IP Office

3600 Series Phone Installation

15-601082 Issue 06a - (21 February 2014)

Notice
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.
For full support, please see the complete document, Avaya Support Notices for Hardware Documentation, document number 03–600759.
For full support, please see the complete document, Avaya Support Notices for Software Documentation, document number 03–600758.
To locate this document on our website, simply go to http://www.avaya.com/support and search for the document number in the search box.

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

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

Warranty
Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).
Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “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.

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

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

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

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

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

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

Heritage Nortel Software
“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Virtualization
Each vAppliance will have its own ordering code. Note that each instance of a vAppliance must be separately ordered. If the end user customer or Avaya channel partner would like to install two of the same type of vAppliances, then two vAppliances of that type must be ordered.
Each Product has its own ordering code. Note that each instance of a Product must be separately licensed and ordered. “Instance” means one unique copy of the Software. For example, if the end user customer or Avaya channel partner would like to install two instances of the same type of Products, then two Products of that type must be ordered.

Third Party Components
“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider
The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

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

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

Trademarks

Downloading Documentation
For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support
See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

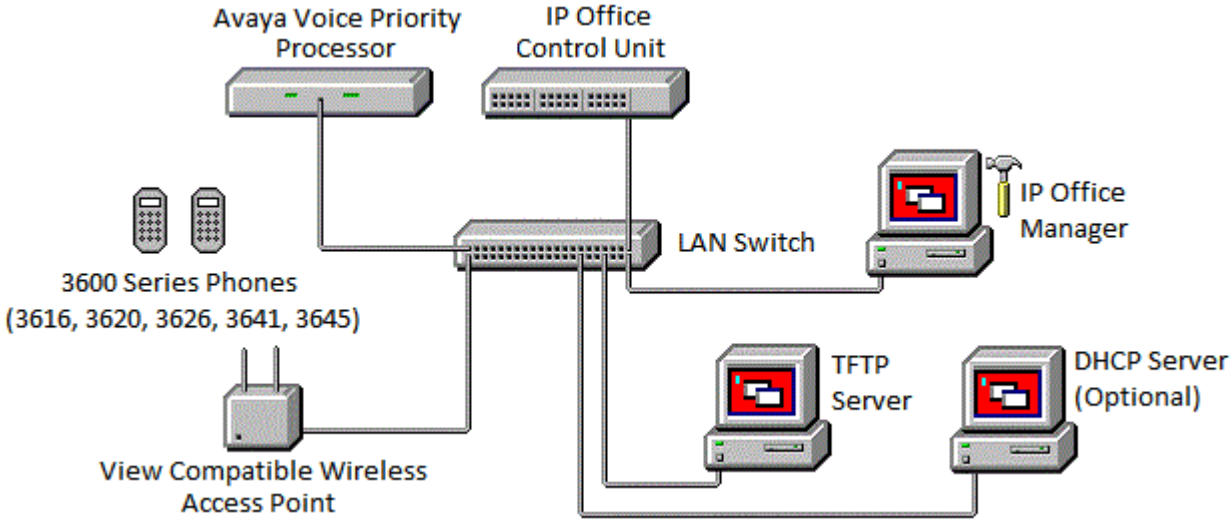
Contents

Chapter 1.
3600 Overview

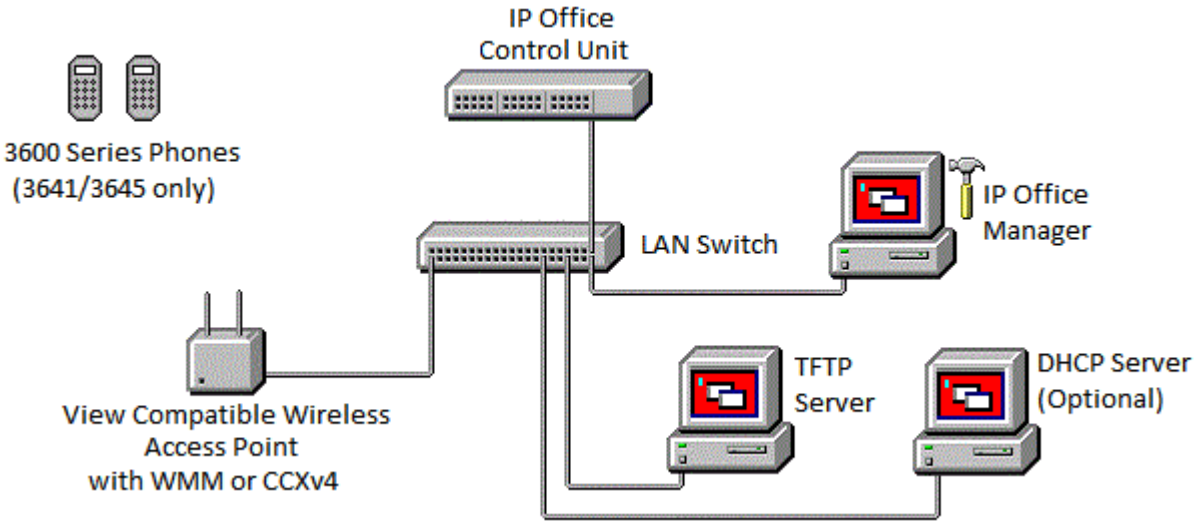
1. 3600 Overview

This manual provide installation notes for the installation of Avaya 3600 Series telephones with an IP Office system. 3600 Series phones are wireless IP telephones. There are two types of installation supported for the 3600 Series telephones:

- **Installation with an Avaya Voice Priority Processor (AVPP)**
  This type of installation must be used for sites including any 3616, 3620 or 3626 telephones. In this installation, information from the 3600 Series phones is routed to IP Office via an Avaya Voice Priority Processor (AVPP). The AVPP provides a Quality of Service (QoS) mechanism that gives preference to voice packets on the wireless medium.



- **Installation with WMM or CCXv4 Access Points**
  This type of installation can be used if the site only includes 3641 or 3645 telephones. In this type of installation, QoS is achieved by using access points that support either WMM or CCXv4.



1.1 Quality of Service Control

In an installation with just one or two wireless IP phones, it is possible that adequate call quality occurs without any QoS control. However, as further devices are added, call quality is very likely to diminish rapidly. Therefore, to maintain call quality, some mechanism for QoS control must be implemented.

For 3600 Series phones, the QoS mechanism can be either the use of an Avaya supplied AVPP (which uses SVP) or the use wireless access points configured for WMM or CCXv4. In all cases only one of the three methods should be used, the methods cannot be mixed in the same installation.

For installations that include any older 3600 Series telephones, the 3616, 3620 and 3626, only the use of the AVPP is supported. For installations that only include newer 3600 Series telephones, the 3641 and 3645, the use of either an AVPP or WMM or CCXv4 is supported.

In all scenarios, the wireless access points must also be Voice Interoperability for Enterprise Wireless (VIEW) compliant.

