



# **IP Office for Linux**

## **H.323 Telephone Installation**

#### Notices

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

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

End User agree 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 Web sites referenced within this site or documentation(s) 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 this product. 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 Web site: <http://www.avaya.com/support>. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

#### Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/LICENSEINFO/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER, AND 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 End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

#### License types

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

#### Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) 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. 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.

#### Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

#### 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 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 Web site: <http://support.avaya.com>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: [securityalerts@avaya.com](mailto:securityalerts@avaya.com).

#### Trademarks

Avaya and Aura are trademarks of Avaya, Inc. The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

#### Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: <http://www.avaya.com/support>

#### Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>

# Contents

## 1. IP Office H.323 IP Phones

1.1 Supported Phones.....	8
1.2 Phone Firmware.....	9
1.3 Simple Installation.....	10
1.4 Installation Requirements.....	11
1.5 Licenses .....	12
1.6 Network Assessment.....	13
1.7 QoS .....	14
1.8 Potential VoIP Problems.....	14
1.9 User PC Connection.....	15
1.10 Power Supply Options.....	16
1.11 File Server Options.....	17
1.12 File Auto-Generation.....	19

## 2. Installation

2.1 Licensing .....	23
2.1.1 Checking the Serial Number.....	23
2.1.2 Adding Licenses.....	24
2.1.3 Reserving Licenses.....	24
2.2 System H.323 Support.....	25
2.2.1 Enabling the H.323 Gatekeeper.....	25
2.2.2 Setting the RTP Port Range.....	26
2.2.3 Configuring SRTP.....	27
2.2.4 Enabling RTCP Quality Monitoring.....	28
2.2.5 Adjusting DiffServ QoS.....	30
2.2.6 System Default Codecs .....	31
2.3 DHCP Settings.....	32
2.3.1 System DHCP Support.....	34
2.3.2 System Site Specific Option Numbers.....	35
2.4 File Server Settings.....	36
2.4.1 System File Server Settings.....	37
2.4.2 Creating/Editing the Settings File.....	38
2.4.3 Loading Software Files onto the System.....	40
2.4.4 Loading Files onto a 3rd Party Server.....	41
2.5 User and Extension Creation.....	42
2.5.1 Auto-Creation.....	42
2.5.2 Manually Creating User.....	43
2.5.3 Manually Creating Extensions.....	43
2.6 Phone Connection.....	45
2.7 Static Address Installation .....	46
2.8 Phone Registration .....	48
2.9 Backup/Restore Settings.....	49
2.9.1 Example File .....	50
2.9.2 IIS Server Configuration.....	51
2.9.3 Apache Server Configuration.....	51
2.10 Listing Registered Phones.....	52
2.11 Other Installation Options.....	52
2.11.1 Remote H.323 Extensions.....	52
2.11.2 VLAN and IP Phones.....	55

## 3. Static Administration Options

3.1 Secondary Ethernet (Hub)/IR Interface Enable/Disable.....	59
3.2 View Details .....	60
3.3 Self-Test Procedure.....	62

3.4 Resetting a Phone.....	63
3.5 Clearing a Phone.....	64
3.6 Site Specific Option Number.....	65

## 4. Restart Scenarios

4.1 Boot File Needs Upgrading.....	69
4.2 No Application File or Application File Needs Upgrading .....	69
4.3 Correct Boot File and Application File Already Loaded .....	69

## 5. Alternate DHCP Server Setup

5.1 Alternate Options.....	73
5.2 Checking for DHCP Server Support.....	74
5.3 Creating a Scope.....	74
5.4 Adding a 242 Option.....	74
5.5 Activating the Scope.....	75
Index .....	77



# **Chapter 1.**

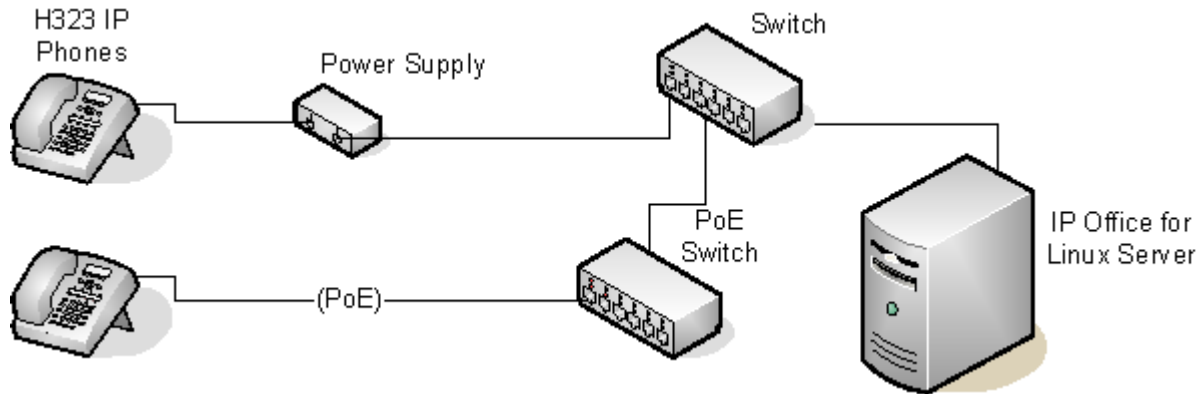
## **IP Office H.323 IP Phones**



# 1. IP Office H.323 IP Phones

This documentation provides notes for the installation of [supported Avaya IP phones](#)<sup>[8]</sup> onto an IP Office for Linux system. It should be used in conjunction with the existing installation documentation for those series of phones, especially the following:

- [9600 Series IP Telephones Administrator Guide](#) (16-300698)
- [1600 Series IP Telephones Administrators Guide](#) (16-601443).



- **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 may refuse to support any installation where the results of a network assessment cannot be supplied. See [Network Assessment](#)<sup>[13]</sup> for further details.

---

## 1.1 Supported Phones

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

Other Avaya IP phones, for example 3600 Series phones used on DECT R4 are covered by separate installation documentation.

H.323 IP Phones	Supported Models	802.3af PoE Class		PC Port
		Class	Idle	
<b>1600 Series</b>	<b>1603</b>	2	4.4W	–
	<b>1603SW</b>	2	4.4W	✓
	<b>1608</b>	2	3.7W	✓
	<b>1616</b>	2	2.7W	✓
<b>9600 Series</b>	<b>9608</b>	1	2.08W	✓
	<b>9611G</b>	1	2.8W	✓
	<b>9621G</b>	2	3.49W	✓
	<b>9641G</b>	2	3.44W	✓

### 1. 1603/1603SW

These phones require a PoE Splitter unit in order to user PoE.



## 1.2 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 for Linux system must only use the firmware supplied pre-installed with the IP Office for Linux system or with its IP Office Manager application. Other versions of IP Phone firmware may not have been tested specifically with IP Office for Linux systems and so should not be used unless IP Office for Linux 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.

- **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](#) 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 for Linux 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 is storing the firmware files.

### Firmware Source Sets

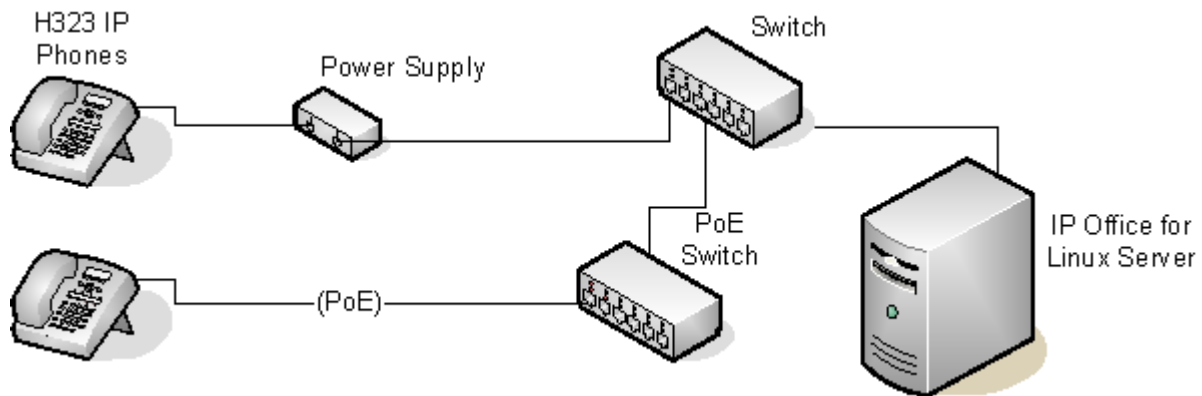
The phone firmware files are installed as part of the IP Office Manager application and are found in the application's installation directory. By default, the directory is found at **c:\Program Files\Avaya\IP Office\Manager**.

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 for Linux system itself.

## 1.3 Simple Installation

The diagram below shows the simplest installation scenario. This has the IP Office for Linux 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 for Linux Server**

The IP Office application on the IP Office for Linux server is performing a number of roles for the phones:

- **DHCP Server**

The IP Office for Linux 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 for Linux 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 for Linux systems as the H.323 Gatekeeper.

- **File Server**

During installation the IP phones need to download [firmware files](#) <sup>[9]</sup> for a file server. This is done using either HTTPS or HTTP in that order. The IP Office for Linux system's own memory can be used as the file source.

- The IP Office for Linux system can act as the file server for up to 50 phones. For larger numbers a separate 3rd-party HTTP server should be used.
- The IP Office for Linux 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.

- **Backup/Restore Server** <sup>[49]</sup>

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 use the IP Office system as the server for this function.

