Avaya Voice Priority Processor

For IP Interfaces

Installation, Setup, and Administration

555-301-102
Part Number 72-9178-02
Issue 5
July 2005

Notice
All efforts were 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. 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.

Note concerning the Avaya Voice Priority Processor:

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 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.

Note concerning shielded cable:

Avaya recommends the use of Sshielded cable is recommended for all external signal connections in order to maintain FCC Part 15 emissions requirements.

Note concerning the Avaya wireless telephones:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (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 not comply with part 15 of the FCC rules and void the user's authority to operate this equipment.

WARNING Avaya products contain no user-serviceable parts inside. Refer servicing to qualified service personnel.

Important Safety Information

Follow these general precautions while installing telephone equipment:

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

DECLARATION OF CONFORMITY

We

SpectraLink Corporation
5755 Central Avenue
Boulder, CO 80301

declare under sole responsibility that the Wireless Business Telephone System Components:

Wireless Telephone Handset Models; SNP2400, RNP2400
Battery Models; BPE100, BPX100
System Controller Models; TGA-116, TGU-116, TGA-104, TGU-104, SVP100
Battery Charger Models; BQC7204, DCE100, DCX100

conform to Directive 89/336/EEC for Electromagnetic Compatibility, R&TTE Directive 1999/5/EEC and LVD Directive 73/23/EEC.

Compliance was demonstrated to the following specifications as listed in the official *Journal of the European Communities*:

EN 61000-6-4:2001 Industrial Emissions:
EN 55022:1994+ A1 Emissions Class A
(SVP100, TGA/TGU-104 & respective power supplies)
EN 55024:1998 Immunity
EN 300-328-1 V1.3.1 2001 ERM
EN 300-489-1/17: 2002 Common, EMC,ERM, RLAN (Class B for Handsets)
EN 300-826 ERM/EMC
EN 50360:2001 SAR
EN 61000 6-2:2001 Immunity
EN 61000 3-2:2000 Harmonic Emissions
EN 61000 3-3:1995 Flicker Emissions
EN 60950:2000 Safety with CB Reports

CE 0678

Mark R. Angliss,
Manager; Quality & Process Engineering, For the SpectraLink Corporation

May 23, 2003
PN 72-0096-00 Rev D

Table of Contents

1. About This Document

This document explains how to install, configure, and maintain the Avaya Voice Priority Processor (AVPP) within an IP telephony system.

1.1 Questions?

If you have questions please contact **Avaya Technical Support at 1 800 242-2121** (USA only) or your local authorized Avaya dealer.

1.2 Icons and Conventions

This manual uses the following icons and conventions.

Caution! Follow these instructions carefully to avoid danger.

Note these instructions carefully.

NORM This typeface indicates a key, label, or button on the Avaya Voice Priority Processor (AVPP) or Wireless Telephone (WT).

2. Avaya Voice Priority Processor Overview

SVP is the Avaya quality of service (QoS) mechanism that is implemented in the Wireless Telephone (WT) and Access Point (AP) to enhance voice quality over the wireless network. SVP gives preference to voice packets over data packets on the wireless medium, increasing the probability that all voice packets are transmitted efficiently and with minimum delay. SVP is fully compliant with the IEEE 801.11, and 802.11b standards.

The Avaya Voice Priority Processor (AVPP) is an Ethernet LAN device that works with the AP to provide QoS on the wireless LAN. Voice packets to and from the Avaya WTs are intercepted by the AVPP and encapsulated for prioritization as they are routed to and from an IP telephony server or gateway.

Avaya WTs support the 802.11e protocol including basic WMM™ and the optional admission control if these are in turn supported by the AP. If the AP supports WMM, the WT automatically discovers and uses it. WMM does not replace the Avaya AVPP.

2.1 Multiple Avaya Voice Priority Processors

Multiple AVPP environments are those which have more than one AVPP in the same subnet in order to accommodate larger systems and higher call capacity.

In a system comprised of multiple Avaya Voice Priority Processors using an IP protocol, a master Avaya Voice Priority Processor must be identified. The master SVP Server must have a static IP address. The WTs and the other AVPPs 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 AVPPs. However, the loss of the master AVPP results in a loss of all communication between all of the AVPPs. This also means that the loss of the master SVP results in the loss of all active calls and WTs cannot check-in until communication with the master is reestablished.

2.2 The Timing function

In the IP PBX environment, AVPPs provide both the connection or "gateway" to the IP PBX for the WTs and the "timing" function for active calls. This "gateway" function is distributed across the AVPPs.