- **SpectraLink Voice Priority (SVP)**
  SpectraLink Voice Priority is a proprietary method of WLAN QoS, developed by Polycom, to ensure enterprise-grade voice quality, battery life and call capacity for SpectraLink Wireless IP Telephones. SVP requires the Avaya Voice Priority Processor (AVPP) Server, which is an Ethernet LAN device that works in conjunction with Wi-Fi access points to ensure QoS over the WLAN. Voice packets to and from the Wireless IP Telephones are forwarded through the AVPP Server to ensure voice prioritization as they are routed between the handset and an IP telephony server.
- **Wi-Fi Standard QoS (Wi-Fi Multimedia - WMM)**
  WMM, WMM Power Save and WMM Admission Control are Wireless Multimedia Extensions (WME) from the Wi-Fi Alliance based on IEEE 802.11e. The combination of these three standards provides enterprise-class QoS in terms of voice quality, battery life and call capacity. The access points must support and enable each of these QoS mechanisms in order to ensure they are utilized. These options are only supported for 3641 and 3645 handsets.
- **Cisco Compatible eXtension (CCXv4)**
  The CCX program allows WLAN client devices operating on Cisco access points to take advantage of Cisco-specific features. When the CCXv4 operating mode is selected on the handset, it operates using the required set of Cisco-specific and industry standard QoS mechanisms. This option is only supported for 3641 and 3645 handsets.

1.2 Security

The following security methods are supported by the handsets:

- **WEP**
  The handset supports Wired Equivalent Privacy (WEP) with both 40-bit and 128-bit encryption.
- **Cisco Fast Secure Roaming (Cisco FSR)**
  Cisco's Fast Secure Roaming (FSR) mechanism uses a combination of standards based and proprietary security components including Cisco Client Key Management (CCKM), LEAP authentication, Michael message integrity check (MIC) and Temporal Key Integrity Protocol (TKIP). FSR provides strong security measures for authentication, privacy and data integrity on Cisco access points.
- **WPA and WPA2 Personal (WPA_PSK/WPA-PSK2)**
  The handset supports WPA and WPA2 Personal, as defined by the Wi-Fi Alliance. WPA2, which is based on the 802.11i standard, provides government-grade security by implementing the Advanced Encryption Standard (AES) algorithm. WPA, which is based on a draft version of the 802.11i standard before it was ratified, uses Temporal Key Integrity Protocol (TKIP) encryption. The Personal version uses an authentication technique called Pre-Shared Key (PSK) that allows the use of manually entered keys to initiate security.
- **WPA2 Enterprise**
  The 3641 and 3645 phones supports WPA2 Enterprise, as defined by the Wi-Fi Alliance. WPA2, which is based on the 802.11i standard, provides government-grade security by implementing the Advanced Encryption Standard (AES) algorithm. The Enterprise version of WPA2 uses 802.1X authentication, which is a port-based network access control mechanism using dynamic encryption keys to protect data privacy. Two 802.1X authentication methods are supported on the Wireless IP Telephone, EAPFAST and PEAPv0/MSCHAPv2. Both of these methods require a RADIUS authentication server to be available on the network and accessible to the phone.
    - Normal 802.1X authentication requires the client to renegotiate its key with the authentication server on every access point handoff, which is a time-consuming process that negatively affects time-sensitive applications such as voice. Fast access point handoff methods allow for the part of the key derived from the server to be cached in the wireless network, thereby shortening the time to renegotiate a secure handoff. The 3600 Series phones support two fast AP handoff techniques: Cisco Client Key Management (CCKM) for Cisco access points and Opportunistic Key Caching (OKC). One of these methods must be configured for support on the WLAN to ensure proper performance of the handset.

1.3 System Components

The installation may require or include the following components:

- **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	**3616** 12	Basic lightweight wireless VoIP phone.
	3620 13	Wireless phone designed for healthcare environments.
	3626 14	Ruggedized wireless phone with push-to-talk functionality.
802.11a/b/g	**3641** 15	Multi-spectrum wireless phone
	3645 16	Multi-spectrum wireless phone with push-to-talk functionality.

- **Avaya Voice Priority Processor (AVPP)** 17
  An AVPP provides QoS control for calls going to and from the wireless network. The AVPP applies a proprietary QoS protocol called SpectraLink Voice Protocol (SVP) to the 3600 Series phone voice traffic. An AVPP is mandatory for installations that include 3616, 3620 and/or 3626 telephones. An separate AVPP is required on each sub-net being used for wireless phone access.

- **Access Points**
  Supplied by Avaya or third party vendor access points provide the connection between the wired Ethernet LAN and the wireless LAN. The access points used must be VIEW compliant (see http://www.spectralink.com/product-information/wi-fi/view-voice-interoperability-enterprise-wireless-program). The number and placement of access points is critical and must be the result of a site survey 22.
  - For installations with an AVPP, the wireless access points must be VIEW compliant and must support the SVP QoS protocol.
  - For installations without an AVPP, the wireless access points must be VIEW compliant and must support either the WMM or CCXv4 (Cisco Compatible Extension) QoS protocols.
    - If Wi-Fi Standard QoS is used, then each access point must be configured for such features as WMM-Power Save; WMM-Admission Control; proper EDCA parameters; DSCP mapping for voice and control traffic; call admission control and Proxy ARP. Consult the appropriate VIEW Configuration Guide for settings.

- **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 is configured as a user and an extension on the IP Office.
  - The IP Office control unit must provide voice compression (VCM) 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 provided depends on the type of IP Office control unit and the IP Office software release.

- **Ethernet Switch**
  Connects 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.
  - The 3626 and 3645 phones can use IP multicast addresses. This requires multicasting to 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. Initial AVPP configuration requires a serial port connection. 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 to distribute software to the wireless phones and the AVPP. The AVPP does not support the IP Office system's internal TFTP server.

- **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.

1.3.1 3616 Wireless Telephone

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

- This type of phone is only supported in installations that use an AVPP for QoS control. It in not supported in installations where WMM or CCXv4 are used.

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.

- This type of phone is only supported in installations that use an AVPP for QoS control. It in not supported in installations where WMM or CCXv4 are used.

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.

- This type of phone is only supported in installations that use an AVPP for QoS control. It in not supported in installations where WMM or CCXv4 are used.

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.

- This type of phone is supported in installations that use an AVPP or WMM or CCXv4 for QoS control.

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.

- This type of phone is supported in installations that use an AVPP or WMM or CCXv4 for QoS control.

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.

1.3.6 Avaya Voice Priority Processor (AVPP)

An AVPP is mandatory for installations that include 3616, 3620 and/or 3626 telephones. However, an installation with an AVPP can still support 3641 and 3645 phones.

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. See AVPP100 Capacity 17.

- 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 ¾" plywood.
- The AVPP can also be rack mounted using a rack mount kit (sold separately).
- Initially AVPP configuration requires 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.

