IP Office - Job Aid

Avaya 3616/3626 Installation

074 Issue 2
21-300050
26th January 2004

Notice Every effort was made to ensure that the information in this book was complete and accurate at the time of printing. However, information is subject to change.

Avaya Web Page The world wide web home page for Avaya is: http://www.avaya.com

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 working on your company's behalf). Be aware that there is a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention If you s*uspect that you are being victimized* by toll fraud and you need technical assistance or support, call the Technical Service Center's Toll Fraud Intervention Hotline at 1.800.643.2353.

Providing Telecommunications Security Telecommunications security of voice, data, and/or video communications is the prevention of any type of intrusion to, that is, either unauthorized or malicious access to or use of, your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or a person working on your company's behalf. Whereas, a "malicious party" is Anyone, including someone who may be otherwise authorized, who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

• Utilization (of capabilities special to the accessed equipment)
• Theft (such as, of intellectual property, financial assets, or toll-facility access)
• Eavesdropping (privacy invasions to humans)
• Mischief (troubling, but apparently innocuous, tampering)
• Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there could be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company, including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Your Responsibility for Your Company's Telecommunications Security The final responsibility for securing both this system and its networked equipment rests with you – an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

• Installation documents
• System administration documents
• Security documents
• Hardware-/software-based security tools
• Shared information between you and your peers
• Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure your:

• Avaya provided telecommunications systems and their interfaces
• Avaya provided software applications, as well as their underlying hardware/ software platforms and interfaces
• Any other equipment networked to your Avaya products

Federal Communications Commission Statement Part 15: Class A Statement. This equipment has 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 instructions, could 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.

Industry Canada (IC) Interference Information This digital apparatus does not exceed the Class A limits for radio noise emissions set out in the radio interference regulations of Industry Canada.

Le Présent Appareil Nomérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A préscrites dans le reglement sur le brouillage radioélectrique édicté par le Industrie Canada.

European Union Declaration of Conformity The "CE" mark affixed to the equipment means that it conforms to the referenced European Union (EU) Directives listed below:

EMC Directive 89/336/EEC

Low-Voltage Directive 73/23/EEC

For more information on standards compliance, contact your local distributor

Contents

3616/3626 Installation on IP Office

Introduction

This document contains information on the installation and configuration of the Avaya 3616/3626 Wireless Telephone on an Avaya IP Office Control Unit. The IP Office Control Unit acts as a routing mechanism for all 3616/3626 telephones on its system. Information is routed from the telephone to the IP Office, to the Avaya Voice Priority Processor (AVPP). The AVPP utilizes Spectralink Voice Priority (SVP) as the Quality of Service (QoS) mechanism that is implemented in the wireless telephone and access point to enhance voice quality. SVP gives preference to voice packets on the wireless medium, increasing the probability that all voice packets are transmitted efficiently. These voice packets are then re-routed through the IP Office and back to the wireless telephone.

These are the IP Office Control Units currently supported with the wireless telephones:

- Avaya IP 403 Office
- Avaya IP 406 Office
- Avaya IP 412 Office

Avaya IP Office – Small Office Edition have a built-in access point, but without Quality of Service (QoS). The access point is configurable via Avaya's IP Office Manager.

Other wireless solutions are available for the Avaya IP Office – Small Office Edition.

Related Documents

The setup for the 3616/3626 wireless telephones also requires the configuration of the AVPP and the individual wireless telephones. These instructions are provided in the following related documents:

- Avaya Voice Priority Processor Installation Manual
- Avaya 3616/3626 Wireless IP Telephone Manual

IP 403/406/412 Office

With IP 403/406/412 Office Control Units, the access point resides on the LAN and is configured based on the manufacturer's guidelines and manuals.

These are the access points that are compliant with the SVP being used by the AVPP, based on SpectraLink:

