



# **IP Office**

## **3600 Series Phone Installation**

#### Notice

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

#### Documentation Disclaimer

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

#### Link Disclaimer

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

#### License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT <http://support.avaya.com/LicenseInfo/> ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s): Designated System(s) License (DS).

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

#### Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

#### Third-Party Components

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

#### Avaya Fraud Intervention

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

#### Trademarks

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

#### Documentation information

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

#### Avaya Support

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

# Contents

	7.1 Wireless Phone Status Messages.....	70
	7.2 Important Information.....	76
	Index .....	77
<b>1. System Overview</b>		
1.1 Overview of the AVPP.....		9
1.2 Wireless Access Points.....		11
1.3 Phones .....		13
1.3.1 3616 Wireless Telephone.....		14
1.3.2 3620 Healthcare Wireless Telephone.....		15
1.3.3 3626 Ruggedized Wireless Telephone.....		16
1.3.4 3641 Wireless Telephone.....		17
1.3.5 3645 Wireless Telephone.....		18
<b>2. Installation</b>		
2.1 Required Software.....		22
2.2 TFTP Server Installation.....		23
2.3 Access Point Installation.....		24
2.4 DHCP Server Installation.....		25
<b>3. AVPP Installation and Configuration</b>		
3.1 AVPP Installation Requirements.....		28
3.2 Connecting to the AVPP.....		29
3.3 Initial AVPP Configuration.....		30
3.4 IP Office AVPP Setup.....		31
3.5 AVPP Maintenance.....		32
3.6 AVPP Configuration Menu.....		33
3.6.1 NetLink SVP-II System.....		33
3.6.2 SVP-II Configuration.....		34
3.6.3 QoS Configuration.....		36
3.6.4 Network Configuration.....		37
3.6.5 Change Password.....		38
3.6.6 System Status.....		39
3.6.7 Error Status.....		40
3.6.8 Network Status.....		41
3.6.9 Software Versions.....		43
<b>4. Phone Configuration</b>		
4.1 Installation Requirements.....		46
4.2 IP Office Auto Registration.....		47
4.3 Phone Software.....		47
4.4 Phone Registration.....		48
4.5 Testing a Wireless Phone.....		51
4.6 IP Office Button Programming.....		52
4.7 Admin Options.....		53
4.7.1 Using the Admin Menu.....		53
4.7.2 3616, 3620, 3626 Admin Menu.....		54
4.7.3 3641 and 3645 Admin Menu.....		55
4.7.4 IP Address.....		56
4.7.5 ESSID.....		57
4.7.6 Security.....		58
<b>5. Certifying the Installation</b>		
5.1 Site Certification.....		60
5.2 Site Survey.....		61
<b>6. Software Maintenance</b>		
6.1 Upgrading Wireless Phones.....		67
<b>7. Miscellaneous</b>		



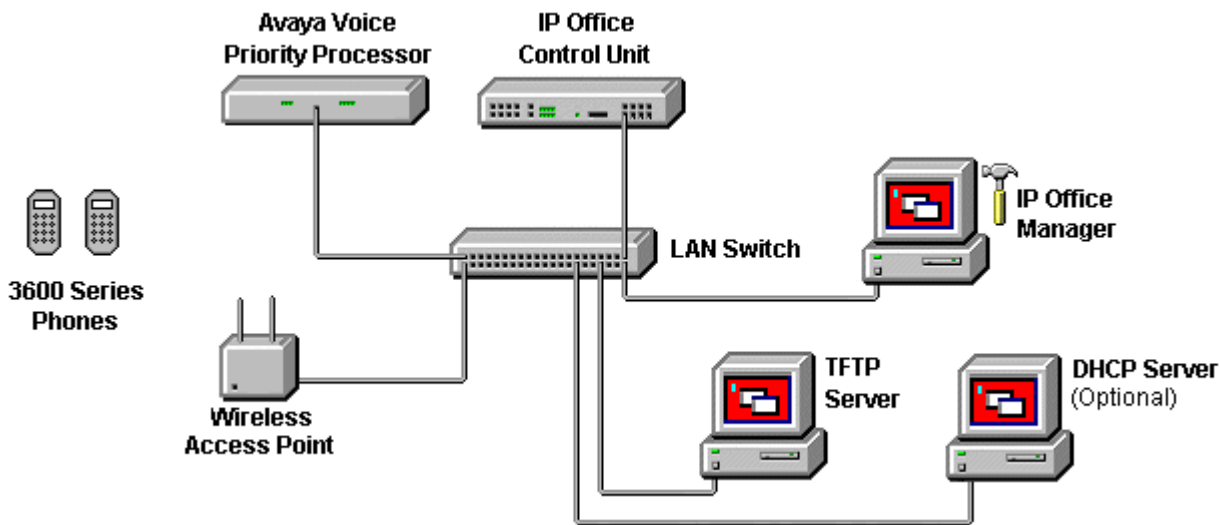
# Chapter 1.

# System Overview



# 1. System Overview

This document contains information on the installation and configuration of the Avaya 3600 Series wireless phones with an IP Office system.



Information is routed from these phones to IP Office via an Avaya Voice Priority Processor (AVPP). The AVPP uses Spectralink Voice Priority (SVP) as the Quality of Service (QoS) mechanism. SVP gives preference to voice packets on the wireless medium, increasing the probability that all voice packets are transmitted efficiently. The use of SVP requires the wireless Access Point to be SVP compatible.

- Avaya 3600 Series Wireless IP Phones  
This is a range of wireless IP phones. Using the 802.11a, 802.11b and 802.11g standard they can be used with a wide range of wireless IP equipment. The 3600 Series phones supported with IP Office are listed below.

WiFi Format	Avaya Phones	
802.11b Only	<a href="#">3616</a> <sup>14</sup>	Basic lightweight wireless VoIP phone.
	<a href="#">3620</a> <sup>15</sup>	Wireless phone designed for healthcare environments.
	<a href="#">3626</a> <sup>16</sup>	Ruggedized wireless phone with push-to-talk functionality.
802.11a/b/g	<a href="#">3641</a> <sup>17</sup>	Multi-spectrum wireless phone
	<a href="#">3645</a> <sup>18</sup>	Multi-spectrum wireless phone with push-to-talk functionality.

- Avaya Voice Priority Processor (AVPP)  
An AVPP is a unit attached to the LAN that ensures quality of service (QoS) for 3600 Series voice calls going to and from the wireless network. AVPP units are required as the current IEEE802.11 wireless LAN standards do not provide a mechanism for differentiating audio packets from data packets. Instead the AVPP applies a proprietary QoS protocol called SpectraLink Voice Protocol (SVP) to the 3600 Series phone voice traffic. An AVPP is required on each sub-net being used for wireless phone access. The AVPP units supported with IP Office are:

AVPP Type	Simultaneous Calls per AVPP	Maximum Number of AVPP's on Network
AVPP010	10	4
AVPP020	20	2
AVPP100	80*	16

\*With the AVPP100 the maximum simultaneous calls per AVPP varies with the number of AVPP's on the network.

- Access Points  
Supplied by Avaya or third party vendors, access points provide the connection between the wired Ethernet LAN and the wireless LAN. The access points used must support the SVP QoS applied to 3600 Series voice traffic by the AVPP. For a complete list of access points supported, go to: [http://www.polycom.com/usa/en/support/voice/wi-fi/wi-fi\\_interoperability.html#download](http://www.polycom.com/usa/en/support/voice/wi-fi/wi-fi_interoperability.html#download).
  - Access points must be positioned in all areas where wireless phones will be used. The number and placement of access points will affect the coverage area and capacity of the wireless system. Typically, the requirements are similar to those of wireless data devices.
- IP Office Control Unit  
Use of 3600 Series phones via an AVPP is supported on all types of IP Office control unit. The IP Office is the telephony switch and each 3600 Series phone must be configured as a user and an extension on the IP Office.

- 
- The IP Office control unit must be fitted with voice compression channels. The number of available channels at any time may restrict the number of calls between 3600 Series phones and other non-IP phones and lines. The method by which voice compression channels are fitted to an IP Office control unit will depend on the control unit type. Refer to the IP Office Installation manual for details, which may have to be fitted as an additional component.
  - Note that whilst the Small Office Edition control unit is able to support a built-in wireless access point, that access point does not provide support the SVP protocol required for Quality of Service (QoS).
  - Ethernet Switch  
Interconnects the multiple network devices, including the AVPP, IP Office and the access points. For small site the IP Office control unit may act as the switch, however for larger sites a dedicated switch is recommended.
  - Although a single Ethernet switch network is recommended, the wireless phones and the AVPP can operate in larger, more complex networks, including networks with multiple Ethernet switches, routers, VLANs and/or multiple subnets. However, in such networks, it is possible for the Quality of Service (QoS) features of the AVPP to be compromised and voice quality may suffer. Any network that consists of more than a single Ethernet switch should be thoroughly tested to ensure any quality issues are detected.
    - The 3600 series wireless phones cannot “roam” from one subnet to another. If routers and multiple subnets are in use, the wireless phones must only use access points attached to a single subnet, or be powered off and back on to switch to a different subnet.
    - IP multicast addresses are used by the 3626 and 3645 wireless phones. This requires that multicasting be enabled on the subnet used for the wireless phones and AVPP servers. Routers are typically configured with filters to prevent multicast traffic from flowing outside of specific domains. The wireless LAN can be placed on a separate VLAN or subnet to reduce the effects of broadcast and multicast traffic from devices in other network segments.
  - Administrative Computer  
A computer is required for setup and maintenance of the AVPP. This computer can be temporarily connected directly to the component or to the network, a dedicated computer is not required. Some installations use a laptop to configure and maintain system components.
  - TFTP Server  
A TFTP server is required in the system to distribute software to the wireless phones and the AVPP. The AVPP units do not support the IP Office internal TFTP server. To download Avaya’s free TFTP server, go to [www.avaya.com/support](http://www.avaya.com/support).
  - DHCP Server (*Optional*)  
The AVPP requires a static IP address. However the 3600 Series phones can use either static addresses or they can use a DHCP server to obtain their addresses.



## 1.1 Overview of the AVPP

The AVPP is connected to the same LAN sub-net as the wireless access points being used for wireless phone operation. The AVPP requires a Cat. 5 cable connection between its network port and the Ethernet switch. The AVPP auto-negotiates to the type of port on the Ethernet switch and supports 10Base-T, 100Base-T, full-duplex and half-duplex port types.

AVPP Type	Simultaneous Calls per AVPP	Maximum Number of AVPP's on Network
AVPP010	10	4
AVPP020	20	2
AVPP100	80*	16

\*With the AVPP100 the maximum simultaneous calls per AVPP varies with the number of AVPP's on the network.

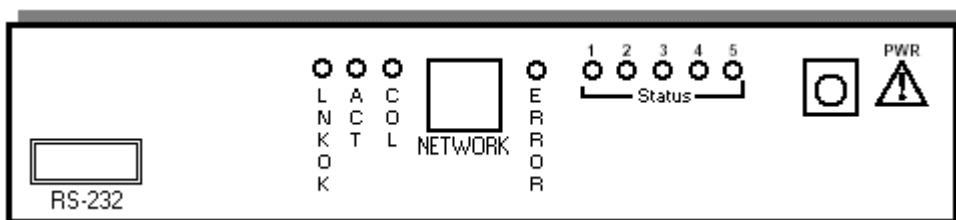
- The AVPP's within a network must be all be the same type.
- The AVPP measures approximately 4 x 12.5 x 7 inches, and weighs about five pounds. The unit can be wall mounted, vertically or horizontally, over  $\frac{3}{4}$ " plywood.
- The AVPP can also be rack mounted using a rack mount kit (sold separately).
- Initially the AVPP requires configuration via a serial port connection. However once basic administration has been performed, further configuration can be done via Telnet access across the LAN.

In a system comprised of multiple AVPP's using an IP protocol, a master AVPP must be identified. The master AVPP server must have a static IP address. The wireless phones and the other AVPP's locate the master by using a static IP address, DHCP, or DNS.

The loss of a non-master AVPP does not significantly affect the operation of the remaining AVPP's. However, the loss of the master AVPP results in a loss of all communication between all of the AVPP's. This also means that the loss of the master AVPP results in the loss of all active calls and wireless phones cannot check-in until communication with the master is re-established.

**The AVPP Front Panel**

The AVPP's front panel contains ports to connect to the LAN, and an administrative computer via an RS-232 port. Status LED's supply information about the AVPP's functionality.



- **RS-232 Port**  
Male DB-9 connector (DTE) used for RS-232 connection to a terminal, terminal emulator, or modem for system administration.
- **Link LED's**
  - LNKOK – Link OK: Lit when there is a network connection.
  - ACT – Activity: Lit if there is system activity.
  - COL – Collision: Lit if there are network collisions.
- **NETWORK**  
Connects to wired (Ethernet) LAN. The AVPP auto-negotiates to the type of port on the Ethernet switch and supports 10Base-T, 100Base-T, full-duplex and half-duplex port types.
- **ERROR LED**  
Lit when the system has detected an error.
- **STATUS LED's**  
Indicate system error messages and status.
  - 1 – heartbeat, indicates gateway is running.
  - 2 – if active calls.
  - 3, 4, 5 – currently unused.
- **PWR**  
Power jack for connection to the AC adapter supplying power to the system. Only use the Avaya-provided Class II AC Adapter with output 24VDC, 1A.

**Multiple AVPP100 Capacity**

The following table shows the capacity of the AVPP100. Note that these are the limitations are for AVPP100's only. Each IP Office model has its own limitations for the maximum number of supporting extensions. For example, IP Office 412 does not support more than 360 extensions.

Number of AVPP100s	Maximum Calls per AVPP	Total Calls		Number of AVPP100s	Maximum Calls per AVPP	Total Calls
1	80	80		9	55	495
2	64	128		10	55	550
3	60	180		11	55	605
4	58	232		12	54	648
5	57	285		13	54	702
6	56	336		14	54	756
7	56	392		15	54	810
8	55	440		16	54	864

## 1.2 Wireless Access Points

Details of those access points that have been used with the AVPP and 3600 Series phones can be obtained from the Spectralink web site.