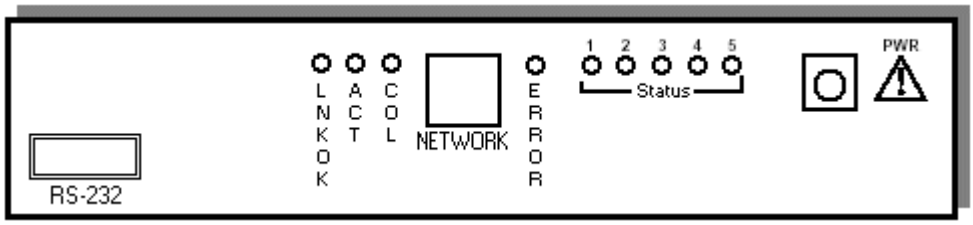
1.3.6.1 AVPP100 Capacity

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.

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

1.3.6.2 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.

1.3.7 Handset Administration Tool

This tool allows configuration of handsets. It allows configuration of individual handset settings either by setting each option individually and thorough application of pre-configured templates. It can also be used to directly upgrade phones through the charging cradle rather than needing to using TFTP. Refer to Avaya 3641/3645 Wireless IP Telephones Handset Administration Tool Installation, Configuration, and Administration manual.

The tool can be downloaded from the Avaya support website (https://support.avaya.com/downloads/download-details.action?contentId=C201291794796550_1&productId=P0258).

1.4 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.

Chapter 2.
Performing Site Surveys

2. Performing Site Surveys

Installation of the wireless network access points is 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.

- **Perform a Site Survey**
  Do not proceed with AVPP and 3600 Series phone installation unless a thorough 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.

2.1 Using a 3616, 3620 or 3626 Phone

Use the following process to perform a site survey using a 3616, 3620 or 3626 phone.

1. With the 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.
4. Scroll to and select **Diagnostics**. Select **Run Site Survey**.
5. Walk the entire coverage area while viewing the display.
6. 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.
7. The **FCN** key toggles between the three coverage modes described below.
   a. **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 access point with the strongest signal to the 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. YY represents negative dBm and lower numbers represent stronger signals. 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.

   b. **Detect Overlaps and Conflicts**
   Press **FCN** to display **Chnl** on the base of the display. The phone shows the channel each access point is using. Ideally each access point should use a unique channel. It is preferable that no overlaps exist. 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 ZZ XXX2 ZZ
      XXX3 ZZ XXX4 ZZ
      Chnl

      - *ZZ* is the channel number that the access point is using.

   c. **Confirm Supported Data Rates**
   Press **FCN** to display **Det1** on the base of the display. The phone shows details for an individual access point. Use this to confirm signal strength and supported data rates. Use the right and left arrow keys to display different access points.

      #: Full MAC
      dB Ch 1b2b5b11b
      Detl

      - *#*: 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) supported by the access point is shown. Those rates 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.
8. When testing is complete, to power off the wireless phone press **Power Off/End Call**.

2.2 Using a 3641 or 3645 Phone

Use the following process to perform a site survey using a 3641 or 3645 phone.

1. With the 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.
4. Scroll to and select **Diagnostics**. Select **Run Site Survey**.
5. The test starts in "single SSID" mode. Use the ***Any*** and ***MyID*** to toggle between single SSID and any SSID modes.
6. The display looks like the following for the multiple AP mode:

```
111111  -22  33  444
111111  -22  33  444
111111  -22  33  444
111111  -22  33  444
Any               Detl
```

- ***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*** – Toggle between "single SSID" and "any SSID" modes.
- ***Detl/Smry*** – Toggle between the multiple access point (summary) display.

7. The following screen shows how the display would look when there are three access points configured with an SSID that matches that of the phone. For example, the first has a signal strength of –28dBm, is configured on channel 2, with a beacon interval of 100ms.

```
ab7bc8  -28  02  100
2ae578  -48  06  200
2ae596  -56  11  100
Any               Detl
```

8. When ***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.

```
ab7b  -28  02 ALPHA
2ae5  -48  06 WSMTES
2ae5  -56  11 voice

MyID              Detl
```

9. In the ***Detl*** (detail) mode the display would appear as follows. The Left/Right arrow keys to change access point.

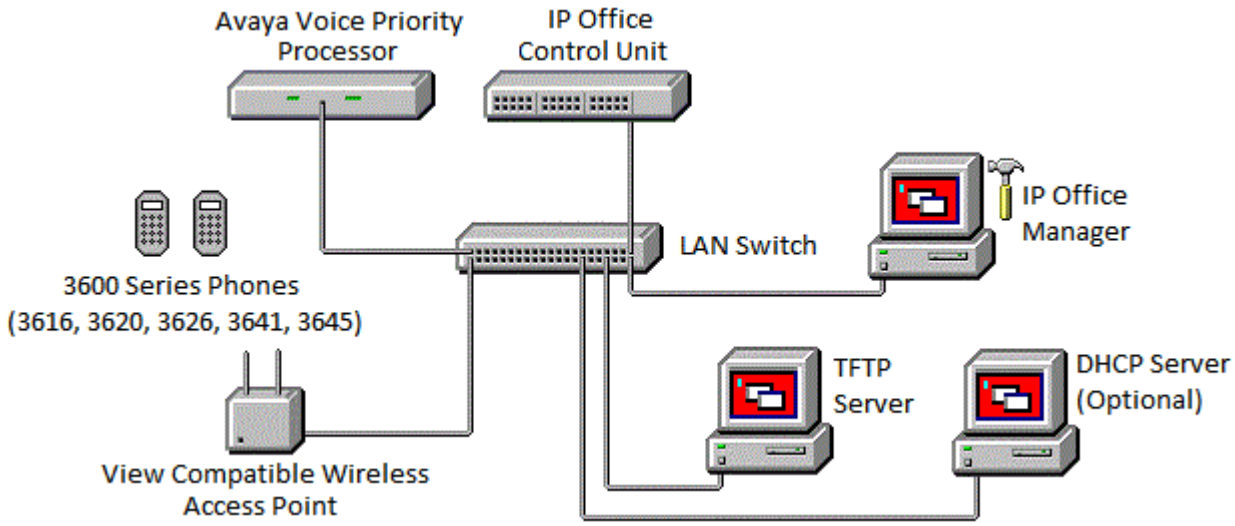
```
i:bbbbbb  sn  ch  bcn
eeeeeeeeeee  DGHI
rrrrrrrrrrrr+xxxx
mmm  G:gggg  P:pppp
Any               Smry
```

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.
eeeeeeeeeee	• 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.
Detl/Smry	• Softkey to toggle between the multiple AP display (summary), and the single AP display (detail).

Chapter 3. Installation

3. Installation

This section covers an installation where an optional AVPP is included in order to perform quality of service control for the 3600 Series phones. This is the installation that must be used if the site includes any 3616, 3620 or 3626 phones.



3.1 Required Software

Both the AVPP (if being used) 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. Do not proceed with installation until you have obtain the necessary software for the AVPP and 3600 Series phones.

