered for a password here are not validated or stored.
     - If not using auto-create extension for a new extension, enter the user's **Login Code** as set in the IP Office configuration.
     - During subsequent phone restarts, even though the password is requested, it will only be validated if the phone's extension number is changed.
2. Test that you can make and receive calls at the extension.

2.6 Extension & User Setup

If installing using auto-create extensions, you can now use IP Office Manager to open the IP Office unit's configuration and alter the extension and user settings for the phone.

The following process covers the minimum extension and user setup required.

1. In Manager, receive the system's configuration.
2. To display the list of existing extensions, click **Extension**.
3. The icon indicates VoIP extensions. A new extension will have been created matching the extension number entered above. In the extension's VoIP tab, the **Compression Mode** default is ***Automatic Selection***.
4. To display the list of existing users, click **User**. In the list of users, a new user will have been created matching the VoIP extension number above.
5. Double-click on the IP phone extension user to display their settings.
6. In the **User** tab, set the user **Name** and **Full Name** as required.
7. Click the **Digital Telephony** tab.
8. For the first three buttons, you must click on the **Action** field and select **Appearance | Appearance**.
9. Click **OK**.
10. When all new IP phone extension have been setup, send the new configuration back to the system. Set the Reboot Mode to Immediate or When Free as extension changes cannot be merged.

2.7 Phone Security

There are a number of methods by which additional security can be implemented to ensure that an IP phone does not adopt the identity of another.

- **Disable Auto-Create Extension**
  Following installation, disabling Auto-Create Extn Enabled in the IP Office Manager System | Gatekeeper tab stops new IP devices from assigning themselves as new extensions.
- **Restrict the IP Address or MAC Address**
  Entering either of these values in the Extension's VoIP tab will restrict usage to that address or device. The MAC address of an IP phone is printed on a label on the base of the phone.
- **Set a User Login Code**
  If a user Login Code is set, then any other IP device trying to log on as that extension must also enter the correct login code. If a login code is set, the user can use hot desk to log off and log on elsewhere.

2.8 Backup Restore

1600 Series H323 IP Telephones support using a HTTP server as the location to which they can backup and restore user specific data. These options are used if the location of the HTTP server for backup/restore has been specified in the phone 46XXsettings file.

- The address of the HTTP server for backup/restore operation is separate from the address of the HTTP server used for phone firmware files downloads.
- The HTTP server being used for backup/restore will require configuration changes to allow the phones to send files to it.

Backup is used when the phone user logs out of the phone. During the log out process, the phone creates a file containing the user specific data and sends that to the BRURI location. The file is named with the user's extension number and _16xxdata.txt, for example ***299_16xxdata.txt***.

Restore is used when a user logs in at the phone. The phone sends a file request for the appropriate file based on the users extension number. If the file is successfully retrieved the phone will import the settings and, after a "Retrieval OK" message, continue as normal. If the file cannot be retrieved, a "Retrieval failed" message is displayed and the phone will continues with its existing settings.

Specifying the BRURI Value

1. Open the 46xxsettings.txt file.
2. Locate the line containing the **SET BRURI** value.
3. If the line is prefixed with **#** characters, remove those and any space.
4. After **SET BRURI**, enter a space and then the address of the HTTP backup server, for example ***SET BRURI http://192.168.0.28***. If necessary you can specify the path to a specific server directory and or include a specific port number, for example ***SET BRURI http://192.168.0.28/backups:8080***.

HTTP Authentication

HTTP authentication can be supported. If set it will be used for both the backup and the restore operations. The authentication credentials and realm are stored in the phone's reprogrammable non-volatile memory, which is not overwritten when new telephone software is downloaded.

Both the authentication credentials and realm have a default values of null. If the HTTP server requires authentication, the user is prompted to enter new credentials using the phone. If the authentication is successful, the values used are stored and used for subsequent backup and restore operations.

Manual Backup/Restore Control

Users can request a backup or restore using the Advanced Options Backup/Restore screen, as detailed in the user guide for their specific telephone model. or specific error messages relating to Backup/Restore.

1600 Series Phone Backup File

The following is an example of a backup/restore file for a 1600 Series phone user.

```
ABKNAME001=Extn201
ABKNUMBER001=201
ABKNAME002=Extn201ad
ABKNUMBER002=201
ABKNAME003=Extn203
ABKNUMBER003=203
Redial=0
Call Timer=0
Visual Alerting=1
Call Log Active=1
Log Bridged Calls=1
Log Line Calls=1
Log Calls Answered by Others=0
Audio Path=2
Personalized Ring=7
Handset AGC=1
Headset AGC=1
Speaker AGC=1
Error Tone=1
Button Clicks=0
Display Language=English
```

The table below lists entries that may be found in the backup file. Note that values are not written unless the setting has been changed by the user.

Field	Description
ABKNAMEmmm **ABKNUMBERmmm**	These paired entries are used for personal contacts entered into the phone. The ***mmm*** value in each pair in replace by a 3 digit number starting with 001. The first line of the pair stores the contact name, the second line stores the phone number for the contact.
LANGUSER	Display language. The language name is stored.
LOGACTIVE	Call log active on (1) or off (0).
LOGBRIDGED	Log bridged calls on (1) or off (0).
LOGLINEAPPS	Log line calls on (1) or off (0).
LOGOTHERANS	Log calls answered by others on (1) or off (0).
OPTAGCHAND	Handset Automatic Gain Control on (1) or off (0).
OPTAGCHEAD	Headset Automatic Gain Control on (1) or off (0).
OPTAGCSPKR	Speaker Automatic Gain Control on (1) or off (0).
OPTAUDIOPATH	Audio Path
OPTCLICKS	Button Clicks on (1) or off (0).
OPTERRORTONE	Error Tone on (1) or off (0).
PERSONALRING	Personalized Ring. A numeric value (1 to 8) for the selected ring is stored.
PHNREDIAL	Redial
PHNSCRONCALL	Go to Phone Screen on Calling on (1) or off (0).
PHNSCRONALERT	Go to Phone Screen on Ringing on (1) or off (0).
PHNTIMERS	Call Timer on (1) or off (0).
PHNVISUALALERT	Visual alerting on (1) or off (0).

HTTP Server Configuration for Backup/Restore

For IIS Web Servers

Create a backup folder under the root directory of your web server. All backup files will be stored in that directory.

For example, if your backup folder is ***C:/Inetpub/wwwroot/backup***, the 46xxsettings.txt file should have a line similar to ***SET BRURI http://www.website.com/backup/***.

1. Using Internet Information Services Manager or Internet Information Services depending on your OS, go to **Start | Settings | Control Panel | Administrative Tools**.
2. Right click on the folder created for backup or right click on **Default Web Site** if there is no specific backup directory.
3. Select **Properties**.
4. In the **Directory** tab, make sure the **Write** box is checked.
5. Additional step for IIS 6.0:
    1. Go to **Start | Settings | Control Panel | Administrative Tools**.
    2. Below **Default Web Site**, select **Web Services Extension**.
    3. Make sure the **WebDAV** option is set to ***Allowed***.

For Apache Web Servers

Create a backup folder under the root directory of your Web server. Make the folder writable by everyone. All backup files will be stored in that directory.

For example, if the backup folder is ***C:/Program Files/Apache Group/Apache2/htdocs/backup***, the 46xxsettings.txt file should have a line similar to ***SET BRURI http://www.website.com/backup/***.

1. Edit your Web server configuration file httpd.conf.
2. Uncomment the two LoadModule lines associated with DAV:

```
LoadModule dav_module modules/mod_dav.so
LoadModule dav_fs_module modules/mod_dav_fs.so
```

    - Note: If these modules are not available on your system, typically the case on some Unix/Linux Apache servers, you have to recompile these two modules (mod_dav & mod_dav_fs) into the server. Other ways to load these modules might be available. Check your Apache documentation at http://httpd.apache.org/docs/ for more details.

3. Add the following lines in the httpd.conf file:

```
#
# WebDAV configuration
#
DavLockDB "C:/Program Files/Apache Group/Apache2/var/DAVLock"
<Location />
Dav On
</Location>
```

4. For Unix/Linux Web servers the fourth line might look more like: DavLockDB/usr/local/apache2/var/DAVLock
5. Create the var directory and make it writable by everyone. Right click **Properties | Security | Add | Everyone | Full Control**.

2.9 Listing Registered Phones

Using TFTP, a list can be obtained from the IP Office system of all the registered RAS users which includes H323 IP phones. For example:

```
Extn2602,2602,192.168.42.2,1720
ains600,2600,192.168.42.10,1026
Extn2601,2601,192.168.42.4,1720
New,2702,192.168.42.200,1720
```

1. In Windows, select **Start | Run** and enter **cmd** for the Windows command line interpreter.
2. If necessary, use **cd** commands to select the directory into which you want the list placed as the current directory.
3. Enter tftp -i xxx.xxx.xxx.xxx get nasystem/h323_ras_list yyyyyyyy.txt where:
   - xxx.xxx.xxx.xxx is the IP address of the IP Office unit.
   - yyyyyyy.txt is the name of a text file that does not already exist in that directory.
4. The TFTP command will confirm when the file has been successfully transferred.
5. To close the command line interpreter window, type exit.
6. Open the text file using Wordpad or a similar tool.

The IP Office Monitor application (Sysmon) can also show how many phones have registered and how many are currently waiting to register. The System | Print trace filter option must be selected to see these messages. This appears as lines of the form:

```
792ms PRN: GRQ from c0a82c15 --- RAS reaches the maximum capacity of 10; Endpoints registered 41
```

2.10 Error Messages

The 4600 Series H323 IP phones issue error messages in English only.

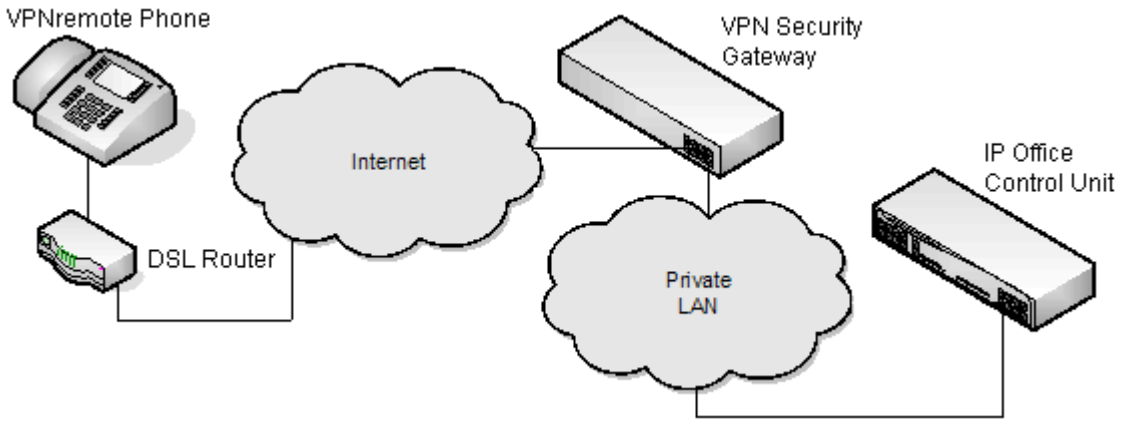
- **Checksum error**
  Downloaded application file was not downloaded or saved correctly. The phone automatically resets and attempts to re-initialize.
- **DHCP: CONFLICT**
  At least one of the IP addresses offered by the DHCP server conflicts with another address. Review DHCP server administration to identify duplicate IP addresses.
- **Failed to set phone IP address**
  The IP phone was originally installed on one switch with Static Addressing and has subsequently been installed on another switch with an active DHCP server assigning dynamic IP addresses. Reset the phone.
- **File too large cannot save file**
  The phone does not have sufficient room to store the downloaded file. Verify the proper filename is administered in the TFTP script file and that the proper application file is located in the appropriate location on the TFTP server.
- **Hardware failure**
  Hardware failure prevented downloading of application file. Replace the phone.
- **IP Address in use by another**
  The phone has detected an IP address conflict. Verify administration to identify duplicate IP addresses.
- **No Ethernet**
  When first plugged in, the IP phone is unable to communicate with the Ethernet. Verify the connection to the Ethernet jack, verify the jack is Category 5, verify power is applied on the LAN to that jack, etc.
- **No file server address**
  The TFTP server IP address in the IP phone's memory is all zeroes. Depending on the specific requirements of your network, this may not be an error. If appropriate, either administer the DHCP server with the proper address of the TFTP server, or administer the phone locally using the ADDR option.
- **Resetting on URQ**
  Restarting following a reboot of the IP Office Unit.
- **System busy**
  The resource being called upon should be checked for its availability. If it appears operational and properly linked to the network, verify addressing is accurate and a communication path exists in both directions between the phone and the resource.
- **Timeout Error**
  Protocol timeout error. Retry. If failure continues, check network congestion, addresses, etc. to identify cause of timeout.
- **TFTP Error**
  Request for file from TFTP server timed out. Check that IP Office Manager or the indicated TFTP source within the IP Office configuration are running and that the 4600 Series phone software files are available.
- **Wrong Set Type**
  Another device is already assigned to the extension number of the IP phone.

Chapter 3.
Other Installation Options

3. Other Installation Options

3.1 VPN Remote Phones

Avaya IP Office VPNremote firmware can be used to connect IP phones at remote locations to the IP Office via IPSec VPN tunnels. IP Office 4.1 and higher supports this with some 4600 Series and 5600 Series IP phones.