1. Using a web browser, browse to [http://www.polycom.com/usa/en/support/voice/wi-fi/wi-fi\\_interoperability.html#download](http://www.polycom.com/usa/en/support/voice/wi-fi/wi-fi_interoperability.html#download).
2. The information provided is covers both access points that have been certified for operation with AVPP's and those that have not been certified but have been used in the field by other installers.

The tables below summarize the lists of access points as of April 2007. These may be subject to change and so should be checked against the web site listed about where additional support notes on specific access points can also be found.

Certified access points are access points that have been tested and certified for operation with an AVPP.

Certified Wireless Access Points	
3COM	Wireless LAN Mobility Switches WX4400, WX1200, WXR100 with AP 3750
ALCATEL-LUCENT	OmniAccess WLAN 4302, 4308, 4324, 6000 with AP 41, 60, 61, 65, 70
ARUBA	Mobility Controllers 200, 800, 2400, 6000 with AP 41, 60, 61, 65, 70
BELAIR NETWORKS	BelAir50, BelAir100, BelAir 200 APs
BLUESOCKET	BlueSecure Controllers (BSC) 1100, 2100, 5000 with BlueSecure AP1500, 1540
CISCO	1121, 1231, 1232, 1310 AP (autonomous mode)
	Aironet 1131 and 1242 APs (autonomous mode)
	4400 Series Wireless LAN Controller (WLC) with Aironet 1100, 1200, 1300 Series APs (lightweight mode)
COLUBRIS NETWORKS	MAP-320, MAP-330 autonomous mode or with Multi-Service Controllers 5200, 5500
EXTREME	Summit WM100, WM1000 Wireless Controllers with Altitude 350-2
MERU NETWORKS	MC505, 1000, 3000 Wireless Controllers with AP150
MOTOROLA (SYMBOL)	Wireless Switch WS5100, WS5000 with AP300
NORTEL	WLAN Security Switch 2350, 2360, 2361, 2380 with AP 2330, 2330A
SIEMENS	HiPath Wireless Controllers C10, C100, C1000 with 2610, 2620 APs
TRAPEZE NETWORKS	Mobility System MXR-2, MX-8, MX-8R, MX-20, MX-400 with MP-372, MP-352

Field verified access points have not be tested and certified for operation with an AVPP but are know to have been used in the field. There may be limitations to their operation and there may be charges for support calls regarding uncertified access points.

Field Verified Wireless Access Points	
AVAYA	Wireless Access Point AP-3, AP-4
	Wireless AP-6, AP-7, AP-8
CISCO	340
	350
	Wireless LAN Service Module (WLSM) with AP 1121, 1131, 1231, 1232, 1242, 1310
CISCO (Airespace)	WLAN controller 2000 with 1000 AP
ENTERASYS	RoamAbout Access Point 2000, 3000, R2
HP	ProCurve 420 Access Point
INTERMEC	MobileLAN Access 2100, 2101, 2102, WA21, WA22
LXE	6250 Access Point
MERU	MC500, 1000, 3000 Controllers with AP 100, 201, 208
PROXIM	Orinoco AP-600b, AP-600g, AP-2000
SYMBOL	Spectrum 24 AP4121, 4131

## 1.3 Phones

The following table summarizes the supported phones.

Feature	3616	3620	3626	3641	3645
Radio Mode/ Frequency	801.11.b (2.4-2.4835GHz)			802.11a (5.15-5.825GHz) 802.11b (2.4-2.4835GHz) 802.11g	
Transmission Type	Direct Sequence Spread Spectrum (DSSS)				
Transmission Data Rate	Up to 11Mbps			Up to 54Mbps	
Radio QoS Method	SpectraLink Voice Priority (SVP)				
Wireless Security	Wired Equivalent Privacy (WEP) 40bit and 128bit.			Wired Equivalent Privacy (WEP) 40bit and 128bit. WPA-PSK. WPA2-PSK.	
FCC Certification	Part 15.247				
Management	DHCP, TFTP				
Voice Encoding	G.711, G.729a/b				
VoIP	CCMS				
Transmit Power	100mW peak, <10mW average.			Adjustable peak value: 5, 10, 20, 30, 40, 50mW.	
Display	2 x 16 alphanumeric characters plus line and status indicators.			5 x 16 alphanumeric characters plus line and status indicators.	
Dimensions Height x Width x Depth	5.5"x2.0"x0.9" 14x5.1x2.3cm		5.5"x2.2"x1.0" 14x5.6x2.5cm	5.4"x2.0"x0.9" 13.7x5.1x2.3cm	5.7"x2.0"x0.9" 14.5x5.1x2.3cm
Weight*	4.2 ounces. 119g.		6.0 ounces. 170g.	3.9 ounces. 111g.	4.2 ounces. 119g.
Standard Battery	Talk	4 hours.			
	Standby	80 hours.			
Extended Battery	Talk	–	–	6 hours.	
	Standby	–	–	120 hours.	
Ultra- Extended Battery	Talk	–	–	8 hours.	
	Standby	–	–	160 hours.	

- \*Weight assumes a standard battery pack.
- If push-to-talk is enabled on 3626 and 3645 phones, battery life is reduced by approximately 35%.

---

### 1.3.1 3616 Wireless Telephone

The Avaya 3616 IP Wireless Telephone is a WiFi (802.11b) telephone that runs using H.323.



The 3616 supports the following features:

- Lightweight innovative design .
- Simple to use.
- 802.11b standard-compatible.
- Radio Frequency 2.4000 – 2.835 GHz (SMI).
- Transmission type Direct Sequence Spread Spectrum (DSSS).
- FCC certification Part 15.247.
- Management of telephones via DHCP and TFTP.
- Voice encoding G711.
- Transmit Power 100mw peak, <10mW average.
- Wired Equivalent Privacy (WEP), 40bit and 128 bit.
- 2x16 character alphanumeric, plus status indicators.
- 4 hours talk time and 80 hours standby.

### 1.3.2 3620 Healthcare Wireless Telephone

The Avaya 3620 IP Wireless Telephone is a WiFi (802.11b) telephone that runs using H.323.



The 3620 supports all of the features of 3616 with the following differences:

- Designed for health care environments
- Waterproof durable design.
- Display Backlight:
- Manufacturer's Liquid damage warranty

---

### 1.3.3 3626 Ruggedized Wireless Telephone

The Avaya 3626 Wireless Telephone is a WiFi standard (802.11b) telephone that runs using H.323.



The 3626 supports all of the features of 3616 with the following differences:

- Designed for industrial environments.
- Ruggedized durable design.
- Push-to-talk (walkie-talkie) feature for broadcast communications between employees.

Note:

- 3626 supports both R1.0 and R2.0 firmware on the set itself. However, as of R3.1 of IP Office, only 3626 phone R1.0 firmware is supported.



### 1.3.4 3641 Wireless Telephone

The Avaya 3641 IP Wireless Telephone is a WiFi telephone that runs using H.323.



The 3641 supports the following features:

- Lightweight innovative design .
- Simple to use.
- 802.11a, 802.11b and 802.11g standard-compatible.
- Transmission type Direct Sequence Spread Spectrum (DSSS).
- FCC certification Part 15.247.
- Management of telephones via DHCP and TFTP.
- Voice encoding G711.
- Wired Equivalent Privacy (WEP) - 40bit and 128 bit. WPA-PSK, WPA2-PSK.
- 5x16 character alphanumeric, plus status indicators.
- 4 hours talk time and 80 hours standby. Extendable with optional battery packs to 8 hours talk time and 160 hours standby.

---

### 1.3.5 3645 Wireless Telephone

The Avaya 3645 IP Wireless Telephone is a WiFi telephone that runs using H.323.



The 3645 supports the following features:

- Lightweight innovative design .
- Simple to use.
- 802.11a, 802.11b and 802.11g standard-compatible.
- Transmission type Direct Sequence Spread Spectrum (DSSS).
- FCC certification Part 15.247.
- Management of telephones via DHCP and TFTP.
- Voice encoding G711.
- Wired Equivalent Privacy (WEP) - 40bit and 128 bit. WPA-PSK, WPA2-PSK.
- 5x16 character alphanumeric, plus status indicators.
- 4 hours talk time and 80 hours standby. Extendable with optional battery packs to 8 hours talk time and 160 hours standby.
- Can be enabled for Push-to-talk (walkie-talkie) feature for broadcast between employees.





# Chapter 2.

# Installation

---

## 2. Installation

### 2.1 Required Software

Both the AVPP and the 3600 Series phones require the correct version of software to operate correctly with the IP Office. They load this software during power up using a TFTP transfer from a TFTP server on the LAN.

The necessary software file to be placed on the TFTP server can be obtained from <http://www.polycom.com/usa/en/support/support.html>. The web site will require you to create an account in order to download software.

1. IP Office Manager  
A PC on which the IP Office Manager application can be run will be required. This can either be a customer PC or an installers PC for the duration of installation. The IP Office Manager application is part of the IP Office Admin suite and can be obtained from the following sources:
  - 1.1. IP Office Administration Applications CD
  - 1.2. IP Office Applications DVD.
  - 1.3. Avaya support web site: <http://support.avaya.com>.
2. TFTP Server Software  
A PC with a fixed IP address and running TFTP server software is required. While the IP Office Manager application can act as a TFTP server this is not recommended for 3600 Series phone and AVPP installation.
  - 2.1. Any third-party TFTP application can be used to provide TFTP support. Such an application is available from Avaya. Perform a search for TFTP on the <http://support.avaya.com> web site to download this application and full instructions for its usage.
3. AVPP Software  
Using a web browser, browse to <http://www.polycom.com/usa/en/support/support.html>. For 3641/3645 phones the minimum AVPP software level is 17x.028. Note that if deploying 3641/3645 phones to an existing AVPP network, it is still be necessary to download and update the AVPP software.
4. 3600 Series Phone Software  
Using a web browser, browse to <http://www.polycom.com/usa/en/support/support.html>. The Avaya phone models are equivalent of the following Polycom models.

Avaya Model	Polycom Model
3616	e340
3620	h340
3626	i340
3641	8020
3645	8030

5. Do not proceed with installation until you have obtain the necessary software for the AVPP and 3600 Series phones.

## 2.2 TFTP Server Installation

A TFTP server is required to update the software in both the AVPP and in the 3600 Series phones. Whilst the IP Office Manager application can provide basic TFTP support it is not recommend for support of AVPP units and 3600 Series phones.

Any third-party TFTP application can be used to provide TFTP support. Such an application is available from Avaya. Perform a search for TFTP on the <http://support.avaya.com> web site to download this application and full instructions for its usage.

If IP Office is being used for DHCP, the IP address of the PC running the TFTP software should be set in IP Office configuration. If using a alternate DHCP server, the IP address of the PC running the TFTP software should be set in the 176 options scope for the H.323 IP phones.

### Materials Required

1. TFTP Server Software
2. Server PC  
With fixed IP address and meeting specification of chosen TFTP software

### Tools Required

1.  Access to an additional network PC from which TFTP server operation can be tested.

### Information Required

1.  IP Address of the TFTP server PC.

### Process

1. Download and install on a suitable server PC the selected TFTP server software. This PC should have a fixed IP address within the network. Note that address if not already known. The address is required for both AVPP and phone configuration.
2. If using the Avaya provided TFTP server,
  - 2.1. Select System | Setup and select the Outbound tab.
  - 2.2. Set the Outbound file path to the folder location where you want to place the AVPP and 3600 Series phone software files.
3. Unpack the AVPP and 3600 Series phone software files and place them into the folder setup on the TFTP server as its root folder.
4. Test and check TFTP operation from another PC on the network. A TFTP client can be run from the Windows by select Start | Run and entering *cmd*. Then enter TFTP for instructions.

---

## 2.3 Access Point Installation

Installation of the wireless network access points will be largely dependant on the manufacturers instructions. That will include instructions on the location of access points in order to ensure sufficient wireless coverage in the required areas of usage.

### 1. Perform a Site Survey

Do not proceed with AVPP and 3600 Series phone installation unless a through site survey has been performed.

Perform a site survey following the instructions provided by the access point manufacturer. Most wireless phone audio problems have to do with access point range, positioning and capacity. Performing a site survey can isolate the access point causing these types of problems. If the wireless phone itself is suspected, conduct a parallel site survey with a wireless phone that is known to be properly functioning.

### Potential Problems

The following are the most common problems encountered which would be revealed by a thorough site survey.

- **In Range/Out of Range**  
Service will be disrupted if a user moves outside the area covered by the wireless LAN access points. Service is restored if the user moves back within range. If a call drops because a user moves out of range, the wireless phone will recover the call if the user moves back into range within a few seconds.
- **Capacity**  
In areas of heavy use, the call capacity of a particular access point may be filled. If this happens, the user will hear three chirps from the wireless phone. The user can wait until another user terminates a call, or move within range of another access point and try the call again. If a user is on a call and moves into an area where capacity is full, the system attempts to find another access point. Due to range limitations, this may be the same as moving out of range.
- **Transmission Obstructions**  
Prior to system installation, the best location for access points for optimum transmission coverage was determined. However, small pockets of obstruction may still be present, or obstructions may be introduced into the facility after system installation. This loss of service can be restored by moving out of the obstructed area, or by adding access points.

### Performing Site Surveys Using 3600 Series Phones

The 3600 Series phones can be put into a site survey mode. For details see section [4.2 Site Survey](#) with chapter 4. Certifying the Installation.



## 2.4 DHCP Server Installation

Use of a DHCP server is optional. The 3600 Series phones use DHCP by default, however they can also be individually configured with a fixed IP address information. The IP Office control unit can be used as a DHCP server, however this is only recommended for 5 or less H.323 IP phones. In other scenarios a separate DHCP server must be used.

The method and process for configuration will depend on the DHCP server software being used. Refer to the manufacturers information for details.

### 1. Information Required

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

- The IP address range and subnet mask the 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 the TFTP server that should provide software to the devices.