1. **IP Office Manager**
   A PC on which the IP Office Manager application can run is required. This can either be a customer PC or an installers PC for the duration of installation. The PC should also provide a serial port for connection to the AVPP for its initial configuration.
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 it is not supported for 3600 Series phone and AVPP installation.
3. **AVPP Software:**
   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. *See https://support.avaya.com/downloads/download-details.action?contentId=C20091012173688840 76&productId=P0258.*
4. **3600 Series Phone Software:**
   The H323 Release 3 (117.058) software for 3600 Series wireless phones is available from the Avaya support website. See https://support.avaya.com/downloads/download-details.action?contentId=C2013117117413380_7&productId=P0853. Load the latest version of the Avaya 3641/3645 Wireless IP Telephone software onto the TFTP Server. The following files should be present:
   1. ***slnk_cfg.cfg***
   2. ***pi1400cc.bin***
   3. ***pd14odcc.bin***
   4. ***pd14shim.bin***
   5. ***pd14udcc.bin***
   6. ***pd14ccc.bin***
5. **Handset Administration Tool:**
   This tool allows configuration and upgrading of phones using a PC connected to the phone's charging cradle. See https://support.avaya.com/downloads/download-details.action?contentId=C201291794796550_1&productId=P0258.

3.2 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 supported for AVPP units and 3600 Series phones. Any third-party TFTP application can be used to provide TFTP support.

If the 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

- TFTP Server Software
- Server PC
  With fixed IP address and meeting specification of chosen TFTP software

Tools Required

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

Information Required

- 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. Unpack the AVPP and 3600 Series phone software files 27 and place them into the folder setup on the TFTP server as its root folder.
3. 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 enter **cmd**. Then enter **TFTP** for instructions.

3.3 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 if no other DHCP server is present on the network.

The method and process for configuration depends 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: • MCIPADD=xx.xxx.xxx.xxx is the H323 Gatekeeper (Callserver) address. Normally, this is the IP Office Unit's LAN1 address. • MCPORT=1719 is the RAS port address for initiating phone registration.

3.4 AVPP Installation

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 ¾" 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 ¾" 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 - ¾" panhead wood screws (or similar device) are required.
4. **Cat.5 Cable**
   RJ45 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 serial cable**
   Required for initial PC serial port access to the AVPP configuration.
3. **PC with the following:**
   a. **Terminal Emulation Program**
      Required for initial PC access to the AVPP configuration.
   b. **IP Office Manager Application**
      Required to configure the AVPP IP address in the IP Office configuration.

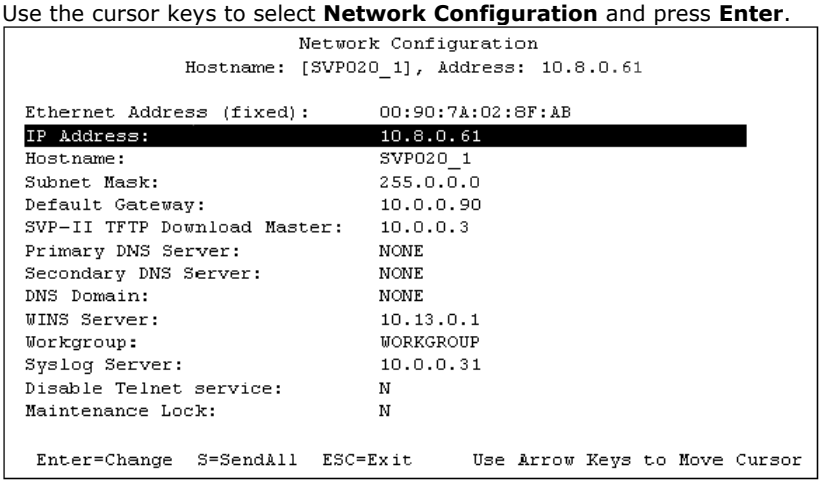
Information Required

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.

3.4.1 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 this 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 61 menu is displayed.
5. Use the cursor keys to select **Network Configuration** and press **Enter**.



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 restarts. Following the restart, the AVPP menus can be accessed using Telnet 60 to complete configuration to match the wireless network.

3.4.2 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.
4. Set the **AVPP IP Address** to match the static IP address of the AVPP unit.
   - 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.
5. Click **OK**. Click  or select **File | Save Configuration** to send the updated configuration back to the IP Office control unit. Click **OK**.

3.4.3 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 a 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.

3.5 Phone Installation

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. Alternatively, use the Handset Administration Tool 19 to configure and upgrade the handsets prior to installation.
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:
   a. **SSID**
   b. **Frequency**. For example 802.11a or 802.11b.
   c. **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:
   a. IP Address for each phone.
   b. Sub-net mask
   c. Default gateway.
   d. Call Server IP (IP Office)
   e. Call Server Port (1719).
5. **Phone User Details**
   For each phone, ensure you have the following information:
   a. Required extension number.

3.5.1 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 a password. Those details are used to auto-create a new user and extension within the IP Office configuration.

- **! WARNING**
  The auto-create options should only be enabled during installation. Following installation of any phones, you must ensure that the auto-create settings are disabled.

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

3.5.2 Phone Registration

At this stage, it should be possible to register the phones with the access points and then to the IP Office system. The following processes cover manual configuration and registration through the administration menu of each individual phone. It is strongly recommended that if installing several phones, the Handset Administration Tool 19 is used.

3.5.2.1 3616/3620/3626 Registration

Use the following process to register 3616, 3620 and 3626 phones.

1. Set the phone into administration mode:
   a. With the phone powered off, simultaneously press and hold the **Start Call** and **End Call** buttons.
   b. After hearing two beeps, release the **Start Call** button, then release the **End Call** button.
   c. 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.
   d. To scroll through the menu options, press **Up**, **Down** and **Select**.
   e. To change the selected option, press **OK** or press **Up** to return to the previous menu level.
2. Select **Network Config**.
   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:
   a. Select **IP Address** and then **Static IP**.
   b. Set the **IP Address**, **TFTP Server IP**, **Default Gateway** and **Subnet Mask** information as required.
   c. Set the **Call Server IP** to the LAN address of the IP Office.
   d. Set the **Call Server Port** to ***1719***.
   e. Set the **AVPP IP** address.
3. 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.
4. Select **Security**.
   Enter the wireless security settings that match those configured for the access points.
5. Select **Phone Config**.
6. Select **License Option**.
   The phones 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***.
   - To change the displayed number, press **Select**.
   - To scroll through the options, press **Up** or **Down**.
   - To select the displayed number, press **Select**.
7. Power cycle the phone.
   a. If the phones software needs to be updated the new software will now be downloaded from the TFTP server. The status bar will increment across the display for each function that is being performed in the download process.
   b. Upon completion of the update process, the handset will re-boot with the new firmware.
8. 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**.