- **Switches**

The IP Office for Linux 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** <sup>[16]</sup>

Each H.323 IP phone requires a power supply. The IP Office for Linux 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 will require a power supply socket at each phone location. Note that for phones using a button module add-on, for example a EU24 or BM32, an individual power supply unit is often a requirement. The type of power supply will depend on the type of phone.

## 1.4 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](#)<sup>[13]</sup> 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](#)<sup>[16]</sup>.

- **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 .

- **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](#)<sup>[72]</sup>. Also the IP Office for Linux system can be configured to only provide DHCP support to Avaya IP phones.

- [Static IP addressing](#)<sup>[46]</sup> can also be used for IP phone installation if required. However that method of installation is not recommended.

- **HTTP File Server**

The IP Office for Linux 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.

- The IP Office for Linux 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.

- **H.323 Gatekeeper**

The IP Office for Linux 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](#)<sup>[12]</sup>.

- **Backup/Restore Server**<sup>[49]</sup>

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.

---

## 1.5 Licenses

The following licensing rules apply to the support of Avaya H.323 IP phones on a IP Office for Linux system. Note that B5800 Branch Gateway uses a different licensing system and different licensing rules. A B5800 Native Station license is required for each H.323 phone on B5800. Please refer to the B5800 Branch Gateway Implementation Guide for more information.

- Each Avaya IP phones is licensed by the addition of **Avaya IP Endpoints** licenses to the IP Office configuration.
  - 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.
- A newly installed IP Office for Linux server with the IP Office application includes a number of 90-day licenses to allow immediate operation of the system. Those temporary licenses include 4 **Avaya IP Endpoint** licenses.

Licenses are issued against a unique feature serial number of the telephone system. To be valid, any licenses entered into the system configuration must be licenses issued against that serial number. B5800 Branch Gateway licenses are issued against a unique PLDS Host ID.

## 1.6 Network Assessment

The IP Office for Linux 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 for Linux 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.

---

## 1.7 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.

## 1.8 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.

## 1.9 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. Except for phones with a G suffix, 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
<b>1600 Series</b>	<b>1603</b>	–
	<b>1603SW</b>	✓
	<b>1608</b>	✓
	<b>1616</b>	✓
<b>9600 Series</b>	<b>9608</b>	✓
	<b>9611G</b>	✓
	<b>9621G</b>	✓
	<b>9641G</b>	✓

---

## 1.10 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 for Linux 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
<b>1600 Series</b>	<b>1603</b>	2	4.4W
	<b>1603SW</b>	2	4.4W
	<b>1608</b>	2	3.7W
	<b>1616</b>	2	2.7W
<b>9600 Series</b>	<b>9608</b>	1	2.08W
	<b>9611</b>	1	2.8W
	<b>9621G</b>	2	3.49W
	<b>9641G</b>	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, an individual power supply must be used rather than connection to a PoE switch.

### 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.

### 9600

These phones only support the use of Power over Ethernet (PoE). If not being supplied by a PoE switch, an Avaya Single Port PoE injector (SPPOE-1A) can be used for each phone.



## 1.11 File Server Options

During installation and maintenance, the phones download various [firmware files](#)<sup>[9]</sup>. 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. 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 for Linux 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 for Linux 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](#)<sup>[49]</sup> 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 for Linux operation, the address of the IP Office for Linux 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 for Linux system.

File Server	Description	Up to X Phones	TFTP	HTTP	HTTPS
<b>IP Office Manager</b>	When running, IP Office Manager can act as a HTTP/TFTP server for file requests from IP phones.	5	✓	✓	–
<b>IP Office for Linux Server</b>	For IP Office for Linux 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 for Linux installation. Various other files can be <a href="#">auto-generated</a> <sup>[19]</sup> by the IP Office if not present on the memory card.	50	✓	✓	✓
<b>3rd Party Software</b>	3rd Party HTTP/TFTP file server software is available from many sources including Avaya.	–	✓	✓	✓



## 1.12 File Auto-Generation

For IP Office for Linux systems configured to use the system's own memory as the [file server](#)<sup>[17]</sup> for the phones, the system will auto-generate the necessary [firmware files](#)<sup>[9]</sup> 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.

- **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](#)<sup>[49]</sup> 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 for Linux 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](#)<sup>[49]</sup> 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.



# 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.

### 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 for Linux system. Verify that you can receive the configuration from the system and send it back.

### 2. Avaya IP Endpoint Licenses

Each phone requires an **Avaya IP Endpoint license** <sup>[12]</sup>. Phones can register without a license but will not operate. The licenses are added to the IP Office configuration using IP Office Manager.

### 3. H.323 Gatekeeper Settings

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

### 4. DHCP Server Setting

DHCP is the recommended method for installation of IP phones on a IP Office for Linux system. This requires a DHCP server configured to support IP phones. The IP Office for Linux system can be used for this. If the customer want to use their own DHCP server, it will require [additional configuration](#) <sup>[72]</sup>.

### 5. 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.

### 6. 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. If automatic creation is not used, entries must be manually created for each extension and user before the phones are installed.

### 7. 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.

### 8. 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.

### 9. Testing

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

### 10. 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](#) <sup>[12]</sup> section for information on licensing rules.

### 2.1.1 Checking the Serial Number

Licenses are issued against a unique feature serial number of the telephone system. For any licenses entered into the system configuration to be valid, they must be licenses issued against that serial number. B5800 Branch Gateway licenses are issued against a unique PLDS Host ID.

1. Using IP Office Manager, retrieve the configuration from the system.
2. Select  **System**.
3. Select the **System** tab.
4. The feature key serial number is shown by the **System Identification** field. For B5800 Branch Gateway systems, the PLDS Host ID is indicated by the **PLDS HOST ID** 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 **System Identification** number [shown](#)<sup>[23]</sup> in the system configuration. This should be shown in the file used to supply the licenses. For B5800 Branch Gateway systems, you must ensure that the licenses match the **PLDS Host ID**.


It is recommended that you cut and paste the license keys from a supplied file rather than typing them in manually.

1. Using IP Office Manager, receive the configuration from the telephone system.
2. Select  **License**. The current licenses in the system configuration are displayed.  
For B5800 Branch Gateways, select **PLDSLICENSE**.
3. To add a license, click on  and select **License**.  
For B5800 Branch Gateway systems, select **PLDSLICENSE** and select **Send PLDS license file to Avaya Branch Gateway**.
4. Enter the license that you have been supplied into the field and click **OK**.
5. 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.
6. Save the configuration back to the system and then receive the configuration from the system again.
7. 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.

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. The **Reserve Avaya IP endpoint license** setting is used to reserve an existing license for the extension.
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](#) <sup>[25]</sup>
- [Setting the RTP Port Range](#) <sup>[26]</sup>
- [Configuring SRTP](#) <sup>[27]</sup>
- [Enabling RTCP Quality Monitoring](#) <sup>[28]</sup>
- [Adjusting Diffserv QoS](#) <sup>[30]</sup>
- [System Default Codecs](#) <sup>[31]</sup>

### 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.

#### Enabling the H.323 Gatekeeper

1. Using IP Office Manager, retrieve the configuration from the system.

2. Select  **System**.

3. Select the **LAN1** tab.

4. Select the **VoIP** sub-tab.



5. Check that the **H.323 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.

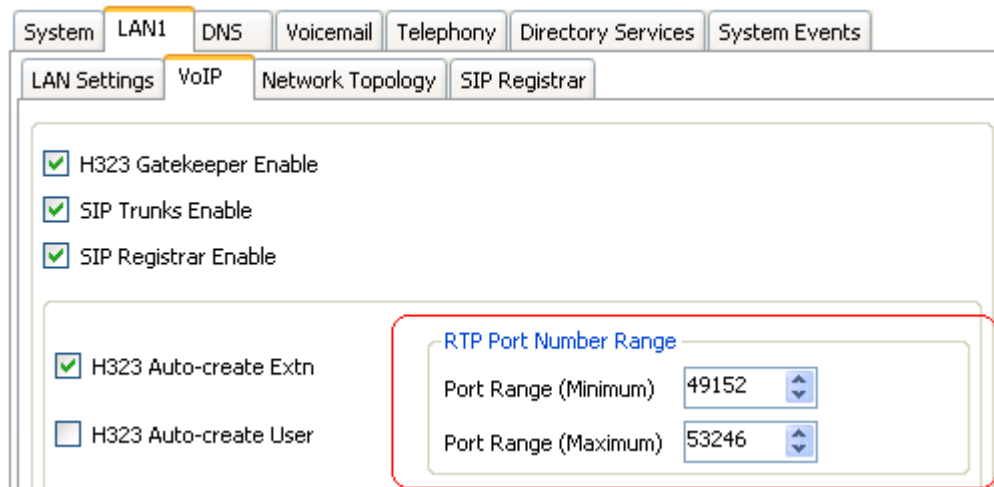
### Checking the Port Range

1. Using IP Office Manager, retrieve the configuration from the system.

2. Select  **System**.

3. Select the **LAN1** tab.

4. Select the **VoIP** sub-tab.



The screenshot shows the IP Office Manager configuration window. The 'System' tab is selected, and the 'LAN1' sub-tab is active. Within the 'LAN1' sub-tab, the 'VoIP' sub-tab is selected. The 'VoIP' sub-tab contains several settings: 'H323 Gatekeeper Enable' (checked), 'SIP Trunks Enable' (checked), 'SIP Registrar Enable' (checked), 'H323 Auto-create Extn' (checked), and 'H323 Auto-create User' (unchecked). A red box highlights the 'RTP Port Number Range' section, which contains two spinners: 'Port Range (Minimum)' set to 49152 and 'Port Range (Maximum)' set to 53246.