Option	Notes
1	Subnet Mask
3	Default Gateway
6	DNS Server If this option and option 15 (Domain Name) are set, server names rather than IP addresses can be used in other options. On the Windows 2000 DHCP server this is set through the scope. Other DHCP servers may allow or require it to be set through Option 6 with multiple addresses separated by a comma and no spaces. At least one address must be a dot decimal IP address.
15	Domain Name On the Windows 2000 DHCP server this is set through the scope. Other DHCP servers may allow or require it to be set through Option 15. This option is necessary if the TFTP server is indicated by name rather than address (not supported on Windows DHCP).
43	Vendor Extensions
60	Vendor Class ID
66	TFTP Server Specifies the TFTP server address. Multiple addresses can be entered with each address separated by a comma and no spaces. Microsoft DHCP servers only support dot decimal IP addresses.
151	AVPP The IP address of the master AVPP. The wireless phone will try the following, in order: the DHCP option 151, then a DNS lookup of "SLNKSVP2" if the DHCP options 6 (DNS Server) and 15 (Domain Name) are configured.
152	OAI Gateway The IP address of the OAI Gateway is one is installed.
176	Avaya Specific Options Sets the IP address of the H323 Gatekeeper. MCIPADD=xxx.xxx.xxx.xxx,MCPORT=1719 where: <ul style="list-style-type: none"> <li>• MCIPADD=xx.xxx.xxx.xxx is the H323 Gatekeeper (Callserver) address. Normally, this is the IP Office Unit's LAN1 address.</li> <li>• MCPORT=1719 is the RAS port address for initiating phone registration.</li> </ul>



# **Chapter 3.**

# **AVPP Installation and Configuration**

---

## 3. AVPP Installation and Configuration

### 3.1 AVPP Installation Requirements

#### Materials Required

The following equipment must be provided by the customer:

1. Power Outlet  
Must accept the Avaya provided AC adapter.
2. Backboard space  
The AVPP is designed to be wall mounted to  $\frac{3}{4}$ " plywood securely screwed to the wall. The AVPP measures approximately 4 x 12.5 x 7 inches, and weighs about five pounds. The unit can be wall mounted, vertically or horizontally, over  $\frac{3}{4}$ " plywood.
  - Alternate Mounting  
The AVPP can also be rack mounted using a rack mount kit (sold separately).
3. Screws  
Required to mount the AVPP to the wall. Four #8 -  $\frac{3}{4}$ " panhead wood screws (or similar device) are required.
4. Cat. 5 Cable  
RJ-45 connector at the AVPP. Used for connection to the Ethernet switch.
5. AVPP Software  
Using a web browser, browse to <http://www.polycom.com/usa/en/support/support.html>. For 3641/3645 phones the minimum AVPP software level is 17x.028. Note that if deploying 3641/3645 phones to an existing AVPP network, it is still be necessary to download and update the AVPP software.

#### Tools Required

1. Drills and Screwdrivers  
Tools for mounted using the materials listed above.
2. DB-9 Female null modem cable  
Required for initial PC access to the AVPP configuration.
3. PC with the following:
  - 3.1. Terminal Emulation Program  
Required for initial PC access to the AVPP configuration.
  - 3.2. IP Office Manager Application  
Required to configure the AVPP IP address in the IP Office configuration.

#### Information Required

1. AVPP IP Address, Subnet Mask and Default Gateway  
The first AVPP must be given a fixed IP address. This address must also be on the same subnet as the access points.
2. TFTP Server IP Address  
For software updates, the AVPP checks the software it has against that found at the specified IP address for its TFTP server.

## 3.2 Connecting to the AVPP

The initial connection to the AVPP must be made via a serial connection to establish the AVPP's IP address. After the IP address is established, connection to the AVPP can be done via the network using Telnet. It is recommended that the basic setup actions occur while the serial connection is made.

### Connecting via the Serial Port

This method is required for initial access to the AVPP. Once it has been configured with an IP address future access can be done via Telnet (see below).

1. Using a DB-9 female, null-modem cable, connect the AVPP to the serial port of a terminal or PC.
2. Run a terminal emulation program (such as HyperTerminal™) or use a VT-100 terminal with the following configuration:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
3. To display the AVPP login screen, press Enter.
4. Enter the default login: admin and default password: admin. These are case sensitive. The [NetLink SVP-II System](#) menu is displayed.

### Connecting via Telnet

Telnet can only be used after the AVPP's IP address is configured. Telnet access can be disabled if required through the [Network Configuration](#) menu. Many terminal emulation programs support Telnet connections, alternately a basic Telnet client can be run within Windows

1. Select Start | Run and enter Telnet.
2. Enter open *xxx.xxx.xxx.xxx* where *xxx.xxx.xxx.xxx* is the IP address of the AVPP.
3. Enter the login name and password.
4. If accepted, the [NetLink SVP-II System](#) menu is displayed.

### 3.3 Initial AVPP Configuration

This process covers the basic initial configuration of the AVPP. However it is recommended that as much of the AVPP configuration as possible is done at that stage.

1. Using a DB-9 female, null-modem cable, connect the AVPP to the serial port of a terminal or PC.
2. Run a terminal emulation program (such as HyperTerminal) or use a VT-100 terminal with the following configuration:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
3. To display the AVPP login screen, press Enter.
4. Enter the default login: admin and default password: admin. These are case sensitive. The NetLink SVP-II System menu is displayed.

```
NetLink SVP-II System
Hostname: [SUPV2_1], Address: 10.8.0.61

System Status
SVP-II Configuration
Network Configuration
Change Password
Exit

Enter=Select      ESC=Exit      Use Arrow Keys to Move Cursor
```

5. Use the cursor keys to select Network Configuration and press Enter.

```
Network Configuration
Hostname: [SVP020_1], Address: 10.8.0.61

Ethernet Address (fixed): 00:90:7A:02:8F:AB
IP Address: 10.8.0.61
Hostname: SVP020_1
Subnet Mask: 255.0.0.0
Default Gateway: 10.0.0.90
SVP-II TFTP Download Master: 10.0.0.3
Primary DNS Server: NONE
Secondary DNS Server: NONE
DNS Domain: NONE
WINS Server: 10.13.0.1
Workgroup: WORKGROUP
Syslog Server: 10.0.0.31
Disable Telnet service: N
Maintenance Lock: N

Enter=Change S=Send&ll ESC=Exit      Use Arrow Keys to Move Cursor
```

6. Select IP Address and press Enter. Enter the static IP address for the AVPP unit.
7. Select Subnet Mask and press Enter. Enter the subnet mask that matches the static IP address.
8. Select Default Gateway and press Enter. Enter the IP address of the default gateway for the subnet on which the AVPP is located.
9. Changing the IP address settings automatically puts the AVPP into Maintenance Lock. The AVPP must be reset in order to set the configuration options.
10. Press Esc. You will be prompted to reset the AVPP. At the reset prompt, press Y (Yes).
11. The AVPP will restart. Following the restart, the AVPP menus can be accessed to complete configuration to match the wireless network.

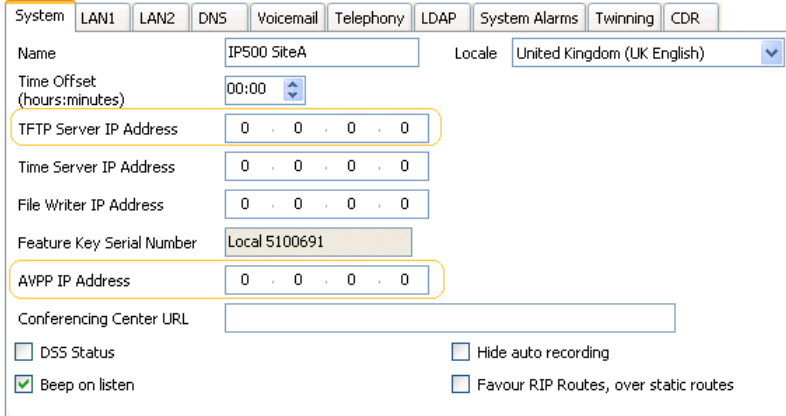
### 3.4 IP Office AVPP Setup

This process is used to add the network location of the AVPP unit to the IP Office configuration.


1. Start IP Office Manager and receive the configuration from the IP Office control unit.

2. Click on  System.

3. Select the System tab.



The screenshot shows the IP Office configuration interface with the 'System' tab selected. The 'AVPP IP Address' field is highlighted with a yellow box. Other fields include Name (IP500 SiteA), Locale (United Kingdom (UK English)), Time Offset (00:00), TFTP Server IP Address (0 . 0 . 0 . 0), Time Server IP Address (0 . 0 . 0 . 0), File Writer IP Address (0 . 0 . 0 . 0), Feature Key Serial Number (Local 5100691), and Conferencing Center URL. There are also checkboxes for DSS Status, Beep on listen, Hide auto recording, and Favour RIP Routes, over static routes.

4. Set the AVPP IP Address to match the static IP address of the AVPP unit.
5. If the IP Office is being used for DHCP support of the 3600 Series phones, set the TFTP Server IP Address to match the IP address of the TFTP server from which the 3600 Series handsets should get their software.
  - If otherwise, the location of the TFTP server for the 3600 Series phones should be set through the DHCP server or through the configuration of the handsets if using static IP configuration.
6. Click OK.
7. Click  or select File | Save Configuration. to send the updated configuration back to the IP Office control unit. Click OK.

---


## 3.5 AVPP Maintenance

### Using SendAll

In an IP system with multiple AVPP's, the SendAll option is provided to speed configuration and ensure identical settings. The S=SendAll option allows you to send that configuration parameter to every AVPP on the LAN.

SendAll can only be used after the IP address is established on each AVPP via the serial connection. If you anticipate identical settings across the LAN, set the IP address and custom hostname (if desired) for each AVPP using the initial serial connection. Connect via the LAN and use SendAll to set identical configuration options for all AVPP's.

If SendAll is to be utilized in your system, all passwords must be identical.

-  Warning  
Do not change the password at the initial configuration if SendAll is desired.

Use the default password and change it globally, if desired, after a LAN connection is established for all AVPP's. If independent administration of each AVPP is desired, the passwords may be set at initial configuration.

- The IP address of the master AVPP can be changed in this menu. After rebooting the system, you can change alias IP addresses in each of the other AVPP servers without error.

### Adding an AVPP

Whenever an AVPP is added to the system, the change is seamless and does not affect the wireless phone calling functionality.

In the IP PBX environment, a new AVPP is detected within two seconds of being added to the system (booted/configured/connected). When detected, any wireless phone that is not active in a call will immediately be forced to check out and check in again. Any wireless phone in a call will immediately switch to the AVPP that should provide its 'timing' function. This switch should not be noticeable to the user since it is similar to a normal handoff between access points. When the call is ended, the wireless phone will be forced to checkout and checkin again.

### Removing an AVPP

Whenever an AVPP is removed from the system, wireless phones that are using the system will be affected. If the removal of the AVPP is intentional, the administrator should lock and idle the system, prior to removing an AVPP.

When an AVPP is removed from the system, it is detected within two seconds. Wireless phones not active on calls are immediately forced to check out and check in again. During the two seconds while the loss of the AVPP is being detected, the audio for the call will be lost.

For wireless phones active in calls, two possible scenarios can occur:

- If the AVPP that was removed was providing the 'gateway' function for the wireless phone, then the call is lost and the wireless phone is forced to check in again.
- If the AVPP that was removed was providing the 'timing' function for the call, then call will switch to the AVPP that should now provide the 'timing' function.

### Changing the Master AVPP

In the event the master AVPP loses communication with the network, the wireless phone system will fail. All AVPP's will lock and all calls will be lost and no calls will be able to be placed. Therefore, if the master AVPP needs replacing, be sure that the system can be brought down with minimal call interruption. Be sure to reset all AVPP's after the master has been replaced. If the IP address of the master is changed, it must be changed in all AVPP's.



## 3.6 AVPP Configuration Menu

### 3.6.1 NetLink SVP-II System

When you connect via the serial port for the first time the following main menu is displayed. Once a name for the AVPP has been entered, on subsequent accesses a screen confirming the name and IP address of the unit is displayed until Enter is pressed.

```
NetLink SVP-II System
Hostname: [SUPU2_1], Address: 10.8.0.61

System Status
SVP-II Configuration
Network Configuration
Change Password
Exit

Enter=Select          ESC=Exit          Use Arrow Keys to Move Cursor
```

- [System Status](#) <sup>[43]</sup>  
Menu for viewing error messages, status of operation and software code version. You can check the version currently installed on AVPP through the System Status menu, see [Software Versions](#) <sup>[43]</sup>.
- [SVP-II Configuration](#) <sup>[34]</sup>  
Allows you to set the mode and reset the system.
  - [QoS Configuration](#) <sup>[36]</sup>  
This sub-menu of the SVP-II Configuration menu is used to alter the QoS settings applied to different signals.
- [Network Configuration](#) <sup>[37]</sup>  
Allows you to set network configuration options, including IP address and hostname.
- [Change Password](#) <sup>[38]</sup>  
Allows you to change the password for AVPP access.

### 3.6.2 SVP-II Configuration

The SVP-II Configuration screen allows you to set the mode of the AVPP for an IP environment. It is also where you can lock the AVPP for maintenance and reset the AVPP after maintenance.

If the IP address is changed, the AVPP will automatically lock for maintenance and the AVPP must be reset upon exit. All active calls are terminated during a reset.

1. From the main menu, scroll to SVP-II Configuration and press Enter.

```
SVP-II Configuration
Hostname: [SVPII_1], Address: 10.8.0.52

SVP-II Mode:                Netlink IP
Ethernet link:              auto-negotiate
System Locked:              N
Maintenance Lock:          N
Inactivity Timeout (min):   20
QoS Configuration
Reset
Reset all SVP servers

Enter=Change  S=SendAll  ESC=Exit    Use Arrow Keys to Move Cursor
```

- SVP-II Mode  
Defaults to *NetLink IP* for an IP environment. Press enter to select and the screen is immediately redrawn with additional options for the IP environment.

```
SVP-II Configuration
Hostname: [SVPII_1], Address: 10.8.0.52

Phones per Access Point:    12
802.11 Rate:                Automatic
SVP-II Master:              10.8.0.52
First Alias IP Address:     0.0.0.0
Last Alias IP Address:      0.0.0.0
Enable H.323 Gatekeeper:    N
SVP-II Mode:                Netlink IP
Ethernet link:              auto-negotiate
System Locked:              N
Maintenance Lock:          N
Inactivity Timeout (min):   20
QoS Configuration
Reset
Reset all SVP servers

Enter=Change  S=SendAll  ESC=Exit    Use Arrow Keys to Move Cursor
```

- Phones per Access Point  
Enter the number of simultaneous calls supported for your type. Access point specifications are detailed in the configuration notes for each brand and type.
- 802.11 Rate  
Select 1MB/2MB to limit the transmission rate between the wireless phones and access points. To allow the wireless phone to determine its rate (up to 11Mb/s), select Automatic.
- SVP-II Master  
The master AVPP must be identified in an IP system. Select one of the following identification options:
  - To statically configure the IP address of the master AVPP in each of the AVPP's, enter the IP address.
  - To statically configure the IP address of the master AVPP in a DHCP server and configure each of the AVPP's to get the information from the DHCP server, enter DHCP. If DHCP is used, the IP address of the master AVPP server must be configured in the DHCP server. For more information about DHCP integration factors, see the wireless phone interface guide for your IP environment.
  - To statically configure the IP address of the master AVPP in a DNS server and configure each of the AVPP's to retrieve this information from the DNS server, enter DNS. If DNS is used, the IP address of the master AVPP server must be configured in the DNS server.