3.5.2.2 3641/3645 Registration

Use the following process to register 3641 and 3645 phones:

1. Set the phone into administration mode:
   a. With the phone powered off, while pressing the **START** key press and release the **END** key.
   b. When the administration menu appears release the **START** key.
   c. 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.
2. Select **Network Config**.
   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:
   a. Select **IP Addresses** and then **Static IP**.
   b. Set the **IP Address**, **TFTP Server IP**, **Default Gateway** and **Subnet Mask** information as required.
   c. Set the **Call Server IP** to the LAN address of the IP Office.
   d. Set the **Call Server Port** to ***1719***.
   e. If installing with an AVPP for QoS control, set the **AVPP IP address**.
3. Select **SSID**.
   Enter the SSID of the wireless network that the phone should use.
4. Select **WLAN Settings**.
   - **For installations using an AVPP:**
     a. Select **Custom** and then **Security**. Enter the security settings that match those configured for the access points..
     b. Select **QoS** and then **SVP**. Check that the QoS settings match those set for the AVPP. The defaults used by the AVPP are ***46*** for **WT in call** and **WT standby**, ***0*** for **Other**.
   - **For installations using WMM:**
     a. Select **Custom** and then **Security**. Enter the security settings that match those configured for the access points.
     b. Select **QoS** and then **Wi-Fi Standard**. Check that the QoS settings match those set for the access points. The defaults are ***46*** for **Voice** and **Control**, ***0*** for **Other**.
   - **For installations using CCXv4:**
     a. Select **CCX**. Select **WPA2-Enterprise**. Enter the security settings that match those configured for the access points.
     b. Select **QoS**. Check that the QoS settings match those set for the access points. The defaults are ***46*** for **Voice** and **Control**, ***0*** for **Other**.
5. 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.
   a. 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.
   b. Once the wireless mode is selected, depending on that selection and the regulatory domain, the **Transmit Power** can be selected.
6. Select **Phone Config**.
7. Select **Telephony Protocol**.
   The phones 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***.
   a. To change the displayed number, press **Select**.
   b. To scroll through the options, press **Up** or **Down**.
   c. To select the displayed number, press **Select**.
   d. Select **IP Office** and set this to **Enable**.
8. Power cycle the phone.
   a. If the phones 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.

b. Upon completion of the update process, the handset will re-boot with the new firmware.

9. 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**.

3.5.2.3 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 password requested matches the IP Office user **Login Code**.

The following messages may be displayed as part of that process.

Display	Possible Cause and Action
123 56789	The phone has located and authenticated and associated with at least one access point. Not shown for WMM installations.
123 5678	The phone is either configured for static IP or, if configured for DHCP, has started DHCP discovery.
123 567	If DHCP is configured, a DHCP response was received which contains a good DNS server configuration.
123 56	Used for AVPP installations only. Not shown for WMM or CCX installations. Indicates one of the following possibilities: • Static IP configuration • AVPP address found in DHCP response, • AVPP address found via DNS lookup.
123 5	All networking functions are complete and the phone is proceeding with establishing the link to the AVPP.
123	The CCMS application has started.
12	At least one IP address for a telephone system has been identified.
1	The phone has registered with the telephone system.
Ext. =XXX #=OK New =	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. Enter the required extension or if # is pressed, the wireless phone will retain the current extension it last used. After a new extension is entered, press # to continue.
Password = ****** # = OK**	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.
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	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. 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. 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. 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.
*** 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).

3.5.3 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 41 before handing over any phones to the users.

3.6 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.

Chapter 4.

Maintenance and Administration

4. Maintenance and Administration

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 it 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 65 settings.

4.1 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.

4.2 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.

- **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.
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**.

4.3 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 pint. 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 phones 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: 0F" 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 suppot 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.

4.4 Using the Phone Admin Menus

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.

4.4.1 3616, 3620, 3626 Admin Menu

The following table lists the Admin menu items. Default settings are indicated by a *.

3616, 3620, 3626 Admin Menu					
Phone Config	**License Option**	Set Current			
	Ext.				
	Password				
	IP Office	IP Ofc Enabled/IP Ofc Disabled			
	OAI ON/OFF	Enable OAI/Disable OAI			
	Push-to-Talk (3626 only)	Allowed Channels	Channel 1*/Channel 2*/Channel 3*/Channel 4*/Channel 5*/Channel 6*/Channel 7*/Channel 8*		
		Allow/Disallow	Allow PTT*/Disallow PTT		
	Admin Password				
Network Config	**IP Address**	Use DHCP*			
		Static IP	Phone IP		
			TFTP Server IP		
			Default Gateway		
			Subnet Mask		
			Syslog Server IP		
			Call Server IP		
			Call Server Port		
			AVPP IP		
			OAI Server IP		
	ESS ID	Learn Once*/Learn Always/Static Entry			
	Security	None*			
		WEP	Authentication	Open System/Shared Key	
			WEP On/Off	Off*/On	
			Key Information	Default Key	
				Key Length	40bit
					128bit
				Key #1	
				Key #2	
				Key #3	
				Key #4	
			Rotation Secret		
		Cisco FSR	Username		
			Password		
		WPA-PSK	Passphrase		
			Pre-shared Key		
		WPA2-PSK	Passphrase		
			Pre-shared Key		
	Reg Domain	None			
	Transmit Power	Maximum*/50mW/30mW/20mW/15mW/10mW/5mW			
Diagnostics	**Run Site Survey**				
	Diagnostics Mode	On/Off*			
	Syslog Mode	Disabled*/Errors/Events/Full			
Restore Defaults					

4.4.2 3641 and 3645 Admin Menu

The following table lists the Admin menu items. Default settings are indicated by a *.

3641/3645 Admin Menu						
Phone Config	**Language**	*English*/Français/Deutsch/Español/Italiano*				
	Telephone Protocol	*Type 030*/Type 033*				
	PTT/Emerg. button	Emergency Dial	Emergency #	*Disable*/Enable*		
			Emergency Number	Enter Number		
				Enter Name		
		PPT (3645 only)	PTT	*Disable*/Enable*		
			Allowed Channels	*Channel 1*/.../Channel 24*		
			Name Channels			
			Priority Channel	*Off*/On*		
				Name Channel		
	Time Zone	*[list] GMT**				
	Daylight Savings	*DST No Adjust*/DST Auto<USA>/DST Auto<AUS>/DST Auto<EURO>*				
	Protected Speed-dial	Enter number				
	Password	*Disable/Enable**				
	Change Password					
	Speakerphone	*Disable/Enable**				
	Clear Extension					
	IP Office	*Disable*/Enable*				
	Auto Ext	*Disable/Enable**				
	Call Log Dial	*Disable/Enable**				
	Dial Plan Rules	*Disable*/Enable*				
		Dial Plan		Country Code		
				Internal Ext Len		
				Intl Access Code		
				LD Access Code		
				Natl Num Len		
				Outside Lin Acc		
	OAI	Disable*/Enable				
	Location Service	RTLS		Disable*/Enable		
		Transmit Interval		15 seconds/30 seconds/1 minute/5 minutes/10 minutes*		
		Location Server IP				
		ELP Port		8552*		
Network Config	**IP Addresses**	Use DHCP *				
		Static IP	Phone IP			
			Default Gateway			
			Subnet mask			
			TFTP Server IP			
			Syslog Server IP			
			Time Server IP			
			Call Server IP			
			Call Server Port			
			AVPP IP			
			OAI Server IP			
	SSID					
	WLAN Settings	Custom*	Security	None *		
				WEP	Authentication	Open System*/ Shared Key
					WEP	Enable/Disable*