The number of active AVPPs is determined dynamically. Whenever AVPPs are added to or removed from the system, the distribution of "timing" function for active calls, as well as the "gateway" function, is affected.

2.3 Internal Gatekeeper

A gatekeeper is required in certain H.323 protocol systems. Currently, a gatekeeper is not supported.

2.4 Avaya Voice Priority Processor Capacity

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.

The table below shows the capacity of an IP Gateway in a multiple SVP Server environment.

SVP Servers	Calls per server	Total Calls	Erlangs	#WTs 10% use	#WTs 15% use	#WTs 20% use
1	80	80	65	500	433	325
2	64	128	111	1000	740	555
3	60	180	160	1500	1067	800
4	58	232	211	2000	1407	1055
5	57	285	262	2500	1747	1310
6	56	336	312	3000	2080	1560
7	56	392	367	3500	2447	1835
8	55	440	415	4000	2767	2075
9	55	495	469	4500	3127	2345
10	55	550	524	5000	3493	2620
11	55	605	578	5500	3853	2890
12	54	648	621	6000	4140	3105
13	54	702	674	6500	4493	3370
14	54	756	728	7000	4853	3640
15	54	810	782	7500	5213	3910
16	54	864	836	8000	5573	4180

2.5 Notes on System Configuration

In an IP system using subnets to differentiate telephony areas, each subnet must have its own SVP Server as well as access points. This is not considered a multiple SVP Server environment since the SVP Servers are separated by the subnet architecture. Multiple SVP Server environments are those which have more than one SVP Server in the same subnet in order to accommodate a high volume of wireless telephony traffic.

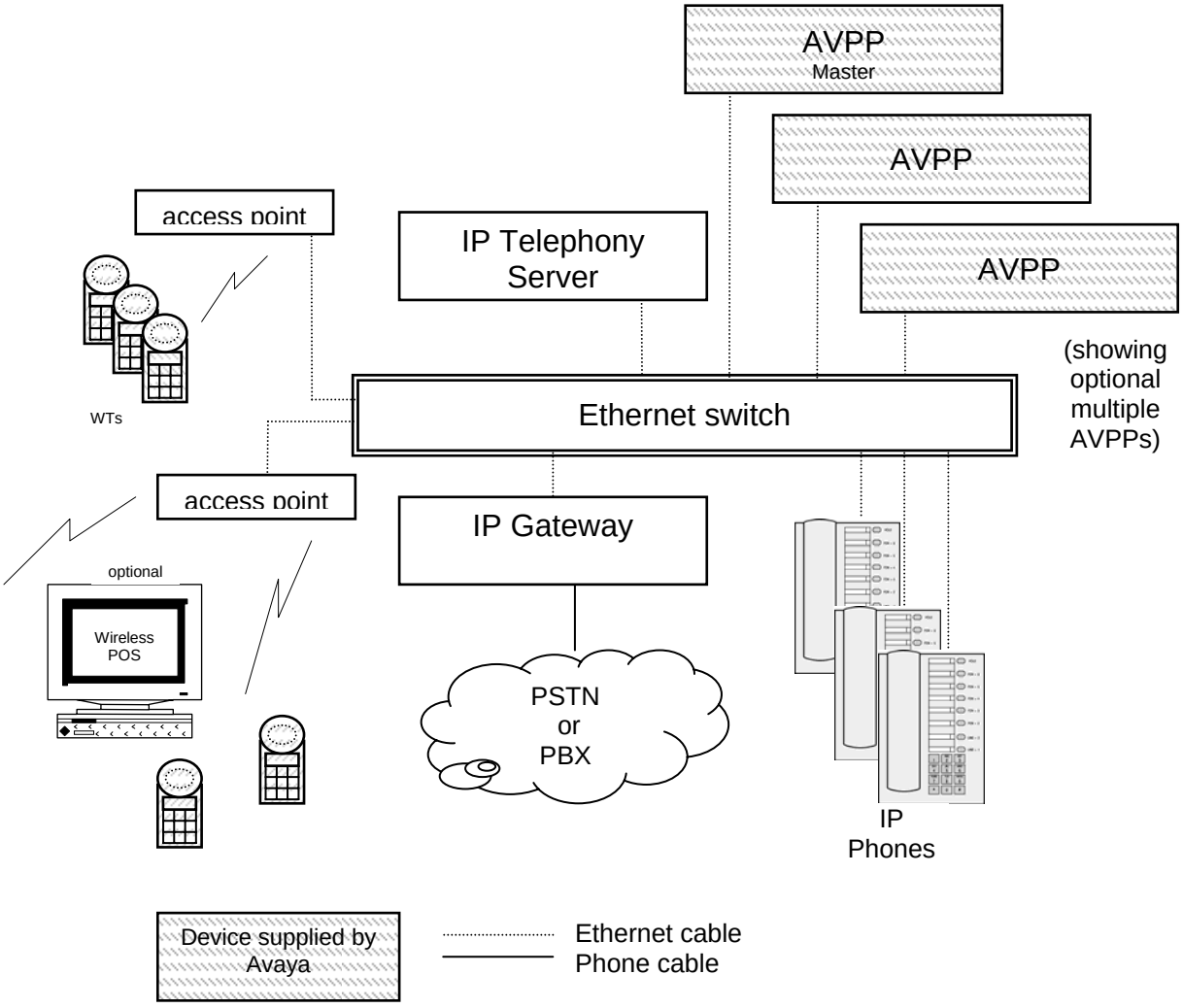
WTs cannot roam between subnets. Any call in progress will be dropped when the user moves out of range. In order to resume functionality in the new subnet area, the user must power cycle the WT. Once the WT achieves communication within the new subnet, normal functionality will return.