- **First Alias IP Address/Last Alias IP Address**  
Enter the range of IP addresses this AVPP may use when acting as a proxy for the wireless phones. Alias IP addresses are not necessary in Avaya systems.
  - **Note**  
All alias addresses must be on the same subnet as the AVPP server and cannot be duplicated on other subnets or AVPP's. There is no limit to the number of addresses that can be assigned, however, the capacity of each AVPP is 500 wireless phones.
- **Enable H.323 Gatekeeper**  
This function is not supported. Enter N (No).
- **Ethernet link**  
The AVPP will auto-negotiate unless there is a need to specify a link speed.
- **System Locked**  
This option is used to take the system down for maintenance. The default entry is N (No). To prevent any new calls from starting, set as Y (Yes). To restore normal operation, return to N.
- **Maintenance Lock**  
The system automatically sets this option to Y (Yes), after certain maintenance activities that require reset (such as changing the IP address). Maintenance Lock prevents any new calls from starting. This option is automatically set by the system and cannot be changed by the system administrator. To clear the Maintenance Lock, reset the system at exit.
- **Inactivity Timeout (min)**  
Set the number of minutes the administrative module can be left unattended before the system closes it. This number can be from 1 to 100. If it is set to zero (0), the administrative module will not close due to inactivity.
- **QoS Configuration**  
Select this option to set the DSCP tags and the 802.1p tags. See [QoS Configuration](#) <sup>36</sup>.
- **Reset System**  
If this option is selected, you will be prompted to reset the AVPP upon exiting this screen. Resetting the AVPP will terminate any calls in progress.

### 3.6.3 QoS Configuration

If QoS Configuration is selected from the SVP-II Configuration screen.

1. From the main menu, scroll to SVP-II Configuration and press Enter.
2. Select QoS Configuration.

```

QoS Configuration
Hostname: [slnk-03e396], Address: 10.13.0.127

Traffic Class  DSCP Tag
-----
Administration Default
  WT (In call) Default
  WT (Standby) Default
    RTP Default
    PBX Default
  Inter-SUP2 Default

Enter=Change  S=SendAll  ESC=Exit    Use Arrow Keys to Move Cursor

```

Tags set packet priorities for QoS. Either DSCP or 802.1p tags may be used.

- DSCP Tag  
DSCP (Differentiated Services Code Point) is a QoS mechanism for setting relative priorities. In the IP header, packets are tagged with a DSCP field for type of service.
- Traffic Class
  - Administration  
Tags set the priority for Telnet, TFTP and other administrative traffic. Administrative traffic can have the lowest priority because it does not require voice quality.
  - WT (In call)/WT (Standby)  
In call traffic requires voice quality and may be set to a higher priority than standby traffic.
  - RTP  
Audio traffic to the IP PBX. It requires voice quality.
  - PBX  
Traffic not audio to the PBX.
  - Inter-SVP2  
The information passing protocol the AVPP servers use to communicate with each other.

### 3.6.4 Network Configuration

The IP address and other network settings are established via the Network Configuration screen. This is also where you may optionally establish a hostname and enter the IP address of the location of any software updates.

For more information about installing software updates via TFTP, see [Software Maintenance](#) <sup>(66)</sup>.

1. From the main menu, scroll to Network Configuration and press Enter. A screen similar to the following is displayed:

```

                                Network Configuration
                                Hostname: [SVPO20_1], Address: 10.8.0.61

Ethernet Address (fixed):      00:90:7A:02:8F:AB
IP Address:                    10.8.0.61
Hostname:                      SVPO20_1
Subnet Mask:                   255.0.0.0
Default Gateway:              10.0.0.90
SVP-II TFTP Download Master:  10.0.0.3
Primary DNS Server:           NONE
Secondary DNS Server:         NONE
DNS Domain:                   NONE
WINS Server:                  10.13.0.1
Workgroup:                    WORKGROUP
Syslog Server:                10.0.0.31
Disable Telnet service:       N
Maintenance Lock:             N

Enter=Change  S=SendAll  ESC=Exit      Use Arrow Keys to Move Cursor

```

- IP Address  
Enter the IP address of the AVPP, defined by your system administrator.
- Hostname (optional)  
Change the default host name, if desired. This is the name of the AVPP to which you are connected, for identification purposes only. You cannot enter any spaces in this field.
- SVP-II TFTP Download Master  
This entry indicates the source of software updates for the AVPP. Valid source locations are:
  - NONE - disables.
  - IP Address - the IP address of the network TFTP server that will be used to transfer software updates to the AVPP.
- DNS Server and DNS Domain  
These settings are used to configure domain name services. Consult your system administrator for the correct settings. These can also be set to DHCP. This will cause the DHCP client in the AVPP to attempt to automatically get the correct setting from the DHCP server. The DHCP setting is only valid when the IP address is also acquired using DHCP.
- WINS servers  
These settings are used for Windows Name Services. Consult your system administrator for the correct settings. These can also be set to DHCP. This will cause the DHCP client in the AVPP to attempt to automatically get the correct setting from the DHCP server. The DHCP setting is only valid when the IP address is also acquired using DHCP.
  - When the name services are set up correctly, the AVPP can translate hostnames to IP addresses. Using Telnet, it is also possible to access the AVPP using its hostname instead of the IP address.
- Workgroup  
As set in WINS.
- Syslog Server  
Logging can be set to Syslog or NONE. If Syslog is set, a message is sent to the Syslog server when an alarm is triggered.
- Disable Telnet service  
Prevents Telnet access into the AVPP server. Reset the AVPP server for the change to take effect. Upon reset the Telnet protocol server is not started.

The AVPP must be reset in order to set the configuration options. If the AVPP is in Maintenance Lock and you press Esc, you will be prompted to reset the AVPP. At the reset prompt, press Y (Yes).

To manually reset AVPP, select Reset in the SVP-II Configuration screen and then press Y (Yes).

---

### 3.6.5 Change Password

The password to access the AVPP may be changed, if desired. From the Main Menu, select Change Password. A screen similar to the following is displayed:

-  Caution  
Remember to keep the password safe as it cannot be reset remotely.

1. From the main menu, scroll to Change Password and press Enter.

```
Change Password
Hostname: [SUPV2_1], Address: 10.8.0.61

Old Password *****
New Password *****
Confirm New Password *****
Set Password
Set Password on all SUP servers

Enter=Select          ESC=Exit          Use Arrow Keys to Move Cursor
```

2. Enter the information. The password parameters are:
  - More than four characters.
  - First character must be a letter; other characters may be numbers and letters.
  - No dashes, spaces or punctuation marks (alphanumeric only).
3. Select Set Password or press S.

### 3.6.6 System Status

Information about system alarms and network status are displayed on various screens, which can be accessed via the System Status menu.

1. From the AVPP main menu select System Status. A screen similar to the following is displayed:

```
System Status Menu
Hostname: [SUPV2_1], Address: 10.8.0.61

Error Status
Network Status
Software Versions
Gatekeeper Database

Enter=Select          ESC=Exit          Use Arrow Keys to Move Cursor
```

2. The screen displays:
  - [Error Status](#) <sup>[40]</sup>  
Displays alarm and error message information.
  - [Network Status](#) <sup>[41]</sup>  
Displays information about the Ethernet network to which the AVPP is connected.
  - [Software Versions](#) <sup>[43]</sup>  
Lists the software version for the Avaya component.
  - Gatekeeper Database  
Not used.
3. Options on the System Status menu provide a window into the real time operation of the components of the system. Use this data to determine system function and to troubleshoot areas that may be experiencing problems.

---

### 3.6.7 Error Status

The Error Status screen displays any alarms that indicate some system malfunction. Some of these alarms are easily remedied and others require a call to Avaya's Customer Support.

1. From the AVPP main menu select System Status.
2. Select Error Status.
3. The screen displays active alarms on the AVPP. The following table displays the list of alarms and a description of the action to take to eliminate the alarm:

Alarm Text	Action
Maximum payload usage reached	Reduce usage, clear alarm
Maximum telephone usage reached	Reduce usage, clear alarm
Maximum access point usage reached	Reduce usage, clear alarm
Maximum call usage reached	Reduce usage, clear alarm
SRP audio delayed	Reduce usage, clear alarm
SRP audio lost	Reduce usage, clear alarm
No IP address	Configure an IP address

3. To clear all clearable alarms, press C.



### 3.6.8 Network Status

Information about the AVPP's connection to the LAN is provided through the Network Status screen.

1. From the AVPP main menu select System Status.
2. Select Network Status. A screen similar to the following is displayed:

```

Network Status
Hostname: [SUPV2_1], Address: 10.8.0.61

Ethernet Address: 00:90:7A:00:77:15           Net: 100/full
System Uptime: 6 days, 02:34                 Max calls: 80

RX:  bytes      packets  errors  drop  fifo  alignment  multicast
      432891547    4112190      0      0      0          0      1321217

TX:  bytes      packets  errors  drop  fifo  carrier  collisions
      1478261799   1311194      0      0      0          0          0

SUP-II Sockets in Use (Last / Max): 0 / 10
SUP-II Access Points in Calls (Last / Max): 0 / 2
SUP-II Telephones in Use (Last / Max): 0 / 1
SUP-II Telephones in Calls (Last / Max): 0 / 2
SUP-II SRP Audio (Delay / Lost): 0 / 0

ESC to Exit

```

- Ethernet Address  
MAC address of the AVPP (hexadecimal).
- System Uptime  
The number of days, hours and minutes since the AVPP was last reset.
- Net  
The type of connection to the Ethernet switch currently being utilized.
  - Data is transmitted over Avaya components by proprietary technology developed by Avaya. The Avaya Radio Protocol (ARP) packets and bytes can be differentiated from other types of transmissions and are used to evaluate system functioning by Avaya customer support and engineering personnel.
- RX  
Ethernet statistics concerning the received packets during System Uptime.
  - bytes - bytes received.
  - packets - packets received.
  - errors - sum of all receive errors (long packet, short packet, CRC, overrun, alignment).
  - drop - packets dropped due to insufficient memory.
  - fifo - overrun occurred during reception.
  - alignment - nonoctet-aligned packets (number of bits NOT divisible by eight).
  - multicast - packets received with a broadcast or multicast destination address.
- TX  
Ethernet statistics concerning the transmitted packets during System Uptime.
  - bytes - bytes transmitted.
  - packets - packets transmitted.
  - errors - sum of all transmit errors (heartbeat, late collision, repeated collision, underrun, carrier).
  - drop - packets dropped due to insufficient memory.
  - fifo - underrun occurred during transmission.
  - carrier - carrier lost during transmission.
  - collisions - packets deferred (delayed) due to collision.
- SVP-II Access Points in Use  
Access points in use by wireless phones, either in standby or in a call. 'Last' is current, 'Max' is the maximum number in use at one time.
- SVP-II Access Points in Calls  
Access points with wireless phones in a call.

- 
- SVP-11 Telephone in Use  
Wireless phone in standby or in a call.
  - SVP-11 Telephone in Calls  
Wireless phone in a call.
  - SVP-11 ARP Audio (Delay)  
ARP audio packets whose transmission was momentarily delayed.
  - SVP-11 ARP Audio (Lost)  
ARP audio packets dropped due to insufficient memory resources.

### 3.6.9 Software Versions

The AVPP and wireless phones, utilize Avaya's proprietary software that is controlled and maintained through software versions. The Software Version screen provides information about the version currently running on the AVPP. This information will help you determine if you are running the most recent version and will assist Avaya engineering and/or customer support in troubleshooting software problems.

1. From the AVPP main menu select System Status.
2. Select Software Version. A screen similar to the following is displayed:

```

                Software Version Numbers
      Hostname: [SVP020_1], Address: 10.8.0.61

SVP Type:           020
Hardware Versions:  33/02
Factory Page:       213.001
Downloader:         213.004 (99cd73ee)
Table of Contents:  173.024 (4553d976)
Functional Code:    174.024 (f4ae1d58)
File System:        175.024 (4bfc9a09)

                ESC to Exit
    
```

Note that the software versions on your system will be different from the versions displayed in the above sample screen.

Name	Major Version Number	Filename
Table of Contents	173	svp100.toc
Functional Code	174	zvmlinux
File System	175	flashfs

- The minor version numbers for these three files must all match.
- The required AVPP software version for the 3641/3645 handsets is 17x.028.



# Chapter 4.

# Phone Configuration

---

## 4. Phone Configuration

### 4.1 Installation Requirements

This section covers registration of the 3600 Series phones following setup and configuration of the wireless network, AVPP, TFTP server and if necessary DHCP server.

#### Pre-Installation Requirements

1.  Battery Charge  
Ensure that the battery pack on the wireless phone is fully charged.
2.  TFTP Server  
The TFTP server has been setup and tested.
3.  Phone Software  
The required 3600 series phone software has been placed onto the TFTP server.
4.  AVPP  
The AVPP has been configured.
5.  Wireless Network  
The wireless access points are operational and that a thorough site survey has been conducted.
6.  DHCP Server *(if being used)*  
The DHCP server, if being used, is running and has the necessary scopes configured to provide the same information as listed for static IP address configuration listed below.