5. Check the **RTP Port Number Range** shown. Remember that the matching RTCP traffic uses the same range plus 1.

- **Port Range (Minimum):** *Default = 49152. Range = 1024 to 64510.*  
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 = 2048 to 65534.*  
This sets the upper limit for the RTP port numbers used by the system.

6. If these settings need to be changed, do so and then save the configuration back to the system.

## 2.2.3 Configuring SRTP

Avaya B5800 Branch Gateway supports Secure Real-Time Transport Protocol (SRTP) on an optional and per-device basis. A system-wide configuration is available that, by default, is applied to an extension when it is created (this is necessary to provide a default option on media security for all SIP and H.323 devices), while configuration for an individual device line takes precedence over system-wide device lines.

**Note:** A system-wide configuration controls all VoIP extension and line Media Security settings which are set to "System Default."

Calls offering SRTP will be negotiated to a SRTP direct media or relay session if both parties support SRTP. Otherwise, a non-direct media call will be established with one party using SRTP.

1. Using IP Office Manager, retrieve the configuration from the system.

2. Select  **System**.

3. Select the **Telephony** tab.

Two new drop-down menus are available: **Media Security (SIP)** and **Media Security (H.323)**. The default selection for SIP is "Prefer" while for H.323 it is "Disable."

**Note:** For IPO mode, the default selection is set to "Disable" for both drop-down menus.

4. From each drop-down menu select either "Disable" or "Enforce."

This configuration determines the default selection of the Media Security option in a new VoIP extension or Trunk. For more information, see the 'SRTP Configuration Table' below.

### SRTP Configuration Table

The configuration options for Media Security are offered at the device level and also at the system level. The settings at the system level determine the setting for a device connection.

Configuration	Detail	Availability
<b>Disable</b>	<p>This setting for any IP endpoint or SIP line/SM line implies that this entity does not or cannot support SRTP. In case of VoIP endpoints, when the gateway relays the media, it will send and receive RTP packets to this endpoint (and depending on the connection, it may encrypt the packets for transmission to the other end of the call).</p> <p>In case of trunks, (SIP line and SM line), the gateway will not advertise support for SRTP and will reject incoming offers proposing only secure media capabilities.</p>	<ul style="list-style-type: none"> <li>• SIP</li> <li>• H.323</li> </ul>
<b>Enforce</b>	<p>This setting implies that the gateway will send and receive only secure media streams from this endpoint. For a SIP line or SM line, this configuration implies that if an incoming offer does not contain SRTP capabilities, then the call will be rejected.</p> <p>Likewise, all outgoing offers on this trunk will offer only secure media capabilities.</p>	<ul style="list-style-type: none"> <li>• SIP</li> <li>• H.323</li> </ul>

## 2.2.4 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.

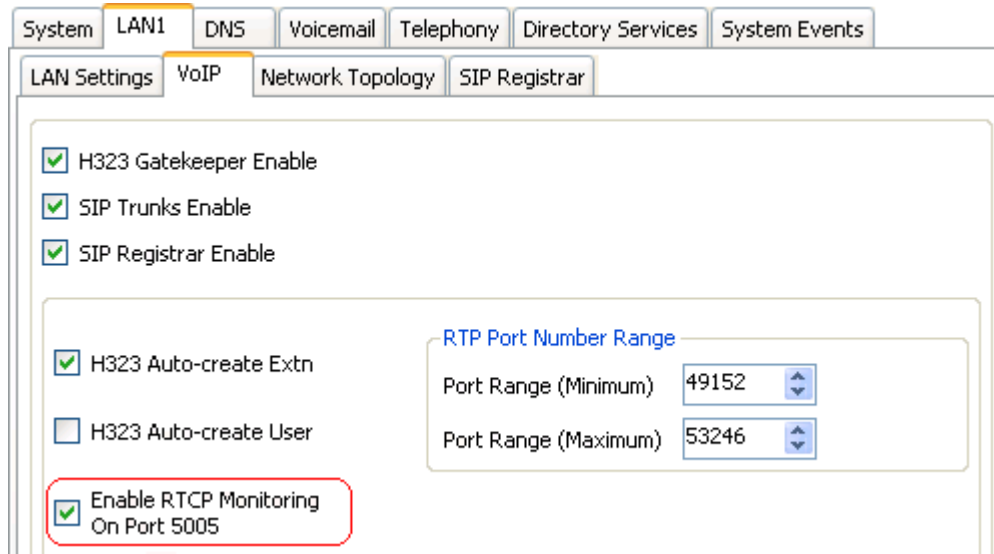
### Enabling the RTCP Quality Monitoring

1. Using IP Office Manager, retrieve the configuration from the system.

2. Select  **System**.

3. Select the **LAN1** tab.

4. Select the **VoIP** sub-tab.



The screenshot shows the IP Office Manager configuration window. The 'System' tab is selected, and the 'LAN1' sub-tab is active. Within the 'LAN1' sub-tab, the 'VoIP' sub-tab is selected. The 'VoIP' sub-tab contains several configuration options: 'H323 Gatekeeper Enable' (checked), 'SIP Trunks Enable' (checked), 'SIP Registrar Enable' (checked), 'H323 Auto-create Extn' (checked), 'H323 Auto-create User' (unchecked), and 'Enable RTCP Monitoring On Port 5005' (checked). The 'Enable RTCP Monitoring On Port 5005' checkbox is highlighted with a red box. To the right of these options, there is a section for 'RTP Port Number Range' with 'Port Range (Minimum)' set to 49152 and 'Port Range (Maximum)' set to 53246.

5. Check that the **H.323 Gatekeeper Enable** setting is selected.

6. If this setting needs to be changed, save the configuration back to the system.

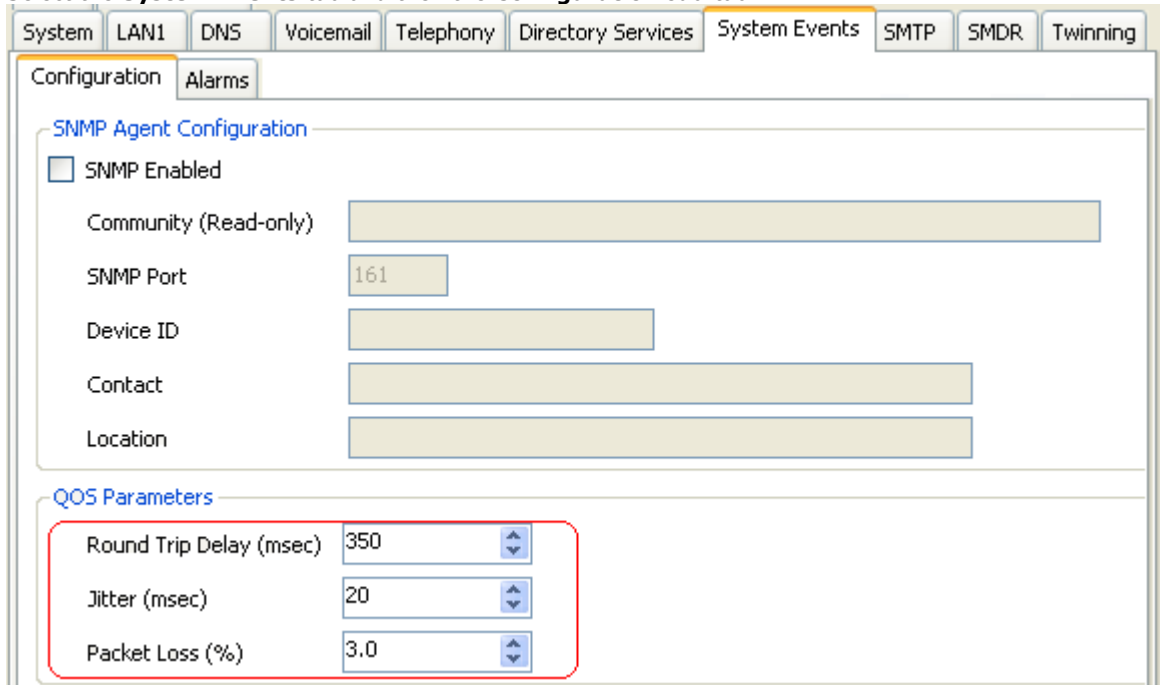
## Setting the Quality of Service Alarm Levels

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.



The screenshot shows the IP Office Manager configuration window. The 'System Events' tab is selected, and the 'Configuration' sub-tab is active. The 'SNMP Agent Configuration' section includes a checkbox for 'SNMP Enabled' (unchecked), and text input fields for 'Community (Read-only)', 'SNMP Port' (161), 'Device ID', 'Contact', and 'Location'. The 'QoS Parameters' section, highlighted with a red box, contains three spinners: 'Round Trip Delay (msec)' set to 350, 'Jitter (msec)' set to 20, and 'Packet Loss (%)' set to 3.0.

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.

