IP Office™ Platform 9.1

IP Office H323 Telephone Installation Notes

15-601046 Issue 20k - (18 October 2016)

© 2016 AVAYA All Rights Reserved.

Notice
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service
THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "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. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)
Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software
"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright
Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization
The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components
"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider
THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws
Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud
“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll 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. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities
Information about Avaya’s security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security. Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation
For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support
See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

1. IP Office H.323 IP Phones

1.1 Supported Phones ... 10
1.2 System Capacity ... 11
1.3 Phone Firmware ... 12
1.4 Simple Installation ... 13
1.5 Installation Requirements ... 14
1.6 Licenses ... 15
1.7 Network Assessment ... 16
1.8 Voice Compression Channels ... 17
1.9 QoS ... 19
1.10 Potential VoIP Problems ... 19
1.11 User PC Connection ... 20
1.12 Power Supply Options ... 21
1.13 File Server Options ... 23
1.14 File Auto-Generation ... 24
1.15 Control Unit Memory Card ... 24
1.16 Registration Blacklisting ... 25

2. Installation

2.1 Licensing ... 29
2.1.1 Checking the Serial Number ... 29
2.1.2 Adding Licenses ... 30
2.1.3 Reserving Licenses ... 30
2.2 System H.323 Support ... 31
2.2.1 Enabling the H.323 Gatekeeper ... 31
2.2.2 Setting the RTP Port Range ... 32
2.2.3 Enabling RTCP Quality Monitoring ... 33
2.2.4 Adjusting DiffServ QoS ... 35
2.2.5 System Default Codecs ... 36
2.3 DHCP Settings ... 37
2.3.1 System DHCP Support ... 38
2.3.2 System Site Specific Option Numbers ... 39
2.4 File Server Settings ... 40
2.4.1 System File Server Settings ... 41
2.4.2 Creating/Editing the Settings File ... 42
2.4.3 Loading Software Files onto the System ... 43
2.4.4 Loading Files onto a 3rd Party Server ... 46
2.5 User and Extension Creation ... 47
2.5.1 Auto-Creation ... 47
2.5.2 Manually Creating User ... 48
2.5.3 Manually Creating Extensions ... 49
2.6 Phone Connection ... 50
2.7 Static Address Installation ... 51
2.8 Phone Registration ... 53
2.9 Backup/Restore Settings ... 54
2.9.1 Example File ... 55
2.9.2 IIS Server Configuration ... 56
2.9.3 Apache Server Configuration ... 56
2.10 Listing Registered Phones ... 57
2.11 Screensaver ... 58
2.12 Other Installation Options ... 59
2.12.1 Remote H.323 Extensions ... 59
2.12.2 VPN Remote Phones ... 61
2.12.3 VLAN and IP Phones ... 63

3. Static Administration Options

3.1 Secondary Ethernet (Hub)/IR Interface Enable/Disable ... 71
3.2 View Details ... 72
3.3 Self-Test Procedure ... 74
3.4 Resetting a Phone ... 75
3.5 Clearing a Phone ... 76
3.6 Site Specific Option Number ... 76

4. Restart Scenarios

4.1 Boot File Needs Upgrading ... 79
4.2 No Application File or Application File Needs Upgrading ... 79
4.3 Correct Boot File and Application File Already Loaded ... 79

5. Infrared Dialing

5.1 Enabling the IR Port ... 83
5.2 Dialing Phone Numbers ... 83
5.3 Beaming Files During a Call ... 84

6. Alternate DHCP Server Setup

6.1 Alternate Options ... 87
6.2 Checking for DHCP Server Support ... 88
6.3 Creating a Scope ... 88
6.4 Adding a 242 Option ... 89
6.5 Adding a 176 Option ... 90
6.6 Activating the Scope ... 91

7. WML Server Setup

7.1 Setting the Home Page ... 95
7.2 Apache Web Server WML Configuration ... 96
7.3 Microsoft IIS Web Server WML Configuration ... 96
7.4 Open URL Entry ... 97

8. SRTP

8.1 Enabling System SRTP ... 100
8.2 Direct Media ... 101

9. Document History

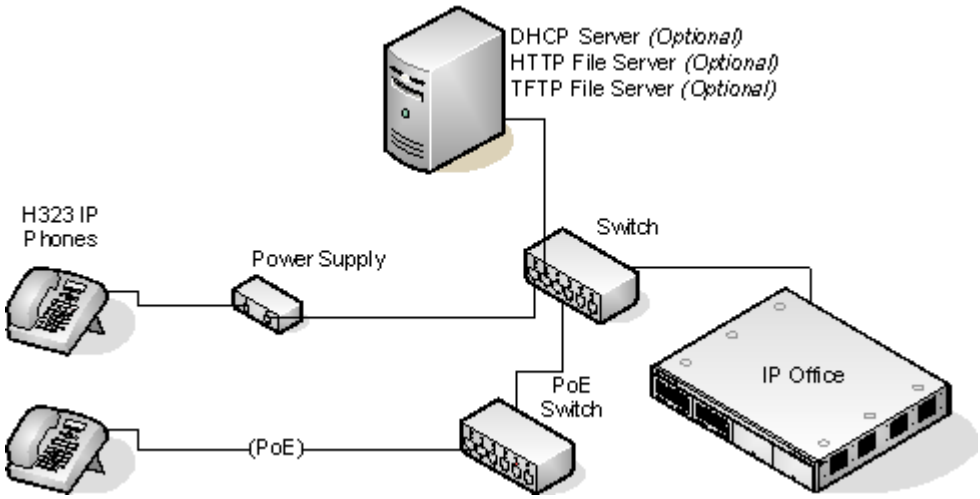
Index ... 105

Chapter 1.
IP Office H.323 IP Phones

1. IP Office H.323 IP Phones

This documentation provides notes for the installation of supported Avaya IP phones 10 onto an IP Office system. It should be used in conjunction with the existing installation documentation for those series of phones, especially the following:

- **Installing and Maintaining Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323**
  http://support.avaya.com/css/P8/documents/101009345
- **Administering Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323**
  http://support.avaya.com/css/P8/documents/101009361
- **VPN Setup Guide for 9600 Series IP Deskphones** *(16-602968)*
  http://support.avaya.com/css/P8/documents/101008050
- **Avaya one-X Deskphone Edition for 9600 Series IP Telephones Application Programmer Interface (API) Guide** *(16-600888)*
  Covers the configuration and use of WML and PUSH interfaces with 9600 Series telephones.
  http://support.avaya.com/css/P8/documents/100165678



- **DHCP versus Static IP Installation**
  Though static IP installation of H.323 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 will refuse to support any installation where the results of a network assessment cannot be supplied. See Network Assessment 16 for further details.

1.1 Supported Phones

This documentation provides installation notes for the following Avaya IP phones supported by IP Office. Other supported Avaya H.323 IP phones, for example DECT R4 3700 Series phones are covered by separate installation documentation.

H.323 IP Phones	Supported Models	802.3af PoE Class		PC Port	IP Office Core Software
		Class	Idle		
1600 Series	**1603**	2	4.4W	–	4.2 Q4 2008 +.
	1603SW	2	4.4W	✓	
	1608	2	3.7W	✓	
	1616	2	2.7W	✓	
4600 Series	**4601**	2	3.5W	–	3.0+
	4602	1	–	–	2.1+.
	4602SW	2	3.5W	✓	
	4606	0	4.1W	✓	Up to 3.2.
	4610SW[1]	2	4.0W	✓	3.0+.
	4612	0	4.1W	✓	Up to 3.2.
	4620	3	4.0W	–	2.0+.
	4620SW	2	–	✓	
	4621SW[1]	2	5.75W	✓	3.0+.
	4624	0	4.1W	✓	Up to 3.2.
	4625	3	6.45W	✓	3.2+
5600 Series	**5601**	2	3.5W	–	3.0+.
	5602	1	–	–	
	5602SW	2	4.1W	✓	
	5610SW[1]	2	3.1W	✓	
	5620	3	3.6W	✓	
	5621SW[1]	2	–	✓	3.2+.
9600 Series	**9620L**	1	2.0W	✓	6.0+
	9620C	2	3.9W	✓	
	9630G	2	4.6W	✓	
	9640	2	3.9W	✓	
	9640G	2	3.9W	✓	
	9650	2	4.7W	✓	
	9650C	2	3.7W	✓	
	9608	1	2.08W	✓	8.0+
	9611G	1	2.8W	✓	
	9621G	2	3.49W	✓	
	9641G	2	3.44W	✓	

1. **VPNremote Support**
   These phones can also be used with VPNremote firmware.

2. **1603/1603SW**
   These phones require a PoE Splitter unit in order to use PoE.

1.2 System Capacity

System capacity encompasses the number of configurable phone extensions and the number of simultaneous IP phone calls.

Extension Capacity

The maximum number of H.323 IP phones supported depends on the type of system.

IP500 V2 systems support up to 384 extensions. To find the capacity for IP phones subtract the number of physical non-IP extensions ports in the system, ie. extension ports on the IP Office control unit and any external expansion modules. Note however that these systems only support a maximum of 148 VCM channels which may also restrict the number of simultaneous VoIP calls, see below.

For Server Edition systems, the IP extension capacity depends on the server type. Refer to the Server Edition documentation for details.

Call Capacity

There are a number of situations where the IP500 V2 system needs to provide a voice compression channel in order for an IP phone to make calls. These channels are provided byVoice Compression Modules 17 (VCMs) installed in the system. The number of VCM channels required and how long the channel is required depends on a number of factors.

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 G.711, G.729 and G.722).
- 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.

1.3 Phone Firmware

The firmware used by Avaya IP phones is upgradeable and different releases of firmware are made available via the Avaya support website. However, H.323 IP phones used on a IP Office system must only use the firmware supplied pre-installed with the IP Office system or with its IP Office Manager application. Other versions of IP Phone firmware may not have been tested specifically with IP Office systems and so should not be used unless IP Office support is specifically mentioned in the firmware's accompanying documentation.

The firmware consists of a number of different types of files:

- **xxupgrade Files**
  The first file that a phone requests when starting up is the ***xxupgrade*** file. This file contains a list of the phone .bin files that are available as part of the firmware set and the version numbers of those files. If the version of a file differs from that which the phone already has loaded, the phone will request the new file. During this process the phone may reboot after loading each file and then request the xxupgrade.txt file again until it has updated all its firmware, if necessary. Separate files are provided for the different phone series:
  - **16xxupgrade.txt**
    This file lists the firmware files that 1600 Series phones should load.
  - **46xxupgrade.scr**
    This file lists the firmware files that 4600 Series and 5600 Series phones should load.
  - **96xxupgrade.txt**
    This file lists the firmware files that 9600 Series phones should load.
  - **96x1Hupgrade.txt**
    This file list the firmware files that 9608, 9611, 9621, and 9641 phones should load.
- **.bin Files**
  Following the instructions in the xxupgrade.txt file, the phone will load any .bin files it requires if their versions differ from that which the phone already has loaded.
- **.tar Files**
  Instead of the .bin file used by other phones, the 9600 Series phones use .tar archive files to download multiple files in a single step and then unpack the .tar files to load their contents.
- **46xxsettings.txt File**
  The last line of the xxupgrade.txt file instructs the phone to load a ***46xxsettings.txt*** file. This is an editable file 42 which can be used to adjust the operation of the phones.
- **.lng Files**
  The firmware may include language files for use by 1600 Series and 9600 Series phones. Which of these language files are loaded is set in the ***46xxsettings.txt*** file.

File Auto-Generation

When the IP Office system is acting as the file server for the phones, it is able to auto-generate the ***46xxsettings.txt*** and ***.lng*** files used by the phones. It will do this if the requested file is not physically present in the location where the system stores the firmware files. The system also uses the user's configuration settings to auto-generate the phone user settings file.

For IP Office Release 9.0, the system can still auto-generate files even when HTTP redirection is used to load the 96x1 Series ***.bin*** files from another file server.

Firmware Source Sets

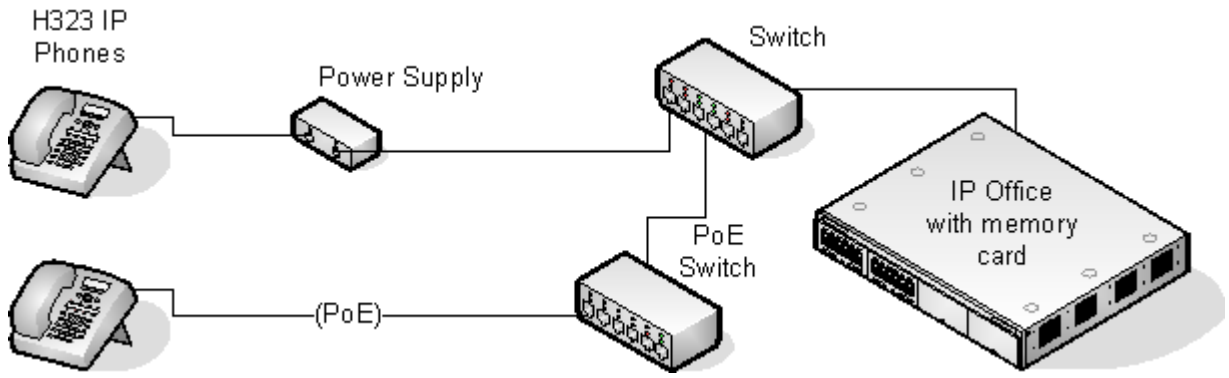
The phone firmware files are installed as part of the IP Office Manager application and are found in the application's installation directory. By default, the directory is found at **c:\Program Files\Avaya\IP Office\Manager**.

The same firmware files can also be obtained directly from the software package used to install IP Office Manager without having to perform the installation. The files are located in the **\program files\Avaya\IP Office\Manager** sub-folder of the installation directory.

Note that these sets of files include .bin files that are also used for other devices including the IP Office system itself.

1.4 Simple Installation

The diagram below shows the simplest installation scenario. This has the IP Office system acting as the DHCP and file servers for all the IP phones registered with it.



This type of installation uses the following equipment:

- **IP Office Server**
  The IP Office system performs a number of roles for the phones:
  - **DHCP Server**
    The IP Office system is acting as the DHCP server for the phones. The DHCP response to the phones includes both IP address settings, details of the file server to use as configured in the IP Office configuration and the systems on address as the H.323 gatekeeper for the phones. The IP Office DHCP function 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.
  - **H.323 Gatekeeper**
    IP phones require an H.323 gatekeeper to which they register. The gatekeeper then controls the connection of calls to and from the phone. In this and all scenarios the IP Office systems as the H.323 Gatekeeper.
  - **File Server**
    During installation the IP phones need to download firmware files 12 from a file server. This is done using either HTTPS, HTTP or TFTP in that order (1600 and 9600 Series phones do not support TFTP). The IP Office control unit memory card can be used as the file source.
    - IP500 V2 systems can act as the file server for up to 50 phones by using their own memory card. Server Edition systems can also act as the file server for up to 50 phones. For larger numbers a separate 3rd-party HTTP server should be used.
  - **Backup/Restore Server** 54
    1600 Series and 9600 Series phones can be configured to backup and restore user and phone settings to a server. The address of this server is set separately from that of the file server used for phone firmware though the same server may be useable. The recommended method is to us the IP Office system as the server for this function.
- **Switches**
  The IP Office has a limited number of LAN connection ports, intended only to connect itself to the existing data network. The addition of IP phones will require the network to include additional port capacity.
- **Power Supplies** 21
  Each H.323 IP phone requires a power supply. The IP Office system does not provide any power to IP phones. The phones can be
  - **Power over Ethernet Supply**
    Most Avaya IP phones can be powered from an 802.3af Power over Ethernet (PoE) power supply. This can be done using PoE switches to support multiple phones or using individual PoE injector devices for each phone.
  - **Individual Power Supply Units**
    An individual power supply unit can be used with each phone. This requires a power supply socket at each phone location. The type of power supply will depend on the type of phone. Note that phones using button modules may need to use an individual power supply unit rather than PoE.

1.5 Installation Requirements

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

- **Network Assessment**
  A network assessment must be completed. Avaya will not support VoIP on a network where a satisfactory network assessment 16 has not been obtained.
- **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 and all the Avaya IP deskphones support Power over Ethernet (PoE). See Power Supply Options 21.
- **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 H.323 IP phones should use CAT5 cabling.
- **LAN Cables**
  Check that an RJ45 LAN cable has been supplied with the IP phone for connection to the power supply unit. You may also need an additional RJ45 LAN cable for connection from the power unit to the customer LAN. This will depend on the type of power supply being used.
  - 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 H.323 IP phones).
- **Voice Compression Channels**
  For IP500 V2 systems, the control 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 17 for full details.
- **DHCP Server**
  The IP Office Unit can perform this role for all the phones. If another DHCP server is used for the network, this may be able to do DHCP for the H.323 IP phones, see Alternate DHCP Servers 86. Also the IP Office system can be configured to only provide DHCP support to Avaya IP phones.
  - Static IP addressing 51 can also be used for IP phone installation if required. However that method of installation is not recommended.
- **HTTP File Server**
  A PC running the IP Office Manager application can perform this role for up to 5 H.323 IP phones. An IP Office control unit with a memory card can use that memory card as the source for up to 50 phones. The IP Office system can act as the file server for up to 50 IP phones. For larger numbers a separate 3rd-party HTTP server should be used.
- **H.323 Gatekeeper**
  The IP Office system performs this role.
- **IP Office Manager**
  A Windows PC running IP Office Manager is required for IP Office configuration changes. The PC should also have System Status Application and IP Office System Monitor installed.
- **IP Telephone Software**
  The software for IP phone installation is installed into the IP Office Manager application's program folder as during the applications installation. It is also included as part of the IP Office for Linux applications installation of the IP Office application on the server.
- **Licence Keys**
  Each Avaya IP phones registered with the system requires an Avaya **Avaya IP Endpoint** licenses to operate. Refer to Licenses 15.
- **Backup/Restore Server** 54
  The phones backup and restore various phone and user settings whenever the user logs on or logs out. This uses files stored on a file server. This is not necessarily the same server as used for the phone firmware files. The IP Office system's own file storage can be used for this function and is the recommended option.

1.6 Licenses

The following licensing rules apply to the support of Avaya H.323 IP phones on a IP Office system.