#### Tools Required

1.  PC with IP Office Manager

#### Information Required

1.  TFTP Server IP Address
2.  AVPP IP Address
3.  Wireless Network  
The wireless access points are operational and that a thorough site survey has been conducted. Ensure that you have the following information about the wireless network:
  - 3.1.  SSID
  - 3.2.  Frequency. For example 802.11a or 802.11b.
  - 3.3.  Security information. For example WEP key and key length if that is the security method being used by the wireless network.
4.  Static IP Address Information  
If not using a DHCP server, ensure that you have the following network information:
  - 4.1.  IP Address for each phone.
  - 4.2.  Sub-net mask
  - 4.3.  Default gateway.
  - 4.4.  Call Server IP (IP Office)
  - 4.5.  Call Server Port (1719).
5.  Phone User Details  
For each phone, ensure you have the following information:
  - 5.1.  Required extension number.

## 4.2 IP Office Auto Registration

The IP Office can allow IP phones including 3600 Series phones to automatically register. During that registration the IP Office will request the extension number required by the phone and password. Those details are used to auto-create a new user and extension within the IP Office configuration.

By default the IP Office options for auto-creation of new extensions and users are enabled, but this should be verified. Also it may be a requirement to disable these options once the new handsets have been registered.

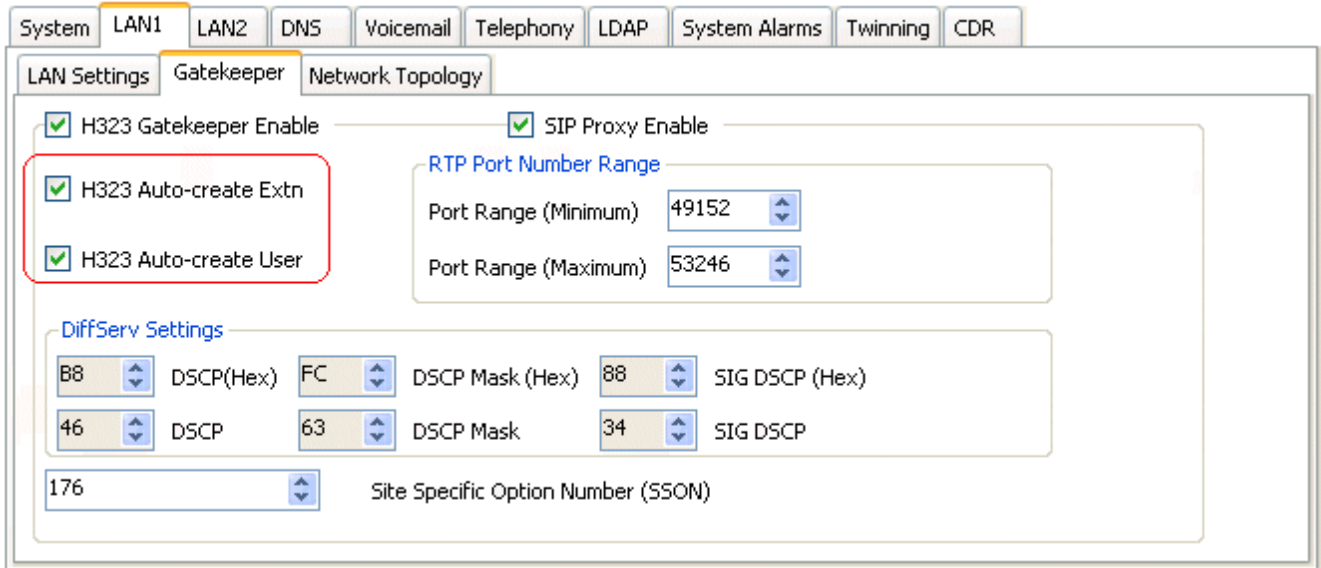
Checking the IP Office IP Phone Auto-Create Settings

1. Start IP Office Manager and receive the configuration from the IP Office control unit.


2. Click on  System.

3. Select the LAN1 tab.

4. Select the Gatekeeper sub-tab.



The screenshot shows the IP Office configuration interface. The 'System' tab is selected, and the 'LAN1' sub-tab is active. Within the 'LAN1' settings, the 'Gatekeeper' sub-tab is selected. The 'H323 Gatekeeper Enable' and 'SIP Proxy Enable' options are checked. The 'H323 Auto-create Extn' and 'H323 Auto-create User' options are also checked and highlighted with a red box. The 'RTP Port Number Range' is set to a minimum of 49152 and a maximum of 53246. The 'DiffServ Settings' section shows various DSCP and SIG DSCP values.

5. To allow 3600 series phones to auto-register, check that the options H323 Auto-create Extn and H323 Auto-create User are enabled.
6. If any changes are made:
  - 6.1. Click OK.
  - 6.2. Click  or select File | Save Configuration. to send the updated configuration back to the IP Office control unit. Click OK.

## 4.3 Phone Software

This process should have already been performed as part of the setup and testing of the TFTP server.

To Download the 3600 Series Phone Software

1. Download the latest 3600 Series phone software.
2. Using a web browser, browse to <http://www.polycom.com/usa/en/support/support.html>. The Avaya phone models are equivalent of the following Polycom models.

Avaya Model	Polycom Model
3616	e340
3620	h340
3626	i340
3641	8020
3645	8030

3. Load the latest version of the 3600 series wireless phone code and place it on the TFTP server. Ensure the files are unzipped in the root directory of the TFTP server.
4. Ensure the TFTP server is started.

---

## 4.4 Phone Registration

### 3616, 3620 and 3626 Phones

1. Do not perform this process until the preceding checks have been completed:
2. Set the phone into administration mode:
  - 2.1. With the phone powered off, simultaneously press and hold the Start Call and End Call buttons.
  - 2.2. After hearing two beeps, release the Start Call button, then release the End Call button.
  - 2.3. If an administration password has been set, it must be entered to display the Admin menu. If no password is set, the Admin menu is displayed.
  - 2.4. To scroll through the menu options, press Up, Down and Select.
  - 2.5. To change the selected option, press OK or press Up to return to the previous menu level.
3. Select Network Config.
  - 3.1. The default mode for IP address operation is DHCP. The following is only required if the phone needs to be switched to static IP address operation:
    - 3.1.1. Select IP Address and then Static IP.
    - 3.1.2. Set the IP Address, TFTP Server IP, Default Gateway and Subnet Mask information as required.
    - 3.1.3. Set the Call Server IP to the LAN address of the IP Office.
    - 3.1.4. Set the Call Server Port to *1719*.
    - 3.1.5. Set the AVPP IP address.
  - 3.2. Select ESSID. If you are accepting broadcast SSID's at your access points, the handset will automatically learn the ESSID information when powering on. If there are multiple wireless networks in range, it will be necessary to enter the SSID of the wireless network that the phone should use.
  - 3.3. Select Security. Enter the wireless security settings that match those configured for the wireless network.
4. Select Phone Config.
  - 4.1. Select License Option. The phone needs to be configured with a telephony protocol number which then ensures the handset checks for the proper software files each time it powers on. Set the value to *009*.
    - 4.1.1. To change the displayed number, press Select.
    - 4.1.2. To scroll through the options, press Up or Down.
    - 4.1.3. To select the displayed number, press Select.
5. Power cycle the phone.
  - 5.1. If the phone's software needs to be updated the new software will now be downloaded from the TFTP server. The status bar will increment fully across the display for each function that is being performed in the download process.
  - 5.2. Upon completion of the update process, the handset will re-boot with the new firmware.
6. The phone will ask for the extension and password. Enter the values required for the user on the IP Office. Once these have been entered, the phone will register with IP Office. Note: The password requested matches the IP Office user Login Code.



## 3641 and 3645 Phones

1. Do not perform this process until the preceding checks have been completed:
2. Set the phone into administration mode:
  - 2.1. With the phone powered off, while pressing the START key press and release the END key.
  - 2.2. When the administration menu appears release the START key.
  - 2.3. If the phone's administration password has been enabled, the phone will require that password to be entered before it displays the administration menu. The default password is 123456. This step is not required if the administration password has not been enabled.
3. Select Network Config.
  - 3.1. The default mode for IP address operation is DHCP. The following is only required if the phone needs to be switched to static IP address operation:
    - 3.1.1. Select IP Addresses and then Static IP.
    - 3.1.2. Set the IP Address, TFTP Server IP, Default Gateway and Subnet Mask information as required.
    - 3.1.3. Set the Call Server IP to the LAN address of the IP Office.
    - 3.1.4. Set the Call Server Port to *1779*.
    - 3.1.5. Set the AVPP IP address.
  - 3.2. Select SSID. Enter the SSID of the wireless network that the phone should use.
  - 3.3. Select Security. Enter the wireless security settings that match those configured for the wireless network.
  - 3.4. Select Reg Domain. The regulatory domain must be set before the wireless frequency and transmit power can be selected. Press LINE and then select the appropriate regulatory domain. *01* = North America. *02* = Europe.
  - 3.5. Once the regulatory domain has been set, the wireless mode can be selected (*802.11a*, *802.11b* or *802.11b/g*). The modes available may vary according to the regulatory domain. If 802.11a is selected, the frequency band or bands to use can also be selected.
  - 3.6. Once the wireless mode is selected, depending on that selection and the regulatory domain, the Transmit Power can be selected.
4. Select Phone Config.
  - 4.1. Select Telephony Protocol. The phone needs to be configured with a telephony protocol number which then ensures the handset checks for the proper software files each time it powers on. Set the value to *033*.
    - 4.1.1. To change the displayed number, press Select.
    - 4.1.2. To scroll through the options, press Up or Down.
    - 4.1.3. To select the displayed number, press Select.
  - 4.2. Select IP Office and set this to *Enable*.
5. Power cycle the phone.
  - 5.1. If the phone's software needs to be updated the new software will now be downloaded from the TFTP server. The status bar will increment fully across the display for each function that is being performed in the download process.
  - 5.2. Upon completion of the update process, the handset will re-boot with the new firmware.
6. The phone will ask for the extension and password. Enter the values required for the user on the IP Office. Once these have been entered, the phone will register with IP Office. Note: The password requested matches the IP Office user Login Code.

## Phone Registration Messages

As part of phone registration, the phone will be requested by the IP Office to enter a extension number and password. The following messages may be displayed as part of that process.

- Note: The password requested matches the IP Office user Login Code.

Display	Possible Cause and Action
Ext. =XXX # =OK New =	<p>Several conditions (new phone, Extension Error, Password Error, and Extension in use) can result in the wireless phone asking the user for a new extension and password. The entry process is described below. When a new extension or password is being entered, the asterisk (*) key can be used to back up and correct an error.</p> <p>Enter the required extension or if # is pressed, the wireless phone will retain the current extension it last used.</p> <p>After a new extension is entered, press # to continue. The wireless phone will then display:</p> <p>Password = ***** # = OK</p> <p>A new password can be entered at this time, or if # is pressed, the wireless phone will continue with its current password. After a new password is entered, press # to continue.</p>
Extension Error	Shown if the IP Office unit does not recognize the extension that the phone is trying to register with. This will last 5 seconds, and then the wireless phone will ask the user to enter a new extension and password.
Password Error # to continue	To enter a new extension and password, press # to continue.
Extension in use # to continue	<p>IP Office will detect when a wireless phone tries to register with the same extension as any phone that is already registered to that extension.</p> <p>To continue, press #. If the user chooses to continue on with the override information, the wireless phone will register with the override bit set. Any phone currently registered with the given extension will be unregistered, and any activity on the currently registered phone will be stopped. If that phone is in a call, it will be dropped.</p> <p>If the user does not want to override the existing extension, either enter a different extension and password, or simply power off the wireless phone.</p> <p>If two wireless phones are assigned to the same extension, the IP Office unit will not properly resolve the registration conflict due to the presence of the AVPP. Both wireless phones may fail to operate properly.</p>
* to Retry # to Restart	Some errors will result in the following display once # is pressed to continue. To immediately retry registering with IP Office, press *. To restart the wireless phone, press # (which will take about 20 seconds).

## 4.5 Testing a Wireless Phone

Verify proper registration and operation of each wireless phone by performing the following tests on each wireless phone in an active wireless area.

1. To power on the wireless phone, press Power On/Start Call. A series of messages are displayed as the wireless phone acquires the system. The wireless phone should display the user extension. Any error messages should clear.
2. Press Power On/Start Call. The extension number should be replaced by information from the IP Office unit and you should hear a dial tone. Place a call and listen to the audio quality. To end the call, press Power Off/End Call.
3. Place a call to the wireless phone and verify ring, answer, clear transmit and clear receive audio.
4. Press Power On/Start Call.
5. Press Power Off/End Call. Any line indicators should turn off and the extension number display will return.
6. Register any further phones.
7. If necessary the IP Office configuration can be altered as required for the user setup, for example user names and button programming.
8. When completed, proceed to [Site Certification](#) before handing over any phones to the users.

---



## 4.6 IP Office Button Programming

Most Avaya phones, including 3600 Series phones, support a number of programmable buttons. These can be used for a range of IP Office functions, detailed in the IP Office Button Programming manual (*15-601012*).

- 3616, 3620 and 3626 Phones  
These phones support 6 programmable buttons. When the phone is on but idle, the button functions can be accessed by pressing LINE and then a key from 1 to 6.
- 3641 and 3645 Phones  
These phones support up to 12 programmable buttons (only support 6 programmable button are available if the phone administration option *IP Office* is disabled). Only the first 9 can be used for appearance functions. Buttons can be accessed in two ways.
  - For the any of the first 9 buttons, when the phone is on but idle by pressing LINE and then a key from 1 to 9.
  - When the phone is on but idle press LINE. The four soft keys below the display will match the first 4 programmable buttons. To access the next set of 4 programmable buttons press LINE again.

### Programming Buttons

By default, every user added to the IP Office system has their first three programmable buttons set as Call Appearance buttons. It is recommend that these are not changed. Note that changes to button programming settings only take effect after the wireless phone is powered off and back on again.