## 2.2.5 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.

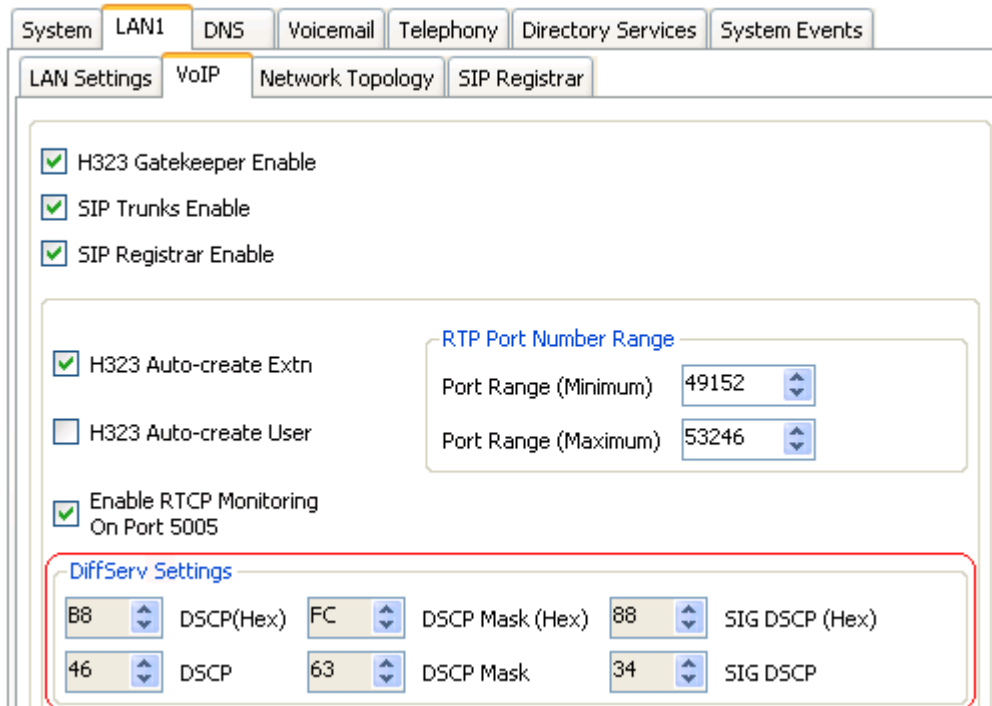
### Enabling the DiffServ QoS Settings

1. Using IP Office Manager, retrieve the configuration from the system.

2. Select  **System**.

3. Select the **LAN1** tab.

4. Select the **VoIP** sub-tab.



System LAN1 DNS Voicemail Telephony Directory Services System Events

LAN Settings VoIP Network Topology SIP Registrar

☒ H323 Gatekeeper Enable

☒ SIP Trunks Enable

☒ SIP Registrar Enable

☒ H323 Auto-create Extn

☐ H323 Auto-create User

☒ Enable RTCP Monitoring On Port 5005

RTP Port Number Range

Port Range (Minimum) 49152

Port Range (Maximum) 53246

DiffServ Settings

B8	DSCP(Hex)	FC	DSCP Mask (Hex)	88	SIG DSCP (Hex)
46	DSCP	63	DSCP Mask	34	SIG DSCP

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.

## 2.2.6 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**.

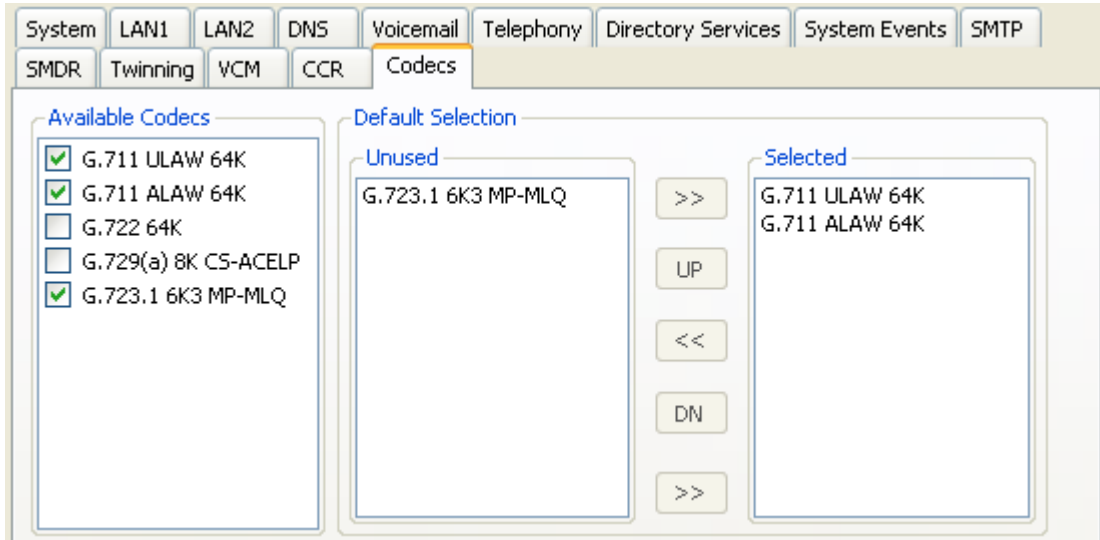
In addition to changing the default codec preference order for all VoIP trunks and extension, the codec preferences used by a particular trunk or extension can be adjusted. However, the use of the common system settings ensures codec consistency between trunks and extensions.

### Changing the Default Codec Preferences

1. Using IP Office Manager, retrieve the configuration from the system.

2. Select  **System**.

3. Select the **Codecs** sub-tab.



The screenshot shows the 'System' configuration window with the 'Codecs' sub-tab selected. The 'Available Codecs' list on the left includes:

- ☒ G.711 ULAW 64K
- ☒ G.711 ALAW 64K
- ☐ G.722 64K
- ☐ G.729(a) 8K CS-ACELP
- ☒ G.723.1 6K3 MP-MLQ

The 'Default Selection' section in the center contains two lists:

- Unused:** G.723.1 6K3 MP-MLQ
- Selected:** G.711 ULAW 64K, G.711 ALAW 64K

Navigation buttons between the lists include: >>, UP, <<, DN, and >>.

4. The **Available Codecs** list shows which codecs the system supports. The codecs in this list which are enabled are those that can be used in other configuration forms including the adjacent default selection.

- **! WARNING:** Deselecting a codec in this list will automatically remove it from any line, system or 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](#)<sup>[72]</sup>.
- 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](#) <sup>34</sup>  
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.
2. [Check the Site Specific Option Numbers](#) <sup>35</sup>  
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](#) <sup>36</sup>  
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.

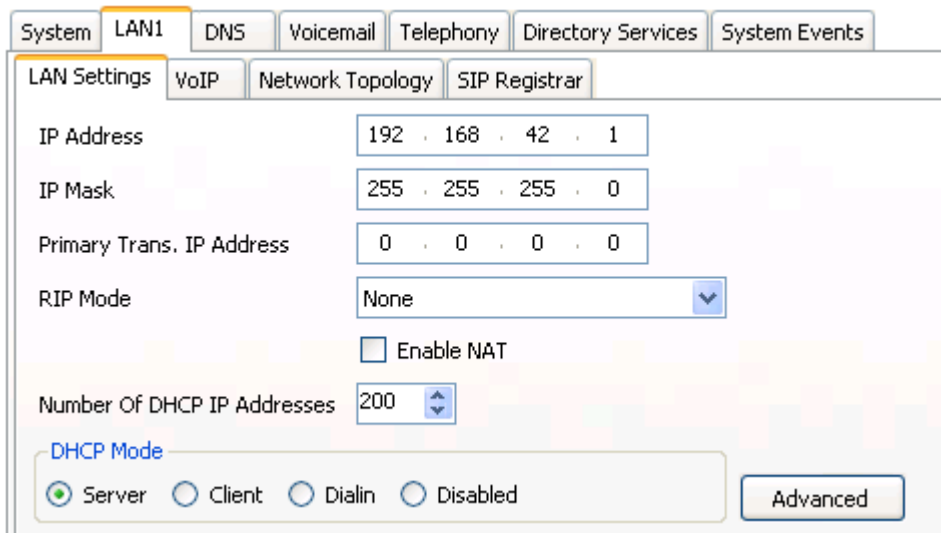
## 2.3.1 System DHCP Support

1. Using IP Office Manager, retrieve the configuration from the system.

2. Select  **System**.

3. Select the **LAN1** tab.

4. Select the **LAN Settings** tab.



System LAN1 DNS Voicemail Telephony Directory Services System Events

LAN Settings VoIP Network Topology SIP Registrar

IP Address 192 . 168 . 42 . 1

IP Mask 255 . 255 . 255 . 0

Primary Trans. IP Address 0 . 0 . 0 . 0

RIP Mode None

☐ Enable NAT

Number Of DHCP IP Addresses 200

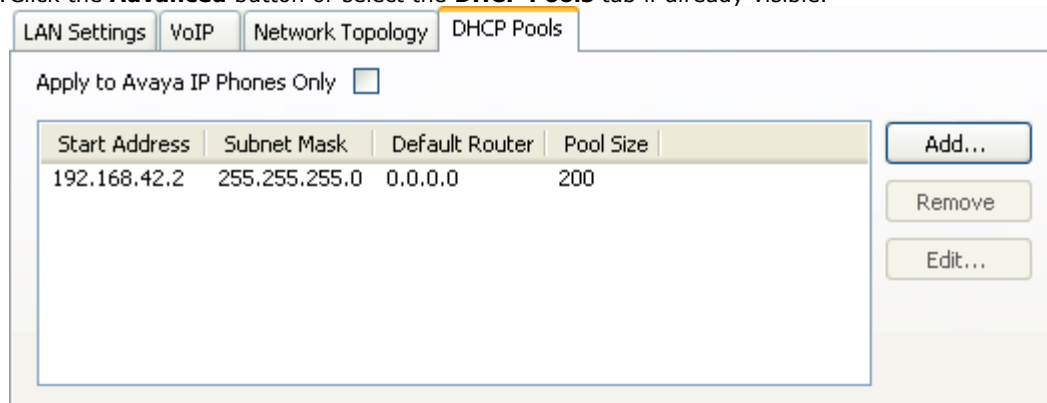
DHCP Mode

☒ Server ☐ Client ☐ Dialin ☐ Disabled

Advanced

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.