3641/3645 Admin Menu						
					Key Information	Default Key
						Key Length
						Key 1-4
					Rotation Secret	
				WPA2-PSK	Passphrase*/Pre-Shared Key	
				WPA-PSK	Passphrase*/Pre-Shared Key	
				Cisco FSR	Username	
					Password	
				WPA2-Enterprise	Authentication	EAP-FAST*/PEAP
					Fast Handoff	CCKM*/OKC
					Username	
					Password	
					Delete [Cert/PAC]	
			QoS	SVP*	DSCP Tags	WT in call (46*)
						WT standby (46*)
						Other (0*)
				Wi-Fi Standard	DSCP Tags	Voice (46*)
						Control (46*)
						Other (0*)
					Admission Control	Mandatory*
						Optional
		CCX	WPA2-Enterprise	Authentication	EAP-FAST*/PEAP	
				Fast Handoff	CCKM*/OKC	
				Username		
				Password		
				Delete [Cert/PAC]		
			QoS	DSCP tags	Voice (46*)	
					Control (46*)	
					Other (0*)	
	Reg Domain	01	802.11a	5.150-5.250/5.250-5.350 DFS/5.470-5.650 DFS/5.470-5.725 DFS/5.725-5.825/5.725-5.850		
			802.11b*	Transmit Power	5mW (7dB)/10mW (10dB)/20mW (13dB)/30mW (15dB)/40mW (16dB)/50mW (17dB)/100mW (20dB)	
			802.11b/g			
		02	"	"		
Diagnostics	**Run Site Survey**					
	Diagnostics	*Disabled*/Enabled*				
	Syslog	*Disabled*/Errors/Events/Full*				
	Error handling Mode	*Halt on Error/Restart on Error**				
Restore Defaults						

4.4.3 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.

4.4.4 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.

4.4.5 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 phon 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.

4.5 Using the AVPP Menus

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 61 menu is displayed.

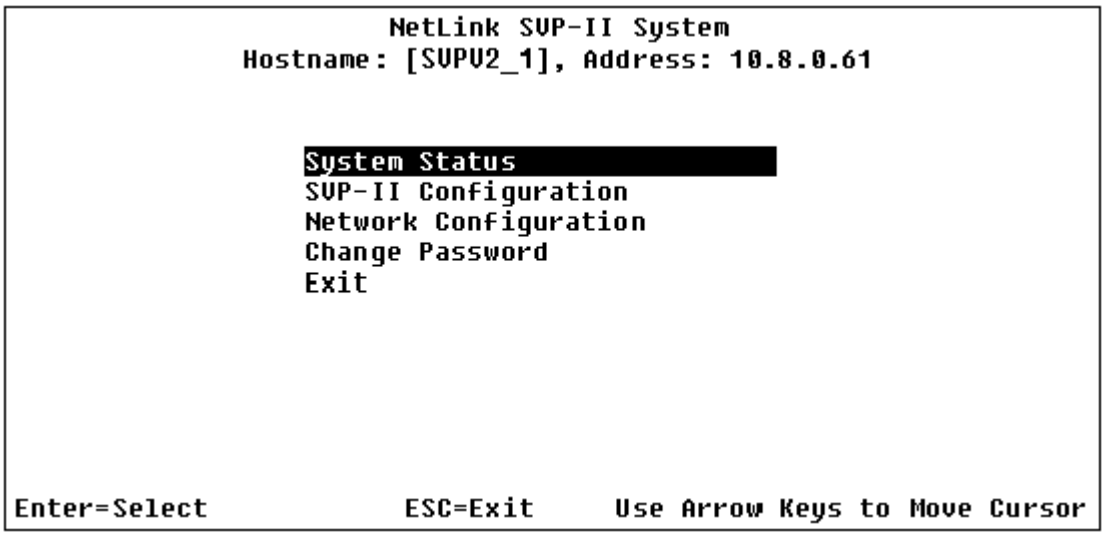
Connecting via Telnet

Telnet can only be used after the AVPP's IP address is configured. Telnet access can be disabled if required through the Network Configuration 65 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 61 menu is displayed.

4.5.1 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.



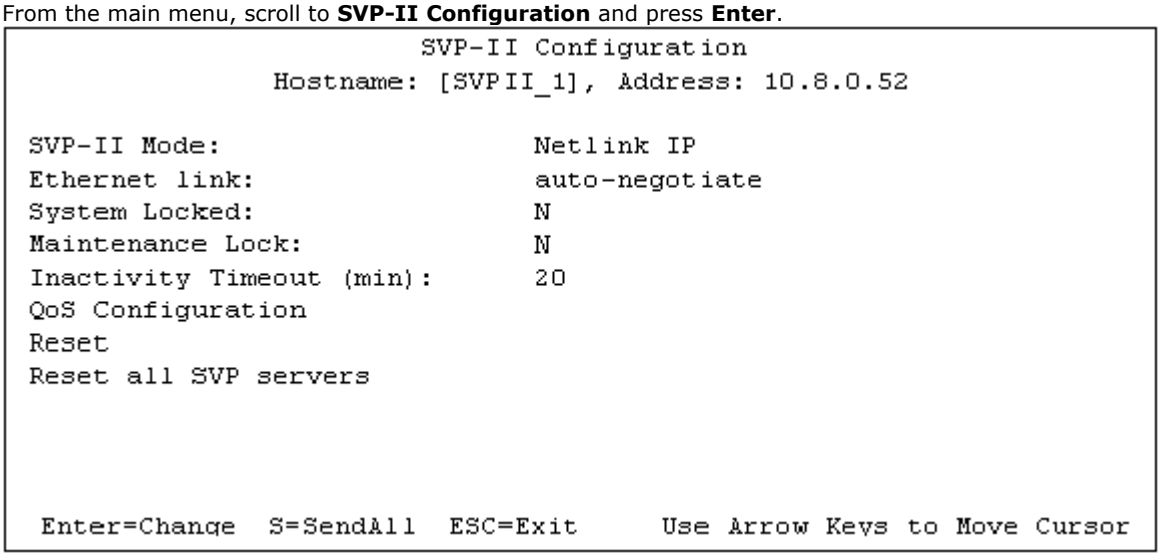
- **System Status** 71
  Menu for viewing error messages, status of operation and software code version. You can check the version currently installed on AVPP through the **System Status** menu, see Software Versions 71.
- **SVP-II Configuration** 62
  Allows you to set the mode and reset the system.
  - **QoS Configuration** 64
    This sub-menu of the SVP-II Configuration menu is used to alter the QoS settings applied to different signals.
- **Network Configuration** 65
  Allows you to set network configuration options, including IP address and hostname.
- **Change Password** 66
  Allows you to change the password for AVPP access.