Key components are:

1. **IP Office VPNremote Phone Firmware**
   This firmware is provided on the IP Office Administrator Applications CD for IP Office 4.1 and higher. IP Office VPNremote firmware is provided for the 4610SW, 4621SW, 5610SW and 5621SW phones only. Other VPNremote phones are not supported.
2. **TFTP Server**
   During installation a TFTP server is required to load the firmware onto the phones. The same TFTP server as being used for internal IP phone extensions can be used.
3. **IP Office VPNremote Phone Licenses**
   The operation of VPNremote phones with IP Office is licensed using VPN IP Extension licenses entered into the IP Office's configuration. The licenses control the number of VPNremote phones supported by the IP Office.
4. **VPN Security Gateway**
   VPNremote phones uses VPN protocols not directly supported by the IPSec VPN tunnels that can be provided by IP Office control units. Therefore the VPN tunnel from the VPNremote phones must end at a compatible VPN gateway device. The device being used must support one of the following methods:

   - **Avaya Gateways**
     Avaya security gateway devices (SG and VSU) use an Avaya proprietary protocol called CCD.

     Avaya SG Series (4.6 firmware or higher). Avays VSU Series (3.2 firmware or higher).

   - **Non-Avaya Gateways**
     Non-Avaya VPN gateways with IKE Extended Authentication (Xauth) with Preshared Key (PSK). Installation notes exists for the following listed below. This does not imply any recommendation of those devices by Avaya or preclude other devices. Note that Avaya cannot guarantee support for services through non-Avaya devices.

Cisco VPN 300 Series Concentrators.	Netgear FVS338 VPN Router.
Cisco PIX 500 Series Security Appliances.	Kentrox Q2300 VPN Router.
Juniper Networks NetScreen Series VPN Devices.	Adtran Netvanta 3305 VPN Router.
Juniper Networks Secure Services Gateway 500 Series.	Sonicwall Tz170 VPN Router.
Juniper Networks Integrated Security Gateway (ISG) Series.	Netgear FVX538 VPN Router.

Installation Documentation

This document only covers notes and differences specific to installation of VPNremote phones with IP Office. The installation and configuration of Avaya VPNremote phones is covered in a number of existing documents available from the Avaya support website (http://support.avaya.com).

Product Section	Title	Doc Reference
VPNremote Phone	VPNremote for the 4600 Series IP Telephones Administrators Guide	19-600753
	Application Notes for Configuring Avaya VPNremote Phone with Juniper Secure Services Gateway using Policy-Based IPSec VPN and XAuth Enhanced Authentication	317687
	Configuring Cisco PIX Security Appliance using Cisco Adaptive Security Device Manager (ASDM) VPN Wizard to Support Avaya VPNremote Phones	317678
	Configuring Cisco PIX Security Appliance with Microsoft Internet Authentication Service and Active Directory using RADIUS to Support Avaya VPNremote Phones	317675
	Configuring Cisco VPN Concentrator to Support Avaya VPNremote Phones	317672
	VPNremote for 4600 Series IP Telephone User Installation and Configuration Quick Start - Pre-Deployment	19-601708
	VPNremote for 4600 Series IP Telephone User Installation and Configuration Quick Start - Self Installer	19-602363
4600 IP Telephones	4600 Series IP Telephone LAN Administrator Guide.	555-233-507
IP Office	Technical Tip 184 - Configuring a VPN Remote IP Phone with a Netgear FVS338 VPN Router.	322690
	Technical Tip 185 - Configuring a VPN Remote IP Phone with a Kentrox Q2300 VPN Router.	322702
	Technical Tip 186 - Configuring a VPN Remote IP Phone with an Adtran Netvanta 3305 VPN Router.	322714
	Technical Tip 190 - Configuring a VPN Remote IP Phone with a Sonicwall Tz170 VPN Router	325830
	Technical Tip 196 - Configuring a VPN Remote IP Phone with a Netgear FVX538 VPN Router.	327056

Supported VPNremote Phone Firmware

Unless otherwise advised, only the firmware provided on the IP Office Administrator Applications CD or DVD should be used for VPNremote phones connected to an IP Office. That firmware is tested with the IP Office release represented by the CD/DVD for correct operation. The firmware is located in a zip file in the folder \bin\VPN Phone.

Whilst other VPNremote firmware releases may be made available by Avaya for download, those firmware release may not have been specifically tested with IP Office.

Licensing VPNremote Phones on IP Office

Use of VPNremote phones with IP Office requires entry of IP400 VPN Phone licenses into the IP Office configuration. The licenses control the number of VPNremote phones that the IP Office will support.

License	RFA Name	SAP Code
VPN IP Extensions	IPO LIC VPN Phone 1	213980
	IPO LIC VPN Phone 5	213981
	IPO LIC VPN Phone 10	213982
	IPO LIC VPN Phone 25	213983
	IPO LIC VPN Phone 50	213984
	IPO LIC VPN Phone 100	213985
	IPO LIC VPN Phone Unlimited	213986
	IPO LIC VPN Phone 10 Trial (45-days)	213987

Configuring the IP Phone for VPNremote

In addition, a VPN Phone Allowed checkbox option is present on the Extension | VoIP settings tab of IP extensions. This checkbox is used to indicate to the IP Office, which IP extensions are VPNremote and therefore require use of a license.

1. Using IP Office Manager, receive the current configuration from the IP Office system.
2. Click on **Extension** and select the entry for the IP extension.
3. Select the **VoIP** tab.
4. Enable **VPN Phone Allowed**.
5. Click **OK**.
6. Repeat this for any other existing IP extensions that are going to be converted to VPN connection.
7. Save the configuration back to the IP Office system.

Configuring 4600 Series VPN Remote Phones for IP Office Licensing

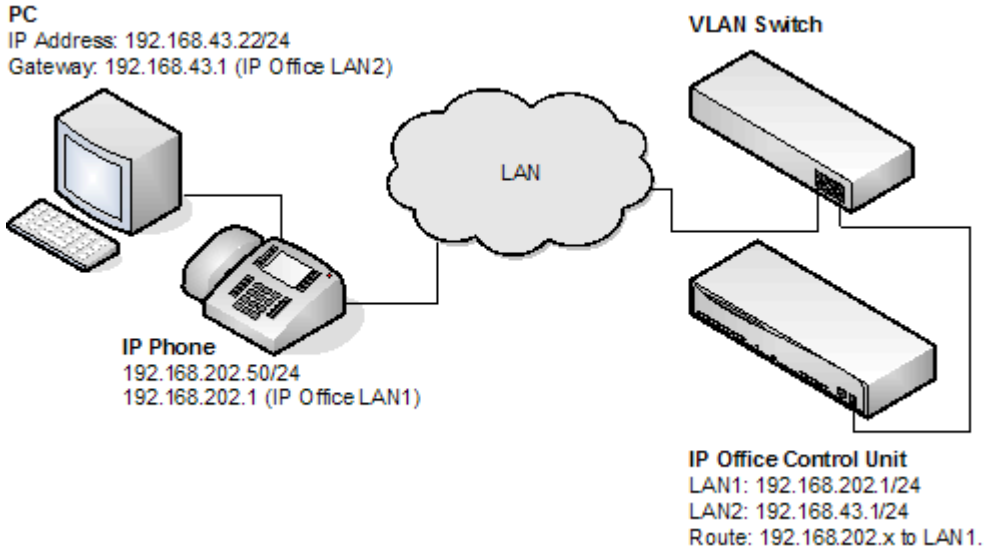
By default, 5600 Series phones running VPNremote firmware use licenses available from the IP Office to which they connect. However 4600 Series phones running VPNremote can be licensed in a number of ways and so need to be instructed to use the IP Office for licensing.

In order to inform that 4600 Series VPNremote phones to use IP Office licensing, the following line must be added to the 46vpnsettings.txt file:

- SET SMBLIC 1

3.2 VLAN and IP Phones

This section describes the configuration of an VLAN networking infrastructure for use with Avaya IP Office and 4600 Series IP Phones. In this example an HP Procurve Ethernet 2626 PWR Ethernet switch is used to manage the VLAN's. A basic understanding of the IEEE 802.2p/q standard is required.



The use of VLAN allows separate collision domains to be created on Ethernet switches. In the case of IP Office and IP Phones the advantages are:

1. It allows PC's to continue in the same IP subnet while IP Phones can use a new and separate IP addressing scheme.
2. Broadcast traffic is not propagated between the PC data network and the IP Phones voice network. This helps performance as otherwise broadcast traffic must be evaluated by all receivers.
3. VLAN networking and traffic prioritisation at layer 2 are closely bound together in the same 802.2 standard. It is therefore easier to maintain L2 QOS when using a VLAN.

The table below shows the three ways in which VLAN can be deployed with an Ethernet Switch. The first two methods require only elementary configuration and as this document assumes both PC and IP Phones share the same Ethernet port, the focus will be the third method (overlapping).

Type	Description	Advantages	Disadvantages
No VLAN	Both Voice and Data occupy the same collision domain	Simple configuration	PC broadcast traffic adverse effect on Voice traffic. Requires two ports per user (one for IP Phone and one for PC).
Physical VLAN	Separate VLAN for data and voice	Simple configuration	Requires two ports on switch (one for IP phone and one for PC.
Overlapping VLAN	A single port on the switch carrying both the IP Phones as well as the PC traffic.	Requires only a single port for both PC and IP Phone. PC broadcast traffic cannot adversely effect Voice traffic.	Complex configuration.

VLAN and DHCP

The use of VLAN has implications on DHCP if DHCP is being used for support of IP phones and or PC's. The table below details the available options when using a single port for PC and IP Phones on a VLAN enabled network.

DHCP Option	Description
None (Static addressing)	Manually configuration of each IP Phone.
Separate DHCP Servers	Two PCs, one for each VLAN.
Multihomed DHCP Server	A single PC with two NIC Cards; one for each VLAN.
DHCP Relay	The option must be supported by the Ethernet switch.

If using DHCP, when the IP Phone starts it will first perform a DHCP discovery without a VLAN tag. If the DHCP reply contains a new VLAN setting (scope option 176), the Phones will release all existing IP parameters and then perform a new DHCP discovery using the supplied VLAN ID. If the IP Phone does not get a new VLAN ID, the phone will continue with the settings provided in the original DHCP reply.

The VLAN ID can also be passed to the phones through the 46xxsettings file. Again if this method is used the IP phone will release all its existing IP parameters and perform a new DHCP discovery on the supplied VLAN ID.

A potential error loop condition can occur if the DHCP server and 46setting files have conflicting VLAN values. This is because the IP Phones release all their IP parameters and restart if their VLAN ID is changed. Another way this error loop can occur is if two DHCP servers are used; The Avaya 4600 IP Phone would repost this condition if it occurs.

As stated, when an IP phone is given a new VLAN ID, via TFTP or DHCP, it will immediately releases its current IP parameters and issue a new DHCP request using the new VLAN ID. In this way, when the IP Phones are first a DHCP reply from the DHCP server on the data VLAN, it contains the VLAN ID of the voice VLAN. The phone will release the data VLAN settings and send a new DHCP request tagged for the voice VLAN.

Data VLAN DHCP Settings

Option	Data VLAN DHCP Settings	Voice VLAN DHCP Settings
IP Address	192.168.43.x	192.168.202.x
Mask	255.255.255.0	255.255.255.0
3: Router	192.168.43.1	192.168.202.1
176	L2Q=1, L2QVLAN=202, VLANTEST=0	MCIPADD=192.168.202.1, MCPORT=1719, TFTPSRVR=192.168.202.X VLANTEST=0

The **VLANTEST** parameter is the length of time the IP Phone is to continue DHCP requests in a VLAN (0 means unlimited time).

Example setup - Overview

The network is devised to allow the user PC to connect to the switch port of the IP Phone. A single cable then connects PC and IP Phone to the Ethernet Switch. For the purpose of this example VLAN 209 is used for voice traffic and VLAN 210 for data traffic. The LAN1 interface of the IP Office control unit resides on the voice VLAN while the LAN2 interface resides in the data VLAN. Communications between the voice and data VLAN's is facilitated by the IP Office control unit's router function.

HP-Switch - Configuration

Shown below are the web and CLI configuration output from the HP Procurve Switch.. These where obtained using the configuration guidelines which can found below.