LAN Settings VoIP Network Topology DHCP Pools

Apply to Avaya IP Phones Only ☐

Start Address	Subnet Mask	Default Router	Pool Size
192.168.42.2	255.255.255.0	0.0.0.0	200

Add... Remove Edit...

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.

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](#)<sup>[65]</sup>. 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.

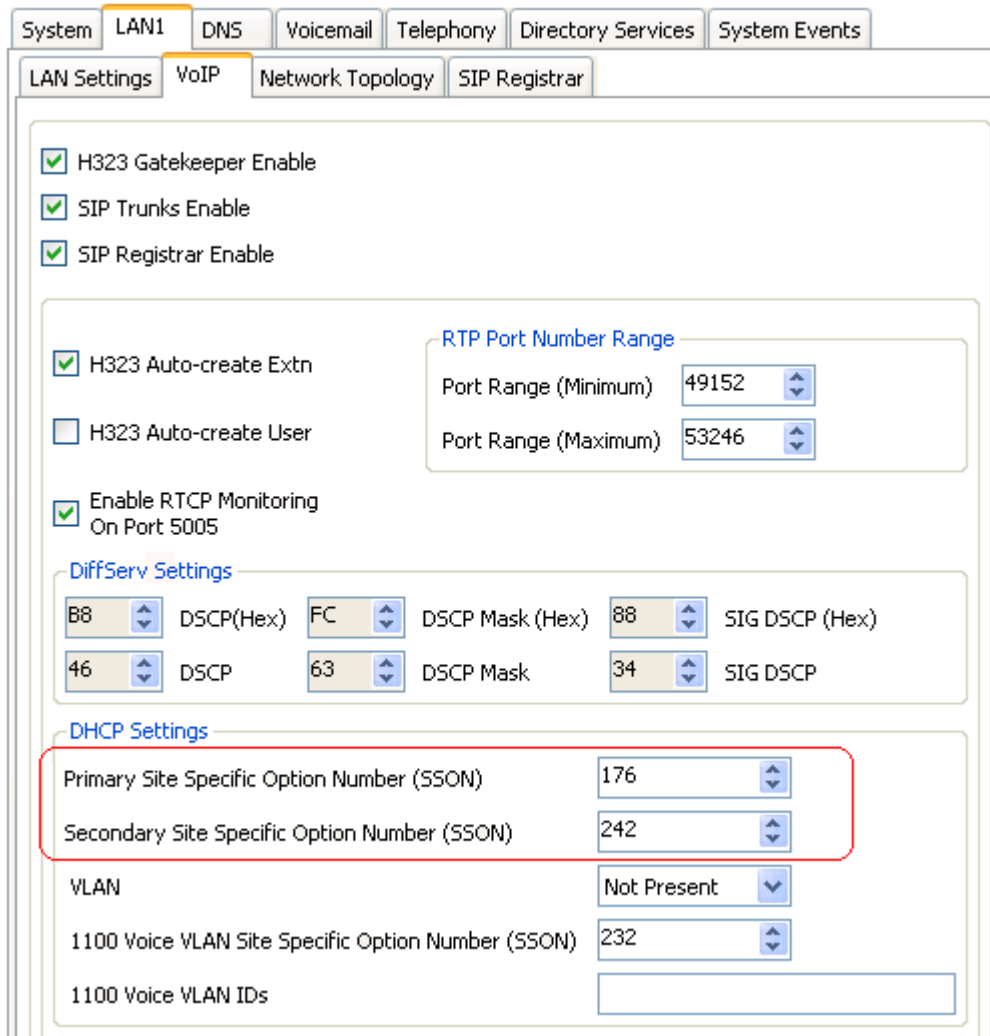
### Changing the Systems SSON Settings

1. Using IP Office Manager, retrieve the configuration from the system.

2. Select  **System**.

3. Select the **LAN1** tab.

4. Select the **VoIP** sub-tab.



The screenshot shows the IP Office Manager configuration interface. The top navigation bar includes tabs for System, LAN1, DNS, Voicemail, Telephony, Directory Services, and System Events. The LAN1 tab is selected, and the sub-tabs below it are LAN Settings, VoIP, Network Topology, and SIP Registrar. The VoIP sub-tab is active, displaying various configuration options. A red box highlights the DHCP Settings section, which includes:

- Primary Site Specific Option Number (SSON): 176
- Secondary Site Specific Option Number (SSON): 242
- VLAN: Not Present
- 1100 Voice VLAN Site Specific Option Number (SSON): 232
- 1100 Voice VLAN IDs: (empty field)

5. Check that the Site Specific Option Number settings match those required for the phone being supported. 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:

- The IP Office system's 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.
- The IP Office Manager application can also act as a file server for up to five (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.

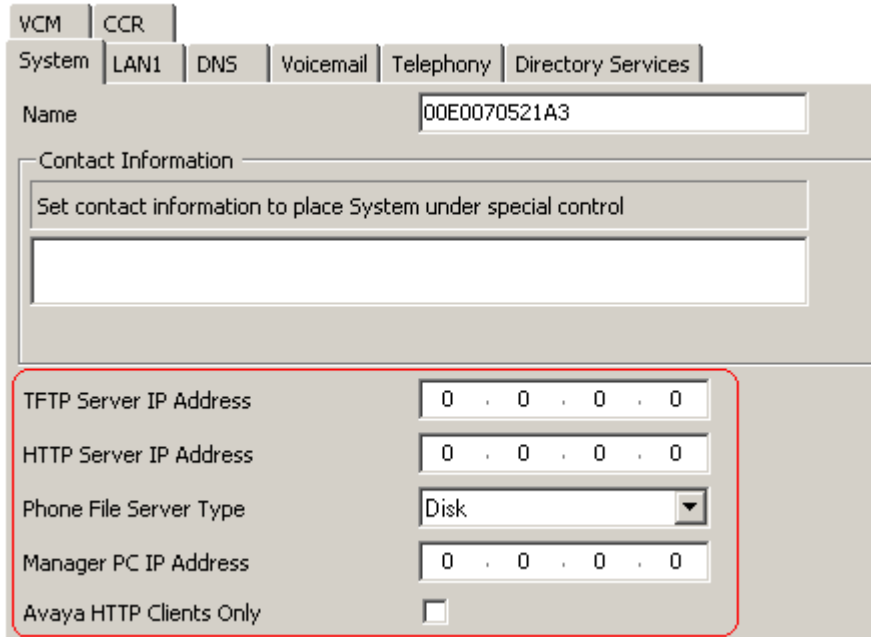
## 2.4.1 System File Server Settings

If the IP Office system is being used for [DHCP support](#)<sup>[32]</sup> 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.

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.

- **Disk**

Use the system's 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 file server addresses in the DHCP response given to phones.

- The **TFTP Server IP Address** default of 0.0.0.0 is a broadcast on the network for a TFTP server.
- The **HTTP Server IP Address** default of 0.0.0.0 is no HTTP request.

5. 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.

6. 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](#)<sup>[9]</sup>. 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 for Linux system as the file server, the IP Office for Linux system will [auto-create](#)<sup>[19]</sup> a suitable **46xxsettings.txt** file based on various IP Office for Linux 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 Windows Notepad or any other 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 LAN Administrator Manual. This manual only contains a limited number of examples of the settings available. Note also that the files contain a wide range of settings used on other Avaya telephone systems that may not work with IP Office for Linux systems.
  - [9600 Series IP Telephones Administrator Guide](#) (16-300698)
  - [1600 Series IP Telephones Administrators Guide](#) (16-601443).
4. A # character at the start of a line comments out the command on that line. Note however that for some options the phones will assume a default value if the option in the **46xxsettings.txt** file is commented out. For example if **SET PHNOL** is commented out, the phones will assume the addition of a **dial 9** prefix to numbers.

### Dialing Prefix

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

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

### 802.1Q Tagging

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

required address.

## 1600/9600 Series Phone Languages

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

Language	1600 File	9600 File
<b>Dutch</b>	mlf_dutch.txt	mlf_9600_dutch.txt
<b>French Canadian</b>	mlf_french_can.txt	mlf_9600_french_can.txt
<b>French</b>	mlf_french_paris.txt	mlf_9600_french_paris.txt
<b>German</b>	mlf_german.txt	mlf_9600_german.txt
<b>Italian</b>	mlf_italian.txt	mlf_9600_italian.txt
<b>Portuguese</b>	mlf_portuguese.txt	mlf_9600_portuguese.txt
<b>Russian</b>	mlf_russian.txt	mlf_9600_russian.txt
<b>Spanish</b>	mlf_spanish.txt	mlf_9600_spanish.txt
<b>Spanish (Latin American)</b>	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](#)<sup>[19]</sup>.

## 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](#)<sup>[49]</sup> for full details.

### 2.4.3 Loading Software Files onto the System

The phone firmware suitable for IP Office for Linux system operation is included as part of the IP Office for Linux 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.