4.5.2 SVP-II Configuration

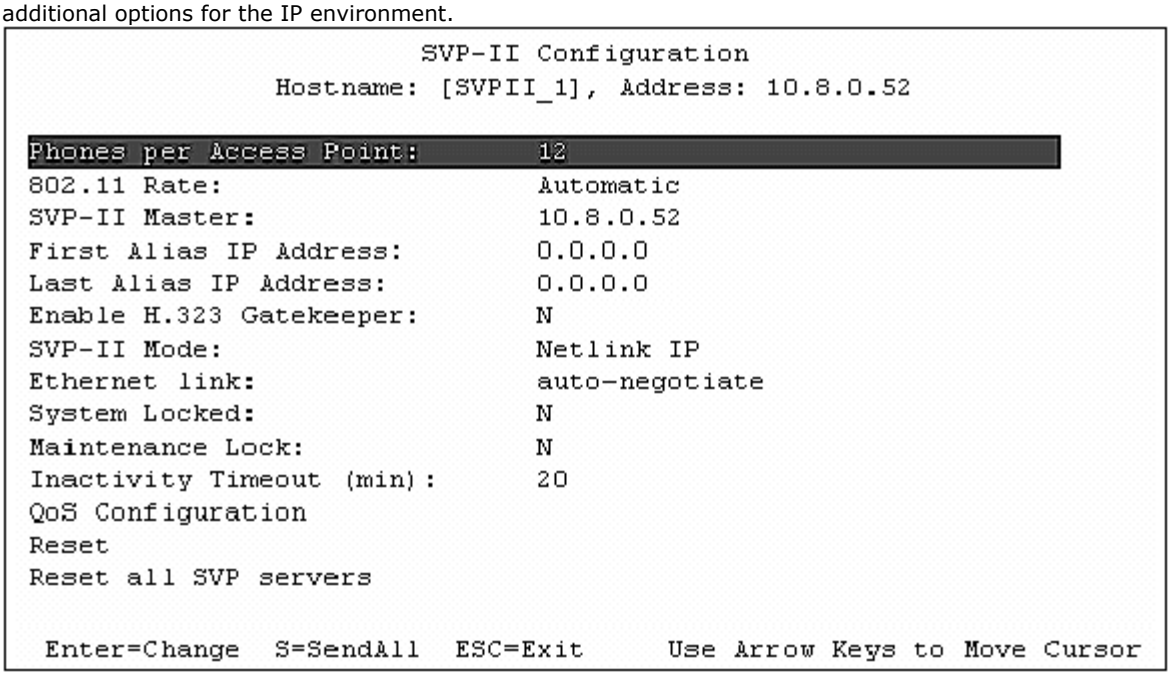
The **SVP-II Configuration** screen allows you to set the mode of the AVPP for an IP environment. It is also where you can lock the AVPP for maintenance and reset the AVPP after maintenance.

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 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.



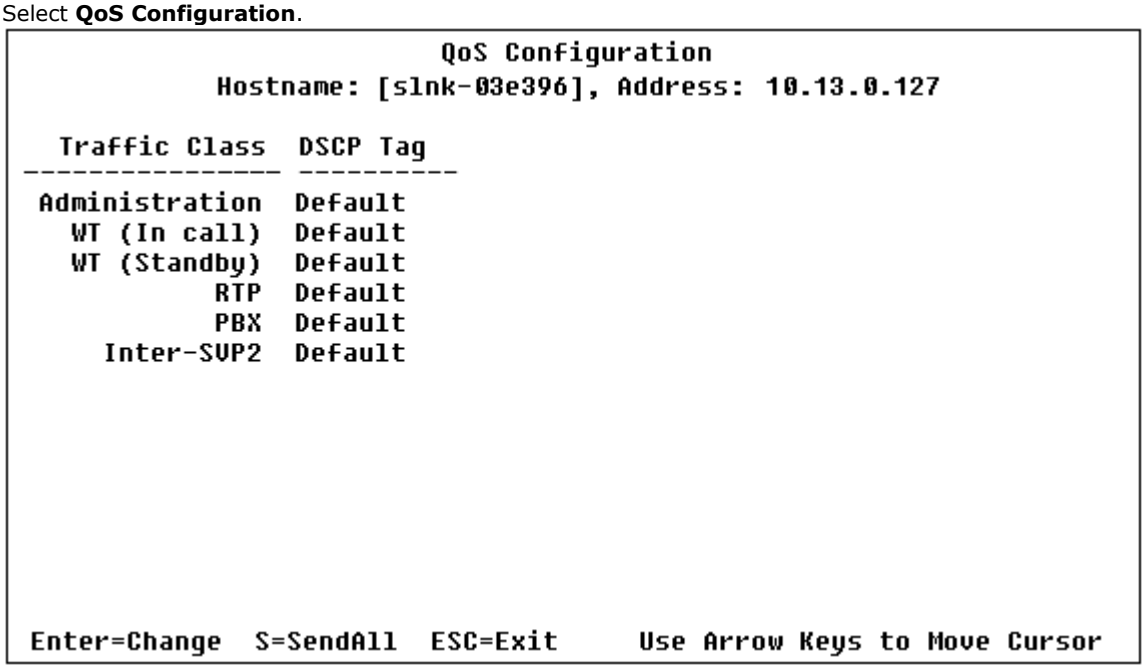
- **Phones per Access Point**
  Enter the number of simultaneous calls supported for your type. Access point specifications are detailed in the configuration notes for each brand and type.
- **802.11 Rate**
  Select 1MB/2MB to limit the transmission rate between the wireless phones and access points. 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 64.
- **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.

4.5.3 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**.



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

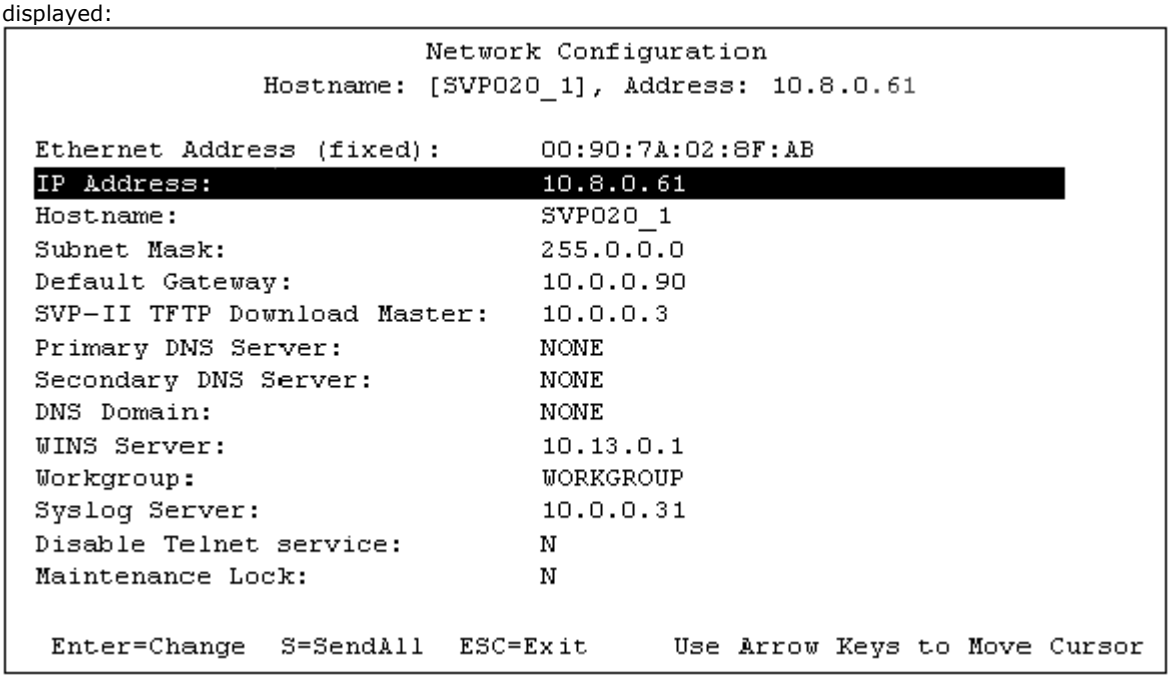
- **DSCP Tag**
  DSCP (Differentiated Services Code Point) is a QoS mechanism for setting relative priorities. In the IP header, packets are tagged with a DSCP field for type of service.
- **Traffic Class**
  - **Administration**
    Tags set the priority for Telnet, TFTP and other administrative traffic. 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.