- An **Avaya IP Endpoint** license is required for each Avaya H.323 IP phones. This includes all 1600, 4600, 5600, 9600, IP DECT, DECT R4, T3 IP and Spectralink.
  - The system will automatically license 12 Avaya IP phones for each IP500 VCM 32 or VCM 64 card installed in the system without requiring additional licenses to be added to the configuration.
  - Additional Avaya IP phones are licensed either by the addition of **Avaya IP Endpoints** licenses above or the conversion of legacy **IP500 VCM Channels** licenses to **Channel Migration** licenses (see below).
  - By default licenses are consumed by each Avaya IP phone that registers with the IP Office in the order that they register. The license is released if the phone unregisters. However, it is possible to reserve a license for particular phones in order to ensure that they phones always obtain a license. This is done through the **Reserve Avaya IP Endpoint Licence** setting of each IP extension.
  - Avaya IP phones without a license will still be able to register but will be limited to making emergency calls only (Dial Emergency short code calls). The associated user will be treated as if logged off and the phone will display *"No license available".* If a license becomes available, it will be assigned to any unlicensed DECT handsets first and then to any other unlicensed Avaya IP phone in the order that the phones registered.

Licenses are issued against a unique feature key/dongle serial number. For IP500v2 control units that number is unique to the System SD card fitted to the system. For Server Edition systems licenses are issued against a unique System Identification of the telephone system. To be valid, any licenses entered into the system configuration must be licenses issued against that serial number.

1.7 Network Assessment

The IP Office system is a pure Voice over IP (VoIP) system. All trunks and telephone extensions connect to the system via the customers data network. It is therefore absolutely imperative that the customer network is assessed and reconfigured if necessary to meet the needs of VoIP traffic.

- **! WARNING: A Network Assessment is Mandatory**
  When installing IP phones on a 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 a recent network assessment and may refuse to provide support if a network assessment with satisfactory results has not been performed.

Current technology allows optimally configured networks to deliver VoIP services with voice quality that matches that of the public phone network. However, few networks are optimally configured and so care should be taken to assess the VoIP quality achievable within 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 occasionally impact voice traffic. In addition, the usual history of growing and developing a network 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.

Network Assessment Targets

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:
  - **G.711:** 20ms.
  - **G.722:** 40ms.
  - **G.729:** 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.

1.8 Voice Compression Channels

Calls to and from IP devices can require conversion to the audio codec format being used by the IP device. For IP Office systems this conversion is done by voice compression channels. These support the common IP audio codecs G.711, G.722, and G.729a.

- For the IP500 V2 control units, channels can be added using IP500 VCM cards and IP500 Combination Cards.
- Server Edition systems provide their own voice compression channels through software without requiring additional hardware.

The voice compression channels are used as follows:

Call Type	Voice Compression Channel Usage
IP Device to Non-IP Device	These calls require a voice compression channel for the duration of the call. If no channel is available, busy indication is returned to the caller.
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. 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.
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.
Voicemail Services and IP Devices	Calls to the IP Office voicemail servers are treated as data calls from the TDM bus. Therefore calls from an IP device to voicemail require a voice compression channel.
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.
T38 Fax Calls	IP Office 5.0+ supports T38 fax on SIP trunks and SIP extensions. Each T38 fax call uses a VCM channel. Within a Small Community Network, a T38 fax call can be converted to a call across an H.323 SCN lines using the IP Office Fax Transport Support protocol. This conversion uses 2 VCM channels. In order use T38 Fax connection, the **Equipment Classification** of an analog extension connected to a fax machine can be set ***Fax Machine***. Additionally, a new short code feature **Dial Fax** is available.

Note: T3 IP devices must be configured to 20ms packet size for the above conditions to apply. If left configured for 10ms packet size, a voice compression channel is needed for all tones and for non-direct media calls.

Measuring Channel Usage

The IP Office system Status Application can be used to display voice compression channel usage. Within the **Resources** section it displays the number of channel in use. It also displays how often there have been insufficient channels available and the last time such an event occurred.

For IP500 VCM cards, the level of channel usage is also indicated by the LEDs (1 to 8) on the front of the IP500 VCM card.

Installing VCM Cards

Refer to the IP Office Installation manual.

1.9 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 have some form of Quality of Service (QoS) mechanism. QoS routers are essential to ensure low speech latency and to maintain sufficient audio 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.

1.10 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.
- **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.

1.11 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 most Avaya 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. The PC's network configuration does not need to be altered from that which it previously used for direct connection to the LAN. This port supports 10/100Mbps ethernet connections. Phones with a G suffix also support 1000Mbps Gigabit connections.

For phones without a PC port, 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 10/100/1000Mbps output for the PC. The adapter is powered from the phone's existing power supply. Refer to the "Gigabit Ethernet Adapter Installation and Safety Instructions" (16-601543).

H.323 IP Phones	Supported Models	PC Port
1600 Series	1603	–
	1603SW	✓
	1608	✓
	1616	✓
4600 Series	4601	–
	4602	–
	4602SW	✓
	4606	✓
	4610SW[1]	✓
	4612	✓
	4620	–
	4620SW	✓
	4621SW[1]	✓
	4624	✓
	4625	✓

H.323 IP Phones	Supported Models	PC Port
5600 Series	5601	–
	5602	–
	5602SW	✓
	5610SW[1]	✓
	5620	✓
	5621SW[1]	✓
9600 Series	9620L	✓
	9620C	✓
	9630G	✓
	9640	✓
	9640G	✓
	9650	✓
	9650C	✓
	9608	✓
	9611G	✓
	9621G	✓
	9641G	✓

1.12 Power Supply Options

Each H.323 IP phone requires a power supply. They do not draw power from the phone system. Listed below are the power supply options that can be used.

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 Avaya H.323 IP phones supported on IP Office also support this standard.

Where a large number of phones is being installed, the use of PoE switches is recommended. For other scenarios, individual PoE injector devices can be used to add PoE power support to the phone's LAN connection from a non-PoE switch.

H.323 IP Phones	Supported Models	802.3af PoE Class	
		Class	Idle
1600 Series	**1603**	2	4.4W
	1603SW	2	4.4W
	1608	2	3.7W
	1616	2	2.7W
4600 Series	**4601**	2	3.5W
	4602	1	–
	4602SW	2	3.5W
	4606	0	4.1W
	4610SW[1]	2	4.0W
	4612	0	4.1W
	4620	3	4.0W
	4620SW	2	–
	4621SW[1]	2	5.75W
	4624	0	4.1W
	4625	3	6.45W

H.323 IP Phones	Supported Models	802.3af PoE Class	
		Class	Idle
5600 Series	**5601**	2	3.5W
	5602	1	–
	5602SW	2	4.1W
	5610SW	2	3.1W
	5620	3	3.6W
	5621SW	2	–
9600 Series	**9620L**	1	2.0W
	9620C	2	3.9W
	9630G	2	4.6W
	9640	2	3.9W
	9640G	2	3.9W
	9650	2	4.7W
	9650C	2	3.7W
	9608	1	2.08W
	9611G	1	2.8W
	9621G	2	3.49W
	9641G	2	3.44W

- These 1603 and 1603SW phones require a separate PoE Splitter unit in order to use PoE.
- Exceeding the Class limit of a PoE port or the total Class support of a PoE switch may cause incorrect operation.
- Note that for phones being used with an add-on button module unit and other accessories the power requirements are higher. For 96x1 phones, set the phone power switch to **H** and treat the phone as Class 3.

1600 Series Phones

These phones can use either PoE as above or can be powered from using 1600 Series plug-top power supply units (PSUs). Different models of PSU exist for the various type of mains power outlets in different countries. The PSU connects to the phone using a barrel connector under the phone.

4600/5600 Series 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.

96x1 Phones

These phones only support a Power over Ethernet (PoE) connector. If not being supplied with a PoE switch, a separate Avaya Single Port PoE injector (SPPOE-1A) can be used for each phone. When

1.13 File Server Options

During installation and maintenance, the phones download various firmware files 12. In order to do this, a phone requests files for an HTTPS server first. If it gets no response, it then tries to obtain the files from an HTTP server. 4600 and 5600 Series phones will then try TFTP. The address of the server to use is provided as part of the DHCP response that the phone received from the DHCP server. If the IP Office system is being used as the DHCP server, the file server address is set as part of the IP Office configuration. For phones installed using static addressing, the file server address is one of the addresses entered during installation.

- Each phone will attempt to request files from the file server every time it is restarted. However, if the phone does not receive any response, it will continue restarting using the existing files that it has in its own memory. Therefore there is no requirement for the file server to be permanently available after initial installation.
    - The IP Office system is currently not supported as a file server for 9608, 9611, 9621, and 9641 phones. This also applies to using the IP Office Manager application acting as the file server. These phones are only supported when using a 3rd-party file server.
- The phones also use a server for the backup and restoration 54 of user settings during phone operation. The address for this server is defined by a separate address set found in the ***46xxsettings.txt*** file. It is not necessarily the same server that is used for the phone firmware. However, for IP Office operation, the address of the IP Office server is recommended for use as the backup/restore file server.

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

File Server	Description	Up to X Phones	TFTP (Port 69)	HTTP (Port 80)	HTTPS (Port 411)
IP Office Manager	When running, IP Office Manager can act as a HTTP/TFTP server for file requests from IP phones.	5	✓	✓	–
IP500 V2 Memory Card	For IP Office control units fitted with a memory card, that card can be used to provided the software files. For IP500 V2 control units the System SD card is a mandatory item and is pre-loaded with the phone firmware files during card creation and upgrades. Various other files can be auto-generated 24 by the IP Office if not present on the memory card.	50	✓	✓	✓
Server Edition	For IP Office systems, the IP Office application can act as the file server. The phone firmware files are installed onto the server as part of the IP Office installation. Various other files can be auto-generated 24 by the IP Office if not present on the memory card.	50	–	✓	✓
3rd Party Software	3rd Party HTTP/TFTP file server software is available from many sources including Avaya.	Unlimited	✓	✓	✓

- For IP Office Release 9.0, for IP Office systems acting as the file server, HTTP redirection can be applied to redirect 96x1 Series phone requests for .bin files to a separate HTTP server.

Control Unit Memory Cards

The memory card used with IP500 V2 systems can be used to store files including those used by Avaya IP Phones.

- The IP500 V2 control unit requires a System SD card at all times. During creation of this card, a full set of IP Office firmware files including those used by Avaya IP phones is placed onto the card.

1.14 File Auto-Generation

For IP Office systems configured to use the system's own memory as the file server 23 for the phones, the system will auto-generate the necessary firmware files 12 in response to a request from a phone if the actual file is not present in the memory. This feature is used for most of the file types except the .bin firmware files.

- **xxupgrade Files**
  The first file that a phone requests when starting up is the ***xxupgrade*** file. This file contains a list of the phone .bin files that are available as part of the firmware set and the version numbers of those files. If the version of a file differs from that which the phone already has loaded, the phone will request the new file. During this process the phone may reboot after loading each file and then request the xxupgrade.txt file again until it has updated all its firmware, if necessary. Separate files are provided for the different phone series:
  - **16xxupgrade.txt**
    This file lists the firmware files that 1600 Series phones should load.
  - **46xxupgrade.scr**
    This file lists the firmware files that 4600 Series and 5600 Series phones should load.
  - **96xxupgrade.txt**
    This file lists the firmware files that 9600 Series phones should load.
  - **96x1Hupgrade.txt**
    This file list the firmware files that 9608, 9611, 9621, and 9641 phones should load.
- **46xxsettings.txt**
  This file will match the file supplied with the IP Office Manager except:
  - The ***BRURI*** value will be set to indicate the IP Office memory as the file server location for backup and restore 54 actions by the phones.
  - The ***LANG1FILE*** to ***LANG4FILE*** values for 1600 Series and 9600 Series phones for non-English language files is determined from the best match to the system locale and the most common user locales in the IP Office system configuration. Languages currently supported are Dutch, French, French (Canadian), German, Italian, Latin Spanish, Portuguese, Russian, Spanish.
- **Language files**
  If the ***46xxsettings.txt*** file is auto-generated, the matching 1600 Series and 9600 Series phone language files specified in that file are also auto-generated.
- **<ext>_16xxdata.txt**
  If the ***46xxsettings.txt*** file is auto-generated, it will specify the IP Office system as the location for phones to backup and restore 54 user settings. If no file exists for a user, a file will be auto-generated. This feature is used for 1600 Series and 9600 Series phones.

In all the cases above, if a matching file is uploaded to the system's memory, the auto-generation of that particular file is overridden.

1.15 Control Unit Memory Card

The memory card used with IP500 V2 systems can be used to store files including those used by Avaya IP Phones.

- The IP500 V2 control unit requires a System SD card at all times. During creation of this card using IP Office Manager, a full set of IP Office firmware files including those used by Avaya IP phones is placed onto the card.

1.16 Registration Blacklisting

The IP Office system blacklists repeated failed H323/SIP registration requests. Whilst blacklisted, further registration attempts from the source IP address or to the H323/SIP extension are ignored.

The blacklisting applies as follows:

- **Source IP Address Blacklisting**
  Registration attempts to a non-existent extension or using the wrong password of an existing extension are logged against the source IP address. The address is blacklisted for 5 minutes after 20 failed attempts in any 20 minute period.
- **Extension Blacklisting**
  Registration attempts to an existing extension using the wrong password are logged against that extension. The extension is blacklisted for 1 minute after 10 failed attempts in any 20 minute period.

When blacklisting occurs, the system generates an System Status Application alarm and adds an entry to its audit log. A system alarm is also generated and can be output using any of the supported system alarm routes (SMTP, SNMP, Syslog).

Chapter 2. Installation

2. Installation

The following is a summary of the major steps in the installation process. The recommended installation method is to use DHCP where possible, to use the IP Office system as the file server and to enable automatic user and extension creation.

Process Summary

1. **IP Office Manager PC**
   Check that IP Office Manager, System Status Application and 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.

2. **Voice Compression Channels**
   For IP500 V2 systems, the control unit must be fitted with voice compression channels 17. Use either SSA or System Monitor application to verify that the voice compression channels are available. SSA list the VCM channels on the **Resources** screen. The initial lines of Monitor output include the item ***VCOMP=*** which will state the number of channels installed in the control unit.

3. **Avaya IP Endpoint Licenses**
   Each phone requires an **Avaya IP Endpoint** license 15. Phones can register without a license but will not operate. The licenses are added to the IP Office configuration using IP Office Manager.

4. **H.323 Gatekeeper Settings**
   The IP Office system has support for H.323 phones enabled by default. However, the setting should be checked.

5. **DHCP Server Setting**
   DHCP is the recommended method for installation of IP phones on a IP Office system. This requires a DHCP server configured to support IP phones. The IP Office system can be used for this. If the customer want to use their own DHCP server, it will require additional configuration 86.

6. **Phone File Server Setting:**
   If the IP Office system is being used for DHCP, it also needs to be configured with the address of the file server. Whichever installation method and file server is selected, the phone firmware files need to be added to the files available on the server.

7. **Extension and User Settings**
   The IP Office system can be configured to automatically create user and extension entries in its configuration for each IP phone that is installed. It automatic creation is not used, entries must be manually created for each extension and user before the phones are installed.

8. **Phone Connections**
   Once the steps above have been completed, the phones can be connected to the network. If using DHCP, the phones will automatically obtain IP address information and other settings and then start loading files. If not using DHCP, the phones will have to be taken through a manual process of entering the IP address information and settings.

9. **Phone Registration**
   Once the phones have downloaded all the files they require from the file server, they will attempt to register with the IP Office system. The phones will prompt for entry of the extension number that they should use.

10. **Testing**
    Operation of the phones should be tested by making a number of calls, including external calls.

11. **Post Installation**
    If Auto-creation was used for the extension and or user entries, those settings should be disabled after installation of all the phones is completed. This manual only details the minimum user configuration necessary for installation. The new users can now be fully configured to meet the customer requirements for those users.

2.1 Licensing

Refer to the Licenses 15 section for information on licensing rules.

2.1.1 Checking the Serial Number

Licenses are issued against a unique feature key/dongle serial number. For IP500 V2 control units that number is unique to the System SD card fitted to the system. For Server Edition systems the System Identification value for the system is used.

To check the serial number:

1. Using IP Office Manager, retrieve the configuration from the system.
2. Select  **System**.
3. Select the **System** tab.
4. For IP500 V2 systems, the feature key serial number is shown by the **Dongle Serial Number** field. For Server Edition systems the feature key serial number is shown by the **System Identification** field.
5. This is the number that must be used to obtain licenses for the system. It should also be used to check any licenses received.

2.1.2 Adding Licenses

Use the following procedure to add licenses to the telephone system configuration. You can add multiple (cumulative) licenses.

You must ensure that the licenses match the **Dongle Serial Number** or **System Identification** number shown 29 in the system configuration. This should be shown in the file used to supply the licenses. It is recommended that you cut and paste the license keys from a supplied file rather than typing them in manually.

To add licenses:

1. Using IP Office Manager, receive the configuration from the telephone system.
2. Select  **License**. The current licenses in the system configuration are displayed.
3. To add a license, click on **Add**.
4. Select **ADI** and click **OK**.
5. Enter the license that you have been supplied into the field and click **OK**.
6. The type of the license should be displayed but with its **License Status** set to ***Unknown***. If the **License Type** was not recognized, check that it has been entered correctly.
7. Save the configuration back to the system and then receive the configuration from the system again.
8. The **License Status** should now be ***Valid***.

2.1.3 Reserving Licenses

This particular process cannot normally be done until the extension entry has been created. If using automatic extension creation (the default), this means that license reservation cannot be done until after initial installation of the phone. However, consideration should be given to using this setting with any existing phones already installed in order to ensure that they retain their licenses if possible following the addition of other phones.

Licenses are normally automatically assigned to extensions in order of registration. However existing extensions can reserve a license in order to ensure they do not become unlicensed when new extensions added to the system manage to register first following a system reboot.

To reserve licenses:

1. Using IP Office Manager, receive the configuration from the telephone system.
2. Select  **Extension** and then select the H.323 extension.
3. Select the **VoIP** tab.
4. Set the **Reserve License** field to ***Reserve Avaya IP endpoint license***.
5. Repeat the process for any other extensions for which you want to reserve the license.
6. Save the configuration back to the telephone system.