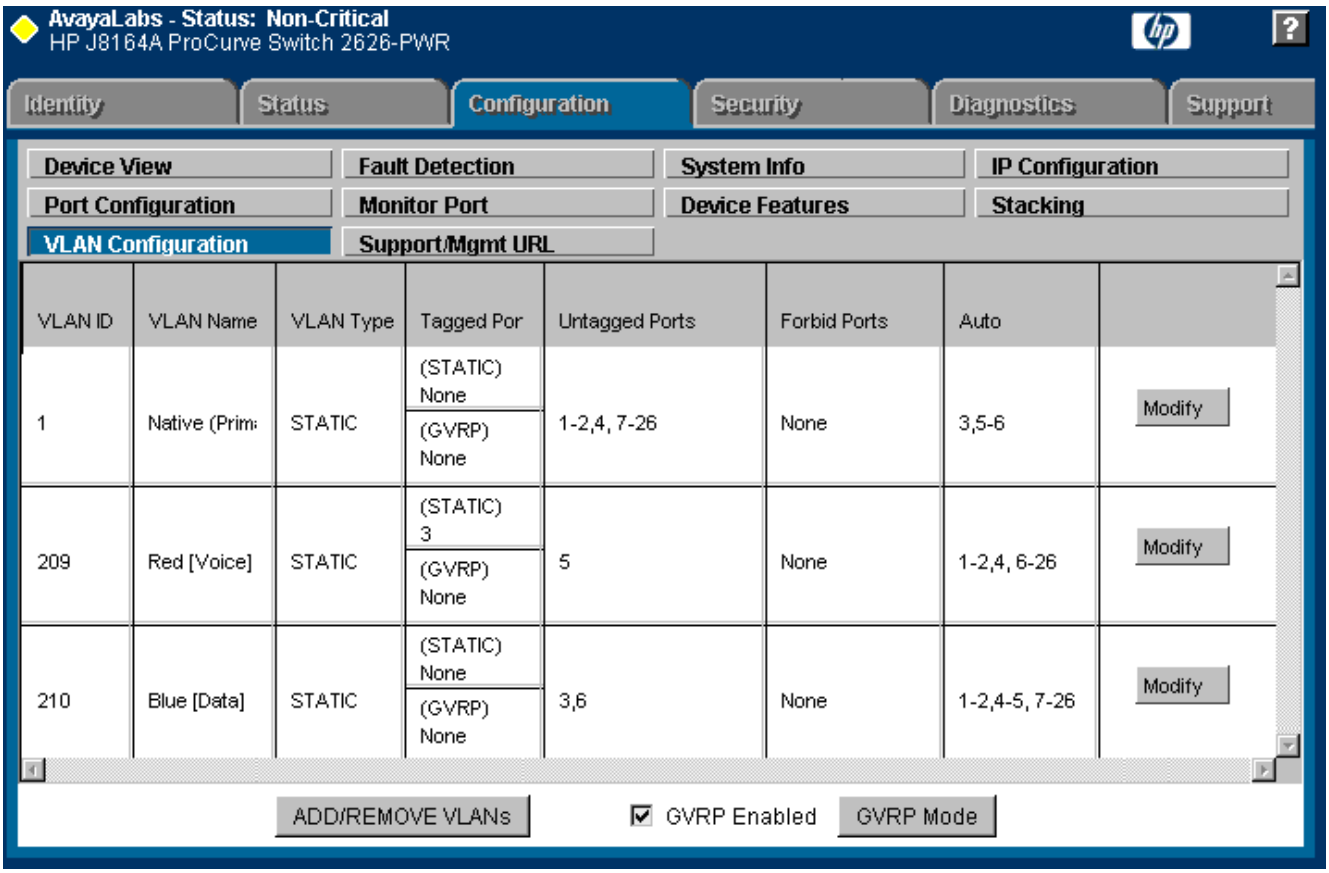


Figure 1 HP Procurve Web Configuration

HP Procurve CLI output

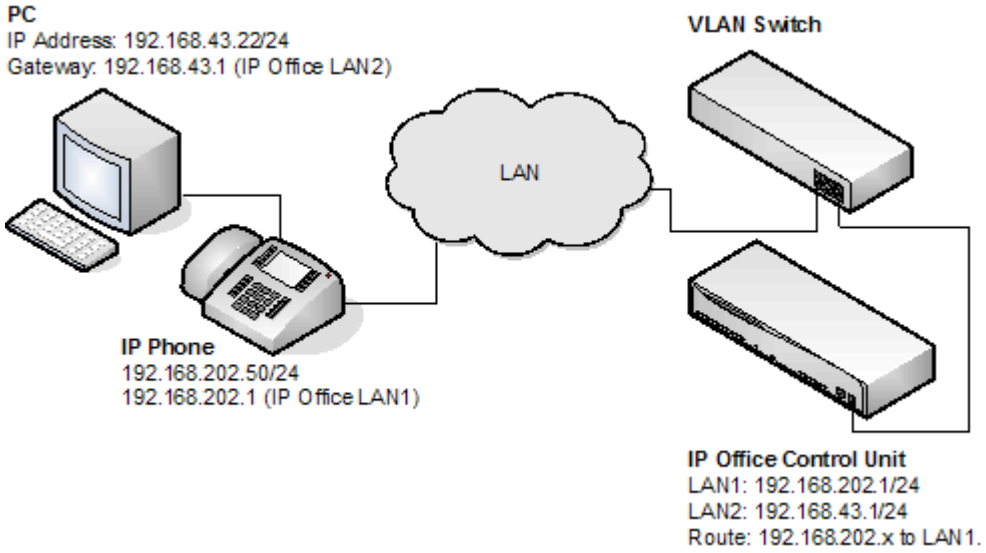
```
; J8164A Configuration Editor; Created on release #H.08.60

hostname "AvayaLabs"
snmp-server community "public" Unrestricted
vlan 1
name "Native"
untagged 1-2,4,7-26
ip address 192.168.202.201 255.255.255.0
no untagged 3,5-6
exit
vlan 209
name "Red [Voice]"
untagged 5
tagged 3
exit
vlan 210
name "Blue [Data]"
untagged 3,6
exit
gvrp
spanning-tree
```

The table below summaries the HP configuration for ports and VLAN's.

Port	VLAN 209 Voice	VLAN 210 Data	Description
3	Tagged	Untagged	This port was added to both VLAN 209 and VLAN 210. However there is an important difference between adding to these VLAN's. When adding port 3 to VLAN 209 the Mode option must be tagged but untagged when adding to VLAN 210.
5	Untagged	–	This port is included only in VLAN 209 and not included in VLAN 210. The Mode option must be set to Untagged for port 5 in this VLAN.
6	–	Untagged	Port 6 is included only in VLAN 210 and not included in VLAN 209. The Mode option MUST be set to Untagged in this VLAN.

The operation of this network is dependant on the functionality defined in HP documentation. Specifically HP refers to this type of VLAN operation as Overlapping VLAN. The configuration relies also on that fact that Avaya 4600 IP Phones support VLAN operation .

Example System Overview



IP Office Configuration
The table below details the configuration for IP Office. Additional configuration is not required by IP Office in support 802.1 Tagging.

Option	Value
IP Address LAN1	192.168.202.1
IP Mask LAN1	255.255.255.0
IP Address LAN2	192.168.43.1
IP Mask LAN2	255.255.255.0
Router	192.168.202.1
Call Server	192.168.202.1

IP Phone- Configuration
For this example the IP phone was configured with fixed IP addressing as shown below:

Option	Value
IP Address	192.168.202.50
IP Mask	255.255.255.0
Router	192.168.202.1
Call Server	192.168.202.1
VLANID	209

VLAN Switch Configuration
The table below summaries the HP configuration for ports and VLAN's.

Port	VLAN 209 Voice	VLAN 210 Data
3	Tagged	Untagged
5	Untagged	–
6	–	Untagged

The PC –Configuration
Shown below is the IP configuration of the PC1; no option in support of 802.1p or 802.1q is enabled on the PC.

Option	Value
IP Address	192.168.43.22
IP Mask	255.255.255.0
Router	192.168.43.1

Summary
On the port on which the PC and IP phone resides two types of Ethernet frames can be received (i.e. sent from Phone or PC).

1. Tagged Packets are sent by IP Phone
2. Untagged packets are sent by PC

When an untagged packet is sent by the PC attached to the IP Phone port it will be propagated only to VLAN 210. This is because when we added the port 3 to VLAN 210 the Mode option was specified as untagged. While for the other VLAN (210) the option Tagged was select for port 3 in VLAN 209. Therefore tagged packets will go to VLAN 209 while the untagged will go to 210.

When a packet is originated from an IP Phone it is tagged. Because the option un-tagged is selected for port 5 in VLAN 209 then the 802.1 tag is removed before the switch forwards the packet to this port. Similarly when an untagged packet is originated and sent by IPO the switch will tag the packet before forwarding LAN port 3.

Chapter 4.
Static Administration Options

4. Static Administration Options

A number of settings can be altered through the phone after installation.

- Values assigned through static administration override any set through the ***46xxsettings.txt*** file. They will remain active for the IP phone until a new boot file is downloaded.

These procedures should only be used if you are using static address installation. Do not use these procedures if you are using DHCP.

- To set parameters for all H323 IP phones on a system, you can edit the 46XXsettings.scr script file.

Hold vs Mute

Many of the static administration features are accessed using key sequences that begin by pressing either **MUTE** or **HOLD**. In most cases it does not matter whether **HOLD** or **MUTE** is used.

Entering Data for Administrative Options

This section describes how to enter data for the administrative options.

1. All local procedures are started by dialling Hold and then a sequence of up to 7 numbers followed by **#**.
2. After the Hold button is pressed, a 6-second timeout is in effect between button presses. If a valid button is not pressed within 6 seconds of the previous button, the collected digits are discarded and no administrative option is started.
3. Attempts to enter invalid data are rejected and the phone emits an error beep.
4. If a numeric digit is entered for a value or for a field of an IP address or subnet mask after only a zero has been entered, the new digit will replace the zero.
5. To go to the next step, press **#**.
6. To backspace within a field depends upon the phone type:
   - **4601, 4602, 5601, 5602:** Speaker key.
   - **4606:** Conference key.
   - **4612 & 4624:** Previous key.
   - **4610, 4620, 4625, 5610, 5620:** Left-most key.

4.1 QOS Option Settings

Administering QoS options is not mandatory, but it is highly recommended. Use the following procedure to set Quality of Service (QoS) options.

1. While the phone is on-hook and idle, press the following sequence: **Hold 7 6 7 #** (**Hold Q O S #**).
2. The current 802.1Q settings are shown in sequence:
   - **L2 audio=**
     This is the phone's current 802.1 audio parameter. To accept the current value, press **#** or enter a value (between 0 and 7) and then press **#**.
   - **L2 signaling=**
     This is the phones 802.1 signaling parameter. To accept the current value, press **#** or enter a value (between 0 and 7) and then press **#**.
   - **L3 audio=**
     This is the phone's Differential Services audio parameter. To accept the current value, press **#** or enter a value (between 0 and 63) and then press **#**.
   - **L3 signaling=**
     This is the phone's Differential Services signaling parameter. To accept the current value, press **#** or enter a value (between 0 and 63) and then press **#**.
3. If no new values were entered during this procedure, **No new values** is displayed. To end the procedure, press **#**.
4. If new values were entered during this procedure, **Save new values?** is displayed. To end the procedure or save the new values, press **#**. **New values being saved is displayed** and the phone returns to normal operation.

4.2 Secondary Ethernet (Hub)/IR Interface Enable/Disable

Use the following procedure to enable or disable the hub interface found on some H323 IP phones (usually marked with a 🖳 symbol). The default for the hub interface is **enabled**.

The same procedure can also be used to enable or disable the IR port found on some H323 IP phones, see Infrared Dialling 62.

1. While the phone is on-hook and idle, press the following sequence: **Hold 4 6 8 #** (**Hold I N T #**). The phones port settings are shown in sequence. The option vary between different models of phone.
   - **PHY2**=
     This is the PC connection LAN socket marked as 🖳 on the phone. Press **1** or **0** to enable or disable the hub interface respectively. To continue, press **#**.
   - **IR=**
     This is the infrared (IR) port located on the front of some H323 IP phones. Press **1** or **0** to enable or disable the hub interface respectively. To continue, press **#**.
2. If you changed the setting, **Save new values?** is displayed. To end the procedure or save the new values, press **#**. If you press **#**, New values being saved is displayed and then returns to normal operation.

4.3 View Details

You can use the following procedure to view a number of phone details. These are in addition to the other static address and local administration options which can also be used to review settings.

1. While the phone is on-hook and idle, press the following sequence: **Hold 8 4 3 9 #** (**Hold V I E W #**).
   - To display the set of details, press ***** at any time during viewing.
   - To end the procedure and restore the user interface to its previous state, press **#**.
2. A sequence of values are displayed. The values available may vary between phone models and the level of IP phone software installed on the phone. To display the next value press *. To exit the information display press #.
   - **Model**
     Shows the phones model number; for example, 4624D02A.
   - **Market**
     Shows 1 for export or 0 for domestic (US). Not displayed on all phone types.
   - **Phone SN**
     Shows the phone's Serial Number.
   - **PWB SN**
     Shows the phone's Printed Wiring Board Serial Number.
   - **PWB comcode**
     Shows the PWB's comcode.
   - **MAC address**
     Shows the phone's MAC address as paired hexadecimal numbers.
   - **L2 tagging**
     Indicates whether L2 tagging is on, off or set to auto.
   - **VLAN ID**
     The VLAN ID used for the phone. The default is 0.
   - **IP address**
     The IP address assigned to the phone.
   - **Subnet mask**
     The subnet mask assigned to the phone.
   - **Router**
     The router address assigned to the phone.
   - **File server**
     The address of the file server assigned to the phone.
   - **Call server**
     The address of the phone's H323 Gatekeeper.
   - **802.1X**
     The current setting for 802.1X operation if being used.
   - **Group**
     This displays the group value set on the phone. Group values can be used to control which options (both firmware and settings) a phone downloads. Refer to the 4600 Series Phones LAN Administrator Guide.
   - **Protocol**
     Display ***Default***.
   - **filename1**
     Shows the name of the phone application file in the phone's memory. These are values from within the boot file loaded and not the actual file name.
   - **10MBps Ethernet** or **100Mbps Ethernet**
     Shows the speed of the detected LAN connection.
   - **filename2**
     Shows the boot file name and level. These are values from within the boot file loaded and not the actual file name.