4.5.4 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 44.

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



- **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).

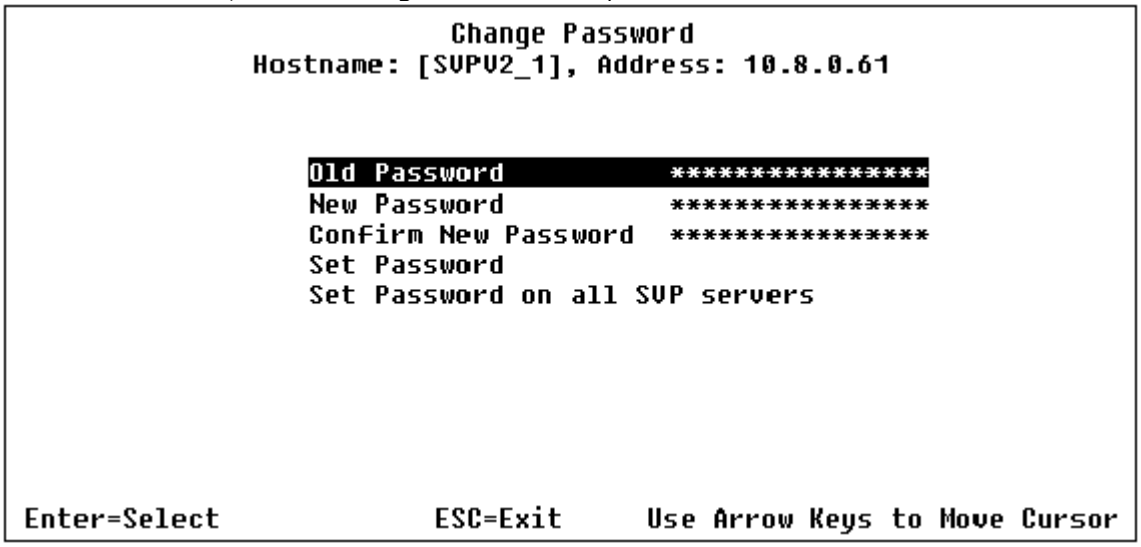
To manually reset AVPP, select **Reset** in the **SVP-II Configuration** screen and then press **Y** (Yes).

4.5.5 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**.

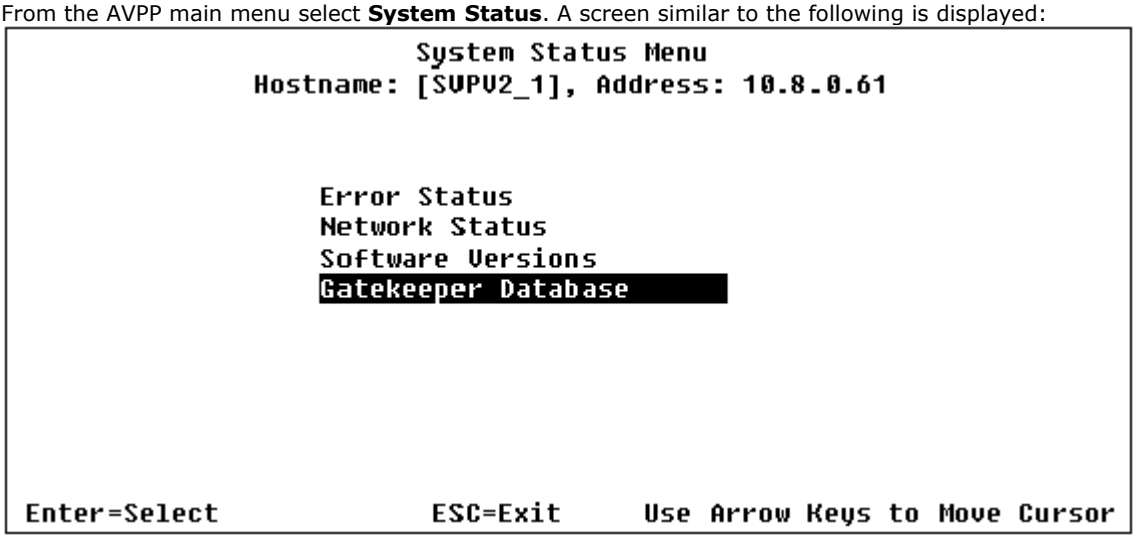


2. Enter the information. The password parameters are:
   - More than four characters.
   - First character must be a letter; other characters may be numbers and letters.
   - No dashes, spaces or punctuation marks (alphanumeric only).
3. Select **Set Password** or press **S**.

4.5.6 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:



2. The screen displays:
   - **Error Status** 68
     Displays alarm and error message information.
   - **Network Status** 69
     Displays information about the Ethernet network to which the AVPP is connected.
   - **Software Versions** 71
     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.

4.5.7 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**.

4.5.8 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: [SVPV2_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

SVP-II Sockets in Use         (Last / Max):      0 /   10
SVP-II Access Points in Calls (Last / Max):      0 /   2
SVP-II Telephones in Use      (Last / Max):      0 /   1
SVP-II Telephones in Calls    (Last / Max):      0 /   2
SVP-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 mulitcast 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-II Telephone in Use**
  Wireless phone in standby or in a call.
- **SVP-II Telephone in Calls**
  Wireless phone in a call.
- **SVP-II ARP Audio (Delay)**
  ARP audio packets whose transmission was momentarily delayed.
- **SVP-II ARP Audio (Lost)**
  ARP audio packets dropped due to insufficient memory resources.

4.5.9 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 5.
Document History

5. Document History

Date	Issue	Changes
21st February 2014	**06a**	• Update to clarify support for installation methods without requiring an AVPP.

Index