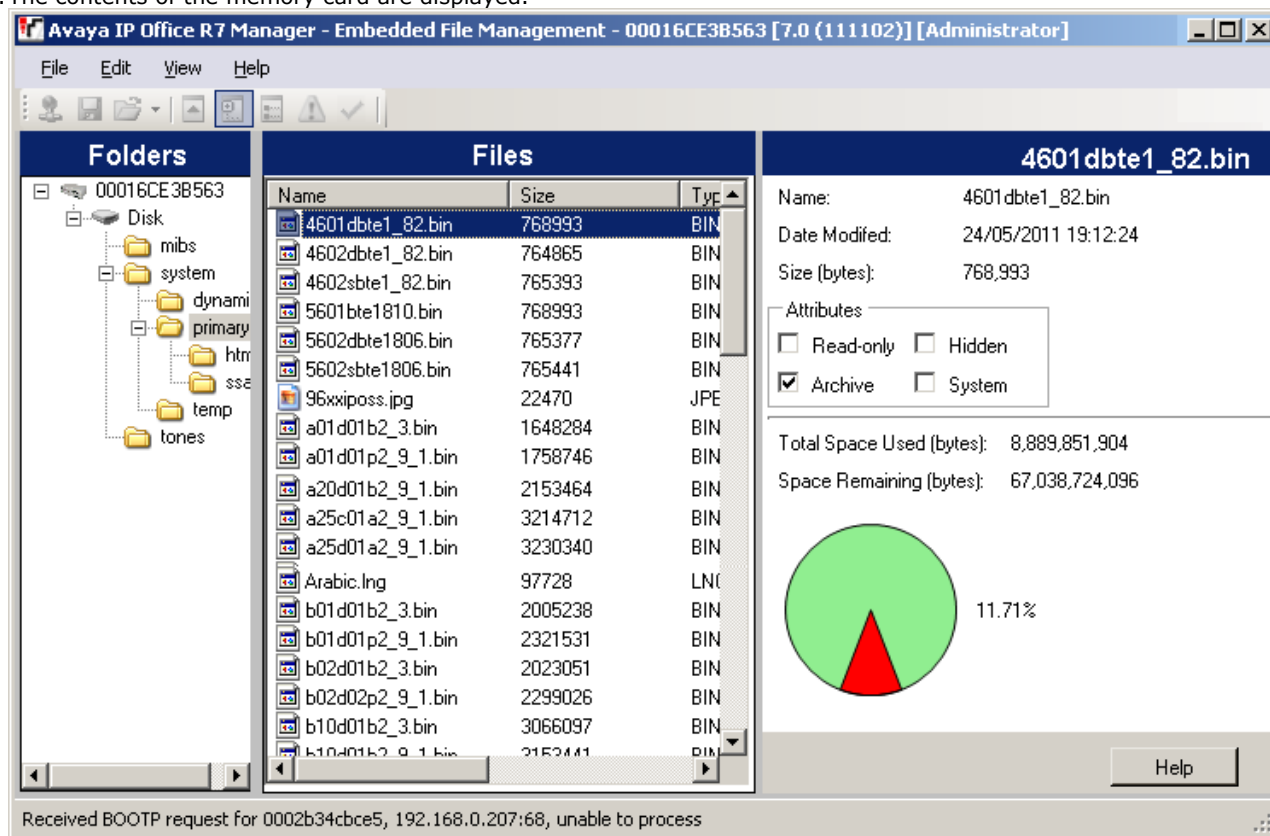
No other firmware should be used with IP Office for Linux unless specifically documented. The firmware installed can be checked and new firmware copied onto the telephone system's disk if necessary.

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. 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**.



### 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 for Linux 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 can 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.


**Note:** Auto-creation is not supported on B5800 Branch Gateway systems.

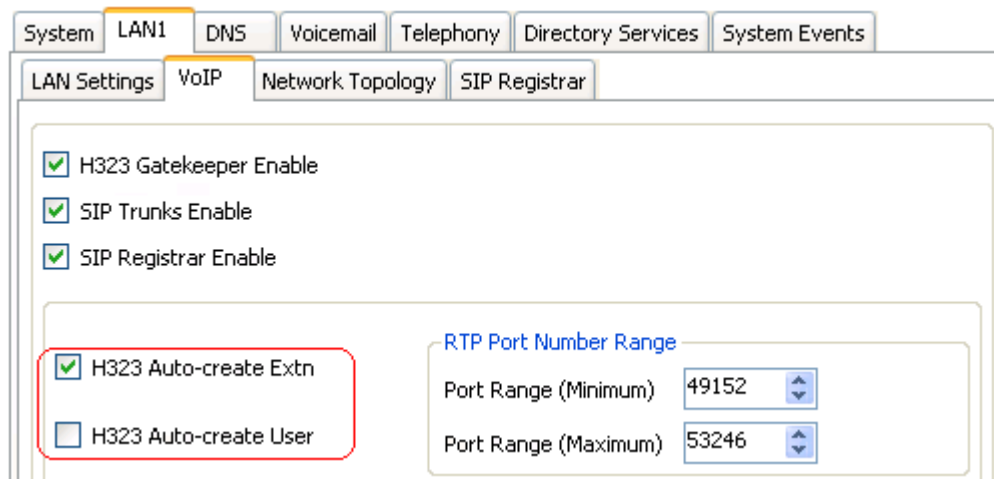
### 2.5.1 Auto-Creation

We recommend that you use Auto-creation to create extensions and user entries. The settings can be disabled after installation.

**Note:** Auto-creation is not supported on B5800 Branch Gateway systems.

#### Switching Auto-Creation On/Off

1. Using IP Office Manager, receive the configuration from the system. Select  **System**.
2. Select the **LAN1** tab.
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](#)<sup>[43]</sup> and or [manually create the user entries](#)<sup>[43]</sup> 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](#)<sup>[42]</sup>, 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.


### Manually Creating 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](#)<sup>[42]</sup>, 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](#)<sup>[43]</sup> or it must be done separately using the process below.


### Manually Creating 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.
  - b. To add the new extension, click **OK**.
3. Save the configuration changes back to the system.

### Codec Selection

If the **Codec Selection** is left set to **System Default**, the extension will use the [system codec preferences](#)<sup>[31]</sup>. 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.

1. Do not start this process until all the preceding steps in the [Installation Summary](#)<sup>[22]</sup> 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](#)<sup>[46]</sup>.
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 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](#)<sup>[48]</sup>.

---

## 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.

### 1600 Series Phones

1. Follow the steps in [Phone Connection](#) <sup>45</sup> until **DHCP** is shown on the phone display. Press \* at this point to switch the phone to static address installation.
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. 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 for Linux 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](#) <sup>55</sup>.
4. 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.
5. 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.
6. The [phone registration](#) <sup>48</sup> 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 (2 7 2 3 8)**.
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](#)<sup>64</sup>, 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 for Linux 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](#)<sup>55</sup>.
  - **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](#)<sup>48</sup> menu is displayed.

---

## 2.8 Phone Registration

For new phones and phones that have been [reset](#)<sup>[63]</sup>, the phone will request an extension number. If [auto-create](#)<sup>[42]</sup> 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](#)<sup>[42]</sup>.

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 #. Any digits entered are not validated or stored.
  - If not using auto-create, enter the user's **Login Code** as set in the IP Office configuration.

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](#)<sup>[19]</sup>. 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](#)<sup>19</sup>, 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	<b>ABKNAMEmmm</b> <b>ABKNUMBERmmm</b>	These paired entries are used for personal contacts entered into the phone. The <i>mmm</i> 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. ✓
	<b>LANGUSER</b>	Display language. The language name is stored. ✓
	<b>LOGACTIVE</b>	Call log active on (1) or off (0). ✓
	<b>LOGBRIDGED</b>	Log bridged calls on (1) or off (0). ✓
	<b>LOGLINEAPPS</b>	Log line calls on (1) or off (0). ✓
	<b>LOGOTHERANS</b>	Log calls answered by others on (1) or off (0). ✓
	<b>OPTAGCHAND</b>	Handset Automatic Gain Control on (1) or off (0).
	<b>OPTAGCHEAD</b>	Headset Automatic Gain Control on (1) or off (0).
	<b>OPTAGCSPKR</b>	Speaker Automatic Gain Control on (1) or off (0).
	<b>OPTAUDIOPATH</b>	Audio Path. ✓
	<b>OPTCLICKS</b>	Button Clicks on (1) or off (0). ✓
	<b>OPTERRORTONE</b>	Error Tone on (1) or off (0). ✓
	<b>PERSONALRING</b>	Personalized Ring. A numeric value (1 to 8) for the selected ring is stored. ✓
	<b>PHNREDIAL</b>	Redial
	<b>PHNSCRONCALL</b>	Go to call screen on calling on (1) or off (0).
	<b>PHNSCRONALERT</b>	Go to call screen on ringing on (1) or off (0).
	<b>PHNTIMERS</b>	Call Timer on (1) or off (0). ✓
	<b>PHNVISUALALERT</b>	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/**.

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/**.