4.4 Self-Test Procedure

1. To start the IP phone self-test procedures, press the following sequence: **Hold 8 3 7 8 #** (**Hold T E S T #**). The phone does the following:
   - Each column of programmable button LED's is lit for half a second from left to right across the phone, in a repeating cycle. The Speaker/Mute LED and the message waiting LED are also lit in sequence.
   - Buttons (other than #) generate a click if pressed.
   - Phones with displays show **Self test #=end** for 1 second after self-test is started. Then a block character (all pixels on) is displayed in all display character locations for 5 seconds. Display of the block character is used to find bad display pixels.
2. One of the following is finally displayed:
   - **If self-test passes:**

     ```
     Self test passed
     #=end
     ```

   - **If self-test fails:**

     ```
     Self test failed
     #=end
     ```

3. To end the self-test, press #. The phone returns to normal operation.

4.5 Resetting a Phone

Resetting a Phone

Resetting a phone clears the phones user settings but retains system settings such as the DHCP and file server addresses.

1. While the phone is on-hook and idle, press the following sequence: **Hold 7 3 7 3 8 #** (**Hold R E S E T #**). **Reset values?** is displayed.
2. To cancel this procedure press *****. To continue press #.
   - **WARNING**
     As soon as you press **#**, all static information will be erased without any possibility of recovering the data.
3. Whilst the system values are reset to their defaults, **Resetting values** is displayed.
4. Once the system values are reset, **Restart phone?** is displayed.
   - To end the procedure without restarting the phone, press *****.
   - To restart the phone, press **#**. The remainder of the procedure then depends on the status of the boot and application files. See Restart Scenarios 58.

Clearing a Phone

Clearing a phone removes all data values including settings such as the DHCP and file server addresses. This returns the phone to almost its original out-of-box state. The phone will still retain the firmware files it has downloaded.

1. While the phone is on-hook and idle, press the following sequence: **Hold 2 5 3 2 7 #** (**Hold C L E A R #**). **Clear all values?** is displayed.
2. To cancel this procedure press *****. To continue press #.
   - **WARNING**
     As soon as you press #, all static information will be erased without any possibility of recovering the data.
3. Whilst the system values are reset to their defaults, **Clearing values** is displayed.
4. Once all values are cleared, the phone will restart as if a new phone.

4.6 Site Specific Option Number

The Site Specific Option Number (SSON) is used by IP phones to request information from a DHCP server that is specifically for the phones and not for other IP devices being supported by the DHCP server. This number must matched by a similarly numbered 'option' set on the DHCP server that define the various settings required by the phone.

The default SSON used by Avaya 4600 and 5600 Series IP phones is 176. The default SSON used by Avaya 1600 Series IP phones is 242. For phones being supported by IP Office DHCP, the SSON used by the phone must be matched by the site specific option numbers set in the IP Office configuration (**System | LAN | Gatekeeper**).

- **WARNING**
  Do not perform this if using static addressing. Only perform this procedure if using DHCP addressing and the DHCP option number has been changed from the normal default (176).

Setting the SSON on an IP Phone:

1. While the phone is on-hook and idle, press the following sequence: **Mute 7 7 6 6 #** (**Mute S S O N #**). **SSON=** is displayed followed by the current value.
2. Enter the new setting. This must be a number between 128 and 255.
3. To cancel this procedure, press ***** or press **#** to save the new value.

Setting the SSON on IP Office

Note that changing the IP Office SSON settings requires the system to be rebooted.

1. In IP Office Manager, receive the system's current configuration.
2. Double-click **System**.
3. Click the **LAN** tab.
4. Select the Gatekeeper sub tab.
5. Set the **Site Specific Option Number (SSON)** fields to the required numbers. For IP Office 4.2+ two SSON field are available.
6. Click **OK**.
7. Send the configuration back to the system. Select Immediate or When Free as the Reboot Mode.

4.7 Automatic Gain Control

Automatic Gain Control (AGC) raises the volume when a caller is speaking quietly and lowers the volume when the caller is loud. AGC can be separately switched on or off for the phone handset, headset and speaker.

The AGC settings for all H323 IP phones can also be set through the 46xxsetting.txt file. On some phones it can also be switched on or off through the phone's user menus.

Switching automatic gain control on/off:

1. While the phone is on-hook and idle, press either **Hold 2 4 2 #** (**Hold A G C #**). The current AGC settings are displayed. Note that these may vary depending on the headset/speaker support provided by the phone model.
   - **Handset AGC =**
     Press the indicated key for the required setting (0 = off and 1 = on) and then press #.
   - **Headset AGC =**
     Press the indicated key for the required setting (0 = off and 1 = on) and then press #.
   - **Speaker AGC =**
     Press the indicated key for the required setting (0 = off and 1 = on) and then press #.
2. The phone should return to it normal idle state.

Chapter 5.
Restart Scenarios

5. Restart Scenarios

The sequence of the restart process depends on the status of the boot and application files on the TFTP server and those already downloaded to the phone. This appendix explains the different scenarios possible.

All of the following start-up processes involve the same initial steps as the phone negotiates with the DHCP and the TFTP server.

- After power is applied the phone displays Restarting….
- Initializing is then displayed.
- When either the application file (if there is one) or the boot code is uncompressed into RAM, Loading is displayed. Since this takes a while, asterisks, then periods, then asterisks are displayed on the second line to indicate that something is happening.
- When control is passed to the code in RAM, Starting is displayed.
- The phone detects and displays the speed of the Ethernet interface in Mbps (that is 10 or 100). The message No Ethernet means the LAN interface speed cannot be determined.
  - The Ethernet speed indicated is the LAN interface speed for both the phone and any attached PC.
- DHCP is displayed whilst the phone obtains an IP address and other information from the LAN's DHCP server. The number of elapsed seconds is incremented until DHCP successfully completes.
  - If the phone has been setup using static addressing (by pressing * when DHCP is shown), it will skip DHCP and use the static address settings it was given.
  - Note that uploading a new boot file at any time erases all static address information.
- TFTP is displayed whilst waiting for a response from the TFTP server. 46XXUPGRADE.SCR is displayed whilst downloading the upgrade script TFTP server.
  - TFTP Error: Timed Out is displayed if the phone cannot locate TFTP server or upgrade script file. If the phone has been previously installed it will continue with the existing files in its memory.
- After the upgrade script is loaded, the sequence depends on the status of the files currently held in the phones memory, compared to those listed in the upgrade script.
  - **Boot File Need Upgrading** 59.
  - **No Application File or Application File Needs Upgrading** 59.
  - **Correct Boot File and Application File Already Loaded** 59.

5.1 Boot File Needs Upgrading

Having processed the upgrade script file, the software determines that the name of the boot code file in the phone does not match that in the upgrade script. The script specifies the name of the new file to load.

- The phone displays the file name and the number of kilobytes loaded.
- The phone displays **Saving to flash** while the new boot file is stored in its flash memory. The percentage of the file stored and the number of seconds that have elapsed are shown. This will usually take longer than it took to download the file.
- The phone displays **Restarting** as it prepares to reboot using the new boot file.
- The phone displays **Initializing**.
- While the new boot file is uncompressed into RAM, the phone displays Loading. Since this takes a while, asterisks, then periods, then asterisks are displayed on the second line to indicate that something is happening.
- When control is passed to the software that has just loaded, the phone displays **Starting**.
- The phone displays **Clearing** whilst the flash memory is erased in preparation for rewriting the code. The percentage of memory erased and number of elapsed seconds are also shown.
- Updating is displayed whilst the boot code is rewritten. The percentage of boot code rewritten and number of elapsed seconds are also shown.
- When the new boot code has been successfully written into the flash memory, the phone resets so that the status of the phone application files can be checked.

Continue with the next procedure; No Application File or Application File Needs Upgrading 59.

5.2 No Application File or Application File Needs Upgrading

This happens with normal application file upgrades. Having processed the upgrade script file, the software determines that the name of the boot file in the phone is the correct version. It next determines that the name of the application file does not match that stored in the phone.

- The phone displays the required file name as it downloads the file from the TFTP server. It also displays the number of kilobytes downloaded.
- **Saving to flash** is displayed. The percentage of file stored and the number of seconds that have elapsed is also displayed. This will usually take longer than it took to download the file.
- The phone is reset so that the new system-specific application file can be executed.
- Continue with the next procedure; Correct Boot File and Application File Already Loaded 59.

5.3 Correct Boot File and Application File Already Loaded

This happens with most normal restarts. Having processed the upgrade script file, the software determines that the name of the boot file in the phone and the phone application file match those specified in the upgrade script.

- System-specific registration with the switch is started. The phone requests the extension number it should use and the password.
  - By default, the phone displays the last extension number it used. To accept, press #.
  - Whilst a password request is shown, password verification is not performed except if the user changes the extension number.
  - The password checked against is the user's Login Code stored in IP Office Manager.
- Upon completion of registration, a dial-tone is available on the phone.

Chapter 6.
Infrared Dialling

6. Infrared Dialling

Some H323 IP phones include an infrared (IR) port at the front of the phone. This includes the 4606, 4612, 4624 and 4620 phone. The port appears as a dark plastic window on the front edge of the phone, just below the normal dialling keys.

You can use the IR port in the following ways:

- **Dial a Number to Start a Call**
  This can be done by beaming the contact information held in a personal organizer address book.
- **Swap Text Files During a Call**
  If calling another IP phone extension that has an IR port, text files can be beamed between extensions.

When using infrared beaming, the following must be remembered:

- The device beaming or receiving must be IrDA compatible. This is the case for most computer and personal organizer IR ports.
- The range of transmission is typically a maximum of 5 feet (1.5 meters) and with a 5° degree spread (this is unlike IR devices used for remote controls which typically beam over a long range and much wider angle spread).
- For details of enabling and using IR beaming from your personal organizer or PC, refer to the manufacturer's information.

Note

- Some personal organizers can be set to beam to modems and mobile phones which use different transmission formats. The personal organizer may need to be set to beaming to another PC/personal organizer for dialling to work.
- These features have been tested with several devices as indicated. However, this is not a commitment to continually test or support those devices against future levels of software.

6.1 Enabling the IR Port

By default, where fitted the IR port on H323 IP phones is enabled. If necessary, it can be disabled.

1. With the phone on-hook and idle, press **Hold 4 6 8 #** (**Hold I N T #**). **PHY2=** and the current status is displayed. This is the setting for the phone's pass-through Ethernet port.
2. To continue, press **#**. IR=. The current status is displayed.
3. Change the status if required by following the displayed prompts and then press #. The phone will restart.

6.2 Dialling Phone Numbers

You can use the IR port to receive phone numbers beamed from an IR enabled PC or pocket organizer device. Any device that can beam contacts in the VCard format (.vcf) can be used.

If you are unsure of the file format used by your IR device, you can try beaming a contact anyway. The display on the IP phone will show the name of the file it received. If that ends in .vcf, then the phone should dial the number in the VCard file.

You will need to remember the following:

- The phone will only dial the first phone number in the VCard file.
- If your IP Office system has been setup to need a prefix for external dialling, that prefix must be in the VCard phone number.

In addition to dialling the phone number digits, the following additional characters can be included in the phone number:

- **m** = Mute
- **c** = Conference
- **h** = Hold
- **t** = Transfer
- **,** (comma) = 2-second pause

The following sections contains examples of dialling contacts by beaming from various different devices.

Palm Organizer

The following was tested using a Palm Vx and M505. The connection setting (**Prefs | Connection**) must be ***Ir to PC/ Handheld***.

1. To enter the address book, click on the phone button or icon.
2. Locate the person or organization that you want to dial.
3. To go to **Address View**, click on the entry.
4. On the letters area of the graffiti pad, make a sweep from the bottom-left to the top-right. A set of icons should appear. Click on the beam icon. Alternatively, click on the menu icon and select Beam Address.

Windows Pocket PC

The following was tested using a Compaq iPAQ Pocket PC:

1. In **Contacts**, select the entry you want to dial.
2. Click **Tools** and then select **Beam Contact**. The Pocket PC will search for and then display the IR enabled devices found. The IP phone should appear on the list.
3. Select the IP phone and the contact information will be beamed to it.

6.3 Beaming Files During a Call

During a call between two IR enabled extensions on the same system, you can also beam files between IR devices at each end.

The types of file sendable and receivable will depend on those supported by the devices sending and receiving, as if they were face to face.

VCard files can be exchanged without being interpreted as a number to dial.

Palm Organizer

The following was tested using a Palm Vx and M505.

1. Inform the caller that you want to beam them a file and to have their Palm positioned in front of their extensions IR port ready to receive.
2. Locate the file that you want to send.
3. On the letters area of the graffiti pad, make a sweep from the bottom-left to the top-right. A set of icons should appear. Click on the beam icon. Alternatively, click on the **Menu** icon and select the displayed **Beam** option. The phones should display the first eight characters and the file extension of the file being transferred.

Chapter 7.
Alternate DHCP Server Setup

7. Alternate DHCP Server Setup

The recommended installation method for H323 IP phones uses a DHCP server. When 5 or less H323 IP phones are being supported, the DHCP can be performed by the IP Office Unit itself. However, if more than 5 H323 IP phones are being supported, a separate DHCP server must be used.

- For IP Office 4.2+ running on an IP500 IP Office system, the full capacity of up to 272 extensions is supported using the IP Office for DHCP.

This document outlines, as an example, the basic steps for using a Windows server as the DHCP server for IP phone installation. However, the principles of defining a scope is applicable to most DHCP servers.

You will need the following information from the customer's network manager:

- The IP address range and subnet mask the H323 IP phones should use.
- The IP Gateway address.
- The DNS domain name, DNS server address and the WINS server address.
- The DHCP lease time.
- The IP address of the IP Office unit.
- The IP address of the PC running Manager (this PC acts as a file server for the H323 IP phones during installation).

7.1 Using a Windows DHCP Server

1. Checking for DHCP

1. On the server, select **Start | Program | Administrative Tools | Computer Management**.
2. Under **Services and Applications** in the Computer Management Tree, locate **DHCP**.
3. If DHCP is not present then you need to install the DHCP components. Refer to the Microsoft documentation.