IP multicast addresses are used by the Avaya i640 WT system. This requires that multicasting be enabled on the subnet used for the Avaya WTs and SVP 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.

2.6 System Diagram

The following diagram shows the AVPP residing on a network with an IP telephony server, wireless LAN access points, and Ethernet switch:



(IP telephony system with multiple AVPPs)

2.7 System Components

- **Avaya e340/h340 and i640 WTs** – Employees can carry WTs to make and receive calls as they move throughout the building. The WTs are to be used on-premises; they are not cellular or satellite phones. They are connected to the facility's existing telephone system and to the GW or IP gateway. Just like wired telephones, they can receive calls directly, receive transferred calls, transfer calls to other extensions, and make outside and long distance calls (subject to the restrictions applied in your facility.)

  The Avaya e340/h340 WT is a lightweight, durable handset specifically designed for mobile workplace use within a facility. The Avaya i640 WT offers a durable design with push-to-talk functionality.

  Avaya WTs can operate on an 802.11b wireless network and can operate at a transmission rate of up to 11Mb/s.

- **Access Points** – supplied by third party vendors, access points provide the connection between the wired Ethernet LAN and the wireless (802.11) LAN. Access points (AP) must be positioned in all areas where WTs will be used. The number and placement of access points will affect the coverage area and capacity of the wireless system. Typically, the requirements for use of Avaya WTs are similar to that of wireless data devices. Contact Avaya, or a certified Avaya distributor, for specific information about your facility's needs.

  The Avaya WTs must connect to access points that use SVP. Contact Avaya, or a certified Avaya distributor, to verify that your AP and its software version are supported.

- **Ethernet Switch** – a component in the wired Ethernet LAN infrastructure. Switches interconnect multiple network devices, including access points and GWs. Ethernet switches are required to provide the higher performance network connections needed to handle combined voice and data traffic.

- **Router** – an optional component in the wired Ethernet LAN infrastructure that separates a wired LAN into segments so that network traffic is restricted to those segments that are directly involved in the communication. Installation of a network router is recommended in larger networks, where there may be significant network traffic not related to the wireless LAN. A router will isolate the wireless LAN from the associated wired LAN so that they are not impacted by each others' traffic. The GWs, the APs, and their associated Ethernet switch must all be on the same "side" of the router.

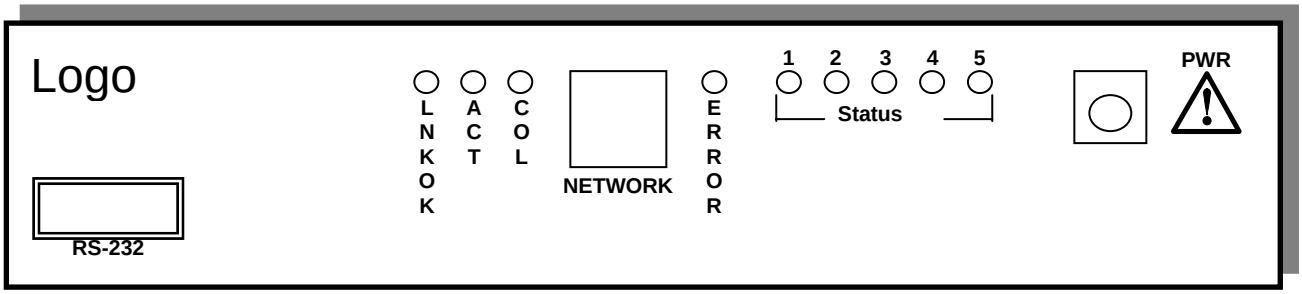
- **AVPP** – the AVPP manages call network traffic. It is a required component to utilize the 11Mb/s maximum transmission speed available in the Avaya WT.