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:

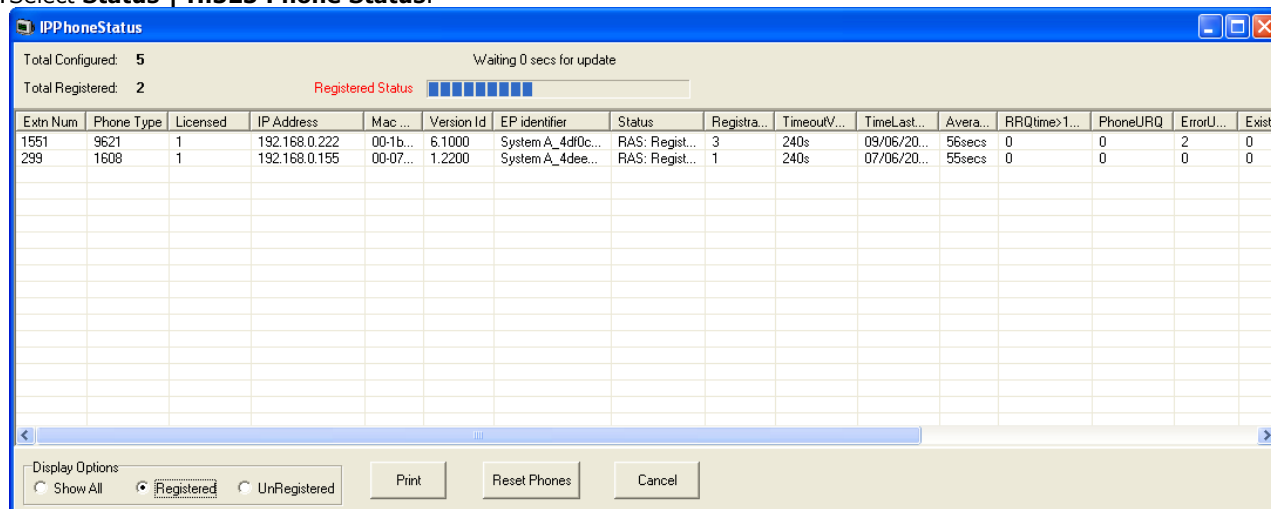
```
#
# WebDAV configuration
#
DavLockDB "C:/Program Files/Apache Group/Apache2/var/DAVLock"
<Location />
  Dav On
</Location>
```

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.

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



The screenshot shows the IPPhoneStatus application window. At the top, it displays 'Total Configured: 5' and 'Total Registered: 2'. Below this is a 'Registered Status' bar with 10 segments, 2 of which are filled. The main part of the window is a table with the following columns: Extn Num, Phone Type, Licensed, IP Address, Mac, Version Id, EP identifier, Status, Registra..., TimeoutV..., TimeLast..., Avera..., RRQtime>1..., PhoneURQ, ErrorU..., and Existl. The table contains two rows of data. Below the table, there are 'Display Options' with radio buttons for 'Show All', 'Registered' (selected), and 'UnRegistered'. There are also buttons for 'Print', 'Reset Phones', and 'Cancel'.

Extn Num	Phone Type	Licensed	IP Address	Mac	Version Id	EP identifier	Status	Registra...	TimeoutV...	TimeLast...	Avera...	RRQtime>1...	PhoneURQ	ErrorU...	Existl
1551	9621	1	192.168.0.222	00-1b...	6.1000	System_A_4d0c...	RAS: Regist...	3	240s	09/06/20...	56secs	0	0	2	0
299	1608	1	192.168.0.155	00-07...	1.2200	System_A_4dee...	RAS: Regist...	1	240s	07/06/20...	55secs	0	0	0	0

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:

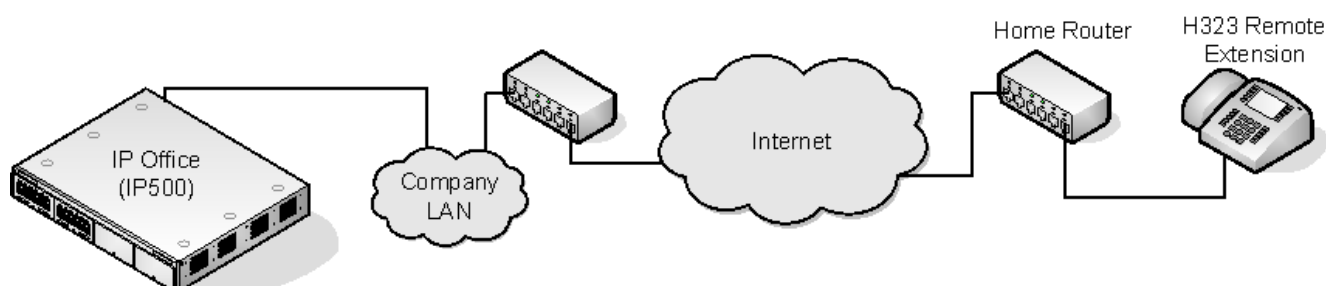
```
792ms PRN: GRQ from c0a82c15 --- RAS reaches the maximum capacity of 10; Endpoints registered 41
```

## 2.11 Other Installation Options

### 2.11.1 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 for Linux 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.



- **Supported Telephones**  
Currently, remote H.323 extension operation is only supported with 9600 Series phones already supported by the IP Office for Linux system.
- **License Requirements**  
By default, only two (2) users can be configured for remote H.323 extension usage. Additional users can be configured if those additional users are licensed and configured with the **Power User** user profile.

### Customer Network Configuration

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

STUN from the IP Office for Linux 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 for Linux system must allow the following traffic.

Protocol	Port	Description
ICMP	–	Incoming ICMP to the IP Office for Linux system's public IP address must be allowed.
UDP	1719	UDP port 1719 traffic to the IP Office for Linux 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 for Linux system.
TCP	1720	TCP port 1720 traffic must be allowed. This is used for H.225 (call signalling).
RTP	Various	The ports in the range specified by the system's <b>RTP Port Number Range (Remote Extn)</b> 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, it will be able to receive RTP/RTCP from that same IP address and port. Configurations otherwise are not covered by this documentation.

## IP Office for Linux System Configuration

This is a summary of the necessary IP Office for Linux system configuration changes. This section assumes that you are already familiar with IP Office for Linux system and [H.323 IP telephone installation](#)<sup>[22]</sup>.

### 1.Licensing

If more than two (2) remote extension users are to be supported, the system must include available **Power User** licenses for those users.

### 2.System Configuration

The following needs to be configured on the IP Office for Linux system LAN interface to which the public IP address is routed.

- Select **System | LAN1 | VoIP**. Check that the **H.323 Gatekeeper Enable** setting is selected.
- 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.
- Select **H.323 Remote Extn Enable**.
- Set the **RTP Port Number Range (Remote Extn)** to encompass the port range that should be used for remote [H.323 extension RTP and RTCP](#)<sup>[26]</sup> traffic. The range setup must provide *at least two (2) 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 for Linux system and the Internet.

- 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.
- 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.

- Within Manager, add a new H.323 extension or edit an existing extension.
- On the **Extn** tab, set the **Base Extension** number.
- On the **VoIP** tab, select **Allow Remote Extn**.
- 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 **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 for Linux 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.

## 2.11.2 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
<b>No VLAN</b>	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)
<b>Physical VLAN</b>	Separate VLAN for data and voice	Simple configuration	Requires two (2) ports on switch; one for IP phone and one for PC
<b>Overlapping VLAN</b>	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
<b>None (Static addressing)</b>	Manual configuration of each IP Phone
<b>Separate DHCP Servers</b>	Two PCs, one for each VLAN
<b>Multihomed DHCP Server</b>	A single PC with two NIC Cards; one for each VLAN
<b>DHCP Relay</b>	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
<b>IP Address</b>	192.168.43.x	192.168.202.x
<b>Mask</b>	255.255.255.0	255.255.255.0
<b>Router</b>	192.168.43.1	192.168.202.1
<b>SSON Scope</b>	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).



# **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:
  - [9600 Series IP Telephones Administrator Guide](#) (16-300698)
  - [1600 Series IP Telephones Administrators Guide](#) (16-601443).

### Using Static Administration Options

The method used to access static administration depends on the type of phone.

#### 1600, 4600 and 5600 Series Phones

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

1. All local procedures are started with the phone idle. Then dialling **MUTE** and then a sequence of up to seven (7) numbers followed by **#**.
2. After the **MUTE** button is pressed, a six (6) second timeout is in effect between button presses. If a valid button is not pressed within six (6) seconds of the previous button, the collected digits are discarded and no administrative options are started.
3. Attempts to enter invalid data are rejected and the phone emits an error beep.
4. If a numeric digit is entered for a value or for a field of an IP address or subnet mask after only a zero has been entered, the new digit will replace the zero.
5. To go to the next step, press **#**.

#### 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 2 7 2 3 8 # (MUTE C R A F T #)**.
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](#)<sup>153</sup>. The hub interface is set to **enabled** by default.

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 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 4 6 8 # (MUTE I N T #)**. 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 **#**.
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 2 7 2 3 8 # (MUTE C R A F T #)**.
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 ports 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 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 8 4 3 9 # (MUTE V I E W #)**.

- 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 phone's 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 2 7 2 3 8 # (MUTE C R A F T #)**.

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 Series Phones

1. To start the IP phone self-test procedure, press the following sequence: **MUTE 8 3 7 8 # (MUTE T E S T #)**. 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 one (1) second after self-test is started. Then a block character (all pixels on) is displayed in all display character locations for five (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 2 7 2 3 8 # (MUTE C R A F T #)**.
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](#)<sup>[64]</sup>.

### 1600 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 7 3 7 3 8 # (MUTE R E S E T #)**. **Reset values?** is displayed.
2. To cancel this procedure press \*. To continue press #.
  - **WARNING**  
As soon as you press #, all static information will be erased without any possibility of recovering the data.
3. Whilst the system values are reset to their defaults, **Resetting values** is displayed.
4. Once the system values are reset, **Restart phone?** is displayed.
  - To end the procedure without restarting the phone, press \*.
  - To restart the phone, press #. The remainder of the procedure then depends on the status of the boot and application files. See [Restart Scenarios](#)<sup>[68]</sup>.