2. Windows DHCP Setup for H323 IP Phones

2a. Creating the Scope

A DHCP scope defines the IP addresses that the DHCP server can issue in response to DHCP requests. Different scopes may be defined for different types of devices.

1. Select **Start | Programs | Administrative Tools | DHCP**.
2. Right-click on the server and select **New | Scope**.
3. The scope creation wizard will be started, click **Next**.
4. Enter a name and comment for the scope and click **Next**.
5. Enter the address range to use, for example from 200.200.200.1 to 200.200.200.15 (remember the host part cannot be 0).
6. Enter the subnet mask as either the number of bits used or the actual mask, for example 24 is the same as 255.255.255.0 and click **Next**.
7. You can specify addresses to be excluded. You can do this either entering a range (e.g. 200.200.200.5 to 200.200.200.7) and clicking **Add**, or entering a single address and clicking **Add**.
   - **Note:** You should exclude the IP Office from this range, as the DHCP Options in the IP Office should be disabled. This is only a recommendation. You can also accomplish this by leaving available addresses outside of the scopes range.
8. Click **Next**.
9. You can now set the lease time for addresses. If set too large, addresses used by devices no longer attached will not expire and be available for reuse in a reasonable time. This reduces the number of addresses available for new devices. If set too short, it will generate unnecessary traffic for address renewals. The default is 8 days. Click **Next** .
10. The wizard gives the option to configure the most common DHCP options. Select **Yes** and then click **Next**.
11. Enter the address of the gateway and click **Add**. You can enter several. When all are entered, click **Next**.
12. Enter the DNS domain (eg. example.com) and the DNS server addresses. Click **Next**.
13. Enter the WINS server addresses and click **Add** and then click **Next**.
14. You will then be asked if you wish to activate the scope. Select **No** and then click **Next**.
15. Click **Finish**. The new scope will now be listed and the status is ***Inactive***.

2b. Adding a 242 Option

In addition to issuing IP address information, DHCP servers can issue other information in response to requests for different specific DHCP option numbers. The settings for each option are attached to the scope.

1600 Series H323 IP phones request option 242 from the DHCP server. The option should include defining the address of the phone's H323 gatekeeper (the IP Office) and the address of the HTTP file server.

1. Right-click on the DHCP server.
2. From the pop-up menu, select **Predefined options**.
3. Select **Add**.
4. Enter the following information:
   - **Name:** 16xxOptions
   - **Data type:** String
   - **Code:** 242
   - **Description:** IP Phone settings
5. Click **OK**.
6. In the string value field, enter the following:

   MCIPADD=xxx.xxx.xxx.xxx,MCPORT=1719,HTTPSRVR=yyy.yyy.yyy.yyy,HTTPDIR=z, VLANTEST=0

   where:

   - ***MCIPADD=*** is the H323 Gatekeeper (Callserver) address. Normally, this is the IP Office Unit's LAN1 address. You can enter several IP addresses, separating each by a comma with no space. This allows specification of a fallback H323 gatekeeper.
     - **Note:** The phones will wait 3 minutes before switching to the fallback and will not switch back when the first server recovers, until the phone is rebooted.
   - ***MCPORT=*** is the RAS port address for initiating phone registration. The default is 1719.
   - ***HTTPSRVR=*** is the HTTP file server IP address. .
   - ***HTTPDIR=*** is the HTTP file directory where the IP phone files are located. This entry is not required if those files are in the server's root directory.
   - ***VLANTEST=*** is the number of minutes phones should attempt to register on a specific VLAN before defaulting back to VLAN 0. This field is optional. A setting of 0 disables the fallback to registering on VLAN 0.
   - The maximum string length is 127 characters. To reduce the length the TFTP Server address can be specified through attaching an Option 66 entry to the Scope. See Alternate Options 70.
7. Click **OK**.
8. Expand the server by clicking on the **[+]** next to it.
9. Click on the scope you just created for the 1600 phones.
10. In the right-hand panel, right-click on the scope and select **Scope Options**.
11. In the general tab, make sure **242** is checked.
12. Verify the String value is correct and click **OK**.

2c. Adding a 176 Option

4600 and 5600 Series H323 IP phones use option 176 rather than option 242 as above.

The option 176 can be setup to use the same HTTP file server as the 1600 Series phones. However some older 4600 Series H3232 IP phones only support TFTP. Therefore the options for a TFTP scope are shown below.

1. Right-click on the DHCP server.
2. From the pop-up menu, select **Predefined options**.
3. Select **Add**.
4. Enter the following information:
   - **Name:** 46xxOptions
   - **Data type:** String
   - **Code:** 176
   - **Description:** IP Phone settings
5. Click **OK**.
6. In the string value field, enter the following:

   MCIPADD=xxx.xxx.xxx.xxx,MCPORT=1719,TFTPSRVR=yyy.yyy.yyy.yyy,TFTPDIR=z, VLANTEST=0

   where:

   - ***MCIPADD=*** is the H323 Gatekeeper (Callserver) address. Normally, this is the IP Office Unit's LAN1 address. You can enter several IP addresses, separating each by a comma with no space. This allows specification of a fallback H323 gatekeeper.
     - Note: The phones will wait 3 minutes before switching to the fallback and will not switch back when the first server recovers, until the phone is rebooted.
   - ***MCPORT=*** is the RAS port address for initiating phone registration.
   - ***TFTPSRVR=*** is the TFTP Server IP Address. Normally, this is the IP address of the PC running Manager.
   - ***TFTPDIR=*** is the TFTP Server directory where the IP phone files are located. This entry is not required if those files are in the TFTP server's default directory.
   - ***VLANTEST=*** is the number of minutes phones should attempt to register on a specific VLAN before defaulting back to VLAN 0. This field is optional. A setting of 0 disables the fallback to registering on VLAN 0.
7. The maximum string length is 127 characters. To reduce the length the TFTP Server address can be specified through attaching an Option 66 entry to the Scope. See Alternate Options 70.
8. Click **OK**.
9. Expand the server by clicking on the **[+]** next to it.
10. Click on the scope you just created for the 4600 phones.
11. In the right-hand panel, right-click on the scope and select **Scope Options**.
12. In the general tab, make sure **176** is checked.
13. Verify the String value is correct and click **OK**.

2d. Activate the Scope

The scope can be manually activated by right clicking on the scope, select **All Tasks** and select **Activate**. The activation is immediate.

You should now be able to start installing H323 IP phones using DHCP. If Manager is being used as the HTTP or TFTP server ensure that it is running on the specified PC.

7.2 Alternate Options

In this document, all IP phone information is issued through the Scope and the Option 176 settings. Depending on the DHCP server, other options may have to be used within the scope.

- **Option 1 - Subnet mask**
- **Option 3 - Gateway IP Address**
  If using more than one address, the total list can contain up to 255 total ASCII characters. You must separate IP addresses with commas with no intervening spaces.
- **Option 6 - DNS server(s) Address**
  If using more than one address, the total list can contain up to 127 total ASCII characters. You must separate IP addresses with commas with no intervening spaces. At least one address in Option 6 must be a valid, non zero, dotted decimal address.
- **Option 15 - DNS Domain Name**
  This string contains the domain name to be used when DNS names in system parameters are resolved into IP addresses. This domain name is appended to the DNS name before the 1600 IP Telephone attempts to resolve the DNS address. Option 15 is necessary if you want to use a DNS name for the HTTP server. Otherwise, you can specify a DOMAIN as part of customizing HTTP as indicated in
- **Option 51 - DHCP Lease Time**
  If this option is not received, the DHCP offer is not be accepted. Avaya recommends a lease time of six weeks or greater. If this option has a value of FFFFFFFF hex, the IP address lease is assumed to be infinite as per RFC 2131, Section 3.3, so that renewal and rebinding procedures are not necessary even if Options 58 and 59 are received. Expired leases cause Avaya IP Telephones to reboot.
  - Avaya recommends providing enough leases so an IP address for an IP telephone does not change if it is briefly taken offline.
  - DHCP standard states that when a DHCP lease expires, the device should immediately cease using its assigned IP address. If the network has problems and the only DHCP server is centralized, the server is not accessible to the given telephone. In this case the telephone is not usable until the server can be reached.
  - Avaya recommends, once assigned an IP address, the telephone continues using that address after the DHCP lease expires, until a conflict with another device is detected. The 1600 Series IP Telephone customizable parameter DHCPSTD allows an administrator to specify that the telephone either:
    - Comply with the DHCP standard by setting DHCPSTD to 1
    - Continue to use its IP address after the DHCP lease expires by setting DHCPSTD to 0. This is the default. If used, after the DHCP lease expires the telephone sends an ARP Request for its own IP address every five seconds. The request continues either forever, or until the telephone receives an ARP Reply. After receiving an ARP Reply, the telephone displays an error message, sets its IP address to 0.0.0.0, and attempts to contact the DHCP server again.
- **Option 52 - Overload Option**
  If this option is received in a message, the telephone interprets the sname and file fields in accordance with IETF RFC 2132, Section 9.3, listed in Appendix B: Related Documentation.
- **Option 53 - DHCP Message Type**
  Value is 1 (DHCPDISCOVER) or 3 (DHCPREQUEST).
- **Option 55 - Parameter Request List**
  Acceptable values are: 1 (subnet mask), 3 (router IP address[es]), 6 (domain name server IP address[es]), 15 (domain name), NVSSON (site-specific option number)
- **Option 57 - Maximum DHCP Message Size**
- **Option 58 - DHCP Lease Renew Time**
  If not received or if this value is greater than that for Option 51, the default value of T1 (renewal timer) is used as per IETF RFC 2131, Section 4.5.
- **Option 59 - DHCP Lease Rebind Time**
  If not received or if this value is greater than that for Option 51, the default value of T2 (rebinding timer) is used as per IETF RFC 2131, Section 4.5

Note

- The H323 IP phones, any Option 66 settings will be overridden by any TFTP entry in Option 176. Using Option 66 as part of the Scope is useful if alternate Gatekeeper addresses are required in the Option 176 settings whilst keeping within the 127 character limit.

Chapter 8.
WML Server Setup

8. WML Server Setup

The 4610SW, 4620, 4620SW, 5610SW, 5620 and 5620 phones can act as WAP (Wireless Access Protocol) browsers. This allows them to view WML (Wireless Markup Language) pages. WML is a page coding language similar to HTML but intended for phone devices with small screens and no full keyboard.

To do WAP browsing, the phones need to be configured to access a home page. That home page can contain links and information appropriate to the customer installation.

This section looks at the setting up and configuration of a simple test system. The aim is to introduce the basic principles of WAP browsing operation.

- For testing and demonstration purposes Avaya host a set of WML files at http://support.avaya.com/elmodocs/avayaip/4620/home.wml.
- Most PC web browsers cannot display .wml files. However Opera is able display WML pages which makes it a useful tool with which to test WML access and operation.

What WML is Supported

The phones are WML 1.2 compliant WAP browsers. However, they do not support all WML 1.2 tags.

For details of those WML 1.2 tags supported, refer to the 4600 Series IP Telephone LAN Administrator's Guide.

WTAI (Wireless Telephony Application Interface) links are supported to allow numbers embedded in WML pages to be dialed from phones.

8.1 Testing 4620 WML Browsing Using Xitami

1. Introduction

Xitami is a small and simple web server application. It is used here to configure one of our LAN PC's as a web server able to provide .wml pages is response to requests from an IP phone.

- **Web Server PC**
  Any Windows PC on the IP Office LAN. Ideally this PC should have a fixed IP address.
- **Server Software**
  Xitami can be obtained from **http://www.imatix.com**. A copy is available on the IP Office Documentation CD. If an alternate Apache or IIS web server is available refer to the section on configuring Apache 76 or IIS 76 for WML files.
- **Sample WML Pages**
  A number of sample pages can be downloaded from **http://support.avaya.com/japple/css/japple?PAGE=ProductArea&temp.productID=107755**.

2. Installing the Web Server

For this test we used a web server called Xitami. It is a simple, small and flexible web server for use on Windows based PC's.

1. On the server PC, run **Xitami.exe** to start installation of the web server.
2. Accept the various defaults.
3. When asked for a **User Name** and **Password**, note the details entered.
4. When finished, select **Run**. The Xitami server appears as an icon.
5. To display the web servers basic properties, double-click . Note the IP addresses.
6. To close the window without stopping the web server, click **Close**.
7. Open the PC's web browser and enter **http://<server IP address>**. You should see the default Xitami web pages.

If there are other PC's on the IP Office LAN they should also be able to browse the web server's IP address.

3. Configuring the Xitami Web Server for WAP

Basic web browsing consist of requests to the web server for .htm and .html text pages and .gif and .jpg images which are then displayed by a browser program. WAP browsing uses different file types, wml for text and .wbmp for images.

The web server needs to be configured to recognize those file types, and several others, as files that might be requested by a WAP browser program. This is done by adding what many web servers refer to as MIME types.

1. On the web server PC, open the folder **C:\Xitami**.
2. Using a plain text editor such as Notepad or WordPad, open the file **Xitami.cfg**.
3. Scroll down the file to the section **[MIME]**. You will see that it is a list of settings for different text, image and application files types.
4. Scroll the end of the file and add the following new set of MIME type for files that are supported by H323 IP phones with a WAP browser.

```
# WAP MIME types
wml=text/vnd.wap.wml
```

5. Save the file.

4. Installing Sample WML Pages

Download the sample pages from Avaya (see the link above).

1. On the web server PC, open the folder **c:\Xitami\webpages**. For Apache and IIS use the appropriate root folder.
2. Create a new sub-folder called 4620.
3. Copy the sample .wml pages into this folder.