1. If not already done, start IP Office Manager and receive the configuration from the IP Office control unit.
2. Click on  User to display the current users and the settings of the first user.
3. Select the Button Programming tab.
4. To program a particular button, double-click on the matching row to display a form through which you can select the required action and enter the required data for the selection action. Refer to the IP Office Button Programming manual (*15-601012*) for details.
5. Click OK to save the button settings.
6. Click OK to save the user settings.
7. Select and repeat for any other users requiring button programming changes.
8. Click OK.
9. Click  or select File | Save Configuration. to send the updated configuration back to the IP Office control unit. Click OK.

## 4.7 Admin Options

### 4.7.1 Using the Admin Menu

The phone administration menu contains configuration options that are stored locally on each wireless phone. These include network and wireless network settings that must be set to match the network and wireless network.

- Note that the options available vary according to the particular model of phone.

#### 3616, 3620 and 3626 Phones

1. With the phone powered off, simultaneously press and hold the Start Call and End Call buttons.
2. After hearing two beeps, release the Start Call button, then release the End Call button.
3. If an administration password has been set, it must be entered to display the Admin menu. If no password is set, the Admin menu is displayed.
4. To scroll through the menu options, press Up, Down and Select.
5. To change the selected option, press OK or press Up to return to the previous menu level.

#### 3641 and 3645 Phones

1. With the phone powered off, while pressing the START key press and release the END key.
2. When the administration menu appears release the START key.
3. If the phone's administration password has been enabled, the phone will require that password to be entered before it displays the administration menu. The default password is 123456. This step is not required if the administration password has not been enabled.

## 4.7.2 3616, 3620, 3626 Admin Menu

The following table lists the Admin menu items. The default settings are shown with an \*.

Admin Menu	2nd Level	3rd Level	4th Level	Admin Menu	2nd Level	3rd Level	4th Level	5th Level	6th Level			
Phone Config	License Option	Set Current		Network Config	Security	None*						
	Ext.					WEP	Authentication	Open System				
	Password						WEP On/Off	Shared Key				
	IP Office	IP Ofc Enabled IP Ofc Disabled						Off*				
	OAI ON/OFF	Enable OAI Disable OAI						On				
	Push-to-Talk (3626 only)	Allowed Channels	Channel 1*			Key Information	Default Key					
			Channel 2*				Key Length		40bit			
			Channel 3*				Key #1					
			Channel 4*				Key #2					
			Channel 5*				Key #3					
			Channel 6*				Key #4					
			Channel 7*									
			Channel 8*									
		Allow/Disallow	Allow PTT* Disallow PTT			Cisco FSR	Username					
Admin Password					Password							
Network Config	IP Address	Use DHCP*		WPA-PSK	Passphrase							
		Static IP	Phone IP		WPA2-PSK	Pre-shared Key						
			TFTP Server IP			WPA2-PSK	Passphrase					
			Default Gateway		Pre-shared Key							
			Subnet Mask									
			Syslog Server IP									
			Call Server IP									
			Call Server Port									
			AVPP IP									
			OAI Server IP									
	ESS ID		Learn Once*									
	Learn Always											
	Static Entry											
				Diagnostics	Run Site Survey							
				Diagnostics Mode	On							
					Off*							
				Syslog Mode	Disabled*							
					Errors							
					Events							
					Full							
				Restore Defaults								

### 4.7.3 3641 and 3645 Admin Menu

The following table lists the Admin menu items. The default settings are shown with an \*.

Admin Menu	2nd Level	3rd Level	4th Level	Admin Menu	2nd Level	3rd Level	4th Level	5th Level	
Phone Config	Telephone Protocol	Type 030*		Network Config	SSID	[enter]			
		Type 033			Security	None *			
	Push to Talk (3645 only)	PPT	Disable *		WEP	Authentication	Open System *		
			Enable				Shared Key		
		Allowed Channels	Channel 1*			WEP On/Off	WEP Off *		
			...				WEP On		
		Channel 24				Key Information	Default Key		
		Name Channels					Key Length		
	Priority Channel	Off*			Key 1-4				
		On			Rotation Secret				
	Name Channel	Name Channel			WPA2-PSK				
		Name Channel			Passphrase *				
	Time Zone	[list]			Pre-Shared Key				
	Daylight Savings	DST No Adjust*			WPA-PSK				
		DST Auto<USA>			Passphrase *				
		DST Auto<AUS>			Pre-Shared Key				
		DST Auto<EURO>			Cisco FSR				
	System Speeddial	Enter number			Username				
	Password	Disable			Password				
		Enable			Reg Domain				
Change Password			01	802.11a		[frequency]			
Speakerphone	Disable			802.11b*					
	Enable			802.11b/g					
Clear Extension				Transmit Power	5mW (7dB)				
IP Office	Disable				10mW (10dB)				
	Enable				20mW (13dB)				
OAI	Disable				30mW (15dB)				
	Enable				40mW (16dB)				
		50mW (17dB)							
		100mW (20dB)							
Network Config	IP Addresses	Use DHCP *		02	"		"		
		Static IP	Phone IP		Run Site Survey				
	Default Gateway		Diagnostics						
	Subnet mask		Disabled *						
	TFTP Server IP		Enabled						
	Syslog Server IP		Syslog						
	Time Server IP		Disabled *						
	Call Server IP		Errors						
	Call Server Port		Events						
	AVPP IP		Full						
OAI Server IP		Error Handling Mode							
		Restart on Error *							
		Halt on Error							

---

## 4.7.4 IP Address

There are two modes in which the wireless phone can operate: DHCP enabled or static IP.

- Use DHCP *\*Default.*  
Will use Dynamic Host Configuration Protocol (DHCP) to assign an IP address each time the wireless phone is turned on. If DHCP is enabled, the wireless phone also receives all other IP address configurations from the DHCP server.
- Static IP  
This option allows you to manually set fixed IP address for the phone and for the various network servers and services it needs. If selected, the phone will prompt for the IP address of each of the configurable network components. When entering addresses, enter the digits only, including leading zeroes. No periods are required.

The various IP addresses and related settings used are:

- Phone IP  
Phone IP refers to the IP address of the wireless phone. This is automatically assigned if DHCP is used. If using static IP configuration, you must obtain a unique IP address for each phone from your network administrator.
- Default Gateway and Subnet Mask  
Default Gateway and Subnet Masks are used to identify subnets, when using a complex network which includes routers. Both of these must be configured (not set to 0.0.0.0 or 255.255.255.255) for the wireless phone to contact any network components on a different subnet. They can be set using either static IP configuration or via DHCP options 3 (default gateway) and 1 (subnet mask) respectively. Contact your network administrator for the proper settings for your network.
  - The wireless phones cannot “roam” across subnets, since they cannot change their IP address while operational. Ensure that all your access points are attached to the same subnet for proper operation. The wireless phone can change subnets if DHCP is enabled, and the wireless phone is powered off then back on when within range of access points on the new subnet.
- Call Server IP and Call Server Port  
This is the IP address of the H323 gatekeeper which in this case is the IP Office unit. The port to use is 1719. If DHCP is being used, the phone will first check option 43, then option 176 and, if options 6 and 15 are also enabled, it will use DNS lookup of server name set in the option 43 or 176 is name rather than IP address is used.
- AVPP IP  
AVPP IP refers to the IP address of the AVPP. If using static IP configuration, this is simply the IP address of the AVPP. The AVPP must be statically configured to have a permanent IP address.
- TFTP Server IP  
TFTP Server refers to the IP address of a TFTP server on the network that holds software images for updating the wireless phones. If this feature is configured (not set to 0.0.0.0 or 255.255.255.255) with either static IP configuration or using DHCP option 66 (TFTP server), or the Boot server/next server (siaddr) field, the wireless phone will check for newer software each time it is powered on or comes back into range of your network. This check takes only a second and ensures that all wireless phones in your network are kept up-to-date with the same version of software.
- OAI Server IP  
OAI Server refers to the IP address of the NetLink OAI gateway. If using static IP configuration, this is the IP address of the NetLink OAI Gateway. If DHCP is being used, the wireless phone will try the DHCP option 152.
- Syslog Server IP  
The IP address of the Syslog server. Use of Syslog itself is controlled through the Diagnostics | Syslog section of the phone administration menu.
- Time Server IP  
The address of the time server from which the phone should obtain the time that it displays when in standby mode. The time displayed is further adjusted through the Phone Config | Time Zone and Phone Config | Daylight Savings sections of the phone administration menus.



## 4.7.5 ESSID

ESSID (Extended Service Set ID) is an option used by 3616, 3620 and 3626 phones to establish the SSID of the wireless network. Broadcast ESSID must be enabled in the access points for ESSID learning to function.

Overlapping wireless systems complicate the use of ESSID learning as the wireless phone in an overlapping area could receive conflicting signals. If this is the situation use Static Entry or Learn Once.

- Learn Once *\*Default*

The Learn Once option allows the wireless phone to scan all ESSIDs for a DHCP server and/or TFTP server. Once either is found, the wireless phone retains the ESSID from whichever access point it associates with at that point. When overlapping wireless systems exist, the Learn Once feature allows the wireless phone to use only the ESSID established at first learn at all subsequent power on. This ESSID is retained by the wireless phone until the ESSID option is re-selected.

- Learn Always

The Learn Always option allows the wireless phone to automatically learn the ESSID at each power on or loss of contact with the wireless LAN (out of range). This may be useful if the wireless phone will be used at more than one site.

- Static Entry

If your access points do not accept broadcast ESSID or if there are overlapping wireless systems in use at the site, enter the correct ESSID manually:

- On the keypad, press the first digit/letter of the ESSID. The digit is displayed.
- Press the first digit/letter of the ESSID again, to scroll through the letters associated with that key. For example, if you press 2 repeatedly, you will see 2, A, B, and C, a, b, and c.
- The following table shows keys that you use to enter non-numeric characters or other characters not represented on the keypad.

To Enter	Press
. - _ ! # \$ % & ' ( ) , : ; / \ = @ ~ 1	1
Space	0
Q q	7
Z z	9

- When the correct entry is displayed, press Up or Down to move on to the next character. Repeat for each digit/letter of the ESSID.
- To save the entry and return to the menu, press Select. To abort and return to the menu without saving any changes, press FCN.

---

## 4.7.6 Security

Note that while the phone displays keys and passwords as they are entered, they are not displayed after the administration menu is exited and then returned to. If wireless security is in use at a site, you must configure each wireless phone with security settings that match that being used by the wireless access points.

- None *\*Default*  
Disables any 802.11 encryption or security authentication mechanisms.
- WEP  
WEP (Wired Equivalent Privacy) is a wireless encryption protocol that scrambles wireless signals for security in the wireless network. Select the entries from the options below to enable the wireless phone to acquire the system.
  - Authentication  
Select either *Open System (\*Default)* or *Shared Key*.
  - WEP On/Off  
To enable the use of WEP select *WEP On*. The default is *WEP Off*.
  - Key Information  
To scroll through the options, press Up and Down:
  - Default Key  
Enter the key # specified for use by the wireless phones. This will be 1 through 4.
  - Key Length  
Select either 40-bit or 128-bit depending on the key length specified for use at this location.
  - Key 1-4  
Scroll to the key option that corresponds to the default key that was entered above. Press 0 and enter the encryption key as a sequence of hexadecimal characters. (Use the 2 and 3 keys to access hexadecimal digits A-F, use the right arrow key to advance to the next digit, and the left arrow key to backspace). For 40-bit keys you will need to enter 10 digits, for 128-bit keys you will need to enter 26 digits. The display will scroll as needed.
- Rotation Secret  
This is used for proprietary WEP key rotation. Refer to your custom document if this feature is supported in your system.
- WPA2-PSK  
The security features of WPA2 (Wi-Fi Protected Access) using PSK (Pre-Shared Key) are available and may be used if supported by the access points in the facility. Select either Passphrase and enter a passphrase between eight and 63 characters in length or Pre-Shared Key and enter the 256-bit key code.
- WPA-PSK  
The security features of WPA (Wi-Fi Protected Access) using PSK (Pre-Shared Key) are available and may be used if supported by the access points in the facility. Select either Passphrase and enter a passphrase between eight and 63 characters in length or Pre-Shared Key and enter the 256-bit key code.
- Cisco FSR (Fast Secure Roaming)  
A proprietary security mechanism devised by Cisco Systems to overcome some shortcomings in the 802.11 Standard WEP encryption, without impacting the ability of the wireless phones to roam from one access point to another with seamless voice. Cisco FSR requires advanced configuration of the Cisco access points in your site. To configure Cisco FSR on your wireless phone, you must enter a Radius server user name and password into each phone.
- Username  
Enter a user name that matches an entry on your Radius server. User names are alphanumeric strings, and can be entered using the same technique as described above for ESSID entry.
- Password  
Enter the password that corresponds to this user name.

# **Chapter 5.**

# **Certifying the Installation**

---

## 5. Certifying the Installation

### 5.1 Site Certification

The installer should not leave the site before performing installation verification.

These tests must be performed in typical operating conditions, especially if heavy loads occur. Testing sequence and procedure is different for every installation. Generally, you should organize the test according to area and volume, placing numerous calls to others who can listen while you perform coverage tests. Note any areas with excessive static or clarity problems and report it to an Avaya engineer.

The coverage test will also require you to put the wireless phone in Site Survey mode and walk the entire coverage area to verify all access points.



Important

The installation is not complete until these certification steps have been performed. Do NOT hand out wireless phones at a site that has not been certified.

## 5.2 Site Survey

### Doing a Site Survey Using a 3616/3620/3626 Phone

1. With the wireless phone powered off, simultaneously press and hold Power On/Start Call and Power Off/End Call.
2. After hearing two beeps, release Power On/Start Call, then release Power Off/End Call.
3. If an admin password has been set, it must be entered to display the Admin menu. If no password is set, the Admin menu is displayed.
4. Scroll to and select Diagnostics.
5. Select Run Site Survey.
6. Walk the entire coverage area while viewing the display.
7. Numbers racing across the wireless phone display indicate access point information is being obtained. A Waiting message indicates the system is not configured properly and the wireless phone cannot find any access points.
8. The FCN key toggles between the three coverage modes described below.