2.2 System H.323 Support

The IP Office system has H.323 support enabled by default. The following sections offer more information on configuring H.323 support:

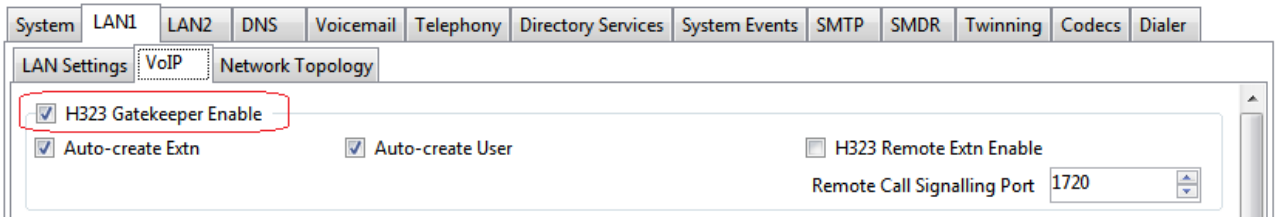
- **Enabling the H.323 Gatekeeper** 31
- **Setting the RTP Port Range** 32
- **Enabling RTCP Quality Monitoring** 33
- **Adjusting DIffServ QoS** 35
- **System Default Codecs** 36

2.2.1 Enabling the H.323 Gatekeeper

Support for H.323 telephones and lines is enabled by default. However, the settings should be checked.

To enable the H.323 Gatekeeper:

1. Using IP Office Manager, retrieve the configuration from the system.
2. Select **System**.
3. Select the **LAN1** or **LAN2** tab depending on which of the system's LAN interfaces you want to use to support H.323 extensions.
4. Select the **VoIP** sub-tab.



5. Check that the **H323 Gatekeeper Enable** setting is selected.
6. If this setting needs to be changed, save the configuration back to the system.

2.2.2 Setting the RTP Port Range

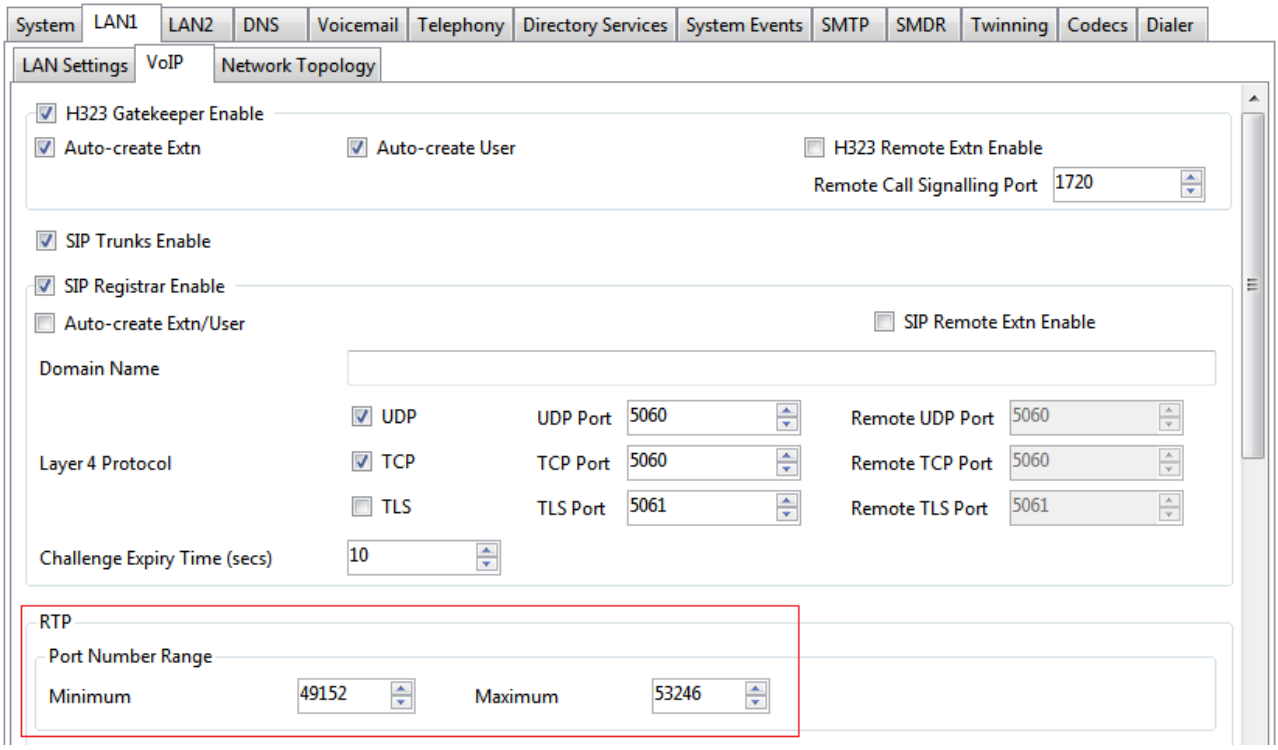
The ports used for H.323 VoIP calls vary for each call. The range for the ports used can be adjusted in order to avoid conflict with other services. If the customer has any internal firewalls or similar equipment that applies port filtering or only forwards traffic based on the port used, the range set here must be allowed by those devices.

For each VoIP call, receive ports are selected from the range defined below. Even numbers in the range are used for the calls incoming Real-Time Transport Protocol (RTP) traffic. The same calls Real-Time Transport Control Protocol (RTCP) traffic uses the RTP port number plus 1, that is the odd numbers.

It is recommended that only port numbers greater than or equal to 49152 but strictly less than 65535 are used, that being the range defined by the Internet Assigned Numbers Authority (IANA) for dynamic usage.

To checking the port range:

1. Using IP Office Manager, retrieve the configuration from the system.
2. Select **System**.
3. Select the **LAN1** or **LAN2** tab depending on which of the system's LAN interfaces you want to use to support H.323 extensions.
4. Select the **VoIP** sub-tab.



5. Check the **Port Number Range** shown in the **RTP** section. Remember that the matching RTCP traffic uses the same range plus 1.
   - **Port Range (Minimum):** *Default = 49152. Range = 1024 to 65280.*
     This sets the lower limit for the RTP port numbers used by the system. Choosing a minimum range of less than 1024 should only be done after careful analysis of the overall configuration.
   - **Port Range (Maximum):** *Default = 53246. Range = 1278 to 65534.*
     This sets the upper limit for the RTP port numbers used by the system. The gap between the minimum and the maximum must be at least 254. Choosing a minimum range of less than 1024 should only be done after careful analysis of the overall configuration.
6. If these settings need to be changed, do so and then save the configuration back to the system.

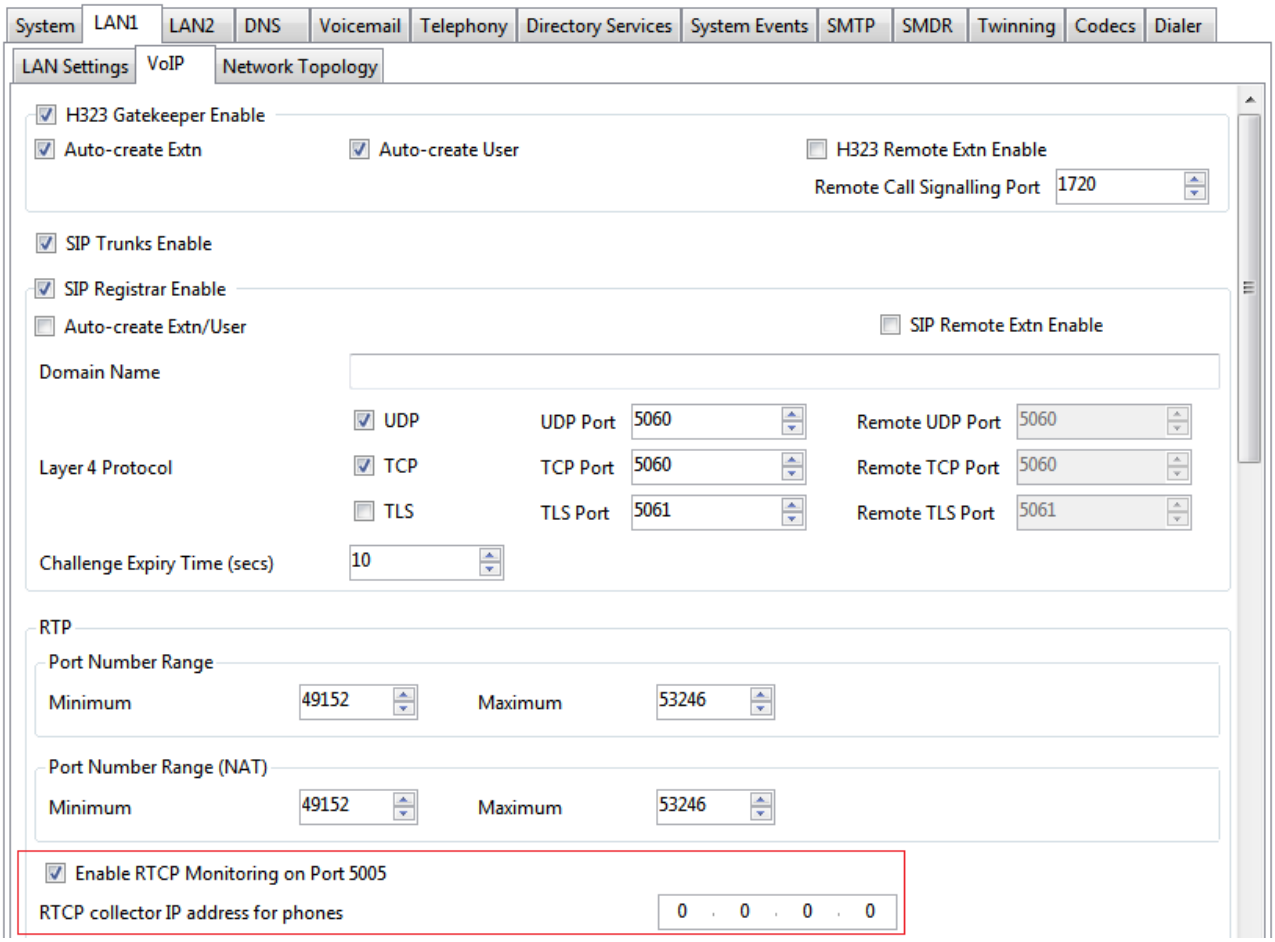
2.2.3 Enabling RTCP Quality Monitoring

Avaya IP phones support call quality monitoring. This is done using port 5005 both on the system and the phones. Enabling the option below instructs the phones to provide call quality information to the IP Office system on that port.

Enabling RTCP monitoring provides the system with measures of packet delay, packet loss and jitter. That information can be accessed using the System Status Application and IP Office System Monitor applications. The system can also be configured to output alarms when the call quality values exceed set levels.

To enable RTCP quality monitoring:

1. Using IP Office Manager, retrieve the configuration from the system.
2. Select  **System**.
3. Select the **LAN1** or **LAN2** tab depending on which of the system's LAN interfaces you want to use to support H.323 extensions.
4. Select the **VoIP** sub-tab.

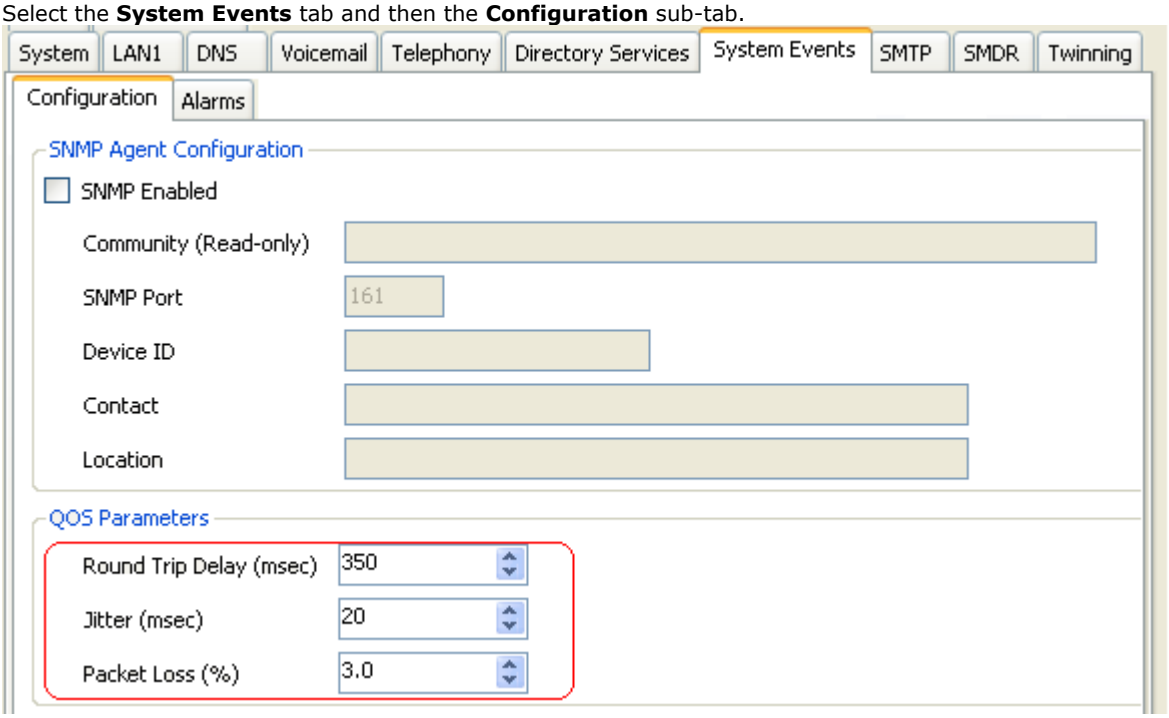


5. Check that the **Enable RTCP Monitoring on Port 5005** setting is selected.
   - By default the RTCP data is sent to the IP Office system. If necessary, you can select to have the data sent to a specific address for collection by a third-party QoS monitoring application. To do this, enter the address in the **RTCP collector IP address for phones** field.
6. If these setting needed changing, save the configuration back to the system.

To set the Quality of Service alarm levels:

The system can send alarms to the System Status Application. It can also send the same alarms to SNMP, emails or Syslog destinations. For details of how to configure these refer to the IP Office Manager documentation. The settings below are used to set the levels which, if exceeded, will cause an alarm to be sent at the end of a call.

1. Using IP Office Manager, retrieve the configuration from the system.
2. Select  **System**.
3. Select the **System Events** tab and then the **Configuration** sub-tab.



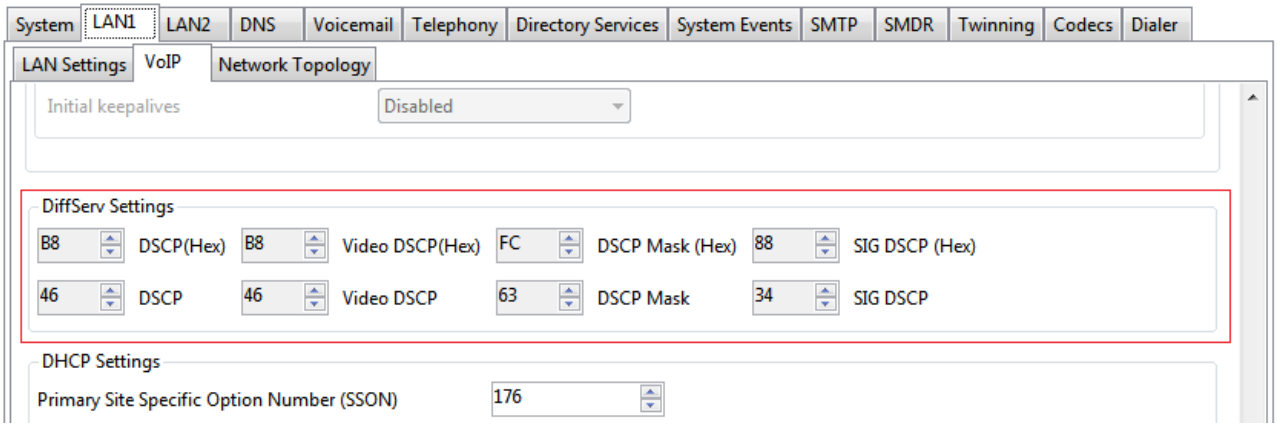
4. The QoS Parameters are used by the system to trigger alarms The default settings match the limits usually acceptable for good call quality,
5. If the settings are adjusted, save the configuration back to the IP Office system.

2.2.4 Adjusting DiffServ QoS

DiffServ is used to apply different 'quality of service' tags to the voice (RTP) and control signal (RTCP) elements of a VoIP call. The IP Office system itself does not apply any different priority to data packets its receives or sends based on their tags. However, when being used in a network where QoS is being used for prioritization by other devices, the IP Office's settings should be set to match those expected for voice calls and their associated control signalling.

To adjust the DiffServ QoS settings:

1. Using IP Office Manager, retrieve the configuration from the system.
2. Select  **System**.
3. Select the **LAN1** or **LAN2** tab depending on which of the system's LAN interfaces you want to use to support H.323 extensions.
4. Select the **VoIP** sub-tab.



5. Check the **DiffServ Settings** that are being used by the system. Note that the 2 rows are linked, the upper row shows the DiffServ values in Hex numbers, the lower row shows the values in decimal. The hex values are equal to the decimal multiplied by 4. Either row can be used to set the required values.
6. If these settings need to be changed, do so and then save the configuration back to the system.

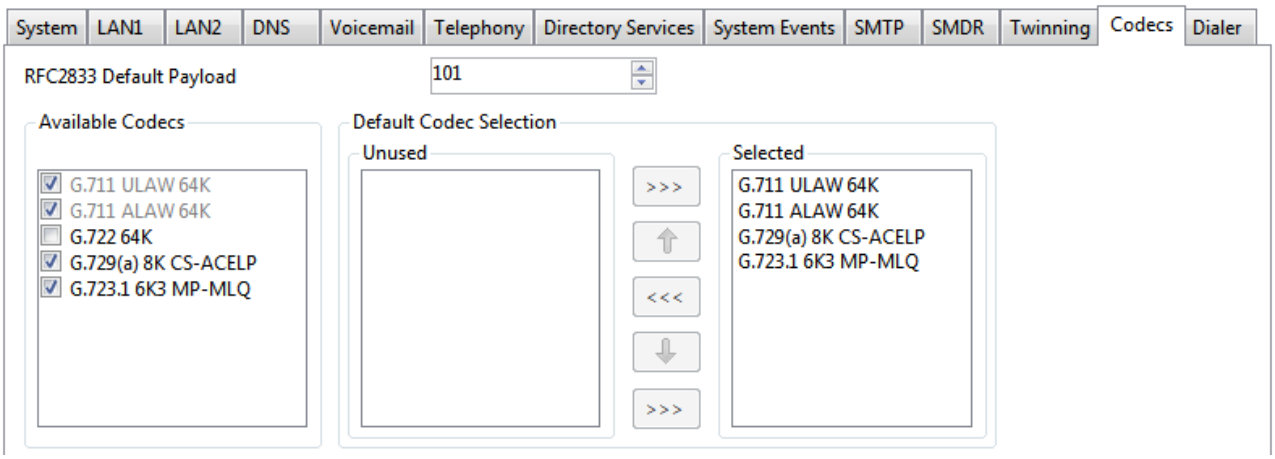
2.2.5 System Default Codecs

By default, all VoIP devices added to the IP Office configuration use the system's default codec preferences. This is shown by the Codec Selection setting on an IP trunk or extension being set to ***System Default***.