4a. Creating a Simple WML Page

As an alternative to using the sample pages provided, you can create a simple .wml page using an editor such as Notepad.

1. Start Notepad.
2. Add the following text:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN¿ "http://www.wapforum.org/DTD/wml_1.2.xml"
<wml>
<card id="card1" title="Hello World!">
<p>Hello world!</p>
</card>
</wml>
```

3. Save the file as index.wml. Notepad may save the file as index.wml.txt. If this happens, rename the file back to index.wml.
4. Copy the file into the folder c:\Xitami\webpages\4620.

4b. Dialling from a WML Page

WTAI (Wireless Telephony Application Interface) allows numbers contained in a WML page to be dialed.

An example WTAI link is shown below:

```
<a href="wtai://wp/mc;200" title="Reception">Call Reception</a>
```

This example link displays as Call Reception and have an adjacent phone icon. Pressing the adjacent display key on the phone will dial the number contained in the link.

8.2 Setting the Home Page

WAP capable H323 IP phones display a key option labeled **Web** when setup with a home page (press **PHONE/EXIT** if in any other menu).

To access the home page, press the adjacent display key. The home page is set by editing the ***46XXsetting.scr*** file found in the IP Office Manager applications program folder.

- For testing and demonstration purposes Avaya host a set of WML files at http://support.avaya.com/elmodocs/avayaip/4620/home.wml.
- Most PC web browsers cannot display .wml files. However Opera is able display WML pages which makes it a useful tool with which to test WML access and operation.

1. Locate the **46XXsettings.txt** file that has been previously downloaded to the phones. This will contain any custom settings for the Avaya IP phones being supported on the system.
    - If only the file 46XXsettings.scr is present rename it as **46XXsettings.txt**.
2. Double-click on **46XXsettings.txt**. The file will open in Notepad. The section relating to WML browsing is towards the end of the file. It will look similar to the following:

```
################ SETTINGS FOR AVAYA 4620 IP PHONE ###################
## 4620 Web Launch page in WML - Default: Avaya hosted
SET WMLHOME http://192.168.42.200/4620/index.wml
## The Proxy server used for your LAN - IP address or human readable name (check your browser settings).
# SET WMLPROXY nj.proxy.avaya.com
## The http proxy server port (check your browser settings).
SET WMLPORT 8000
## Exceptions: You must use an IP address not a DNS name
# Example: SET WMLEXCEPT 111.222.333.444
## Text coding for the web pages defaulted to ASCII.
SET WMLCODING ASCII
#################### END OF AVAYA 4620 IP PHONE ####################
```

3. Edit **SET WMLHOME** to be the address of the sample index.wml file on the web server. In this example; ***http://192.168.42.200/4620/index.wml***.
4. If DNS is being used to access the web server by IP name, the **SET DOMAIN** and **SET DNSSRVR** lines at the start of the 46XXsettings.scr file should be edited to match the LAN settings. The preceding #'s should be removed from the lines to make them active.
5. Close and save the file.
6. Restart the phones. Once the phone has restarted it should display **Web** as one of the screen option.

8.3 Apache Web Server WML Configuration

Apache is an open-source web server that is available on many platforms. Basic familiarity with Unix is necessary to configure it. The following is a step-by-step guide for configuring Apache Web-server:

1. To set MIME types in Apache, a plain text file called **httpd.conf** is used.
2. The location for this file varies depending on the individual setup, but the most usual path is **/etc/httpd/conf/httpd.conf**. If the operating system is Windows, then look for a folder called **conf** under where Apache is installed.
3. Using a text editor, open **httpd.conf**.
4. Scroll down to the **AddType** section (usually at the bottom of the file) and add the following line: `AddType text/vnd.wap.wml wml`
5. Save the file.

8.4 Microsoft IIS Web Server WML Configuration

Microsoft Internet Information Server (IIS) is configured through the Internet Service Manager.

The following step-by-step guide can be used to set up MIME types necessary for WML:

1. Select **Start | Control Panel | Administrative Tools | Internet Services Manager**.
2. Right-click on Server and select **Properties**.
3. In the **Computer MIME Map** section, click **Edit**.
4. Click **New Type** and create a new file type using the parameters below:
   - **Associated extension:** wml
   - **Content type:** text/vnd.wap.wml
5. Click **OK**.
6. Stop and restart the web server so that the newly added MIME types are picked up.

8.5 Open URL Entry

This document provides sample WML code on how to develop WML pages implementing a text box-based go to a URL function. This code allows a user to enter a URL into a text entry area and link to that site.

Please note that these are examples, not an exhaustive list. All WML code is presented in italics.

Case 1. Input Box Followed by an Anchor Tag

Description: The user enters a URL into the text entry box and clicks on the URL to retrieve it.

```
<input name="url" title="Name" />
<anchor title="get it">
Go Get It
<go method="get" href="$(url)">
</go>
</anchor>
```

Case 2. Input Box Followed by an A Tag

```
<input name="url" title="Name" />
<a href="$(url)">Go Get It</a>
```

Case 3. Input Box Followed by a Submit Button

```
<input name="url" title="Name" />
<do type="submit" name ="submit" label = "Submit">
<go method="get" href="$(url)">
</go>
</do>
```

Case 4. Input Box Followed by an Anchor Tag Where the Anchor Tag Already Displays HTTP://

This method displays http so that the user only has to type in the URL at the end of http://.