SpectraLink Voice Priority (SVP) Compliance Matrix

Manufacturer	Make/Model	FH/DS	Software Version		Calls per Access Point
			SVP Certified	Field Verified	
Alvarion	BreezeNET Pro. 11 Series[1]	FH	4.4.2 or 5.0.103		3
Cisco	Aironet 340	DS	10.13	11.03, 11.07, 1.10t	6
Cisco	Aironet 350[2]	DS	11.03	11.07, 11.10t	7
Cisco	Aironet 4500 & 4800 Turbo DS	DS	8.12 & 8.24	8.55	5
Cisco	Aironet 3500	FH	8.12	8.24	3
Proxim	Orinoco AP 1000	DS	D3.78S6 3.83	7.4a	5
Symbol	Spectrum 24 FH	FH	4.01-S2	4.02-12	3
Telxon	Air-I/O 802FH UAP	FH	8.12	8.24	3
Telxon	802 DS & 802 DS 11	DS	8.12	8.24	5
Avaya	Wireless Access Point AP-1, AP-2	DS		3.83, 3.92	6
Avaya	Wireless Access Point AP-3	DS		1.4 (v 222)	7
Cisco	Aironet 1200	DS		11.40t	7
Enterasys	Roamabout AP2000	DS		V6.02	6
Intermec	Mobile LAN Access 2100, 2101, 2102	DS		1.51 or later	6
LXE	6250 Access Point	DS		3.83	6
Proxim	AP 2000	DS		7.4, 1.3	6
Symbol	Spectrum 24 DS	DS		2.21-23, 2.51-21, 3.50-18	6
Teklogix	9150 Wireless Gateway	DS		E301R, J041	4

1 Alvarion BreezeNET Pro.11 Series software version 4.4.5 is ***not*** compatible with Avaya Wireless Telephones

2 Cisco Aironet 350 software version 11.21T is ***not*** compatible with Avaya Wireless Telephones

FH/DS: Frequency Hopping (FH) Avaya Wireless Telephones support 1 Mb/s data rate only. Direct Sequence (DS) Avaya Wireless Telephones support up to 11 Mb/s data rates.

Software Version:

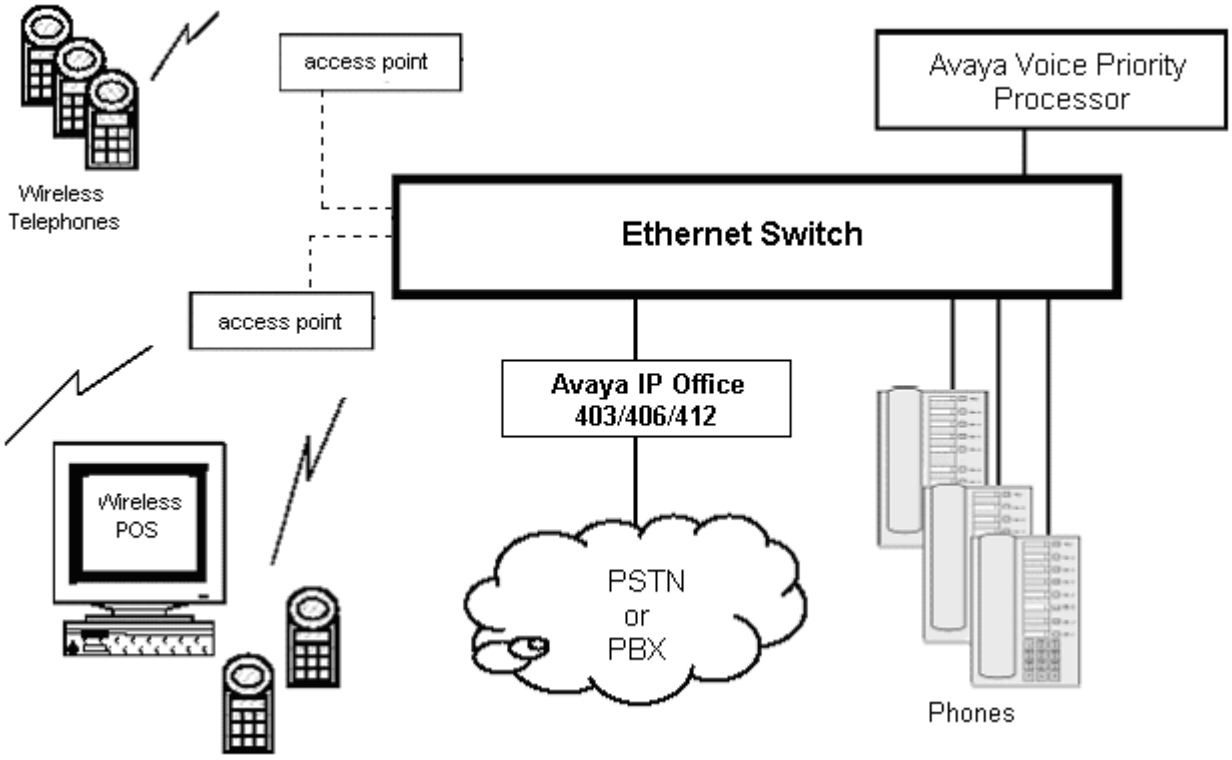
SVP Certified - The access point software has been fully tested and approved by SpectraLink Engineering

Field Verified - The access point software has been verified in field installations, but has not been tested by SpectraLink Engineering

Calls per Access Point: A conservative estimate of the number of simultaneous calls per access point at an average data rate of 2 Mb/s

System Configuration

The following diagram shows the Avaya IP 403/406/412 Office residing on a network with a wireless LAN access point, the AVPP and 3616/3626 telephones:



(Example Only)

Installation and Configuration

A sample configuration set-up is available following the instructions below.