In addition to changing the default codec preference order for all VoIP trunks and extension, the codec preferences used by a particular trunk or extension can be adjusted. However, the use of the common system settings ensures codec consistency between trunks and extensions.

To change the default codec preferences

1. Using IP Office Manager, retrieve the configuration from the system.
2. Select  **System**.
3. Select the **Codecs** sub-tab.



4. The **Available Codecs** list shows which codecs the system supports. The codecs in this list which enabled are those that can be used in other configuration forms including the adjacent default selection.
   - **! WARNING:** Deselecting a codec in this list automatically removes it from all line and extension codec lists where it was being used.
5. The **Default Selection** section is used to set the default codec preference order. This is used by all IP (H.323 and SIP) extensions and lines on the system that have their **Codec Selection** setting set to ***System Default***. This is the default for all new added IP extension and lines.
6. If these settings need to be changed, do so and then save the configuration back to the system.

2.3 DHCP Settings

The recommendation for H.323 phone installation is to use DHCP, especially if a large number of phones are being installed. Using DHCP simplifies both the installation and maintenance.

There are a number of options around which server is used for the DHCP support for the H.323 phones:

- If the IP Office system is to be used as a DHCP server for the network, use the processes below to check and configure the system's DHCP settings.
- If a separate DHCP server is used by the customer's network, that DHCP server may need to be configured to support DHCP requests from IP phones, see Alternate DHCP Server Setup 86.
- The IP Office can be configured to only provide DHCP support for Avaya phones. That option can be used to allow it to be used in conjunction with a separate customer DHCP server. This removes the need to configure the customer's DHCP server for IP phone support.

- **! WARNING**
  Enabling an additional DHCP server in a network can cause connection issues for all devices on the network. Ensure that you, the user, and the user's network administrator all agree upon the correct choice of DHCP server option.

Enabling IP Office DHCP Support

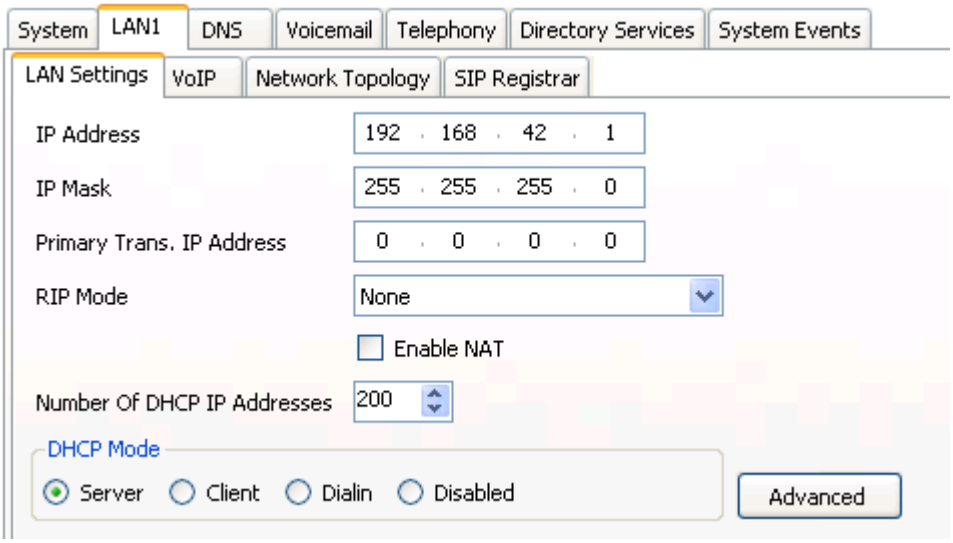
The following are the main steps for enabling the IP Office system to support DHCP operation for IP phones.

1. **Enable DHCP and Set the Number of Addresses** 38
2. **Check the Site Specific Option Numbers** 39
   The IP Office defaults match the defaults used by Avaya IP phones. However it is important to check these values and to be aware of their potential usage.
3. **Set the File Server Settings** 40
   If the IP Office system is set to provide DHCP for IP phones, that role includes telling the phones the location of the file server they should use for phone firmware, even if that file server is not the IP Office system.

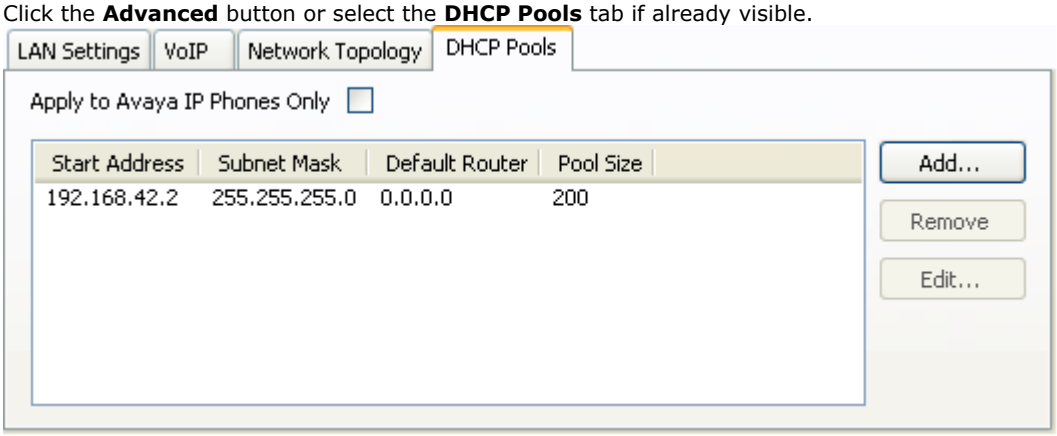
2.3.1 System DHCP Support

To change the system's DHCP settings:

1. Using IP Office Manager, retrieve the configuration from the system.
2. Select  **System**.
3. Select the **LAN1** or **LAN2** tab depending on which of the system's LAN interfaces you want to use to support H.323 extensions.
4. Select the **LAN Settings** tab.



5. If the **DHCP Mode** is set to ***Server***, the **Number of DHCP IP Addresses** value set how many IP addresses the system can issue. Those addresses are use the IP Address of the system as the starting point.
6. Click the **Advanced** button or select the **DHCP Pools** tab if already visible.



7. The settings on this tab allow adjustment of the DHCP setting including adding multiple ranges of DHCP numbers that the IP Office system can support. Note that address ranges outside those of the IP Office systems own subnet may also require the creation of appropriate IP routes to ensure traffic routing between the subnets.
8. If the **Apply to Avaya IP Phone Only** option is selected, the IP Office will act as a DHCP server for Avaya phones only. This option cannot be used if also supporting 1100 Series and 1200 Series phones.
9. If the settings have been changed, save the configuration back to the system.

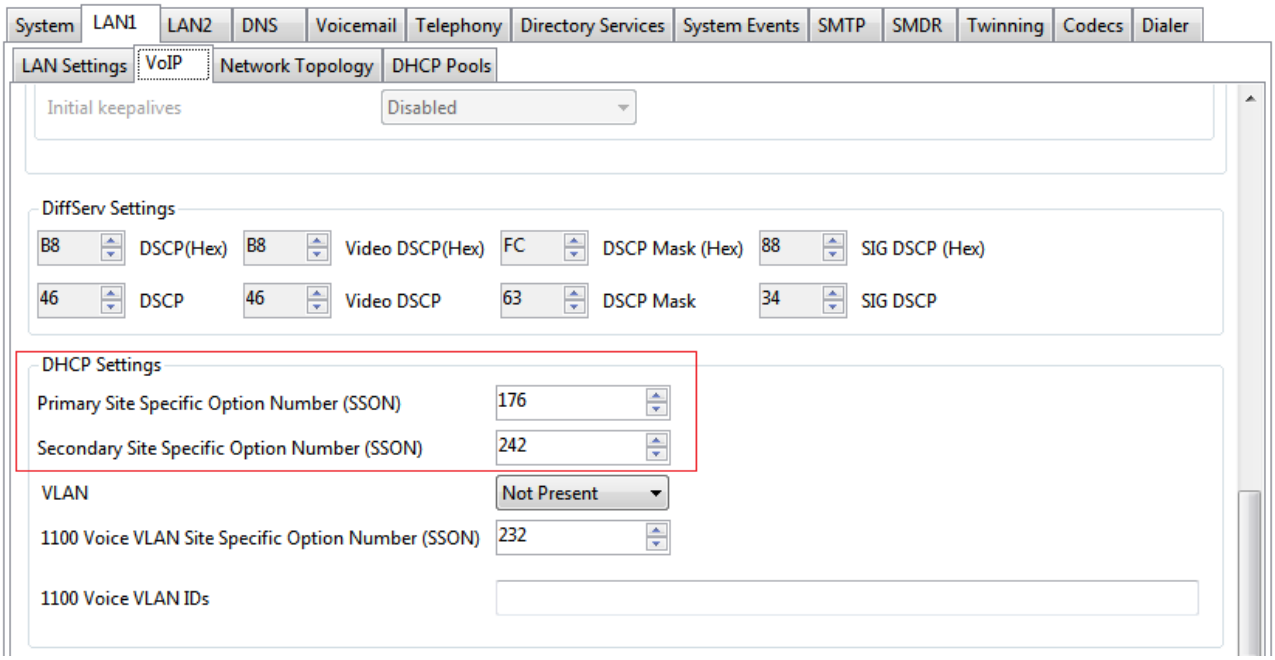
2.3.2 System Site Specific Option Numbers

When requesting address settings from a DHCP server, each phone also requests additional information that the DHCP server may have. It does this by sending a Site Specific Option Number (SSON). If the DHCP server has information matching the SSON, that information is included in the DHCP response.

4600 and 5600 Series phones use 176 as their default SSON. 1600 and 9600 Series phones use 242 as their default SSON. However, through the phone's own menus the SSON it uses can be altered 76. For those phones using the IP Office system for DHCP, the SSON numbers that the IP Office supports are set in the IP Office system's configuration. The values used by the phones and supported by the IP Office system must match.

To changing the system's SSON settings:

1. Using IP Office Manager, retrieve the configuration from the system.
2. Select  **System**.
3. Select the **LAN1** or **LAN2** tab depending on which of the system's LAN interfaces you want to use to support H.323 extensions.
4. Select the **VoIP** sub-tab.



5. Check that the Site Specific Option Number settings match those required for the phone being supported. The default for 4600 and 5600 Series phones is 176. The default for 1600 and 9600 Series phones is 242.
6. If this setting needs to be changed, save the configuration back to the system.

2.4 File Server Settings

As part of the installation process, the phone will request files from a file server. If being installed using DHCP, they obtain the address of the file server as part of the DHCP response from the DHCP server. If being statically installed, the file server address is entered into the phone as part of the static addressing process.

The file server options are:

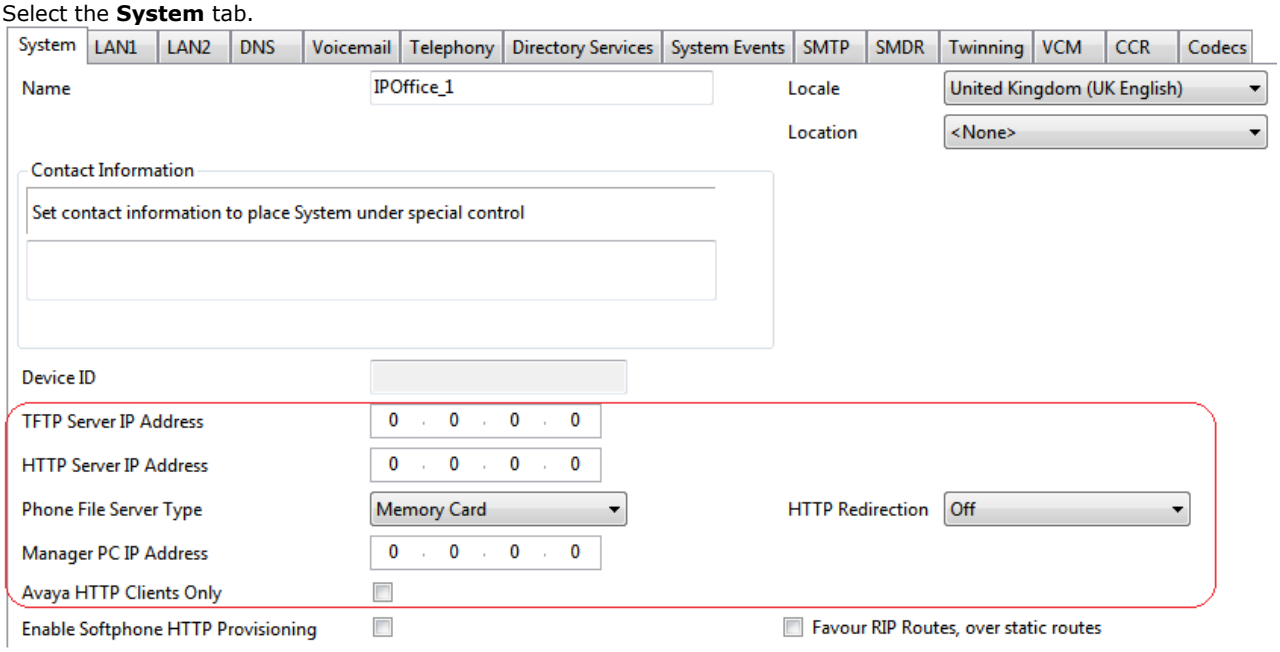
- For IP500 V2 systems, the IP Office system's own memory card can be used as the source for the files. For Server Edition systems, the system's own disk can be used as the source for the files used by the phones. This is the recommended option and can be used for up to 50 phones.
    - For IP Office Release 9.0, HTTP redirection can be used to allow a separate server to provide the binary files for 96x1 phones whilst the IP Office system provides all other files.
- The IP Office Manager application can also act as a file server for up to 5 phones.
- If either of the options above are not acceptable, a 3rd party HTTP file server is required. The necessary phone firmware files then need to be loaded onto that server.

2.4.1 System File Server Settings

If the IP Office system is being used for DHCP support 37 for the IP phones, various settings in the IP Office system's configuration are used to set the file server addresses sent to the phones in the DHCP responses.

To change the file server settings:

1. Using IP Office Manager, retrieve the configuration from the system.
2. Select **System**.
3. Select the **System** tab.



4. Check the **Phone File Server Type** setting.
   - ***Memory Card*** *(IP500 V2)*
     Use the systems own memory card by providing its own IP address as the TFTP and HTTP file server values in the DHCP response. This is the default setting.
   - ***Disk*** *(Server Edition)*
     Use the systems own memory by providing its own IP address as the TFTP and HTTP file server values in the DHCP response. This is the default setting.
   - ***Manager***
     Use the IP Office Manager application as the TFTP and HTTP file server. This option is only supported for a maximum of 5 IP phones. This option uses the separate **Manager PC IP Address** set in the configuration. The default of 0.0.0.0 is used by the system to broadcast for any available IP Office Manager application on the network.
   - ***Custom***
     This option uses the separate **TFTP Server IP Address** and **HTTP Server IP Address** values set in the configuration as the files server addresses in the DHCP response given to phones.
     - **TFTP Server IP Address**
       This field is used if the **Phone File Server Type** is set to ***Custom***. The **TFTP Server IP Address** default of 0.0.0.0 is a broadcast on the network for a TFTP server.
     - **HTTP Server IP Address**
       This field is used if the **Phone File Server Type** is set to ***Custom***. It is also used if **HTTP Redirection** is set to ***Phone Binaries***. The **HTTP Server IP Address** default of 0.0.0.0 is no HTTP request.
5. If using the ***Disk*** or ***Memory Card*** settings are selected for the **Phone File Server Type**, for 96x1 phones the **HTTP Redirection** option can be used to send requests for phone binary files to a separate file server set by the **HTTP Server IP Address**. This allows the IP Office system to supply all files for the phones, including auto-generated files, except the binaries which come from the separate server.
6. The **Avaya HTTP Clients Only** option can be used to restrict the system to responding to file requests from Avaya phones and applications only. This option should not be used if the system is also supporting 1100 and or 1200 Series phones.
7. If any changes have been made, save the configuration back to the system.

2.4.2 Creating/Editing the Settings File

During installation, the phones request files first downloading an **xxupgrade** file from the file server. They then follow the instructions within that file to request further files if necessary. Various different xxupgrade files exist for the different phone series. These are provided as part of the phone firmware 12. The xxupgrade files should not be edited or changed in any way.

The last line of all the xxupgrade files instructs the phones to request the ***46xxsettings.txt*** file. This file can be used to set site specific settings for all the Avaya H.323 IP phones being supported on a particular site.

When using the IP Office system as the file server, the IP Office system will auto-create 24 a suitable ***46xxsettings.txt*** file based on various IP Office system configuration settings. It will only do this if there is no actual ***46xxsettings.txt*** file available on the server.

Manually Editing the File

1. Locate the ***46xxsettings.txt*** file on the file server.
2. Using a plain text editing tool, open the ***46xxsettings.txt*** file.
3. Edit the file as required. The file contains numerous comments and notes. Further details of the various settings are contained in the appropriate Avaya LAN Administrator Manual for the type of phone. Note that the files contain a wide range of settings used on other Avaya telephone systems that may not necessarily work or be supported with IP Office systems.
4. A **#** character at the start of a line comments out the command on that line.

Dialing Prefix

For IP Office systems the addition or removal of dialing prefixes is done by the IP Office system rather than individual phones, the use of enhanced dialing rules through the phone settings file is not supported.