- Detect dBm Coverage

Press FCN to display *-dBm* on the base of the display. The phone is now showing the signal strength of the top four access points it can contact.

```

XXX1 YY XXX2 YY
XXX3 YY XXX4 YY
-dBm
    
```

- *XXX1* through *XXX4* are the last four digits of the MAC addresses of the access points. The primary access point, the access point which had the strongest signal to this wireless phone, is displayed first, followed by the next three access points in order of signal strength.
- *YY* is the power level in dBm at which this wireless phone heard the associated access point. Although shown as a positive number, *YY* represents negative dBm and lower numbers represent stronger signals. For example, a displayed value of 40 indicates -40dBm, and is therefore a stronger signal than a display of 50 (which indicates -50dBm). At least one access point's reading should be stronger than -70 dBm in all areas.
- Note any areas that have inadequate dBm readings. Coverage issues are best resolved by adding and/or relocating access points.
- Detect Overlaps and Conflicts  
Press FCN to display *Chn* on the base of the display. The phone is now showing the channel that each access point is using. Ideally each access point should be using a unique channel. It is preferable that no overlaps exist anywhere in your facility. If that is not possible, then any location that shares two access points with the same channel should also show at least two access points with stronger signals that do not conflict.

```

XXX1 YY XXX2 YY
XXX3 YY XXX4 YY
Chn1
    
```

- *XXX1* through *XXX4* are the last four digits of the access points' MAC address.
- *ZZ* is the channel number that the access point is using.
- Note any areas that have access points that are in contention for the same channel. Overlap issues may be resolved by re-assigning channels to the access points or by relocating the access points.

---

- Confirm Supported Data Rates

Press FCN to display *Det1* on the base of the display. The phone is now showing full details for an individual access point. Use this to confirm signal strength and supported data rates. Use the right arrow key to display the second best access point, arrow again to the third best, and so on to the fourth best. The left arrow key steps you back to the first best.

```
#:          Full MAC
dB  Ch     1b2b5b11b
Det1
```

- #: the number (1-4) of the access point.
- Full MAC: the MAC address of the access point.
- dB: the signal strength of the access point.
- Ch: the channel of the access point.
- 1b2b5b11b is an example of the data rates that may be displayed. Each data rate (1,2,5.5, or 11Mbit/sec) that is supported by the access point is shown. Those rates that are in the Basic Rate set (sometimes referred to as "required" rates) are indicated by a 'b' following the rate number. The Supported and Basic data rate(s) should be the same on all access points as is appropriate for your environment.

9. When testing is complete, to power off the wireless phone press Power Off/End Call.

Doing a Site Survey Using a 3641 or 3645 Phone

1. With the wireless phone powered off, simultaneously press and hold Power On/Start Call and Power Off/End Call.
2. After hearing two beeps, release Power On/Start Call, then release Power Off/End Call.
3. If an admin password has been set, it must be entered to display the Admin menu. If no password is set, the Admin menu is displayed.
4. Scroll to and select Diagnostics.
5. Select Run Site Survey.
6. When the test is started, it is by default in "single SSID" mode. When the Any soft key is pressed (softkey A) all access points regardless of SSID, are displayed and the softkey changes to say MyID. Pressing the MyID soft key will revert the display to the "single SSID" mode and change the softkey back to Any.
7. The display would look like the following for the multiple AP mode:

```

1 1 1 1 1 1 - 2 2 3 3 4 4 4
1 1 1 1 1 1 - 2 2 3 3 4 4 4
1 1 1 1 1 1 - 2 2 3 3 4 4 4
1 1 1 1 1 1 - 2 2 3 3 4 4 4
Any                               Det1

```

- 1 1 1 1 1 1 – The last three octets of the on-air MAC address for a discovered access point.
- 2 2 – The signal strength from the access point.
- 3 3 – The channel number of the access point.
- 4 4 4 – The beacon interval configured on the access point.
- Any/MyID – Softkey to toggle between "single SSID" and "any SSID" modes.
- Det1/Smry – Softkey to toggle between the multiple access point (summary) display, and the

The following screen shows how the display would look when there are three access points configured with an SSID that matches that of the Wireless IP Telephone. The first has a signal strength of -28dBm, is configured on channel 2, with a beacon interval of 100ms. The second has a signal strength of -48dBm, is configured on channel 6, with a beacon interval of 200ms. The third has a signal strength of -56dBm, is configured on channel 11 with a beacon interval of 100ms.

```

a b 7 b c 8 - 2 8 0 2 1 0 0
2 a e 5 7 8 - 4 8 0 6 2 0 0
2 a e 5 9 6 - 5 6 1 1 1 0 0
Any                               Det1

```

When the Any SSID mode is selected, the summary display contains the first six characters of the access points SSID instead of the beacon interval as in the example below.

```

a b 7 b - 2 8 0 2 A L P H A
2 a e 5 - 4 8 0 6 W S M T E S
2 a e 5 - 5 6 1 1 v o i c e
MyID                               Det1

```

---

In the DetI (detail) mode the display would appear as follows. The Left/Right arrow keys will move between access points.

```
i : b b b b b b s n c h b c n
e e e e e e e e e e D G H I
r r r r r r r r r r r r r r + x x x x
m m m G : g g g g P : p p p p
Any Smry
```

Where:

- i* Index of selected AP (value will be from 0 to 3 inclusive).
- bbbbbb* The last three octets of the BSSID for a discovered access point.
- sn* Signal strength in -dBm.
- ch* Channel.
- bcn* Beacon interval.
- eeeeeeeeeeee* SSID (the first 11 characters).
- DGHI* Standards supported.
- rrrrrrrr* Rates supported. Basic rates will have a "b" following the rate.
- +* more rates are supported than those displayed.
- xxxx* WMM or UPSD if those QoS methods are supported.
- mmm* Security mode.
- G:gggg* Group key security.
- P:pppp* Pairwise key security.
- Any/MyID* Softkey to toggle between "single SSID" and "any SSID" modes.
- DetI/Smry* Softkey to toggle between the multiple AP display (summary), and the single AP display (detail).



# **Chapter 6.**

# **Software Maintenance**

---

## 6. Software Maintenance

Both the AVPP and the 3600 Series phones check and obtain their software via TFTP. Therefore TFTP transfer must be supported across the LAN between these devices and their configured TFTP server. Both types of device check their current software against that available whenever they are restarted.

When necessary Avaya, or its authorized distributors will provide information about software updates and how to obtain that software. That software should be unpacked to the appropriate TFTP server and the devices restarted.

- **3600 Series Wireless Phones**  
The wireless phones use proprietary software programs. The software versions that are running on the wireless phones can be displayed during power on by holding down Power On/Start Call button. For 3600 Series phones, the location of the TFTP server is allocated by the DHCP server or if statically addresses set through the phone's [Admin](#) [53] menu.
- **AVPP**  
The AVPP uses proprietary software programs. The software versions that are running on the system components can be displayed via the System Status | Software Version menu. At startup, the AVPP uses TFTP to check the software version it is running against the version in the TFTP location. If there is a discrepancy, the AVPP will download the version in the TFTP location. For the AVPP the location of its TFTP server is set by the SVP-II TFTP Download Master field in its [Network Configuration](#) [37] settings.

## 6.1 Upgrading Wireless Phones

After software updates are obtained, they must be transferred to the appropriate location in the LAN to update the code used by the wireless phones.

The wireless phones allow over-the-air transfer of software updates from the designated TFTP server to the wireless phones. The downloading function in the wireless phone checks its software version every time the wireless phone is turned on. If there is any discrepancy the wireless phone immediately begins to download the update.

### Normal Download Messages

When the wireless phone is powered on, it displays a series of messages indicating that it is searching for new software, checking the versions and if necessary downloading. The list below shows the normal message progression:

1. **Checking Code**  
The wireless phone is contacting the TFTP server to determine if it has a newer version of software that should be downloaded.
2. **Erasing Memory**  
The wireless phone has determined that a download should occur and is erasing the current software from memory. This message also displays a progress bar. When the progress bar fills the display line the erase operation is complete.
3. **Updating Code**  
The wireless phone is downloading new software into memory. The number icons at the bottom of the display indicate which file number is currently being downloaded. This message also displays a progress bar. When the progress bar fills the display line the update operation is complete on that file.

When the update is complete, the wireless phone displays the extension number and is ready to use.

### Download Failure or Recovery Messages

The list below shows the display messages which indicate a failure or recovery situation during the download process.

- **Server Busy**  
The wireless phone is attempting to download from a TFTP server that is busy downloading other phones and refusing additional downloads. The wireless phone will automatically retry the download every few seconds.
- **TFTP ERROR(x):yy**  
A failure has occurred during the TFTP download of one of the files. (x) = The file number which was being downloaded; yy is an error code describing the particular failure. Possible error codes are:
  - 01 = TFTP server did not find the requested file.
  - 02 = Access violation (reported from TFTP server).
  - 07 = TFTP server reported "No such user" error. Check the TFTP server configuration.
  - 81 = File put into memory did not CRC. The wireless phone will attempt to download the file again.
  - FF = Timeout error. TFTP server did not respond within a specified period of time.
- **Erase Failed**  
Download process failed to erase the memory in the wireless phone. This operation will retry.
- **Warning**  
The wireless phone has attempted some operation several times and failed, and is now waiting for a period of time before attempting that operation again.



# Chapter 7.

## Miscellaneous

---

## 7. Miscellaneous

### 7.1 Wireless Phone Status Messages

Wireless phone status messages provide information about the wireless phone's communication with the access point and host phone system. The following table summarizes the status messages, in alphabetical order.

- **3 chirps**  
The wireless phone is not able to communicate with the best access point, probably because that access point has no bandwidth available. Action: None. This is only a warning, the call will hand off to the best access point once it becomes available.
- **Address Mismatch**  
Wireless IP telephone software download files are incorrect or corrupted. Action: Download new software.
- **Assoc Failed**  
The wireless IP telephone association was refused by the access point. MAC address of the access point is displayed. Action: Check the wireless IP phone and access point security settings.
- **Assoc Timeout**  
The wireless IP telephone did not receive an association response from the access point. The MAC address of the access point is displayed. Action: Check the wireless IP phone and access point security settings.
- **Auth Failed**  
Phone authentication was refused by the access point. The MAC address of the access point is displayed. Action: Check the wireless IP phone and access point security settings.
- **Auth Timeout**  
The phone did not receive an authentication response from the access point. The MAC address of the access point is displayed. Action: Check the wireless IP phone and access point security settings.
- **ASSERTxxx.c Line yyy**  
The phone has detected a fault from which it cannot recover. Action: Record the error code so it can be reported. Turn the wireless phone off then on again. If error persists, try registering a different wireless phone to the phone port. If error still persists, contact Technical Support and repeat the error.
- **Bad Code Type xx**  
The phone's current loaded software does not match the selected license type. Action: Download the correct phone software and restart the phone.
- **Bad Config**  
Some needed configuration parameter has not been set. Action: Check all required wireless phone configuration parameters for valid settings.
- **Bad SSID**  
The wireless phone is configured for "static SSID" (as opposed to "Learn once" or "Learn always" and no SSID has been entered. Action: Enter an SSID in the configuration settings or change to one of the "Learn" modes.
- **Bad Phintl File**  
The phone software files loaded are incorrect or corrupted. Action: Download the correct phone software and restart the phone.
- **Bad Program File**  
The phone software files loaded are incorrect or corrupted. Action: Download the correct phone software and restart the phone.
- **Can't Renew DHCP**  
The DHCP server is not responding to the initial renewal attempt. Action: Check the IP address configuration in the DHCP server.
- **Charging...**  
The wireless phone is charging in the desktop charger. Action: No action needed.
- **Charge Complete**  
The wireless phone is now fully charged. Action: No action needed.
- **Checking Code**  
The wireless phone is contacting the TFTP Server to determine if it has a newer version of software that should be downloaded. Action: None, this message should only last for approximately one second. If message remains displayed, power off and contact customer support for a replacement phone.
- **Checking DHCP IP**  
The wireless phone is retrieving DHCP information from the DHCP server. Action: None. This is information only.

- **CRC Code Error**  
The software which has been TFTP downloaded has a bad redundancy code check. Action: Try the download again, it is possible the software was corrupted during download. If the error repeats, check that the download image on the TFTP server is not corrupted.
- **Code Mismatch!**  
The software loaded into the wireless phone is incorrect for this model phone. Action: Replace the software image on the TFTP server with software that is correct for the phone model.
- **DCA Timeout**  
The phone has detected a fault for which it cannot recover., possible due to a failure to acquire any network. Action: Restart the phone.
- **DHCP Error 1**  
Action: The wireless phone cannot locate a DHCP server. It will try every 4 seconds until a server is located.
- **DHCP Error 2**  
Action: The wireless phone has not received a response from the server for a request to an IP address. It will retry until a server is found.
- **DHCP Error 3**  
Action: The server refuses to lease the wireless phone an IP address. It will keep trying.
- **DHCP Error 4**  
Action: The server offered the wireless phone a lease that is too short. The minimum lease time is 10 minutes but Spectralink recommend at least one hour minimum lease time. The wireless phone will stop trying. Re-configure the server and power cycle the wireless phone.
- **DHCP: Error 5**  
Failure during WEP key rotation process.
- **DHCP Lease Exp**  
The wireless phone's DHCP lease has expired, and the call (if any) cannot continue. Action: The wireless phone failed to renew its DHCP lease, either because the DHCP server is not running, or because the configuration has been changed by the administrator. The wireless phone will attempt to negotiate a new lease, which will either work, or change to one of the above DHCP errors (1-4).
- **DHCP NACK error**  
A NACK (Negative ACKnowledge)was received from the DHCP server. Action: The DHCP lease currently in use by the wireless phone is no longer valid, which forces the wireless phone to restart. This problem should resolve itself on the restart. If it does not, the problem is in the DHCP server.
- **DL Not On Sector**  
The phone software files loaded are incorrect or corrupted. Action: Download the correct phone software and restart the phone.
- **DO NOT POWER OFF**  
The wireless phone is in a critical section of the software update. Action: None. Do not remove the battery or attempt to power off the phone while this is displayed. Doing so may require the phone to be returned to Avaya to be recovered.
- **Duplicate IP**  
The wireless phone has detected another device with its same IP address. Action: If using DHCP, check that the DHCP server is properly configured to avoid duplicate addresses. If using static IP, check that the wireless phone was assigned a unique address.
- **Erase Failed**  
Download process failed to erase the memory in the wireless phone. Action: Operation will retry but may eventually report the error "int. error: OF" Power cycle the phone.
- **Erasing Memory**  
The wireless phone has determined that a download should occur and is erasing the current software from memory. Action: None. When the progress bar fills the display line the erase operation is complete.
- **Error!...**  
A fatal software error has occurred. All handset operation is halted and any call is lost. Action: This message appears during Halt on Error mode. An error message is displayed below Error!. Note the details of the message and restart the handset.
- **Extension Error**  
Displayed for 5 seconds when all of the IP Offices contacted indicate that they do not recognize the current extension as valid. Action: The user will be asked to enter a valid extension and password.
- **Extension in use**  
The phone is trying to register with an extension that is already registered on IP Office.