```
<input name="url" title="Name" value="http://" />
<anchor title="GET">
Go Get it
<go method="get" href="$(url)">
</go>
</anchor>
```

Index

1

100Mbps Ethernet 52
10Mbps 14
10MBps Ethernet 52
1151C1 20
1151C1/1151C2 30
1151C2 20
1152A1 30
150ms 15
1719,TFTPSRVR 67
176 option 67
192.168.202.x 43
192.168.202.X VLANTEST 43
192.168.42.200/4620/index.wml 75
192.168.43.x 43
19-inch 20
1b 28
1U 20
1W 20

2

25ms 16
264V AC 20
2a 67
2b 67
2c 67
2-second 63

3

3.5W 20
30A Switch Upgrade Base 20
3600 7
3616 7
3b 31
3-party
  configuring 12
3rd 13

4

4.0W 20
4.1W 20
4.6W 20
4.9W 20
45-days 40
4600 7, 28, 38, 40, 43, 66, 72
  created 67
4600 Series IP Telephone LAN Administrator's Guide 40
  refer 72
  see 66
4600 Site Specific Settings 28
4601dape1_82.bin 22
4601dbte1_82.bin 22
4602dape1_82.bin 22
4602dbte1_82.bin 22
4602sape1_82.bin 22
4602sbte1_82.bin 22
4602SW 7, 19, 20
4606 7, 19, 20
  includes 62
4610SW 7, 19, 20, 40, 72
4620 7, 20, 28, 62, 72, 73
  relating 75
4620IP 19
4620SW 7, 19, 40, 72
4621SW 7, 40
  applies 20
4622
  support 7
4624D 20
4624D01 20
4624D02A 52
4625SW 20, 40
46setting files 43
46vpnsettings.txt file 40
46xx
  VPNremote 40
46xxOptions 67
46XXsetting.scr 75
46XXsetting.scr file
  editing 75
46xxsetting.txt file 56
46xxsettings file 43
46XXsettings.scr 28
  back 75
  edit 50
46XXsettings.scr file
  46XXsettings.txt 75
  start 75
46XXsettings.txt 26, 28
  46XXsettings.scr file 75
46xxsettings.txt file
  Creating 28
46XXupgrade.scr 58
46xxupgrade.scr file
  lines 28
46xxupgrade.scr file instruct
  phone 28
47
  63HZ 20
4a 73
4b 73

5

5.0W 20
5.9W 20
5601ape1810.bin 22
5601bte1810.bin 22
5602dape1806.bin 22
5602dbte1806.bin 22
5602sape1806.bin 22
5602sbte1806.bin 22
5602SW 7, 19, 20
5610SW 7, 19, 40, 72
5620SW 7, 19
5621SW phones 40

6

6.0W 20
6.45W 20
63HZ
  47 20
64ms 16
6k3 16

7

7.7W 20
792ms PRN 37

8

8.0W 20
801.11b 7
802.11a/b/g 7
802.11b 7
802.1p 43
802.1Q 31, 43, 51

802.3af 20
8k 16
9
9.9W 20
90
PSU requires 20
A
a10d01b2_2.bin 22
a20d01a2_2.bin 22
a20d01b2_2.bin 22
AC 20
access point 7
Access Points 7
Action 29, 33
Activate
Scope 67
Active Directory using RADIUS 40
Add 20, 29, 40, 43, 73, 76
clicking 67
ADDR 38
address 14, 18, 22, 31, 33, 38, 43, 54, 55, 58, 62, 63, 66, 67, 70, 73, 75
PC 26
address programming 31
Address View 63
AddType 76
AddType text/vnd.wap.wml wml 76
Administrative 52, 67, 76
Administrative Details 52
administrative options 50, 52
Administrative Tools 67, 76
Adtran Netvanta 3305 VPN Router 40
Advanced 75
AGC 56
ains600,2600,192.168.42.10,1026 37
All LAN 14
All Tasks 67
Alternate 12, 26, 66, 70
Alternate DHCP Servers 12, 26
Avaya IP 66
Alternate Options 70
Anchor Tag 77
Anchor Tag Already Displays HTTP
Anchor Tag Where 77
Anchor Tag Where
Anchor Tag Already Displays HTTP 77
Apache 76
Apache Web Server 76
Apache Web-server 76
Apache-Tomcat 40
Appearance 29, 33
Appendix 58
appendix explains 58
application file 38, 52, 58, 59
Application File Already Loaded 59
Application File Needs Upgrading 59
Application Notes
Configuring 40
Applications 15, 22, 38, 40, 52, 54, 58, 59, 67, 73, 75
applies 18, 32, 38, 58
4621SW 20
ASCII
defaulted 75
ASDM 40
attaching
Option 66 67
Audio 51
Auto-create Extn Enable 26, 33
Automatic Gain Control 56
Automatic Selection 33
auto-negotiated 16
autorun 22
autorun during PC 22
Avaya 19, 20, 23, 40, 43, 66, 75
escalated 15
including 22
number 7
Avaya 1151C1 20
Avaya 1151C2 20
Avaya 1152A1 Power Distribution Unit 20
Avaya 30A Switch Upgrade Base
fitting 19
Avaya 4622SW IP Telephone 40
Avaya Gateways 40
Avaya H.323 IP 7
Avaya IP 40, 43
Alternate DHCP Servers 66
Avaya IP Office 40, 43
Avaya P333T-PWR Switch 20
Avaya SG Series 40
Avaya Voice Priority Processor 7
Avaya VSU Series 40
Avaya WebLM 40
Avaya WebLM Software 40
AvayaLabs 43
Avays VSU Series 40
Avoid Hubs 18
AVPP 7
B
b10d01b2_2.bin 22
b20d01a2_2.bin 22
b20d01b2_2.bin 22
back 31, 67
46XXsettings.scr 75
index.wml 73
IP 19, 30
Manager PC's 23
back spacing 31
backlight 20
Backup 18, 20
bbla0_83.bin 22
Beam Address 63
Beam Contact 63
Beaming
Files During 64
beaming files 64
bin/VPN Phone 40
Blue 43
boot 7, 31, 50, 52, 54, 58, 59
Boot File 7, 31, 50, 52, 58, 59
Boot File Needs Upgrading 59
Browsing Using Xitami 73
Button Programming 29
C
c0a82c15 37
cabling 14
Connections 18
Call 7, 14, 16, 18, 28, 32, 33, 38, 40, 43, 73, 76
During 64
subnet 31

Call 7, 14, 16, 18, 28, 32, 33, 38, 40, 43, 73, 76
Swap Text Files During 62
call answering 7
Call Reception 73
Call Server 43
call signalling 16
called 46xxsettings.txt 28
called CCD 40
Callserver 67
CallSv 31
CallSvPort 31
card1 73
cat 5 14
CAT3 20
Existing 14
CAT5 14, 18, 20
CAT5 cabling 14
Catalyst
changes 20
provide 20
Category 14, 38
cause 18
timeout 38
CD 22, 40, 73
CD/DVD 40
changes 13, 14, 22, 23, 26, 28, 29, 31, 32, 33, 43, 50, 51, 55, 59, 63
Catalyst 20
checkbox 40
Cisco
Configuring 40
Cisco Adaptive Security Device Manager 40
Cisco Catalyst 20
Cisco PIX 500 Series Security Appliances 40
Cisco PIX Security Appliance
Configuring 40
Cisco VPN 300 Series Concentrators 40
Cisco VPN 3000 Series Concentrators 40
Clearing 59
CLI configuration 43
clicking
Add 67
Close 15, 37, 73, 75, 76
cmd
Windows 37
codecs 16
Compact Flash 23
Compaq iPAQ Pocket PC 63
Compression Mode 33
Computer Management 67
Computer Management Tree 67
Computer MIME Map 76
Concentrator 40
conf 76
configuration 7, 14, 15, 19, 22, 26, 29, 33, 38, 40, 43, 55, 66, 72, 75, 76
file source 23
Microsoft IIS 76
configuration back 23, 29, 33, 40, 55
Configuration Quick Start 40
configuring
3-party 12
Application Notes 40
Cisco 40
Cisco PIX Security Appliance 40
File Source 23
VPN Remote 40
CONFLICT 38
Connect 14, 16, 18, 19, 40, 43
LAN 30
Connections 14, 19, 20, 30, 38, 40, 51, 52, 63
Cabling 18
Contacts 62, 63
Control Panel 76
Control Unit Memory Card
Using 23
Control Unit Settings 26
Correct Boot File 59
Creating 43
4600 67
46xxsettings.txt File 28
Scope 67
Simple 73
Currently VPNremote Phone 40

D

Data 15, 16, 18, 19, 20, 30, 31, 43, 54, 67
Data occupy 43
data VLAN's 43
Data/Common/WML/samples 73
def06r1_8_3.bin 22
def24r1_8_3.bin 22
Default 16, 31, 33, 40, 51, 54, 55, 59, 63, 67, 73
ASCII 75
defaults 54
defines 43, 55, 66
IP 67
Definity 66
Deployment Guide 40
DHCP 12, 14, 15, 22, 31, 38, 43, 50, 54, 55, 58, 70
alternate 66
connection 30
installation 13
introduction 7
preparation 26
windows 67
DHCP Address Installation 30, 31
DHCP addressing 55
DHCP function 13
DHCP Options 43, 55, 67
DHCP Relay 43
DHCP Server 12, 13, 14, 22, 26, 30, 31, 38, 43, 55, 66, 67, 70
DHCP server assigning 38
DHCP Settings 43
DHCP Setup
H.323 IP Phones 67
dialling 62, 63, 73
dialling contacts 63
Dialling Phone Numbers 63
DiffServ 18
IP Office supports 18
DiffServ QoS 18
Digital Telephony 33
Direct Media 16
Disable Auto-Create Extension 33
display 26, 29, 30, 31, 32, 33, 51, 52, 53, 54, 55, 56, 58, 59, 63, 64, 73, 75, 77
IR 63
displayed Beam option 64
displays Clearing 59
displays Initializing 30, 59
displays Loading 59

DNS 66, 67, 70, 75
DNS Domain Name 66, 70
DNS Server Address 66, 70
Doc Reference 40
DOCTYPE wml PUBLIC 73
Documentation CD 73
Double-click System 55
Duplicate IP Addressing 18
during
Call 64
Manager 14
DVD 40

E

Edit SET WMLHOME 75
editing 76
46XXsetting.scr file 75
46XXsettings.scr 50
Embedded Voicemail Memory 13, 22
END OF AVAYA 4620 IP PHONE 75
END OF FILE 28
Endpoints 37
End-to-End Matching Standards 18
English 38
Enter 14, 22, 23, 26, 29, 30, 31, 32, 33, 37, 40, 51, 55, 63, 70, 73, 75, 77
subnet 67
WINS 67
Enter cmd 23, 37
Enter tftp 37
entered during 51
error messages 38
escalated
Avaya 15
etc/httpd/conf/httpd.conf 76
Ethernet 18, 38, 43, 58, 63
Power 20
Ethernet LAN 20
Ethernet Switch 43
EU24 20
EU24BL 20
Example setup - Overview 43
Excessive Utilization 18
Existing
CAT3 14
Ext 32
extension 33
Extension ID 29
Extension Number 14, 26, 29, 32, 33, 59
IP phone 38
extensions 7, 14, 16, 26, 29, 32, 33, 38, 40, 62, 64, 75, 76
phone requests 59
user changes 59
Extn 29, 33
Extn2601,2601,192.168.42.4,1720 37
Extn2602,2602,192.168.42.2,1720 37

F

file 22, 23, 26, 28, 32, 37, 38, 40, 43, 52, 54, 58, 59, 62, 63, 64, 67, 73, 75, 76
phone displays 59
File Source
Configuring 23
File Writer
set 23
filename1 52
filename2 52
Files During
Beaming 64
FileSv 31
Find 53
Finish 67, 73
fitting
Avaya 30A Switch Upgrade Base 19
following
H.323 IP 7
form 23, 26, 37
Quality 18
Full Name 33

G

G.711 16
G.723 16
G.729a 16
G.729b 16
gatekeeper 12, 13, 14, 26, 31, 33, 55, 67, 70
Gatekeeper Enabled 26
Gatekeeper Settings 26
GEN
phone 20
GEN1 20
GEN1 4612 20
GET 77
Get It 77
Get It</a 77
gif 73
GRQ 37
gvrp 43

H

H.08.60 43
H.232 19
H.323 7, 12, 13, 14, 15, 16, 19, 20, 22, 26, 28, 37, 38, 50, 51, 55, 56, 62, 63, 66, 67, 70, 73, 75
H.323 Gatekeeper 12, 13
H.323 IP 13, 14, 16, 19, 22, 26, 28, 37, 38, 50, 51, 55, 56, 62, 63, 66, 70, 73, 75
following 7
including 20
installing 15, 67
number 7
provide 12
H.323 IP phone requires 20
H.323 IP phones 7, 12, 13, 14, 16, 19, 20, 22, 26, 28, 37, 51, 56, 63, 66, 70, 73, 75
DHCP Setup 67
H323 Gatekeeper 14, 67
Hello World 73
Hold 31, 51, 52, 53, 54, 56, 63
home page 28, 72, 75
hostname 43
HP 43
HP Procurve 43
HP Procurve CLI 43
HP Procurve Ethernet 2626 PWR Ethernet 43
HP Procurve Switch 43
HP-Switch 43
href 73, 77
htm 73
HTML 72, 73
httpd.conf 76

I

i10c01a2_2.bin 22
i10d01a2_2.bin 22
i20d01a2_2.bin 22

IEEE 802.2p/q
understanding 43
IEEE 802.3af 19, 20
IIS 76
IIS 5.0 76
IIS Admin Service' 76
IKE Extended Authentication 40
Immediate 29, 33, 67
Important Note 62
Inactive 67
includes 12, 13, 15, 26, 37, 43, 63, 73
4606 62
Avaya 22
H.323 IP 20
PC 19
WAN Ethernet 18
index.wml 75
back 73
index.wml file 75
index.wml.txt 73
Infrared Dialling 62
Initializing 30, 59
Input Box Followed 77
installation 18, 22, 26, 28, 30, 33, 40, 50, 54, 66, 72, 73, 75
DHCP 7
large 13
requirements 14
small 12
static address 31
Installation Documentation 40
Installation Requirements 14
installing
H.323 IP 15, 67
IP 14
Sample 73
VCM 16
Web Server 73
Internet 40, 76
Internet Authentication Service 40
Internet Service Manager 76
Introduction 7, 73
IP 12, 13, 15, 16, 18, 22, 23, 26, 28, 29, 32, 33, 37, 38, 40, 43, 50, 54, 55, 58, 59, 62, 66, 70, 72, 73, 75
back 19, 30
defines 67
install 14
match 31
power 20
Select 63
start 53
use 7
IP address 13, 14, 18, 22, 23, 26, 29, 30, 31, 33, 37, 38, 43, 58, 66, 67, 70, 73, 75
ip address 192.168.202.201 255.255.255.0 43
IP Address and/or MAC Address 29
IP Address LAN2 43
IP Gateway 66
IP Mask 31, 43
IP Mask LAN1 43
IP Mask LAN2 43
IP Office 7, 12, 13, 14, 15, 16, 18, 20, 22, 23, 26, 28, 29, 31, 32, 33, 37, 38, 40, 43, 54, 55, 59, 63, 66, 67, 73, 75
IP Office Administration CD 26
IP Office Administrator 22, 40
IP Office Administrator Applications CD 22
IP Office Documentation CD 73
IP Office Embedded Voicemail 22
IP Office Engineers 73
IP Office Engineers Toolkit 73
IP Office IP Endpoint 7
IP Office LAN 73
IP Office Licensing 40
IP Office Manager 7, 12, 14, 22, 28, 29, 32, 33, 38, 40, 55, 59, 75
IP Office Manager application 7, 12, 14, 22
IP Office Manager PC 14
IP Office Manager System 33
IP Office Monitor application 26, 37
IP Office supports 7
DiffServ 18
IP Office System 7, 12, 15, 16, 23, 37, 40, 54, 63
IP Office Unit 7, 12, 13, 14, 16, 18, 22, 23, 26, 31, 37, 38, 66, 67
IP Office Unit configuration 14
IP Office Unit Memory Card 22
IP Office Unit's LAN1 67
IP Office's configuration 40
IP Office's data 16
IP Office's LAN1 22, 26
IP Office's TDM 16
IP phone 7, 12, 13, 14, 19, 20, 22, 26, 29, 30, 33, 40, 43, 50, 53, 55, 62, 63, 66, 67, 70, 73, 75
extension number 38
IP Phone Inline Adaptor 20
IP Phone Software 7, 22, 26
IP Phone Software Version 7
IP Softphone Fails To Register With 40
IP Telephone 14, 40, 66, 72
IP Telephone LAN Administrator's Guide 66, 72
IP Telephone R2.3 LAN Administrator Guide 40
IP Telephone Software 14
IP Telephones Administrators Guide 40
IP400 40
IP403 7, 16
IP406 7, 13, 16, 22, 23, 26
IP406 V1 7, 16
IP406 V2 7, 13, 16, 22, 23, 26
IP412 7, 16
IPO 40, 43
IPO LIC 40
IPSec VPN 40
IPSets Firmware 22
IPSets Firmware/4601dbtel1_82.bin 23
IR 51, 62, 63, 64
display 63
PC/Handheld 63
IR beaming 62
IR Interface Enable/Disable 51
IR port 51, 62, 63, 64
IR port ready 64
IrDA 62
ISG 40

J

J8164A Configuration Editor 43
Java 40
jpg 73
JRE 40
Juniper Networks Integrated Security Gateway 40
Juniper Networks NetScreen 40
Juniper Networks NetScreen Series VPN 40

Juniper Networks Secure Services Gateway 500 Series 40