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`.

1600/9600 Series Phone Languages

In addition to English, the 1600 and 9600 phones can support up to 4 other languages. This is done by the phones, which download the language files specified in the ***46xxsettings.txt*** file. Currently 9 non-English language files are provided as part of the IP Office Manager installation.

Language	1600 File	9600 File
Dutch	mlf_dutch.txt	mlf_9600_dutch.txt
French Canadian	mlf_french_can.txt	mlf_9600_french_can.txt
French	mlf_french_paris.txt	mlf_9600_french_paris.txt
German	mlf_german.txt	mlf_9600_german.txt
Italian	mlf_italian.txt	mlf_9600_italian.txt
Portuguese	mlf_portuguese.txt	mlf_9600_portuguese.txt
Russian	mlf_russian.txt	mlf_9600_russian.txt
Spanish	mlf_spanish.txt	mlf_9600_spanish.txt
Spanish (Latin American)	mlf_spanish_latin.txt	mlf_9600_spanish_latin.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. If using the IP Office system as the file server, the appropriate language files based on the IP Office system configuration can be provided using file auto-generation 24.

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 Settings 54 for full details.

Screensaver

You can specify how many minutes before an idle phone displays a screensaver image and the name of the image file. See Screensaver 58.

2.4.3 Loading Software Files onto the System

For Server Edition systems, the phone firmware suitable for IP Office system operation is included as part of the IP Office system's installation onto the server. Therefore no further action is required if using the system as the file server for phone installation. The firmware is also included as part of IP Office Manager and is copied onto the PC when IP Office Manager is installed. No other firmware should be used with IP Office unless specifically documented. The firmware installed can be checked and new firmware copied onto the telephone system's disk if necessary.

The phone firmware suitable for IP Office system operation is supplied as part of the IP Office Manager software and is copied onto the PC when IP Office Manager is installed. No other firmware should be used with IP Office unless specifically documented.

There are a number of methods by which the firmware installed with IP Office Manager can be copied onto the telephone system's memory card. The method used depends mainly on the type of control unit.

- **! WARNING**
  A memory card should never be removed from a running system without either the card or the system first being shutdown. IP Office Manager should be used to shutdown the memory card before it is removed from the system.
- For IP Office operation, only the phone .bin files need to be present on the memory card. Other files required by the phones are automatically generated by the system in response to requests from the phones.

IP500 V2 Control Unit

The system's System SD card is used to store the files. This is a mandatory card that is present in all IP500 V2 systems. The firmware files are loaded onto the card in a number of ways:

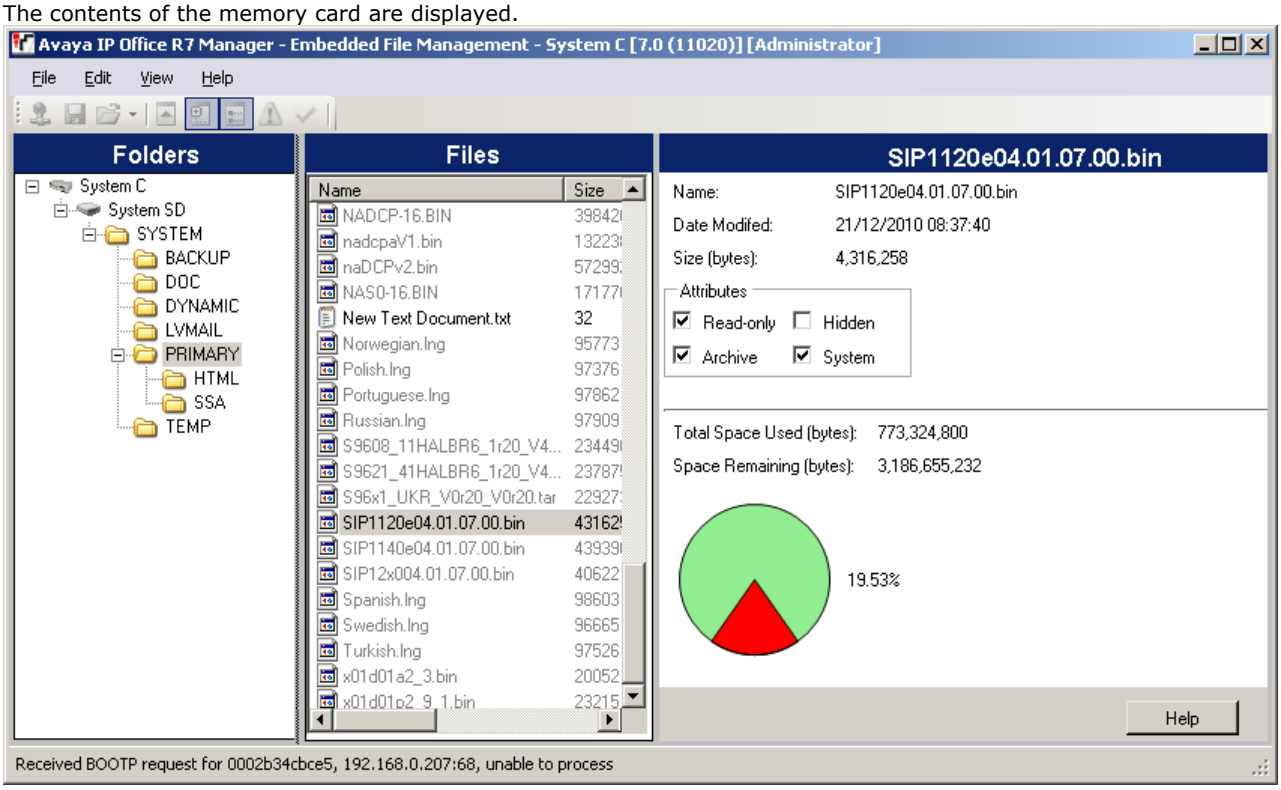
- If the system was upgraded using the **Recreate SD Card** option in IP Office Manager, the firmware is automatically copied onto the card as part of that process.
- If the system was upgraded using IP Office Manager's Upgrade Wizard, if the **Upload System Files** option was selected, the firmware is copied onto the card as part of that process. The **Upload System Files** option is enabled by default.

If you think the correct files are not present, you can use the embedded file manager part of IP Office Manager to check the files on the card and to copy the files onto the card if necessary.

Using Embedded File Manager to Check/Upload Files

Embedded file manager allows you to remote see the files on the memory card used by the telephone system. It also allows you to upload new files.

1. In IP Office Manager, select **File | Advanced | Embedded File Management**.
2. The **Select IP Office** menu is displayed.
3. Select the telephone system and click **OK**.
4. Enter the name and password for the system. These are the same as used for configuring the system.
5. The contents of the memory card are displayed.



6. For an IP500 V2, use the folder tree to navigate to ***System SD | SYSTEM | PRIMARY***. For a Server Edition system, use the folder tree to navigate to ***system | primary***.

7. Individual files can be copied onto the card by using drag and drop or by selecting **File | Upload System Files**. The whole set of phone firmware files that IP Office Manager has available can be copied by selecting **File | Upload Phone Files**.

    - The source files can be found on the IP Office Manager PC in ***C:\Program Files\Avaya\IP Office\Manager\memory Cards\Common\system\primary***.

Manually Copying Files

Files can be copied onto the memory card by placing it into a PC with a suitable memory card slot.

- **! WARNING**
  A memory card should never be removed from a running system without first being shutdown.IP Office Manager should be used to shutdown the memory card before it is removed from the system.

1. Using IP Office Manager, select **File | Advanced | Memory Card Command | Shutdown**.
2. The **Select IP Office** menu is displayed.
3. Select the telephone system and click **OK**.
4. Enter the name and password for the system. These are the same as used for configuring the system.
5. You may be prompted for which card you want to shutdown. Select **System** and click **OK**.
6. On the back of the control unit, check that the LED for the memory card slot is off before removing the memory card.
7. Place the card into the PC's memory card slot and examine the contents.
8. For an IP500 V2 system, use the folder tree to navigate to ***System SD | SYSTEM | PRIMARY***. The source files can be found on the IP Office Manager PC in ***C:\Program Files\Avaya\IP Office\Manager\memory Cards\Common\system\primary***.
9. When the card is reinserted into the system, card usage is automatically restarted.

2.4.4 Loading Files onto a 3rd Party Server

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

The same firmware files can also be obtained directly from the software package used to install IP Office Manager without having to perform the installation. The files are located in the **\program files\Avaya\IP Office\Manager** sub-folder of the installation directory.

Note that these sets of files include .bin files that are also used for other devices including the IP Office system itself.

2.5 User and Extension Creation

When a new H.323 telephone registers with the system, the IP Office can automatically create a new extension entry for the telephone in its configuration. It can also automatically create a new user entry for the telephone. Alternatively if the phone registers using an extension number for which entries already exist, those entries are used so long as no other phone is already using them.

For new installations, the use of Auto-creation is recommended for ease of installation. The auto-create options must be disabled after installation. If Auto-creation is not used, extension and user entries need to be manually added to the configuration before attempting to install the phones.

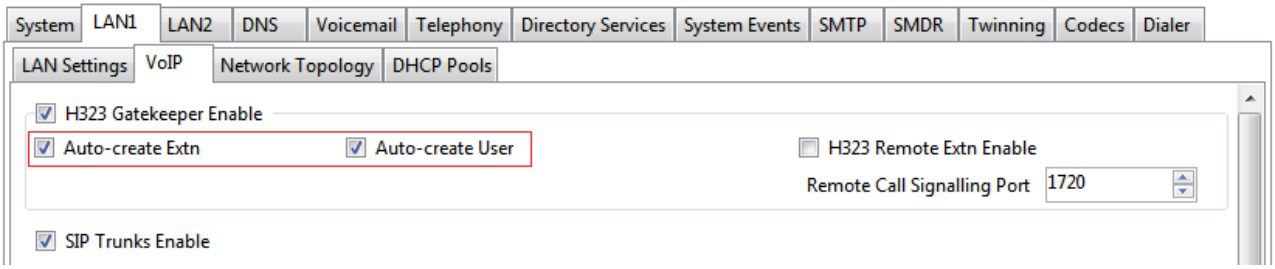
2.5.1 Auto-Creation

When installing a large number of phones, unless the configuration has been pre-built, auto-creation can be used to simplify the installation process.

- **Auto Disablement of Auto Create**
  Leaving the auto-create extension and user settings enabled is strongly deprecated. For Release 9.1 and higher, the system automatically disables the settings 24-hours after they are enabled.

To switch auto-create on/off:

1. Using IP Office Manager, receive the configuration from the system. Select **System**.
2. Select the **LAN1** or **LAN2** tab depending on which of the system's LAN interfaces you want to use to support H.323 extensions.
3. Select the **VoIP** sub-tab.



4. The **H.323 Auto-create Extn** and **H.323 Auto-create User** settings are used for H.323 phone installation. Set these as required for the installation. If either option is not enabled, it will be necessary to manually create the extension entries 49 and or manually create the user entries 48 before installing the phones.
5. If the settings have been changed, save the configuration back to the system.

2.5.2 Manually Creating User

If the **Auto-create User** option is not enabled 47, you must manually create a user entry for each phone being installed. Use the procedure below to manually create an entry. It will also prompt whether a matching extension entry should also be created.

To manually create user entries:

1. Using IP Office Manager, receive the system's configuration.
2. To display the list of existing users, click  **User** in the left-hand panel. Right-click on the right-hand panel and select **New**.
   a. 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.
   b. Click on the **Button Programming** tab. For the first three buttons, you must click on the **Action** field and select **Appearance | Appearance**.
   c. Click on **OK**.
   d. IP Office Manager will prompt whether it should also create a matching extension. If the **Auto-create Extn** option is not enabled, select ***H.323 Extension*** and click **OK**. Otherwise, select ***None*** and click **OK**.
3. Save the configuration changes back to the system.

2.5.3 Manually Creating Extensions

If the **Auto-create Extn** option is not enabled 47, you must manually create an extension entry for each phone being installed. This can be done either as part of the process of manually creating users 48 or it must be done separately using the process below.

To manually create extension entries;

1. Using IP Office Manager, retrieve 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**.
   a. In the **Extn** tab, set the following:
      - **Extension ID**
        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. This value is used to associate the extension with the user who has the same extension number.
      - **Phone Password**
        This is the password used to register the phone with the IP Office system. If not set, the matching user's 48 **Login Code** is used.
   b. To add the new extension, click **OK**.
3. Save the configuration changes back to the system.

To select the require codec:

If the **Codec Selection** is left set to ***System Default***, the extension uses the system codec preferences 36. In most cases this is preferred and any changes required should be made at the system level to ensure consistency for all IP trunks and extensions.

However, if required, the **Codec Selection** of each individual trunk and extension can be adjusted to differ from the system defaults.

1. Using IP Office Manager, retrieve the system's configuration.
2. To display the extension's settings, click  **Extension** in the left-hand panel.
3. Select the **VoIP** tab.
4. Change the **Codec Selection** to ***Custom***.
5. The **Unused** and **Selected** lists can be used to select which codecs the device uses and their order of preference.
6. Save the configuration changes back to the system.

2.6 Phone Connection

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

To connect the phone:

1. Do not start this process until all the preceding steps in the Installation Summary 28 have been completed.
2. Connect the network LAN cable to the data-in socket of the power supply being used for the phone.
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.
4. The phone's message indicator should glow red for a few seconds. The phone will then begin its software loading process. After a short delay, the phone displays **Initializing** and then **Loading...**. The loading phase may take a few minutes.
   - If the phone has an existing software boot file (ie. it has been previously installed), it will load that file and then display **Starting...**.
   - If the phone displays **No Ethernet**, check the connection to the LAN.
5. The phone displays **DHCP** and a timer as it attempts to request an IP address and other information from a DHCP server.
   - **To switch to static address installation**
     Press ***** whilst DHCP is shown. See Static Address Installation 51.
6. 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.
7. Once DHCP has completed successfully, the phone will request files from the file server indicated in the DHCP response. The first file requested details the other files that the phone should also load. The phone will first make its file request using HTTPS. If this fails it will make the same request using HTTP. If that fails it will make a final request using TFTP. If all requests for a file fail, the phone will fallback to using the current version of the file it has in its own memory.
8. The phone will go through a cycle of requesting files, loading files and then transferring the files into its flash memory.
9. Following file loading, the phone displays **Ext. =**. See Phone Registration 53.

2.7 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 used and that static addressing is avoided. Following any boot file upgrade of the phone's firmware, static address information may require reinstallation.

The use of static address installation is not supported with 4601 and 5601 phones.

1600, 4600 and 5600 Series Phones

1. Follow the steps in Phone Connection 50 until **DHCP** is shown on the phone display. Press * at this point to switch the phone to static address installation. Existing 4600 and 5600 Series phones can be made to start static address installation while idle by pressing **MUTE 27238 2337 #** (**MUTE CRAFT ADDR #**).
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 H.323 gatekeeper. For IP Office systems this is the IP address of the IP Office LAN.
    - **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 LAN. 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 *****. Press **#** to accept the value.
    - **VLAN ID =**
      For details of VLAN configuration see VLAN and IP Phones 63.
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.
7. The phone registration 53 menu is displayed.

9600 Series Phones

1. When the option *** to program** is displayed, press the * key.
2. When **Enter code** is displayed, enter the administrative procedures passcode and press #. The default passcode is ***CRAFT*** (***27238***).
3. Scroll the menu to **ADDR** and select this option to start the address procedure.
4. The list of required addresses is shown. If the phone had any existing values they are shown. Otherwise if the phone is new or has been cleared 76, all the addresses are set to 0.0.0.0.
5. Set each address in turn by highlighting it and selecting **Change**. Enter the new address value and then select **Save**. To enter a . in IP addresses press *. The values that need to be set 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.
   - **Call Server =**
     This is the address of the H.323 gatekeeper. For IP Office systems this is the IP address of the IP Office LAN.
   - **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 LAN. 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.
   - **HTTP File Server** =
     This is the address of the HTTP file server from which the phone should request software and settings files.
   - **HTTPS File Server** =
     This is the address of the HTTPS file server from which the phone should request software and settings files. The phone will attempt to use this address, if set, before using HTTP.
   - **802.1Q =**
     To change the setting press *****. Press **#** to accept the value.
   - **VLAN ID =**
     For details of VLAN configuration, see VLAN and IP Phones 63.
   - **VLAN Test =**
     When using VLAN, this is the time in seconds the phone will wait from a response from the DHCP server in the VLAN before falling back to normal non-VLAN operation.
6. When all the values are set as required press **Back**.
7. Press **Exit**. The phone will restart using the new values.
8. The phone registration 53 menu is displayed.

2.8 Phone Registration

For new phones and phones that have been reset 75, the phone will request an extension number. If auto-create 47 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 47.

To register a phone:

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.
   - **Password =**
     The password used is as follows:
     - If using auto-create for a new user and extension, just enter any number and press #. The digits entered are not validated or stored by the system.
     - If not using auto-create, enter the **Phone Password** as set in the IP Office configuration for the extension. If a **Phone Password** has not been set, the system checks against the matching user's **Login Code**. Pre-IP Office Release 9.0 systems only use the matching user's **Login Code**.
2. Test that you can make and receive calls at the extension.

2.9 Backup/Restore Settings

1600 and 9600 Series H.323 IP Telephones support using an HTTP server as the location to which they can backup and restore user-specific data. The address for this backup server is set separately from that of the file server used for phone firmware.

These options are used if the location of the HTTP server for backup/restore has been specified in the phone ***46xxsettings.txt*** 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.
- If the IP Office system is being used as the file server for phone installation, it can also be used for the phone backup and restore functions. That includes file auto-generation 24. When using auto-generation, some settings within the restore file are based on the user's IP Office settings. This is therefore the recommended solution where possible.

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 as a prefix to ***_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 user's 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 continue with its existing settings.

Specifying the BRURI Value

If you are using the IP Office system as the file server it is recommended that you also use it as the backup and restore server. This option requires no additional configuration. If there is no ***46xxsettings.txt*** file on the IP Office system, it will auto-generate the file when it is requested by a phone and will include its own IP address as the backup/restore server address. If there is ***46xxsettings.txt*** file on the IP Office system, you can edit the backup/restore server address manually using the process below to set it to match the system's IP address.

If you want to use another server, edit the BRURI value in the ***46xxsettings.txt*** file. You will also need to ensure that the server being used is configured to allow the uploading of files to the specified folder on the server.