### 9600 Series Phones

1. Restart the phone or remove and then reapply power.
2. When the option **\* to program** is displayed, press the \* key.
3. When **Enter code** is displayed, enter the administrative procedures passcode and press #. The default passcode is **CRAFT (2 7 2 3 8)**.
4. Scroll to the desired menu and select it.
5. Scroll the menu to **Reset Values**.
6. Press **Reset** to confirm the action. The phone user settings are cleared and the phone restarted.

---

## 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 **A 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 Series Phones

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

### 9600 Series Phones

1. Restart the phone or remove and then reapply power.
2. When the option **\* to program** is displayed, press the \* key.
3. When **Enter code** is displayed, enter the administrative procedures passcode and press #. The default passcode is **CRAFT (2 7 2 3 8)**.
4. Scroll to the desired menu and select it.
5. Scroll the menu to **Clear**.
6. Press **Clear** again to confirm the action. The phone settings are cleared and the phone restarted.



### 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 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](#) [35].

- **! 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 Series Phones

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

#### 9600 Series Phones

1. While the phone is on-hook and idle, press the following sequence: **MUTE 2 7 2 3 8 # (MUTE C R A F T #)**.
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.

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 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](#) 
  - [No Application File or Application File Needs Upgrading](#) 
  - [Correct Boot File and Application File Already Loaded](#) 

## 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.

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](#) .

## 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.

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](#) .

## 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.

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 user's Login Code stored in IP Office Manager.
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.**

## **Alternate DHCP Server Setup**

---

## 5. 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)



## 5.1 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.

- Avaya recommends providing 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.
- Avaya recommends, once assigned an IP address, the telephone continues using that address after the DHCP lease expires, until a conflict with another device is detected. The 1600 Series IP Telephone customizable parameter DHCPSTD allows an administrator to specify that the telephone either:
  - comply with the DHCP standard by setting DHCPSTD to 1
  - or
  - 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.

---

## 5.2 Checking for 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](#)<sup>[74]</sup> of addresses for use by IP phones.

## 5.3 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.

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](#)<sup>[74]</sup> 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.

## 5.4 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.

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,HTTPODIR=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.
- **HTTPODIR=** 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](#)<sup>[73]</sup>.

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](#)<sup>[75]</sup>.

## 5.5 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.



# Index

## 1

10Mbps 11  
1151C1/1151C2 45  
1152A1 45  
150ms 13

## 2

264V AC 16

## 3

3.5W 16  
30A Switch Upgrade Base 16  
3rd-party  
    HTTP 10  
    TFTP 17

## 4

4600 7, 38, 55, 72  
4602SW 7, 15, 16  
4606 7, 15, 16  
4610SW 7, 15, 16  
4620 7, 16, 38  
4620IP 15  
4620SW 7, 15  
4621SW 7  
    applies 16  
4622  
    support 7  
4624D 16  
4624D01 16  
4624D02A 60  
4625SW 16

## 5

5602SW 7, 15, 16  
5610SW 7, 15  
5620SW 7, 15

## 7

792ms 52

## A

AC 16  
access point 7  
address programming 46  
administrative options 58, 60  
Alternate DHCP Servers 10, 22  
    Avaya IP 72  
Alternate Options 73  
Appendix 68  
application file 60, 68, 69  
Applications 13, 17, 60, 63, 68, 69  
Auto-create Extn Enable 22  
Avaya 7, 13, 15, 16, 17, 55, 72  
Avaya 1151C1 16  
Avaya 1151C2 16  
Avaya 1152A1 Power Distribution Unit 16  
Avaya 30A Switch Upgrade Base 15  
Avaya H.323 IP 7  
Avaya P333T-PWR Switch 16  
Avaya Voice Priority Processor 7  
AVPP 7

## B

Backup 14, 16  
Button Programming 42

## C

cabling 11  
    Connections 14  
call answering 7  
Call Server 55  
CallSv 46  
CAT3 11, 16  
CAT5 11, 14, 16  
Catalyst 16  
CD 17  
Cisco Catalyst 16  
CLI configuration 55  
cmd 52  
configuring  
    3rd-party 10  
Connect 11, 14, 15, 45, 55  
Connections 11, 15, 16, 45, 59, 60  
    Cabling 14  
Control Unit Settings 22  
Correct Boot File 69

## D

Data 13, 14, 15, 16, 45, 46, 55, 63  
Default 46, 59, 63, 65, 69  
DHCP 10, 11, 13, 17, 46, 55, 58, 63, 65, 68, 73  
    alternate 72  
    connection 45  
    introduction 7  
    preparation 22  
DHCP Address Installation 45, 46  
DHCP addressing 65  
DHCP Options 55, 65  
DHCP Relay 55  
DHCP Settings 55  
DiffServ 14  
DiffServ QoS 14  
DNS 72, 73  
Duplicate IP Addressing 14

## E

Embedded Voicemail Memory 17  
Endpoints 52  
End-to-End Matching Standards 14  
Enter TFTP 52  
Ethernet 14, 55, 68  
    Power 16  
Ethernet LAN 16  
Ethernet Switch 55  
Excessive Utilization 14  
Extension ID 42  
extensions 7, 11, 22, 42, 48  
    phone requests 69  
    user changes 69

## F

FileSv 46

## G

Gatekeeper 10, 11, 22, 46, 65, 73  
GEN 16

## H

H.08.60 55  
H.232 15  
H.323 7, 15, 17  
hostname 55  
HP 55  
HP Procurve 55

---

HP Procurve CLI 55  
HP Procurve Ethernet 2626 PWR Ethernet 55  
HP Procurve Switch 55

## I

IEEE 802.2p/q 55  
IEEE 802.3af 15, 16  
Initializing 45, 69  
Introduction 7  
IP Gateway 72  
IP Mask 46, 55  
IP Office Administration CD 22  
IP Office Administrator 17  
IP Office Embedded Voicemail 17  
IP Office IP Endpoint 7  
IP Office System 7, 10, 13, 52, 63  
IP Office Unit configuration 11  
IP Office Unit Memory Card 17  
IP Phone Inline Adaptor 16  
IP Phone Software 7, 17, 22  
IP Telephone 11, 72  
IP403 7  
IP406 7, 17, 22  
IP406 V1 7  
IP406 V2 7, 17, 22  
IP412 7  
IPO 55  
IPSets Firmware 17  
IR 59

## J

J8164A Configuration Editor 55

## L

L2 55  
L2 QOS 55  
L2Q 55  
L2QVLAN 55  
LAN 11, 14, 15, 16, 45, 55, 59, 60, 68, 72  
LAN Cables 11, 15, 16, 45  
LAN Socket 11, 59  
LED 16, 62  
Licence Keys 11  
Listing  
    Registered 52  
Loading 68, 69

## M

MAC 60  
MAC Address 60  
Maintenance Manual 7  
Manager application 10, 17, 22, 38, 46  
Manager Installation 7, 11  
Manager PC 22  
MCIPADD 55  
MCPORT 55  
MG 7  
Microsoft 73  
Microsoft DHCP 73  
Mid-Span Power Unit 16  
Minimum Assessment Target 13  
Mode option 55  
multicast 14  
Multihomed 55  
MultiVantage 72

## N

Network Access 14

network assessment 7, 13  
NIC Cards 55  
No Ethernet 45, 68  
non-IP 7, 48

## O

Other H323 IP 7  
Overlapping VLAN 55

## P

Packet Loss 13  
Password 48, 69  
PC Ethernet LAN 15  
PC Port 15  
PC Softphone 7  
Phone Connection 45  
phone displays 48, 69  
Phone Manager 7  
Phone Security 42  
PHY2 59  
PoE 16  
Potential VoIP Problems 14  
power 11, 14, 15, 45, 48, 68  
    Ethernet 16  
    IP 16  
power conditioning 14  
power supply  
    PSU 11, 14, 16, 45  
Preferences 22  
preinstalled 22  
preparation 22, 69  
Print 52, 60  
Printed Wiring Board 60  
Program 11, 17, 46  
Protection 14  
PWB comcode 60

## Q

QoS 14  
Quality 7, 13, 14

## R

RAM 68, 69  
RAS 52  
Reboot 42, 65, 69  
Registered  
    Listing 52  
registration 48, 69  
Reset System Values 63  
Resetting 63  
Restarting 68  
RFC2474 14  
RJ45 11  
    matching 16  
    provides 16

## S

Save 46, 59, 65, 69  
Scope 55, 72, 73  
script file 58, 68, 69  
Secondary Ethernet 59  
Self-Test Procedure 62  
Serial Number 60  
Setup 42, 55, 63, 68  
Site Specific Settings 38  
Small Installation 10  
Small Office Edition 7, 11, 14, 17, 22  
Spare Wire 16

Speaker/Mute LED 62  
SSON 65  
static address 7, 17, 22, 45, 46, 58, 60, 68  
Static Administration Options 58  
Static IP 7, 11, 22  
subnet mask 46, 72  
SV 7  
SW 15  
Sysmon 52  
System Overview 55

**T**

Tag 55  
TFTP 17  
Timed Out 68  
timeout 17  
Tools 17, 38, 52  
ToS 14

**U**

Unrestricted 55  
Untagged 55

**V**

VCM 22  
    number 7  
VCOMP 22  
VLAN 46, 55  
Voice 7, 11, 13, 14, 15, 22, 55  
Voice Compression Module 11, 22  
voicemail 14, 42  
VoIP 7, 11, 13, 14, 42, 48

**W**

WAN 14  
Watts 16  
Web 38, 55  
Windows 52, 72, 73  
    Windows Notepad 38  
WML 38  
Wordpad 52







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

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

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

© 2012 Avaya Inc. All rights reserved.