Juniper Secure Services Gateway using Policy-Based 40

K

Kentrox Q2300 VPN Router 40

L

L2 43, 51
L2 QOS 43
L2 signaling 51
L2Q 43
L2QVLAN 43
L3 51
L3 signaling 51
LAN 18, 19, 20, 38, 40, 43, 51, 52, 58, 66, 72, 73
  Connect 30
  match 75
  PC 14
LAN Administrator's Guide 66, 72
LAN Cables 14, 19, 20, 30, 75
LAN PC's 73
LAN Socket 14, 51
LAN1 23, 26, 31, 43, 67
LAN2 43
LAN's DHCP 58
Large Installation 13
Leave Manager 26
LED 20
  waiting 53
Licence Keys 14
license key 14
LINE 20, 30
lines 37, 40, 58, 59, 73, 75, 76
  46xxupgrade.scr file 28
  Monitor 26
Listing
  Registered 37
Loading 58, 59
Loading… 30
login 33
Login Code 32, 33

M

M505 63, 64
MAC 33, 40, 52
MAC Address 33, 40, 52
Maintenance Manual 7
manage
  VLAN's 43
Manager 12, 13, 22, 23, 26, 28, 29, 31, 33, 40, 66, 67, 75, 76
  during 14
Manager application 12, 22, 26, 28, 31
  Open 75
Manager Installation 7, 14
Manager PC 23, 26, 75
Manager PC's
  back 23
Manager's TFTP Log 26
Mandatory 15, 51
Manually Creating Extensions 29
match 18, 29, 33, 55, 59
  IP 31
  LAN 75
  RJ45 20
May 2007 7
Mbps 58
MCIPADD 43, 67
MCPORT 43, 67
Menu icon 63, 64
MESSAGES button 32
MESSAGES button flashing 0.5 32
MG 7
Microsoft 40, 70, 76
  Refer 67
Microsoft DHCP 70
Microsoft IIS Web Server 76
Microsoft Internet Information Server 76
Microsoft Windows 2000/server 76
Microsoft Windows NT 76
Microsoft Windows XP 76
Mid-Span Power Unit 20
MIME 76
  set 73
Minimum Assessment Target 15
Minimum Firmware 40
MMC 76
Mode option 43
Mode option MUST 43
Monitor 15
  lines 26
multicast 18
Multicasting 18
Multihomed 43
MultiVantage 66

N

Name 14, 19, 22, 26, 29, 33, 37, 40, 43, 52, 59, 63, 67, 70, 73, 75, 77
Name Details 26
nasystem/h323_ras_list yyyyyyyy.txt 37
Native 43
Netgear FVS338 VPN Router 40
Network Access 18
network assessment 7, 15
New 18, 26, 29, 31, 32, 33, 43, 50, 51, 55, 58, 59, 67, 73, 76
New Type 76
New,2702,192.168.42.200,1720 37
Next 59, 67
NIC Cards 43
No Ethernet 30, 38, 58
No new 51
Non-Avaya 23, 40
Non-Avaya Gateways 40
non-IP 16, 32
  number 7
non-IP extension 32
non-VoIP extension 29
Notepad 73, 75, 76
NT 4.0 76
Number 14, 16, 19, 20, 26, 29, 31, 32, 33, 40, 50, 52, 55, 58, 59, 63, 64, 67, 72, 73
  Avaya 7
  H.323 IP 7
  non-IP 7
  Start 62
  VCM 7

O

OK 23, 29, 33, 40, 55, 67, 76
on/off 32, 56
onthe phone button 63
Open 18, 26, 33, 37, 76, 77
  Manager application 75

Open 18, 26, 33, 37, 76, 77
PC's 73
Open URL Entry 77
operate 76
Option 14, 20, 22, 28, 37, 38, 40, 43, 50, 51, 52, 55, 64, 67, 70, 75, 76
Option 15 70
Option 176 70
requesting 67
Option 66 70
attaching 67
Option Settings 51
options exist 14
OR 75
Other H.323 IP 7
Overlapping VLAN 43

P

p>Hello world!</p 73
Packet Loss 15
page coding 72
Pages 72, 73, 75, 76, 77
pages implementing 77
Palm 63, 64
Palm Organizer 63, 64
Palm Vx 63, 64
part 22, 28, 40, 67
Scope 70
Password 32, 59, 73, 75
PC 7, 22, 23, 31, 40, 43, 51, 58, 62, 63, 66, 73, 75
address 26
include 19
LAN 14
running 67
PC Ethernet LAN 19
PC Port 19
PC Softphone 7
PC/Handheld
Ir 63
PC/personal 62
PC's 43
PC1 43
PCs 43
PC's 19
Open 73
PC's web 73
phone 7, 12, 13, 14, 15, 16, 18, 19, 22, 26, 29, 31, 33, 38, 40, 43, 50, 51, 52, 53, 54, 55, 56, 58, 59, 63, 64, 66, 67, 70, 72, 73, 75
46xxupgrade.scr file instruct 28
connection 30
dialling 63
GEN 20
infrared dialling 62
registration 32, 37
security 33
Phone Connection 30
phone displays 32, 59, 75
file 59
phone during installation 14, 26, 66
Phone Manager 7
Phone Manager Pro PC Softphone 7
phone obtains 58
phone requests 28, 40, 75
extension 59
phone requires 14
phone returns 51, 53
Phone Security 29, 33
Phone SN 52
PHONE/EXIT 75
phone's Differential 51
phone's Differential Services 51
phone's IP Mask 31
phones look 12
phones need 67, 72
Phones share 43
PHY2 51, 63
Pocket PC 63
PoE 20
PoE input 20
Potential Problems 18
Potential VoIP Problems 18
power 14, 18, 19, 30, 32, 38, 58
Ethernet 20
IP 20
power conditioning 18
power over ethernet 19, 20
Power over Ethernet Options 20
power supply 14, 18, 20, 30
Power Supply Conditioning 18
Power Supply Options 20
Power Supply Unit 14, 20, 30
Predefined 67
Pre-Deployment 40
Preferences 26
Prefs 63
preinstalled 26
preparation 26, 59
Preshared Key 40
Press Web 75
Print 33, 37, 52
Printed Wiring Board 52
Printed Wiring Board Serial Number 52
prioritisation 43
prioritization 18
Product Section 40
Program 14, 22, 31, 67, 73, 75
Program Files/Avaya/IP Office/Manager 75
Program Files/Avaya/IP Office/Toolkit/Data/Common/WML/samples 73
Properties 73, 76
Protection 18
Protocol timeout 38
provide switching 19
provides 14, 15, 16, 18, 19, 22, 28, 40, 43, 73, 77
Catalyst 20
H.323 IP 12
RJ45 20
Proxy 75
PSK 40
PSU 20
PSU requires
90 20
PWB comcode
Shows 52
PWB SN 52

Q

QoS 18, 51
QoS Option Settings 51
Quality 7, 15, 18
form 18
Service 51

R

RAM 58, 59
RAS 37, 67
RAS users 37
Reboot 23, 29, 33, 55, 59, 67, 75
  Restarting following 38
Reboot Mode 55
  Set 29, 33
Reception">Call Reception</a 73
Red 30, 43
refer 7, 20, 40, 43, 62, 73
  4600 Series IP Telephone LAN Administrator's Guide 72
  Microsoft 67
Registered 40, 67
  Listing 37
registration 32, 59, 67
relating
  4620 75
Release 2.0 Administrator Guide 40
Release 4.3 Administration Guide 40
repost 43
requesting
  Option 176 67
Reset System Values 54
reset sytem values 54
Resetting 54
restart 12, 22, 32, 38, 43, 54, 58, 59, 63, 75, 76
Restart Scenarios 58
Restarting following
  reboot 38
Restarting… 58
RFA Name 40
RFC2474 18
RJ45 14
  matching 20
  provides 20
RJ45 Ethernet LAN 14
RJ45 LAN 14
Run 7, 12, 14, 18, 20, 22, 23, 26, 31, 37, 38, 40, 66, 73, 75, 76
  PC 67

S

Sample 75, 77
  Installing 73
SAP Code 40
Save 31, 38, 40, 51, 55, 59, 73, 75, 76
savilltech.com 67
Scope 43, 66
  Activate 67
  Creating 67
  part 70
Scope Options 43, 67
scr 75
scr extension 75
Screen OS 5.1.0 40
script file 38, 50, 58, 59
Secondary Ethernet 51
see 12, 14, 15, 26, 28, 29, 30, 31, 32, 37, 50, 51, 54, 56, 67, 73, 75
  4600 Series IP Telephone LAN Administrator's Guide 66
select 23, 29, 32, 33, 37, 40, 43, 55, 64, 67, 73, 75, 76
  IP 63
  System 26
Select Add 67
select All Tasks 67
Select File 26, 75
Select Immediate 55
Select No 67
Select Start 23, 37, 67, 76
Select View 26, 75
Select Yes 67
Self Installer 40
self test 53
Self-Test Procedure 53
sendable 64
Serial Number 52
Series 7, 20, 28, 38, 40, 43, 66, 72
Series H.323 IP phones 38
Series IP Phone 28
Series phone 38
Server 12, 13, 22, 23, 38, 40, 43, 58, 66, 67, 70, 73, 75, 76
Service 18, 22, 40, 67, 76
  Quality 51
  Type 18
Services signaling 51
Set 15, 22, 26, 28, 31, 32, 33, 38, 43, 50, 51, 52, 56, 62, 63, 64, 67, 70, 72, 75, 76
  File Writer 23
  MIME 73
  Reboot Mode 29, 33
  SSON 55
SET DNSSRVR 75
SET DOMAIN 75
SET L2Q 28
SET SMBLIC 40
SET WMLCODING ASCII 75
SET WMLEXCEPT 111.222.333.444 75
SET WMLHOME 75
SET WMLPORT 8000 75
SET WMLPROXY nj.proxy.avaya.com 75
SETTINGS FOR AVAYA 4620 IP PHONE 75
Setup 29, 33, 43, 54, 58, 63, 75, 76
Several H.323 IP phones 62
SG 40
Shows 12, 13, 18, 37, 43, 53, 63
  PWB's comcode 52
Simple 43, 72
  Creating 73
site specific option number 55
Site Specific Settings 28
Small Installation 12, 13
Small Office Edition 7, 13, 14, 16, 18, 22, 23, 26
snmp-server 43
Spare Wire 20
Spare Wire Power Options 20
Speaker/Mute LED 53
Specifically HP 43
SSON
  Setting 55
Start 18, 23, 26, 31, 37, 40, 43, 58, 59, 67, 73, 76
  46XXsettings.scr file 75
  IP 53
  Number 62
start installing 67
Start Manager 75
Start Notepad 73
static address 7, 22, 26, 30, 38, 50, 52, 58
  installation 31
Static Administration Options 50

Static IP 7, 14, 26
Static IP Installation 7
Step 30, 31, 58, 66
stores 23, 32, 38, 59
String
  Verify 67
Submit Button 77
subnet 43, 66
  called 31
  Enter 67
subnet mask 31, 66, 67
support.avaya.com 40
Supported 12, 13, 14, 15, 16, 18, 20, 22, 23, 30, 31, 40, 43, 62, 64, 66, 70, 72, 73
  4622 7
SV 7
SW 19
Swap Text Files During
  Call 62
Sysmon 37
System 7, 14, 18, 20, 22, 23, 29, 33, 37, 38, 43, 50, 54, 55, 64, 66, 72, 75, 76
  select 26
System | System 22
System Name 26
System Overview 43
system-specific 59
System-specific registration 59

T

Tag 43, 72, 77
Tagged Packets 43
Technical Tip No 40
text/vnd.wap.wml 73, 76
TFTP 12, 13, 15, 31, 37, 38, 40, 43, 54, 58, 59, 66, 67, 70, 75
  control unit memory card 23
  installation 14
  introduction 22
  preparation 26
  timeout waiting 22
TFTP Application 13
TFTP Error 38, 58
TFTP Introduction 22
TFTP Log 22, 26, 75
TFTP Server 12, 13, 14, 22, 23, 26, 31, 38, 40, 54, 58, 59, 66, 67, 70, 75
TFTP Server Name 70
TFTP Server Options 13, 14
TFTPDIR 67
TFTPLog 26
TFTPSRVR 43, 67
These 7, 16, 20, 22, 30, 33, 37, 43, 50, 52, 62, 77
These require
  VPNremote 7
Third-TFTP Software 22
Timed Out 38, 58
timeout 22
  cause 38
Timeout Error 38
timeout waiting
  TFTP 22
Tomcat 40
toolkit 73
Tools 22, 28, 37, 63, 67, 76
ToS 18
Trial 40
txt file 28
Type 7, 12, 15, 16, 20, 23, 37, 43, 64, 67, 73, 76, 77
  Service 18

U

Under Services 67
understanding
  IEEE 802.2p/q 43
unit's 43
Unix 76
Unrestricted 43
Untagged 43
upgrading
  application file 59
  boot file 59
URL
  user enters 77
URQ 38
US 52
use 12, 14, 18, 20, 23, 29, 32, 33, 37, 38, 40, 43, 50, 51, 52, 54, 58, 59, 62, 63, 66, 67, 73, 75
  IP 7
  VCM 16
user 14, 18, 19, 26, 29, 32, 33, 37, 40, 43, 52, 56, 59, 73, 76, 77
user changes
  extension 59
User Details 14
user enters
  URL 77
User Name Details 26
User PC Connection 19
User Setup 33
user's Login Code 32, 33, 59
Using 7, 13, 16, 18, 20, 22, 26, 28, 32, 33, 37, 38, 40, 43, 50, 55, 58, 59, 62, 63, 64, 66, 67, 70, 73, 76
  Control Unit Memory Card 23
Using Manager 23
Using Option 66 70
Using Windows 2000 Server 67

V

VCard 63, 64
VCard file 63
VCard phone 63
vcf 63
VCM 26
  installing 16
  number 7
  use 16
VCM 10 16
VCM 16 16
VCM 20 16
VCM 24 16
VCM 30 16
VCM Channels 7, 16
VCOMP 26
Verify 38
  String 67
View 22, 26, 52, 72
View Administrative Details 52
VLAN 31, 43, 67
vlan 209 43
vlan 210 43
VLAN ID 31, 43
VLAN networking 43
VLAN Switch Configuration 43
VLAN's

VLAN's
manage 43
VLANID 43
VLANTEST 43, 67
Voice 7, 14, 15, 16, 18, 19, 26, 43
voice compression 18, 26
channels 16
installation 14
Voice Compression Channel Capacity 16
Voice Compression Channels 16, 26
Voice Compression Module 14, 26
voice signalling 18
voice traffic 15, 19, 43
voicemail 18, 23, 29
Voicemail Server PC 18
VoIP 7, 14, 15, 18, 29, 32, 33, 40
VPN 40
VPN Devices 40
VPN Phone Allowed 40
VPN Phone Allowed checkbox option 40
VPN Phone Unlimited 40
VPN phones 40
VPN Remote
Configuring 40
VPN Remote Phones 40
VPN Security Gateway 40
VPN Security Gateway Device 40
VPN Wizard 40
VPNremote
46xx 40
These require 7
VPNremote Phone 40
VPNremote Phone Firmware 40
VPNremote Phone License File 40
VPNremote Phone Licenses 40
VSU 40

W

waiting
LED 53
WAN 18
WAN Ethernet
including 18
WAP 72, 75
Web Server 73
WAP browsing 72
WAP browsing uses 73
WAP MIME 73
WAPFORUM//DTD WML 1.1//EN"¿ 73
WARNING 15, 31, 54, 55
Watts 20
wbmp 73
Web 28, 40, 43, 73, 75, 76
web browsing 28, 73
Web Launch 75
Web Server 75, 76
Installing 73
WAP 73
web server needs 73
Web Server PC 73
WebLM 40
WebLM server 40
website 40
When Free 29, 33, 55
Windows 13, 23, 28, 62, 66, 70, 73, 75, 76
2000 67
cmd 37
pocket PC 63
Windows 2000/server 76
Windows Notepad 28
Windows NT 76
Windows PC 73
Windows Pocket PC 63
Windows XP 76
winnt/system32/inetsrv/iis 76
WINS 66
Enter 67
Wireless Access Protocol 72
Wireless Markup Language 72
Wireless Telephony Application Interface 72, 73
Within Manager 26
WML 28, 72, 73, 75, 76, 77
WML browsing 75
WML Page 73
wml pages 73
WML Server Setup 72
Wordpad 37, 73
Worst Case 20
wp/mc;200 73
Wrong Set Type 32, 38
WTAI 72, 73
www.wapforum.org/DTD/wml_1.2.xml 73

X

x10d01a2_2.bin 22
x20d01a2_2.bin 22
Xauth 40
XAuth Enhanced Authentication 40
Xitami 73
Xitami.cfg 73
Xitami.exe 73
Xitami/webpages 73
Xitami/webpages/4620 73
xml 73
xx.xxx.xxx.xxx 67
xxx.xxx.xxx.xxx 37
xxx.xxx.xxx.xxx,MCPORT 67

Y

yyy.yyy.yyy.yyy 67
yyy.yyy.yyy.yyy,TFTPDIR 67
yyyyyyy.txt 37

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

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

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

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

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

© 2009 Avaya Inc. All rights reserved.
Avaya
Unit 1, Sterling Court
15 - 21 Mundells
Welwyn Garden City
Hertfordshire
AL7 1LZ
England.

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

Web: http://marketingtools.avaya.com/knowledgebase