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 spaces.
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, 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 programmable, non-volatile memory, which is not overwritten when new firmware is downloaded.

Both the authentication credentials and realm have a default value 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 feature as detailed in the user guide for the specific telephone model.

2.9.1 Example File

The following is an example of a backup/restore file for a 1600 Series phone user. Note that values are not written unless the setting has been changed from its default.

If the backup and restore is being done using file auto-generation 24, those items indicated by ✓ are controlled by values stored and supplied by the user's IP Office settings.

File	Fields	Description
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	**ABKNAME*mmm*** **ABKNUMBER*mmm***	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 call screen on calling on (1) or off (0).
	PHNSCRONALERT	Go to call screen on ringing on (1) or off (0).
	PHNTIMERS	Call Timer on (1) or off (0). ✓
	PHNVISUALALERT	Visual alerting on (1) or off (0). ✓

2.9.2 IIS Server Configuration

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/***.

To configure an IIS server:

1. Go to **Start | Settings | Control Panel | Administrative Tools** and select, depending on the Windows version, **Internet Information Services Manager** or **Internet Information Services**.
2. Right-click on the folder created for backup. 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. Ensure that the **WebDAV** option is set to ***Allowed***.

2.9.3 Apache Server Configuration

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/***.

To configure an Apache server:

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>
    ```

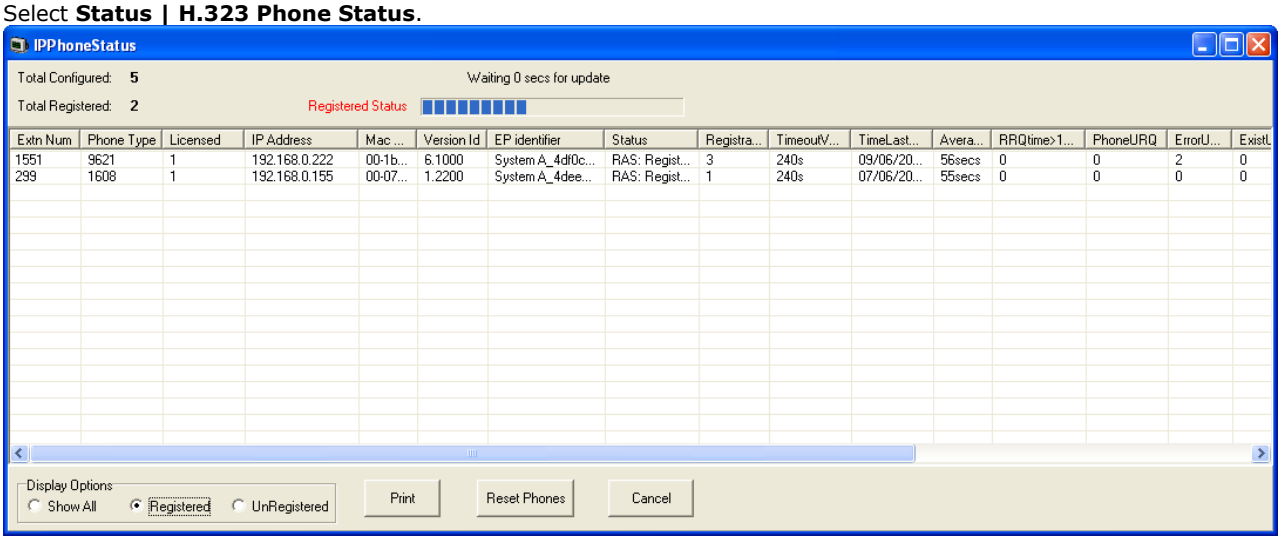
4. For Unix/Linux Web servers the fourth line might look more like: DavLockDB/usr/local/apache2/var/DAVLock
5. Create the **var** directory and make it writable by everyone. Right-click **Properties** and select **Security | Add | Everyone | Full Control**.

2.10 Listing Registered Phones

The IP Office System Monitor application can be used to check which phones are registered with the system.

To view registered phones in System Monitor:

1. Start IP Office System Monitor and connect to the IP Office system.
2. Select **Status | H.323 Phone Status**.



IP Office System Monitor 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. The following appears as lines of the form:

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

2.11 Screensaver

After a set idle time, 9600 Series phones can display a screen saver image. Whilst the phone remains idle, this image is moved to another random position on the screen every 5 seconds.

For phones being fully supported by the IP Office system, a default file is automatically provided by the IP Office system by default. If otherwise:

- The timeout for the screensaver and the name of the image file are set through customizing the 46xxsettings.txt file.
- The image file to use must be loaded onto the file server used by the phones.

Image Requirements

- **Format:** JPG images.
- **Maximum Pixel Size:**
  The image must be smaller than the screen size of the phone. If the image is larger, it will not be displayed. When several types of phones are present using the same image, the image must be below the size maximums of all the phone type. If using the 46xxsettings.txt file to specify the screen saver settings, it is possible to specify a separate image for each phone type.

Phone	Maximum Size	Phone	Maximum Size	Phone	Maximum Size
9611	160x160	**9621G**	320x160	**9650**	320x240
9620	320x160	**9630**	320x240	**9650C**	320x240
9620L	320x160	**9640**	320x240		
9620C	320x160	**9641G**	320x240		

- **Color Displays:** Color depth is 16 bit. A separate color image looks best.
- **Non-Color Displays:** Best results are achieved with a single grayscale logo image. 2 levels of grayscale are also supported.
- **Transparency:** To invoke a transparent background, use a background color of 0,255,0 (brightest possible green).

Replacing the Default System File

The default IP Office settings use an image file called ***96xxiposs.jpg***. Using the embedded file manager 43 within IP Office Manager, replace the existing file in the system's **/primary** folder with your custom image.

Reboot the phones in order for them to load the new image.

Customized Operation

Default operation uses the single image *96xxiposs.jpg* which you can replace with your own image. If using a *customized 46xxsettings.txt* 42 file, you can implement set the idle timeout for displaying the screensaver and the image name.

1. Create a customer JPG file meeting the requirements specified above. For this example we used the file name *logo.jpg*.
2. Download the current ***46xxsettings.txt*** file from the file server being used by the phones.
3. Add the following lines to the ***46xxsettings.txt*** file:

   ```
   ## SET SCREENSAVER filename
   SET SCREENSAVER logo.jpg

   ## SET SCREENSAVERON time in minutes before activating
   SET SCREENSAVERON 40
   ```

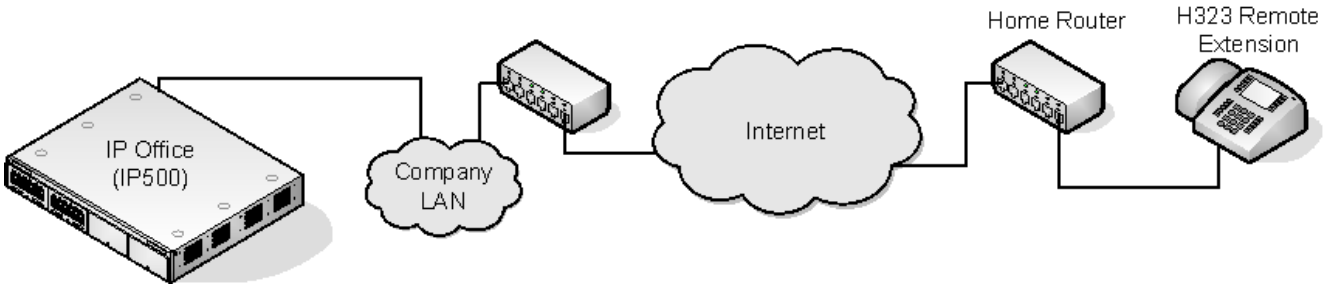
   - Using Separate Images for Each Phone Type
     Added the above to the start of the file affects all types of phone. Adding different settings to each of the different MODEL4 sections of the file for each phone type allows separate images to be used for each phone type.
4. Upload the new files to the file server used by the phones.
5. Reboot the phones in order for them to load the new settings and image.

2.12 Other Installation Options

2.12.1 Remote H.323 Extensions

For IP Office Release 8.0+, the configuration of remote H.323 extensions is supported without needing those extensions to be running special VPN firmware. This option is intended for use in the following scenario:

- The customer LAN has a public IP address which is forwarded to the IP Office system. That address is used as the call server address by the H.323 remote extensions.
- The user has a H.323 phone behind a domestic router. It is assumed that the domestic router allows all outbound traffic from the home network to pass through and allows all symmetric traffic. That is, if the phone sends RTP/RTCP to a public IP address and port, it will be able to receive RTP/RTCP from that same IP address and port. Configurations otherwise are not covered by this documentation.



  - The system can be configured to support remote H.323 extensions in the case where NAT is used in the connection path. This could be the case where the IP Office is located behind a corporate NAT/Firewall router and/or the H.323 phone is located behind residential NAT enable router. The use of this option and the interaction and configuration of external third party elements is beyond the scope this help file.
  - When the public IP address of the corporate router is unknown, you need to configure a STUN server in the the IP Office LAN's **Network Topology** settings. Note however that this option is not supported if the **Firewall/NAT Type** is set to ***Symmetric Firewall*** or ***Open Internet***.
  - Enabling the **Allow Remote Extn** option also makes visible the configuration of the **RTP Port number Range (NAT)** settings.
- **Supported Telephones**
  Currently, remote H.323 extension operation is only supported with 9600 Series phones already supported by the IP Office system.
- **License Requirements**
  By default, only 4 users can be configured for remote H.323 extension usage. Additional users can be configured if those additional users are licensed and configured with either ***Teleworker*** or ***Power User*** user profiles.

Customer Network Configuration

The corporate LAN hosting the IP Office system requires a public IP address that is routed to the LAN interface of the IP Office system configured for remote H.323 extension support.

STUN from the IP Office system to the Internet is used to determine the type of NAT being applied to traffic between the system and the Internet. Any routers and other firewall devices between the H.323 phone location and the IP Office system must allow the following traffic.

Protocol	Port	Description
ICMP	**–**	Incoming ICMP to the IP Office system's public IP address must be allowed.
UDP	**1719**	UDP port 1719 traffic to the IP Office system must be allowed. This is used for H225 RAS processes such as gatekeeper discovery, registration, keepalive, etc. If this port is not open the phone will not be able to register with the IP Office system.
TCP	**1720**	TCP port 1720 traffic must be allowed. This is used for H.225 (call signalling). The address used can be adjusted using the **Remote Call Signaling Port** setting.
RTP	**Various**	The ports in the range specified by the system's **RTP Port Number Range (NAT)** settings must be allowed.
RTCP		
UDP	**5005**	If the system setting **Enable RTCP Monitoring on Port 5005** has been enabled, traffic on this port must be allowed to include remote H.323 extensions in the monitoring.

User Network Configuration

It is assumed that the domestic router allows all outbound traffic from the home network to pass through and allows all symmetric traffic. That is, if the phone sends RTP/RTCP to a public IP address and port, the router will allow it to receive RTP/RTCP from that same IP address and port.

IP Office System Configuration

This is a summary of the necessary IP Office system configuration changes. This section assumes that you are already familiar with IP Office system and H.323 IP telephone installation 28.

1. **Licensing**
   If more than 4 remote extension users are to be supported, the system must include available ***Teleworker*** and or ***Power User*** licenses for those users.

2. **System Configuration**
   The following needs to be configured on the IP Office system LAN interface to which the public IP address is routed.

   a. Select **System | LAN1/LAN2 | VoIP**. Check that the **H.323 Gatekeeper Enable** setting is selected.

   b. Due to the additional user and extension settings needed for remote H.323 extension configuration, we assume that the extension and user entries for the remote H.323 extensions and users are added manually.

   c. Select **H.323 Remote Extn Enable**.

   d. Set the **Remote Call Signalling Port** if a different value from the default is required. The default 1720 matches the port also used by internal extensions.

   e. Set the **RTP Port Number Range (NAT)** to encompass the port range that should be used for remote H.323 extension RTP and RTCP 32 traffic. The range setup must provide *at least two ports per extension being supported*.

3. **Network Topology Configuration**
   STUN can be used to determine the type of NAT/firewall processes being applied to traffic between the IP Office system and the Internet.

   a. Select the **Network Topology** tab. Set the **STUN Server IP Address** to a known STUN server. Click **OK**. The Run STUN button should now be enabled. Click it and wait while the STUN process is run. The results discovered by the process will be indicated by **!** icons next to the fields.

   b. If STUN reports the **Firewall/NAT Type** as one of the following, the network must be reconfigured if possible, as these types are not supported for remote H.323 extensions: ***Static Port Block***, ***Symmetric NAT*** or ***Open Internet***.

4. **H.323 Extension Configuration**
   H.323 remote extensions use non-default settings and so cannot be setup directly using Auto-create.

   a. Within Manager, add a new H.323 extension or edit an existing extension.

   b. On the **Extn** tab, set the **Base Extension** number.

   c. The other settings are as standard for an Avaya H.323 telephone. Regardless of direct media configuration, direct media is not used for remote H.323 extensions.

5. **User Configuration**
   The following settings are used to specify whether a user is allowed to use a remote H.323 extension.

   a. On the **User** tab, set the **User Profile** to ***Teleworker*** or ***Power User***.

   b. Select **Enable Remote Worker**.

Phone Configuration

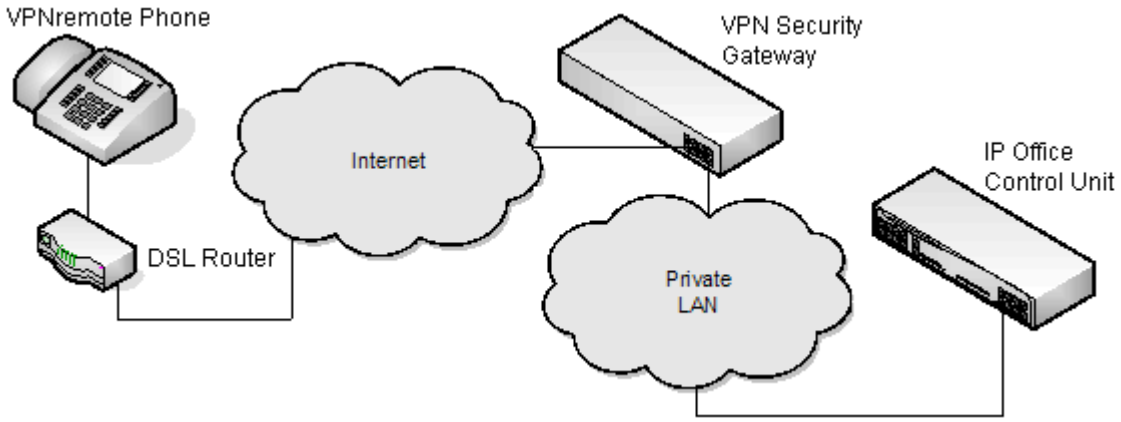
The phones do not require any special firmware. Therefore, they should first be installed as normal internal extensions, during which they will load the firmware provided by the IP Office system.

Once this process has been completed, the address settings of the phone should be cleared and the call server address set to the public address to be used by remote H.323 extensions.

It is assumed that at the remote location, the phone will obtain other address information by DHCP from the user's router. If that is not the case, the other address setting for the phone will need to be statically administered to match addresses suitable for the user's home network.

2.12.2 VPN Remote Phones

Avaya IP phones at remote locations can be connected to the IP Office system via IPSec VPN tunnels. This is supported for 4610SW, 4621SW, 5610SW and 5621SW phones. It is also supported for 9600 Series phones.



Additional components required for remote phones over VPN are:

1. **IP Office VPNremote Phone Firmware**
   This firmware is included with the IP phone firmware set.
2. **VPN Security Gateway**
   The IP Office system does not support all the IPSec features needed for VPNremote phones using its own IPSec tunnels. Therefore the VPN tunnel from remote phones must end at a suitable alternate VPN gateway device. The device 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) Avaya VSU Series (3.2 firmware or higher)

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

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

Title	Doc Reference
VPNremote for the 4600 Series IP Telephones Administrators Guide	19-600753
VPN Setup Guide for 9600 Series IP Telephones	16-602968
VPNremote for 4600 Series IP Telephone User Installation and Configuration Quick Start - Self Installer	19-602363

Supported VPNremote Phone Firmware

Unless otherwise advised, only the firmware provided on the IP Office Administrator Applications DVD should be used for VPNremote phones connected to an IP Office. That firmware is tested with the IP Office release 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.

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 the extensions that are VPNremote and therefore require use of a license.

1. Using IP Office Manager, retrieve 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 VPNremote 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.

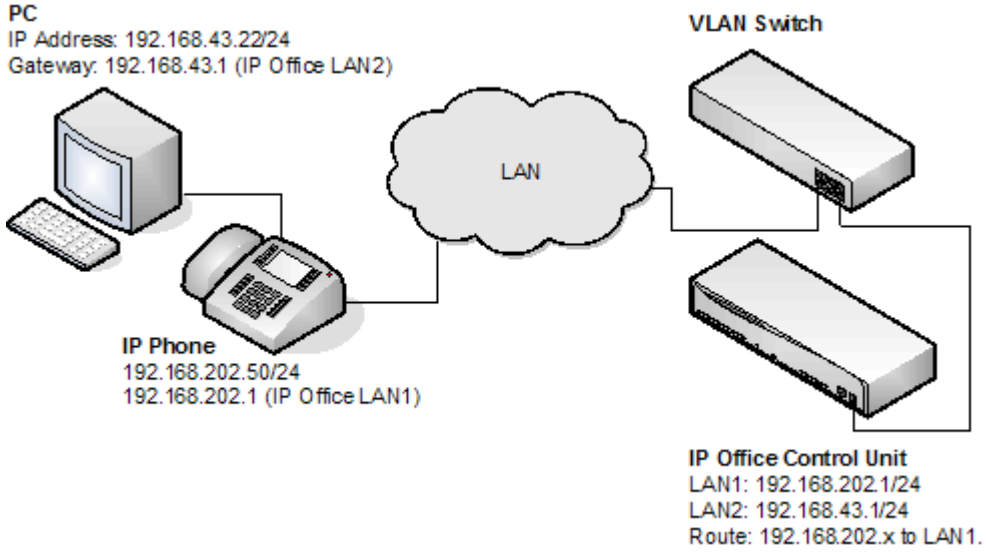
In order to inform 4600 Series VPNremote phones to use IP Office licensing, the following line must be added to the ***46vpnsettings.txt*** file:

- SET SMBLIC 1

2.12.3 VLAN and IP Phones

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 PCs 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 prioritization 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 since 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 (2) ports per user; one for IP Phone and one for PC)
Physical VLAN	Separate VLAN for data and voice	Simple configuration	Requires two (2) 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 PCs. 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)	Manual 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 first makes a DHCP request without a VLAN tag.