If you have IP Office 403/406/412, do the following to set-up the 3616/3626 wireless telephones:

1. To create the configuration files for each phone, you must first download the following software from the SpectraLink website **http://spectralink.com/service/software.html**:
   - For the Avaya Voice Priority Processor (AVPP) software, look under **NetLink SVP Server Avaya AVPP Server** and do the following:
     I. Download the .EXE.
     II. Extract the necessary files by unzipping the ZIP file.
     III. Place the following files into the "**Manager**" directory: **FLASHFS**, **SVP100.TOC** and **ZVMLINUX**.
   - For the Avaya Wireless Telephone software, look under **NetLink Wireless Telephone – IP Avaya 3606** and do the following:
     I. Download the .EXE.
     II. Extract the necessary files by unzipping the ZIP file.
     III. Place the following files into the "**Manager**" directory: **pd06ccc.bin** and **slnk_cfg.cfg**.
2. Refer to the manufacturer's documentation to configure the access point with the following information:
   - AVPP IP Address
   - Individual telephone name
   - Frequency Channel
   - Security Key information
3. Using a network cable, connect the Avaya IP Office 403/406/412's LAN port to the AVPP's Network port.
4. Configure the AVPP: please refer to the Avaya Voice Priority Processor Installation Manual.
5. Create a configuration file for each AVPP terminal.
   - From Program Files/…/Manager, copy and rename the configuration file for each AVPP terminal based on the last 6 digits of the MAC address. Example – copy the **slnk_cfg.cfg** file and rename it **sl123456.cfg**, assuming the terminal's MAC address is **xxxxxx123456**.
6. Configure the 3616/3626 telephones: Refer to the Avaya 3616/3626 Wireless IP Telephone Installation and Configuration Guide.

Sample Set-up

Below is a sample configuration designed as a quick reference. If more detailed information is required, please refer to the appropriate manuals as referenced in the step-by-step instructions.

Sample information

Item	IP Address
Avaya Voice Priority Processor (AVPP)	192.168.42.3
Avaya IP Office 403/406/412	192.168.42.1
PC	192.168.42.10

AVPP Configuration Screen via Hyperterminal

Title	State	Comment
Error Status	Alarms	System error display
Network Status		Status of network
Software Versions		Current software version on the AVPP

AVPP Configuration

Hostname: Sample1, Address: 192.168.42.3

Title	State	Comment
Phones per access point	3	Dependent on the access point
802.11 Rate:	Automatic/ 1MB 2MB only	Data rate speed
SVP-II Master:	192.168.42.3	AVPP IP address
SVP-II Mode:	Netlink IP	Leave as default
Ethernet link:	Auto-negotiate	Leave as default
System Locked:	N	Leave as default
Maintenance Lock:	N	Leave as default
Reset System	Y/N	Leave as default

AVPP Network Configuration

Title	State	Comment
Ethernet Address (fixed):	00:90:7A:01:24:93	Leave as default
IP Address:	192.168.42.3	The AVPP unit
Hostname:	Sample1	System host name
Subnet Mask:	255.255.255.0	Leave as default
Default Gateway:	192.168.42.1	IP Office Unit
SVP-II TFTP Download Master:	192.168.42.10	PC containing AVPP Software
Primary DNS Server:	NONE	Leave as default
Secondary DNS Server:	NONE	Leave as default
DNS Domain:	NONE	Leave as default
WINS Server:	NONE	Leave as default
Workgroup:	WORKGROUP	Leave as default
Syslog Server	NONE	Leave as default
Maintenance Lock:	N	Leave as default

Telephone Set-up

- Boot up the phone by simultaneously pressing the Green and Red keys. Release the Green key while still holding down the Red key. This will display the MAC address.
- Use 0 to Edit and Select.
- FCN to navigate back one screen.
- The Red button to end programming.

Configure the following information on the telephone

Title	State	Comment
IP Address	Static or DHCP	Select IP address mode
ESS ID (SSID)	Network Name (SSID)	SSID of the access point
License Mgmt	9	Leave as default
Encryption	Match the configuration on the access point	
Ext.	Extension Number	Use the extension created from User
Password	Extension Password	Enter password for the phone extension from User

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

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

Email: contact@avaya.com
Web: http://www.avaya.com.