- 
- **Files Too Big**  
The phone software files loaded are incorrect or corrupted. Action: Download the correct phone software and restart the phone.
  - **Flash Config Error**  
The phones internal configuration is corrupt. Action: Select Restore Defaults from the phone Admin menu.
  - **Incompatible**  
The switch is rejecting the software version presented by the phone. Action: If this condition persists, contact the system administrator.
  - **Initializing...**  
The wireless phone is performing power on initialization. Action: None. This is information only.
  - **Internal Err. ##**  
The wireless phone has detected a fault from which it cannot recover. Action: Record the error code so that it can be reported. Turn the wireless phone off and then on again. If the error persists, try registering a different wireless phone to the phone port. If error still persists, contact Avaya Technical Support and report the error.
  - **Low Battery (and beep)**  
Action: On call: the battery icon displays and a soft beep will be heard when the user is on the wireless phone and the battery charge is low. User has 15–30 minutes of battery life left. Action: Not on call: The battery icon displays whenever the battery pack charge is low The message Low Battery and a beep sound indicate a critically low battery charge when user is not on the wireless phone. The wireless phone will not work until the battery pack is charged.
  - **Multiple GW Res**  
More than one SVP server has responded. Action: Caused by two or more wireless phones sharing the same IP address. Assign unique IP addresses to each wireless phone.
  - **Multiple SVP Reg**  
The phone has received responses from multiple AVPP's. Action: This can happen if the phone has been configured to use a different AVPP and then powered up before the previous server has had time to determine that the phone is no longer connected to it. The problem should resolve itself after about 30 seconds.
  - **Must Upgrade SW!**  
The phone software is incompatible with the hardware. Action: Download the correct phone software and restart the phone.
  - **Net Busy**  
The phone cannot obtain sufficient bandwidth to support a call. The MAC address of the access point is displayed. Action: Try calling again later.
  - **No Answer**  
The called party did not answer. Action: No action, not an error.
  - **No AVPP IP**  
The wireless phone is configured for "static IP" (as opposed to "use DHCP") and no valid AVPP address has been entered. Action: Enter a valid AVPP IP address in the configuration setting or change to "use DHCP".
  - **No AVPP Response**  
The AVPP is not responding to requests from the wireless phone. Action: This may be caused by bad radio reception or a problem with AVPP. The wireless phone will keep trying to fix the problem for 20 seconds, and the message may clear by itself. If it does not, the wireless phone will restart. Report this problem to the system administrator if it keeps happening.
  - **No AVPP Server**  
This indicates one of the following:
    - The wireless phone cannot locate AVPP. Action: IP address configuration of the AVPP is wrong or missing.
    - AVPP is not working. Action: Check error status screen on the AVPP.
    - No LAN connection at the AVPP. Action: Verify the AVPP connection to LAN.
  - **No Call Server**  
This indicates that while there has been a response from the H323 Gatekeeper (the IP Office) it is not responding to the Registration Request message.
  - **No Call Server IP**  
The phone cannot obtain an IP address for the H323 Gatekeeper (the IP Office).
  - **No DHCP Server**  
The phone is unable to contact the DHCP server.



- No Extension  
The phone has not obtained or been set with a an extension number. Action: Enter a valid extension.
- No Func Code  
The phone software files loaded are incorrect or corrupted. Action: Download the correct phone software and restart the phone.
- No Gateway IP  
The phone is configured for static IP addresses and no valid unicast IP address is assigned for gateway configuration. Action: Configure a valid IP address in the Admin menus.
- No Host IP  
The wireless phone is configured for "static IP" (as opposed to "use DHCP") and no valid host IP address (the wireless phone's IP address) has been entered. Action: Enter a valid IP address in the configuration settings or change to "use DHCP".
- No IP Address  
Invalid IP. Action: Check the IP address in the configuration settings or change to "use DHCP".
- No IP Office  
The No IP Office message may include an error indication:
  - The wireless phone is not administered on IP Office. Action: The wireless phone is not properly configured. Verify that the extension and password in the wireless phone match those administered on the IP Office unit.
  - IP Office is not working. Action: Verify that IP Office is operational. If so, follow standard troubleshooting procedures for IP Office.
  - No LAN connection at the access point or the IP Office. Action: Verify the IP Office connection to LAN and all access points.
  - The wireless phone cannot locate the IP Office. Action: IP address configuration of IP Office is wrong or missing.
- No Net Access  
This indicates one of the following:
  - Cannot authenticate/associate with access point. Action: Verify the access point configuration.
  - Incorrect WEP settings. Action: Verify that all the WEP settings in the wireless phone, match those in the access points.
- No Net Found/No APs  
This indicates one of the following:
  - No radio link. Action: Verify that the access point is turned on.
  - No SSID - Autolearn not supported (or) incorrect SSID. Action: Verify that the SSID of the wireless LAN and enter or Autolearn it again if required.
  - AP Does not support appropriate data rates. Action: Check the access point configuration against the configuration documentation for the access point.
  - Out of range. Action: Try getting close to an access point. Check to see if other wireless phones are working within the same range of an access point. If so, check the SSID of this wireless phone.
  - Incorrect security settings. Action: Verify that all the security settings match those of the access point.
- No Net Found  
The phone cannot find a suitable access point. The MAC address and signal strength of the "best" non-suitable access point are also shown. Action: Check that the phone and the access point SSID and security settings match.
- No Reg Domain  
Regulatory Domain not set. Action: Configure the Regulatory Domain of the wireless phone.
- No SSID  
Attempting to run site survey mode without an SSID set. Action: Restart the phone and statically configure the SSID through the Admin options.
- No SVP IP  
The phone is configured for "static IP" and no valid AVPP has been entered. Action: Enter a valid AVPP address.
- No SVP Response  
The phone has lost contact with the AVPP. The IP address of the AVPP is also shown. Action: This may be caused by bad radio reception of a problem with the AVPP. The phone will keep trying to make contact for 20 seconds during which the message may clear itself if contact is established.

- 
- **No SVP Server**  
The phone cannot locate the AVPP. Action: Check the address configured in the phone is using static addressing. Check the AVPP.
  - **No SVP Server / No DNS Entry**  
The phone cannot perform DNS lookup of the AVPP. Action: Verify that a proper address has been entered for the AVPP on the DNS sever.
  - **No SVP / No DNS IP**  
The phone cannot perform DNS lookup of the AVPP as it has no IP address for the DNS server. Action: Check the operation of the DHCP server.
  - **No SW Found**  
A required software component has not be found. Action: Check that the phone license type has a corresponding entry in the sink\_cfg.cfg file on the TFTP server and that the files list are present on the TFTP server.
  - **Not Installed!**  
A required software component is missing. Action: Check that all required software files are on the TFTP server, if over-the-air downloading is being used. If the error repeats, contact Avaya Technical Support.
  - **Password Error**  
The phone is not encrypting the challenge string correctly. This indicates that the password set in the phone disagrees with the password administered in IP Office. Action: Enter the correct password in the phone.
  - **Press END**  
Your call has ended. Action: To return to standby mode, press Power Off/End Call.
  - **Restarting...**  
The wireless phone is in the process of rebooting. There will be a 20 second delay in an attempt to let potential network/system errors clear. Action: None.
  - **Retry/Restart**  
The wireless phone is waiting for user input, prior to retrying the registration process or restarting after a delay. Action: See Avaya IP Office Integration Factors.
  - **Select License**  
The correct protocol has not been selected from the license set. Action: Using the administrative menus, select one license from the set to allow the phone to download the appropriate software.
  - **Server Busy**  
The wireless phone is attempting to download from a TFTP server that is busy downloading other devices and refusing additional downloads. Action: None, the wireless phone will automatically retry the download every few seconds.
  - **Service Unavailable / Restarting...**  
An error has caused the handset to lose the call. It is now attempting to restart and return to standby. Action: This occurs when Restart on Error operation has been selected.
  - **Storing Config**  
The phone is in the process of storing changes to its configuration.
  - **SVP Service Rej.**  
The AVPP has rejected a request from the phone. Action: The phone will restart and attempt to re-register with the AVPP.
  - **System Busy**  
AVPP is busy or out of resources. The IP address of the AVPP is also shown. Action: All call paths are in use, try calling again in a few minutes.
  - **System Error**  
An internal failure has occurred in AVPP. Action: If this condition persists, contact the system administrator.
  - **System Locked (with Busy Tone)**  
AVPP is locked. Action: Try calling again later.

- **TFTP ERROR(x):yy**  
A failure has occurred during a TFTP software download. (x) = The file number which was being downloaded; yy is an error code describing the particular failure. Possible error codes are:
  - 01 = TFTP server did not find the requested file.
  - 02 = Access violation (reported from TFTP server).
  - 07 = TFTP server reported "No such user" error.
  - 81 = File put into memory did not CRC.
  - FF = Timeout error. TFTP server did not respond within a specified period of time.
- **Action: Error code 01, 02 or 07 - check the TFTP server configuration.**
- **Action: Error code 81 - the wireless phone will attempt to download the file again.**
- **Action: For other messages, power off the wireless phone, then turn it on again to retry the download. If the error repeats, note it and contact Technical Support.**
- **Too Many Errors**  
The phone continues to reset and cannot be recovered. Action: Fatal error, arrange for the phone to be replaced.
- **Trying xxx.xxx.xxx.xxx**  
The phone is attempting to register with IP Office at IP xxx.xxx.xxx.xxx. Action: None. The display is a progress indicator and may not appear long enough to recognize during a normal check-in.
- **Undefined Error**  
The system is rejecting the registration of the wireless phone with an unrecognized error code. Action: If this condition persists, contact the Avaya system administrator.
- **Unknown xx:yy:zz**  
The phone software files loaded are incorrect or corrupted. Action: Download the correct phone software and restart the phone.
- **Unreachable**  
Dialed number does not exist.
- **Updating...**  
The wireless phone is internally updating its software images. Action: None. The wireless phone may do this briefly after a download. This is information only.
- **Updating Code...**  
The wireless phone is downloading new software into memory. The number icons at the bottom of the display indicate which file number is currently being downloaded. Action: None. When the progress bar fills the display line, the update operation is complete on that file.
- **Updating Options**  
This messages appears the first time the handset is powered on and following restoring it to default settings.
- **Waiting...**  
The wireless phone has attempted some operation several times and failed. Action: None. The wireless phone is waiting for a specific period of time before attempting that operation again.
- **Wrong Code Type**  
Internal consistency check failure. Action: Check that the license type is set to 09 (3616, 3620 and 3626 phones) or 33 (3641 and 3645 phones).
- **Wrong Set Type**  
The set type administered on IP Office disagrees with the set type for the wireless phone.
- **(No message shown)**  
There is no voice path. Action: Verify that the audio codec is set correctly (either G.729a or G.711).
- **(No message shown)**  
Messages are left at the principal station but the MSG icon is not lit on the wireless phone. Action: Verify that "Message Lamp Ext", on the station form for the wireless phone, is set to the extension of the principal station.

---

## 7.2 Important Information

### Safety Information

Follow these general precautions when installing phone equipment:

- Never install phone wiring during a lightning storm.
- Never install phone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated phone wires or terminals unless the phone line has been disconnected at the network interface.
- Use caution when installing or modifying phone lines.

### Shielded Cables

Avaya recommends the use of shielded cables for all external signal connections, in order to maintain FCC Part 15 emissions requirements.

### Avaya Voice Priority Processor (AVPP)

The AVPP 10, 20 and 100 have been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

### 3600 Series Wireless Phones

These devices comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference
2. This device must accept any interference received, including interference that may cause undesired operation.



#### Warning

- Changes or modifications to this equipment, not approved by Avaya, may cause this equipment to be non-compliant with part 15 of the FCC rules and void the user's authority to operate this equipment.
- Avaya products contain no user-serviceable parts inside. Refer servicing to qualified service personnel.

---

# Index

## A

- Access Point Installation 24
- Admin Menu 54, 55
  - Using 53
- AVPP
  - Connecting 29
  - Overview 9
- AVPP Installation Requirements 28
- AVPP Maintenance 32

## C

- Certification 60
- Change Password 38
- Connecting
  - AVPP 29

## D

- DHCP Servers 25

## E

- Error Status 40
- ESSID 57

## H

- Healthcare Wireless Telephone 15

## I

- Important Information 76
- Initial Configuration 30
- Installation Requirements 46
- IP Address 56
- IP Office Auto Registration 47
- IP Office AVPP Setup 31
- IP Office Button Programming 52

## N

- NetLink SVP-II System Menu 33
- Network Configuration 37
- Network Status 41

## O

- Overview
  - AVPP 9

## P

- Phone Registration 48
- Phone Software 47
- Phone Specifications 13

## Q

- QoS Configuration 36

## R

- Required Software 22
- Ruggedized Wireless Phone 16

## S

- Security 58
- Software Maintenance 66
- Software Versions 43
- Survey 61
- SVPP-II Configuration 34
- System Overview 7
- System Status Menu 39

## T

- Testing
  - Wireless Phone 51
- TFTP Server Installation 23

## U

- Upgrading
  - Wireless Phones 67

## Using

- Admin Menu 53

## W

- Wireless Access Points 11
- Wireless Phone Status Messages 70
- Wireless Phones
  - Testing 51
  - Upgrading 67
- Wireless Telephone 14





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

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

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

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

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

© 2008 Avaya Inc. All rights reserved.

Avaya  
Unit 1, Sterling Court  
15 - 21 Mundells  
Welwyn Garden City  
Hertfordshire  
AL7 1LZ  
England.

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

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