- If the DHCP reply contains a new VLAN setting as part of the SSON scope, the phones will release all its existing IP address and makes a new DHCP request using the newly supplied VLAN ID
- If the IP Phone does not get a new VLAN ID, it will continue with the settings provided in the original DHCP reply

A VLAN ID can also be passed to a phone through the ***46xxsettings.txt*** file that it loads. Again the IP phone will release all its existing IP parameters and then make a new DHCP request using the newly supplied VLAN ID.

In the example below, the when the IP phones receives a DHCP response from the DHCP server on the data VLAN, that response contains the VLAN ID of the voice VLAN. The phone then releases the original data VLAN settings it obtained and sends a new DHCP request to the voice VLAN.

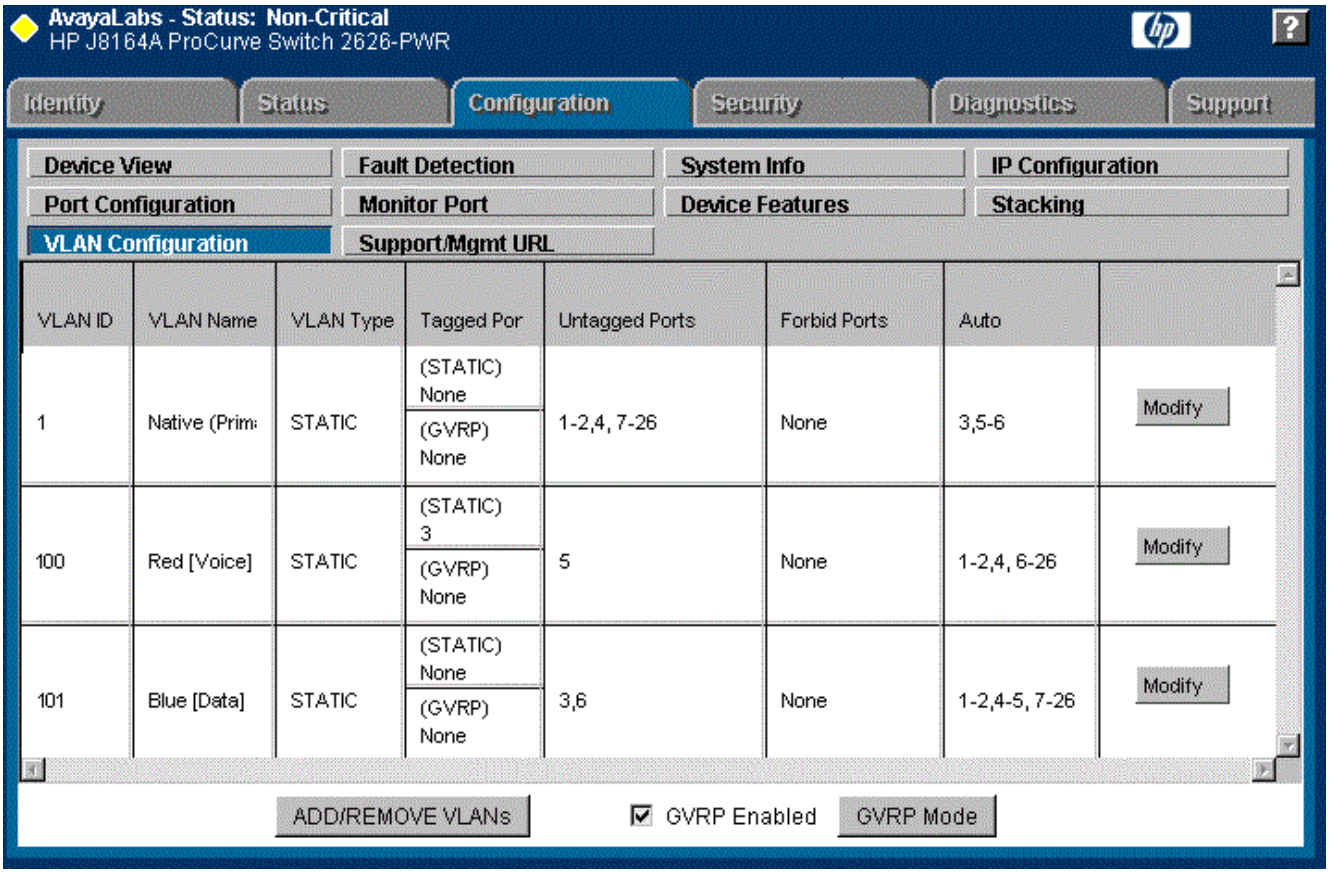
Option	Data VLAN DHCP Settings	Voice VLAN DHCP Settings
IP Address	192.168.43.x	192.168.202.x
Mask	255.255.255.0	255.255.255.0
Router	192.168.43.1	192.168.202.1
SSON Scope	L2Q=1, L2QVLAN=202, VLANTEST=0	MCIPADD=192.168.202.1, MCPORT=1719, HTTPSRVR=192.168.202.X VLANTEST=0
The **VLANTEST** parameter is the length of time the IP Phone should make 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 100 is used for voice traffic and VLAN 101 is used 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. Communication between the voice and data VLANs 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 were obtained using the configuration guidelines found below.



HP Procurve CLI output

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

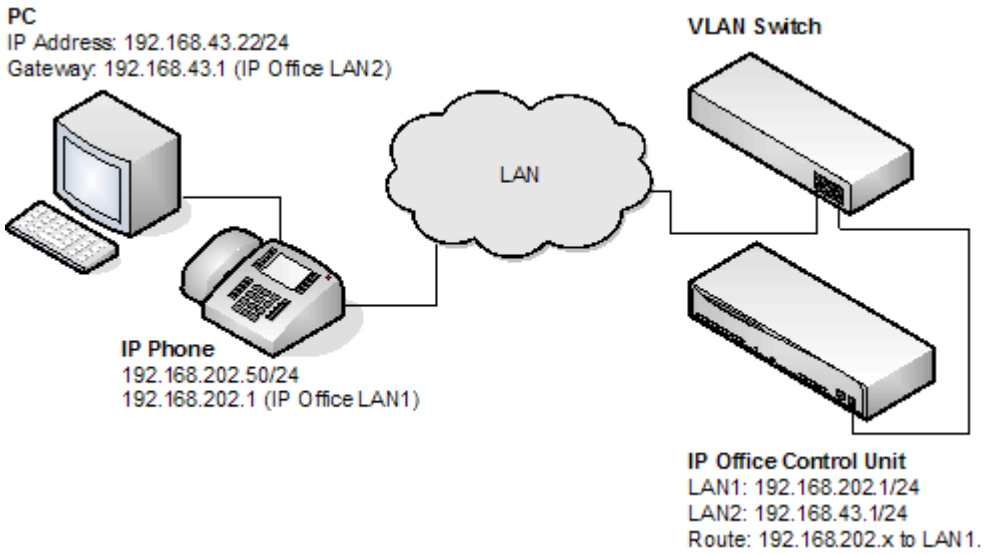
hostname "AvayaLabs"
snmp-server community "public" Unrestricted
vlan 1
name "Native"
untagged 1-2,4,7-26
ip address 192.168.202.201 255.255.255.0
no untagged 3,5-6
exit
vlan 100
name "Red [Voice]"
untagged 5
tagged 3
exit
vlan 101
name "Blue [Data]"
untagged 3,6
exit
gvrp
spanning-tree
```

The table below summaries the HP configuration for ports and VLANs.

Port	VLAN 209 Voice	VLAN 210 Data	Description
3	**Tagged**	**Untagged**	This port was added to both VLAN 100 and VLAN 101. **Note:** When adding port 3 to VLAN 100 the Mode option must be tagged, but it must be untagged when adding to VLAN 101.
5	**Untagged**	**–**	This port is included only in VLAN 100 and not included in VLAN 101. The Mode option must be set to Untagged for port 5 in this VLAN.
6	**–**	**Untagged**	Port 6 is included only in VLAN 101 and not included in VLAN 100. 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**.

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 of 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
In the example below, the IP phone was configured with fixed IP addressing.

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	100

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

Port	VLAN 100 Voice	VLAN 101 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
From the port on which the PC and IP phone reside, you can receive two types of Ethernet frame (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 101. This is because when we added the port 3 to VLAN 101 the **Mode** option was specified as untagged. While for the other VLAN (101) the option **Tagged** was selected for port 3 in VLAN 101. Tagged packets will thereby go to VLAN 100 while the untagged will go to 101.

When a packet originates from an IP Phone it is tagged. Since the option 'untagged' is selected for port 5 in VLAN 100, 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 3.

Static Administration Options

3. Static Administration Options

A number of settings can be altered through the phone after installation. These procedures should only be used if you are using static address installation. Do not use these procedures if you are using DHCP except if you are attempting to reassign a phone that has been previously statically installed.

- To set parameters for all H.323 IP phones on a system, you can edit the ***46xxsettings.txt*** script file. However, values assigned through static administration override any set through the ***46xxsettings.txt*** file. They remain active for the IP phone until a new boot file is downloaded.
- This section of documentation only includes a subset of the administration options. For a full list refer to the appropriate LAN administrator's manual:
- **Installing and Maintaining Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323**
  http://support.avaya.com/css/P8/documents/101009345
- **Administering Avaya 9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones H.323**
  http://support.avaya.com/css/P8/documents/101009361
- **VPN Setup Guide for 9600 Series IP Deskphones** *(16-602968)*
  http://support.avaya.com/css/P8/documents/101008050
- **Avaya one-X Deskphone Edition for 9600 Series IP Telephones Application Programmer Interface (API) Guide** *(16-600888)*
  Covers the configuration and use of WML and PUSH interfaces with 9600 Series telephones.
  http://support.avaya.com/css/P8/documents/100165678

Using Static Administration Options

The method used to access static administration depends on the type of phone. Many of the static administration features are accessed using key sequences that begin by pressing either **MUTE** or **HOLD**. In recent firmware releases, preference has been given to using **MUTE** and some phones, for example the 1600 Series, only support **MUTE**.

1600, 4600 and 5600 Series Phones

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

1. With the phone idle, press **MUTE**. After pressing **MUTE**, if a valid button is not pressed within 6 seconds of the previous button the collected digits are discarded and the phone returns to idle.
2. Dial **27238** (**CRAFT**).
3. Dial the digits for the required command followed by **#**.
   - Attempts to enter invalid data are rejected and the phone emits an error beep.
   - 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.
   - To go to the next step, press **#**.
   - 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.

9600 Series Phones

Administrative procedures for 9600 Series phones can only be accessed by restarting the phone.

1. While the phone is on-hook and idle, press the following sequence: **MUTE 27238 # (MUTE CRAFT #)**.
2. Scroll the menu to the action required and select it.
3. When the selected procedure is finished, the phone will return to the procedures menu.
4. When all the required procedures have been completed, press **Exit**. The phone will restart using the new settings.

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

Use the following procedure to enable or disable the hub interface found on many Avaya IP phones which can be used for user PC connection 20. The hub interface is set to **enabled** by default.

For 4600 Series and 5600 Series phones, the procedure below can also be used to enable or disable the IR port found on some H.323 IP phones; see Infrared Dialling 82.

For 9600 Series phones, the procedure below also allows you to adjust the port speed and duplex setting of the PC port and the phone's LAN port.

1600, 4600 and 5600 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 27238 468 #** (**MUTE CRAFT INT #**). The phones port settings are shown in sequence. The options 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 H.323 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 the set returns to normal operation.

9600 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 27238 # (MUTE CRAFT #)**.

2. Scroll the menu to **INT**.

3. Select the port that you want to adjust. The options are **Ethernet** and **PC Ethernet**.

4. Use the < and > buttons to scroll through the port's possible settings. The additional option ***Disabled*** is available for the PC Ethernet port.

5. Press **Save**.

6. Select another procedure or press **Exit** to restart the phone.

3.2 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.

1600, 4600 and 5600 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 27238 8439 #** (**MUTE CRAFT VIEW #**).
   - To display the 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 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 H.323 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 Phone 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.

9600 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 27238 # (MUTE CRAFT #)**.
2. Scroll the menu to **VIEW** and start the procedure.
   - **Model -** Shows the phone's model number; for example, 4624D02A.
   - **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 -** Shows the phone's MAC address as paired hexadecimal numbers.
   - **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 Phone LAN Administrator Guide.
   - **Protocol -** Display ***Default***.
   - **Application File -** 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.
   - **Ethernet -** Shows the speed of the detected LAN connection.
   - **Boot File -** Shows the boot file name and level. These are values from within the boot file loaded and not the actual file name.
   - **Proxy Server -** Shows the details of the selected proxy server.
   - **Voice Language File** - The name of the language file the phone is using. This is blank when using the phone's default language (English).
3. Press **Back**.
4. Select another procedure or press **Exit** to restart the phone.

3.3 Self-Test Procedure

1600, 4600 and 5600 Series Phones

1. To start the IP phone self-test procedure, press the following sequence: **MUTE 27238 8378 #** (**MUTE CRAFT TEST #**). The phone does the following:
   - Each column of programmable button LEDs 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.

9600 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 27238 # (MUTE CRAFT #)**.
2. Scroll the menu to **Test**.
3. Press **Test** again to confirm the action.

3.4 Resetting a Phone

Resetting a phone resets all the system values and most of the system initialization values. The procedure does not affect user-specified data and settings (e.g. Contact data, Options settings, login extension or password, etc.). To remove all such data, refer to Clearing a Phone 76.

1600, 4600 and 5600 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 27238 73738 #** (**MUTE CRAFT RESET #**). **Reset values?** is displayed.
2. To cancel this procedure press *****. To continue press #.
   - **! WARNING**
     As soon as you press **#**, all static information is 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 78.

9600 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 27238 # (MUTE CRAFT #)**.
2. Scroll the menu and select **Reset Values**.
3. Press **Reset** to confirm the action. The phone user settings are reset as the phone restarts.

3.5 Clearing a Phone

Clearing all system initialization values back to their default settings and deleting all user-specific data is intended primarily for repair and for use when the phone is given to a new user. This returns the phone near to its original, out-of-box state. The phone will yet retain the firmware files it has already downloaded.

Note: Some parameters, such as button clicks, error tones, and personalized ringing, may be set for a specific user via the **MENU**. These user settings will be restored when you register the user to the phone because those parameters are configured in IP Office. All other settings (e.g. Contact data, Options settings, etc.) will be cleared from the phone.

1600, 4600 and 5600 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 27238 25327 #** (**MUTE CRAFT CLEAR #**). **Clear all values?** is displayed.
2. To cancel this procedure press *****. To continue press #.
   - **! WARNING**
     As soon as you press #, all static information is 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 it is a new phone.

9600 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 27238 # (MUTE CRAFT #)**.
2. Scroll the menu and select **Clear**.
3. Press **Clear** again to confirm the action. The phone settings are cleared and the phone restarts.

3.6 Site Specific Option Number

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

The default SSON used by Avaya 4600 and 5600 Series phones is **176**. The default SSON used by Avaya 1600 Series and 9600 Series phones is **242**. For phones being supported by IP Office DHCP, the SSON used by the phone must match one of the site specific option numbers set in the IP Office configuration 39.

- **! 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.

1600, 4600 and 5600 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 27238 7766 #** (**MUTE CRAFT SSON #**). **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.

9600 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 27238 # (MUTE CRAFT #)**.
2. Scroll the menu to **SSON** and start the procedure.
3. Enter the new SSON number that the phone should use when it next restarts.
4. Press **Save**.
5. Select another procedure or press **Exit** to restart the phone.

Chapter 4.
Restart Scenarios

4. Restart Scenarios

The sequence of the restart process depends on the version of the phone boot file already downloaded to the phone as well as those on the file server. This appendix explains the different scenarios possible.

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

Restart scenario:

1. After power is applied, the phone displays **Restarting...** followed by **Initializing...**.
2. 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.
3. When control is passed to the code in RAM, **Starting** is displayed.
4. 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.
5. 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.
6. Once DHCP has completed successfully, the phone will request files from the file server indicated in the DHCP response. The first file requested details the other files that the phone should also load. The phone will first make its file request using HTTPS. If this fails it will make the same request using HTTP. If that fails it will make a final request using TFTP. If all requests for a file fail, the phone will fallback to using the current version of the file it has in its own memory.
7. After the upgrade script is loaded, the sequence depends on the status of the files currently held in the phone's memory, compared to those listed in the upgrade script file.
   - **Boot File Needs Upgrading** 79
   - **No Application File or Application File Needs Upgrading** 79
   - **Correct Boot File and Application File Already Loaded** 79

4.1 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.

Restart scenario:

1. The phone displays the file name and the number of kilobytes loaded.
2. 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.
3. The phone displays **Restarting** as it prepares to reboot using the new boot file.
4. The phone displays **Initializing**.
5. 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.
6. When control is passed to the software that has just loaded, the phone displays **Starting**.
7. 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.
8. Updating is displayed whilst the boot code is rewritten. The phone also displays the percentage of boot code rewritten and the number of elapsed seconds.
9. 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 79.

4.2 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.

Restart scenario:

1. The phone displays the required file name as it downloads the file from the TFTP server. It also displays the number of kilobytes downloaded.
2. **Saving to flash** is displayed. The phone also displays the percentage of file stored and the number of seconds that have elapsed. This will usually take longer than it took to download the file.
3. 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 79.

4.3 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.

Restart scenario:

1. 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 is checked against is the extension's **Phone Password** stored in IP Office Manager. If a **Phone Password** has not been set, the system will also check the matching user's **Login Code**. Pre-IP Office Release 9.0 systems only use the matching user's **Login Code**.
2. Upon completion of registration, a dial-tone is available on the phone if it has also been able to obtain an **Avaya IP Endpoint** license.

Chapter 5.
Infrared Dialing

5. Infrared Dialing

Some H.323 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 five (5) feet (or 1.5 meters) with a 5° degree spread (this is unlike IR devices used for remote controls which typically beam over a longer range and have a wider angle spread).
- For details of enabling and using IR beaming from your personal organizer or PC, refer to the manufacturer's information.

Notes:

- 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.

5.1 Enabling the IR Port

By default, where fitted, the IR port on H.323 IP phones is enabled. If necessary it can be disabled.

To change the IR port setting:

1. With the phone on-hook and idle, press **MUTE 27238 468 # (MUTE CRAFT INT #)**. **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.

5.2 Dialing 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.

5.3 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 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 extension's 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 6.
Alternate DHCP Server Setup

6. Alternate DHCP Server Setup

The recommended installation method for H.323 IP phones uses a DHCP server. This section outlines by example, the basic steps for using a Windows server as the DHCP server for IP phone installation. The principles of defining a scope are 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 H.323 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 H.323 IP phones during installation)

6.1 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 IP telephone attempts to resolve the DNS address. Option 15 is necessary if you want to use a DNS name for the HTTP server.
- **Option 51 - DHCP Lease Time**
  If this option is not received, the DHCP offer is not accepted. Avaya recommends a lease time of six (6) 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.
  - Provide enough leases so that 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.
  - 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 (5) 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 name 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: On H.323 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.

6.2 Checking for DHCP Server Support

To check the DHCP server support:

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.

If the DHCP server role is supported, the first stage is to create a scope 88 of addresses for use by IP phones.

6.3 Creating a 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.

To create a scope:

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 by entering a range (e.g. 200.200.200.5 to 200.200.200.7) and clicking **Add**, or by 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 addresses. 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 set to ***Inactive***.

Having created the scope that will be used by the IP phones, a set of options 89 need to be added matching the Site Specific Options Number (SSON) that the phones will use. The SSON used by 1600 and 9600 Series phones by default is 242.

6.4 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 and 9600 Series H.323 IP phones use SSON 242 to request additional information from a DHCP server. The option should include defining the address of the phone's H.323 gatekeeper (the IP Office) and the address of the HTTP file server.

To add a 242 option:

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=*** the H.323 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 H.323 gatekeeper.
     Note: The phones will wait three (3) minutes before switching to the fallback and will not switch back when the first server recovers, until the phone is rebooted.
   - ***MCPORT=*** the RAS port address for initiating phone registration. The default is 1719.
   - ***HTTPSRVR=*** the HTTP file server IP address.
   - ***HTTPDIR=*** 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.
   - 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 87.
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 and 9600 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**.

Having created a 242 option and associated with the scope we want used by the IP phones, we now need to activate the scope 91.

6.5 Adding a 176 Option

4600 and 5600 Series H.323 IP phones use SSON 176 to request additional information from a DHCP server. The option 176 scope can be set up to use the same HTTP file server as shown for 1600 Series phones in the previous example 89. However, some older 4600 Series H.323 IP phones only support TFTP so the options for a TFTP scope are shown below.

To add a 176 option:

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=*** the H.323 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 H.323 gatekeeper.
     Note: The phones will wait three (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.
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 87.
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**.

6.6 Activating 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 H.323 IP phones using DHCP. If Manager is being used as the HTTP or TFTP server, ensure that it is running on the specified PC.

Chapter 7.
WML Server Setup

7. 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 full details of WML support and setup refer to **Avaya one-X Deskphone Edition for 9600 Series IP Telephones Application Programmer Interface (API) Guide** *(16-600888)*.

7.1 Setting the Home Page

WAP-capable H.323 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 hosts 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 to 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 to ***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.

7.2 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.

7.3 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.

7.4 Open URL Entry

This section provides sample WML coding on how to develop WML pages implementing a go-to URL function in the form of a text box. 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>
```

Chapter 8.

SRTP

8. SRTP

For IP Office Release 9.1, SRTP is supported.

- **Support IP Office Modes:**
  SRTP is supported in all IP Office modes except Basic Edition modes.
- **Supported Phones:**
  It can be applied to SIP and H323 extensions. However, there may be restrictions for some specific models of IP telephone.
  - Supported for H323 on 96x1 Series telephones.
  - Supported for SIP on Avaya and 3rd-party telephones.
- **Supported Trunks:**
  It can be applied to all types of IP lines (SIP, SM and IP Office (SCN)) except external H323 trunks.
- **Licensing and Capacity:**
  The use of SRTP does not require any licenses. However, the use of SRTP impacts on the call capacity of the IP Office system.
  - For IP500 V2 systems with IP500 VCM cards, those cards are used to support SRTP and reduce the impact on the system call capacity. This does not apply to combination cards.

8.1 Enabling System SRTP

By default, all IP extensions and lines are configured to automatically match the top-level system settings for SRTP, whether disabled or enabled. This simplifies enabling SRTP by ensuring that all devices are using the same SRTP settings. Using this approach, once SRTP is enabled, the only device level configuration required is to disable SRTP on those lines or devices for which it is not required.

The exception to the above is SIP lines for which SRTP is disabled by default. This is due to the low number of SIP line providers who currently support SRTP. However, SIP lines can be configured to also match the system level settings if required.

To enabled system level SRTP:

1. Receive the configuration from the system.
2. Click **System** and select the **VoIP Security** tab.
3. For **Media Security**, select the level of STRP operation required:
   - **Disabled**
     STRP is not used for connections.
   - **Best Effort**
     Support both RTP and SRTP. Use SRTP if matching SRTP settings can be negotiated with the remote end end. This requires the remote end to support srtp rfc5939 (capability negotiation for SRTP). Otherwise use RTP. Note that E129 phones does not support **Best Effort**.
   - **Enforce**
     Use SRTP only. The call is not allowed if the remote leg does not support matching SRTP.
   - **Advanced Settings**
     After selecting either ***Best Effort*** or ***Enforce*** as the STRP method, it is recommended that all other SRTP settings are left at their defaults. The default SRTP flags and crypto suite settings were chosen so that they work with all Avaya H323 and SIP devices. For example, the majority of Avaya implementations don't support RTCP encryption and Avaya H323 phones only support the SHA_80 crypto suite.
4. Click **OK**.

To disable SRTP on an extension or line:

1. Click on **Extension** or **Line** and select the required extension or line.
2. Select the **VoIP** tab.
3. Change the **Media Security** setting to ***Disabled***.
4. Click **OK**.
5. Repeat for any other extension or line for which SRTP should not be used.

8.2 Direct Media

If direct media is configured, the system tries to negotiate direct media between the call ends. When SRTP is involved, addition to checking for matching VoIP criteria (for example matching codec support), the system also checks for matching Media Security and media security advanced settings (SRTP flags and crypto suites). Any incompatibility prohibits the call using direct media.

- Calls between call legs set to different **Media Security** levels (***Disabled***, ***Best Effort*** or ***Enforce***) will not use direct media.

Chapter 9.
Document History

9. Document History

23rd January 2014	18c	• Removed WML sections. Added additional requirement for dialing CRAFT in all static administration actions.
28th January 2014	19b	• Correction. 96x1 phones now supported for remote VPN access.
19th January 2014	19c	• Clarification that user Login Code is still checked if extension Phone Password is not set. • Reinforced statements that auto-create options should be disabled after installation.
5th March 2015	20a	• Auto-disable of auto create. • Phone registration password not stored. • Remove references to systems not supported for IP Office Release 9.1. • Added notes on registration blacklisting. • Added screensaver notes.
10th March 2015	20b	• Updated screenshots for 9.1. • Added Remote Call Signalling Port. • Added RTCP collector IP address for phones.
6th May 2015	20c	• Updated 9600 documentation references. • Statement that WML/PUSH API 9 still supported.
15th May 2015	20d	• Update that 96X1 series phones also support SBM24 button modules. Also treat as Class 3 when using button modules (set power switch to **H**) [83673]
20th August 2015	20e	• Minor text correction.
8th October 2015	20f	• Correction to User PC Connections 20 page.
2nd November 2015	20g	• Remove note regarding VCM codec 17 being fixed to G729 for paging.
16th December 2015	20h	• Replace incorrect appearance of <%MIDSZE%> authoring variable.
12th April 2016	20i	• Correction. Number of unlicensed H323 remote extension users is 4.
7th July 2016	20j	• Clarification to the LAN descriptions.
18th October 2016	20k	Clarification around enhanced dialing parameters (not supported).

Index

1

10Mbps 14
1151C1/1151C2 50
1152A1 50
150ms 16

2

25ms 17
264V AC 21

3

3.5W 21
30A Switch Upgrade Base 21
3rd-party
    HTTP 13
    TFTP 23

4

4600 9, 42, 61, 63, 86, 94
4602SW 9, 20, 21
4606 9, 20, 21
    includes 82
4610SW 9, 20, 21, 61, 94
4620 9, 21, 42, 82, 94
    relating 95
4620IP 20
4620SW 9, 20, 61, 94
4621SW 9, 61
    applies 21
4622
    support 9
4624D 21
4624D01 21
4624D02A 72
4625SW 21, 61

5

5602SW 9, 20, 21
5610SW 9, 20, 61, 94
5620SW 9, 20
5621SW 61

6

64ms 17

7

792ms 57

A

AC 21
access point 9
Active Directory using RADIUS 61
address programming 51
AddType 96
administrative options 70, 72
administrative tools 96
Adtran Netvanta 3305 VPN Router 61
Alternate DHCP Servers 13, 28
    Avaya IP 86
Alternate Options 87
Apache 96
Appendix 78
application file 72, 78, 79
Application Notes
    Configuring 61
Applications 16, 23, 61, 72, 75, 78, 79, 95
ASCII
    defaulted 95
ASDM 61
Auto-create Extn Enable 28
auto-negotiated 17
Avaya 9, 16, 20, 21, 23, 24, 61, 63, 86, 95
Avaya 1151C1 21
Avaya 1151C2 21
Avaya 1152A1 Power Distribution Unit 21
Avaya 30A Switch Upgrade Base 20
Avaya 4622SW IP Telephone 61
Avaya Gateways 61
Avaya H.323 IP 9
Avaya P333T-PWR Switch 21
Avaya SG Series 61
Avaya Voice Priority Processor 9
Avaya VSU Series 61
Avaya WebLM 61
Avays VSU Series 61
AVPP 9

B

Backup 19, 21
Beam Address 83
Beam Contact 83
Beaming
    Files During 84
bin/VPN Phone 61
Button Programming 47

C

cabling 14
    Connections 19
call answering 9
Call Server 63
call signalling 17
CallSv 51
CAT3 14, 21
CAT5 14, 19, 21
Catalyst 21
CD 23, 61
CD/DVD 61
Cisco
    Configuring 61
Cisco Adaptive Security Device Manager 61
Cisco Catalyst 21
Cisco PIX 500 Series Security Appliances 61
Cisco PIX Security Appliance
    Configuring 61
Cisco VPN 300 Series Concentrators 61
CLI configuration 63
cmd 57
codecs 17
Compact Flash 24
Compaq iPAQ Pocket PC 83
Computer MIME Map 96
Concentrator 61
configuring 61
    3rd-party 13
    Application Notes 61
    Cisco 61
    File Source 24
    VPNremote 61
Connect 14, 17, 19, 20, 50, 61, 63
Connections 14, 20, 21, 50, 61, 71, 72, 83
    Cabling 19
Contacts 82, 83
Control Panel 96
Control Unit Memory Card
    Using 24

Control Unit Settings 28
Correct Boot File 79
D
Data 16, 17, 19, 20, 21, 50, 51, 63, 75
Default 17, 51, 61, 71, 75, 76, 79, 83, 95
Deployment Guide 61
DHCP 13, 14, 16, 23, 51, 63, 70, 75, 76, 78, 87
  alternate 86
  connection 50
  introduction 9
  preparation 28
DHCP Address Installation 50, 51
DHCP addressing 76
DHCP Options 63, 76
DHCP Relay 63
DHCP Settings 63
DiffServ 19
DiffServ QoS 19
Direct Media 17
DNS 86, 87, 95
Duplicate IP Addressing 19
E
Embedded Voicemail Memory 23
Endpoints 57
End-to-End Matching Standards 19
Enter TFTP 57
Ethernet 19, 63, 78, 83
  Power 21
Ethernet LAN 21
Ethernet Switch 63
Excessive Utilization 19
Extension ID 47
extensions 9, 14, 17, 28, 47, 53, 61, 82, 84, 95, 96
  phone requests 79
  user changes 79
F
File server
  HTTP redirection 12
File Source 24
File Writer 24
FileSv 51
G
G.711 17
G.722 17
G.729a 17
G.729b 17
Gatekeeper 13, 14, 28, 51, 76, 87
GEN 21
H
H.08.60 63
H.232 20
H.323 9, 20, 23
hostname 63
HP 63
HP Procurve 63
HP Procurve CLI 63
HP Procurve Ethernet 2626 PWR Ethernet 63
HP Procurve Switch 63
HTTP redirection 12, 23, 41
I
Idle image 58
IEEE 802.2p/q 63
IEEE 802.3af 20, 21
IIS 96
IIS 5.0 96
IIS Admin Service 96
IKE Extended Authentication 61
index.wml 95
Infrared Dialling 82
Initializing 50, 79
Input Box Followed 97
Internet 61, 96
Internet Information Server 96
Internet Service Manager 96
Introduction 9
IP Gateway 86
IP Mask 51, 63
IP Office Administration CD 28
IP Office Administrator 23, 61
IP Office Embedded Voicemail 23
IP Office IP Endpoint 9
IP Office Licensing 61
IP Office System 9, 13, 16, 17, 24, 57, 61, 75, 83
IP Office TDM 17
IP Office Unit configuration 14
IP Office Unit Memory Card 23
IP Phone Inline Adaptor 21
IP Phone Software 9, 23, 28
IP Telephone 14, 61, 86, 94
IP400 61
IP403 9, 17
IP406 9, 17, 23, 24, 28
IP406 V1 9, 17
IP406 V2 9, 17, 23, 24, 28
IP412 9, 17
IPO 61, 63
IPO LIC 61
IPSets Firmware 23
IR 71, 82, 83, 84
IrDA 82
ISG 61
J
J8164A Configuration Editor 63
JRE 61
Juniper Networks
  Integrated Security Gateway 61
  NetScreen 61
K
Kentrox Q2300 VPN Router 61
L
L2 63
L2 QOS 63
L2Q 63
L2QVLAN 63
LAN 14, 19, 20, 21, 50, 61, 63, 71, 72, 78, 86, 94, 95
LAN Cables 14, 20, 21, 50, 95
LAN Socket 14, 71
LED 21, 74
Licence Keys 14
Listing
  Registered 57
Loading 78, 79
M
M505 83, 84
MAC 61, 72
MAC Address 61, 72
Maintenance Manual 9
Manager application 13, 23, 28, 42, 51, 95
Manager Installation 9, 14

Manager PC 24, 28, 95
MCIPADD 63
MCPORT 63
MG 9
Microsoft 61, 87, 96
Microsoft DHCP 87
Microsoft IIS Web Server 96
Microsoft Internet Information Server 96
Mid-Span Power Unit 21
MIME 96
Minimum Assessment Target 16
Minimum Firmware 61
MMC 96
Mode option 63
multicast 19
Multihomed 63
MultiVantage 86

N

Netgear FVS338 VPN Router 61
Network Access 19
network assessment 9, 16
NIC Cards 63
No Ethernet 50, 78
Non-Avaya 24, 61
non-IP 9, 17, 53
NT 4.0 96

O

Open URL Entry 97
Other H323 IP 9
Overlapping VLAN 63

P

Packet Loss 16
page coding 94
Palm 83, 84
Password 53, 79, 95
PC Ethernet LAN 20
PC Port 20
PC Softphone 9
PC/Handheld
  Ir 83
PC/personal 82
Phone Connection 50
phone displays 53, 79, 95
Phone Manager 9
Phone Security 47
PHY2 71, 83
Pocket PC 83
PoE 21
Potential VoIP Problems 19
power 14, 19, 20, 50, 53, 78
  Ethernet 21
  IP 21
power conditioning 19
power supply
  PSU 14, 19, 21, 50
Pre-Deployment 61
Preferences 28
preinstalled 28
preparation 28, 79
Preshared Key 61
Press Web 95
Print 57, 72
Printed Wiring Board 72
Program 14, 23, 51, 95
Protection 19
Proxy 95
PSK 61
PWB comcode 72

Q

QoS 19
Quality 9, 16, 19

R

RAM 78, 79
RAS 57
Reboot 24, 47, 76, 79, 95
Redirect 12
Registered 61
  Listing 57
registration 53, 79
Reset System Values 75
Resetting 75
Restarting 78
RFA Name 61
RFC2474 19
RJ45 14
  matching 21
  provides 21

S

Sample 95, 97
SAP Code 61
Save 51, 61, 71, 76, 79, 95, 96
Scope 63, 86, 87
Screensaver 58
script file 70, 78, 79
Secondary Ethernet 71
Self Installer 61
Self-Test Procedure 74
Serial Number 72
Setup 47, 63, 75, 78, 83, 95, 96
SG 61
Site Specific Settings 42
Small Installation 13
Small Office Edition 9, 14, 17, 19, 23, 24, 28
SMBLIC 61
Spare Wire 21
Speaker/Mute LED 74
SSON 76
Start Manager 95
static address 9, 23, 28, 50, 51, 70, 72, 78
Static Administration Options 70
Static IP 9, 14, 28
subnet mask 51, 86
support.avaya.com 61
SV 9
SW 20
Sysmon 57
System Overview 63

T

Tag 63, 94, 97
TFTP 23
Timed Out 78
Timeout 23
  Screensaver 58
Tools 23, 42, 57, 83, 96
ToS 19

U

Unix 96
Unrestricted 63
Untagged 63

URL 97

V

VCard 83, 84
VCF 83
VCM 17, 28
    installing 17
    number 9
VCOMP 28
VLAN 51, 63
Voice 9, 14, 16, 17, 19, 20, 28, 63
Voice Compression Module 14, 28
voicemail 19, 24, 47
VoIP 9, 14, 16, 19, 47, 53, 61
VPN 61
VPNremote 61
VSU 61

W

WAN 19
WAP 94, 95
Watts 21
Web 42, 61, 63, 95, 96
WebLM 61
Windows 24, 57, 82, 86, 87, 95, 96
    Windows 2000/Server 96
    Windows Notepad 42
    Windows Pocket PC 83
    Windows XP 96
Wireless Access Protocol 94
Wireless Markup Language 94
Wireless Telephony Application Interface 94
WML 94, 95, 96, 97
Wordpad 57
WTAI 94

X

Xauth 61

© 2016 Avaya Inc. All rights reserved.