  SVP is the Avaya quality of service (QoS) mechanism that is implemented in the WT and AP to enhance voice quality over the wireless network. SVP gives preference to voice packets over data packets on the wireless medium, increasing the probability that all voice packets are transmitted efficiently and with minimum or no delay. SVP is fully compliant with the IEEE 802.11 and 802.11b standards.

- **Administrative computer** – Required for setup and maintenance of the AVPP. This computer may 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** – Required in an IP system to distribute software to the WTs and AVPP. May be on a different subnet than the IP gateway, IP telephony server, and APs.

2.8 The Front Panel of the Avaya Voice Priority Processor

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



RS-232 Port – male DB-9 connector (DTE) used for RS-232 connection to a terminal, terminal emulator, or modem for system administration.

Link LEDs –

LNKOK – lit when there is a network connection.

ACT – lit if there is system activity.

COL – lit if there are network collisions.

NETWORK – connects to wired (Ethernet) LAN.

ERROR LED – lit when the system has detected an error.

STATUS LEDs – indicate system error messages and status.

1 – heartbeat, indicates gateway is running.

2 – if active calls.

3, 4, **5** – currently unused

PWR (power jack) – connects to the AC adapter supplying power to the system.

Use only the Avaya-provided Class II AC Adapter with output 24VDC, 1A.

3. Installing the Avaya Voice Priority Processor

As shown in the system diagram the AVPP is connected to the Ethernet switch. The specifications covered here allow for great flexibility in physical placement of the components within stated guidelines.

See the *Setup and Administration* document for your vendor's IP system for information on LAN requirements, network infrastructure and IP addressing.

3.1 Required Materials

The following equipment must be provided by the customer.

- **Power Outlet** – must accept Avaya-provided AC adapter.
- **Backboard space** – the AVPP is designed to be wall mounted to ¾" plywood securely screwed to the wall.
- **Screws** – required to mount the AVPP to the wall. Four #8 - ¾" panhead wood screws (or similar device) are required.
- **Cat. 5 Cable** – RJ-45 connector at the AVPP. Connection to Ethernet switch.

3.2 Locate the Avaya Voice Priority Processor

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).

Locate the AVPP in a space with:

- Sufficient backboard mounting space (for wall mount) and proximity to the LAN access device (switched Ethernet hub) and power source.
- Easy access to the front panel, which is used for cabling.
- A maximum distance of 325 feet (100 meters) from the Ethernet switch.

3.3 Install the Avaya Voice Priority Processor

Rack Mounting the AVPP

The rack mount kit is designed for mounting equipment in a standard 19 inch rack and should contain the following equipment:

Mounting plates – two for each AVPP to be mounted.
Screws – four rack mount screws for each AVPP to be mounted.

To rack mount the AVPP:

1. Remove the corner screws from the AVPP

2. Screw the U-shaped end (round screw holes) of the two mounting plates to the AVPP.
3. Screw the other end of the two mounting plates (oblong screw holes) to the rack.
4. Repeat steps 1-3 for each additional AVPP. The mounting plate is designed to provide the correct minimum spacing between units. When mounting multiple units, stack the units in the rack as closely as possible.

Mount the AVPP to Wall

The AVPP can be mounted either horizontally or vertically.

To mount the AVPP:

1. Using a 1/8 inch drill bit, drill four pilot holes, on 1.84 by 12.1 inch centers (approximately equivalent to 1-13/16 inch by 12-1/8 inch).
2. Insert the #8 x 3/4 inch screws in the pilot holes and tighten, leaving a 1/8 to 1/4 inch gap from the wall.

Connect AVPP to LAN

1. Using a Cat. 5 cable, connect the **NETWORK** port on the AVPP to the connecting port on the Ethernet switch.

Connect Power

2. Connect the power plug from the AC adapter to the jack labeled **PWR** on the AVPP.

Use only the provided Class II AC Adapter with output 24VDC, 1A.

3. Plug the AC adapter into a 110VAC outlet to apply power to the AVPP.
4. The system will cycle through diagnostic testing and the LEDs will blink for about one minute. When the system is ready for use:
   - The **ERROR** LED should be off.
   - **Status 1** should be blinking.

After the AVPP is installed, you must configure the Avaya WTs. For WT configuration, see the *Setup and Administration* document for your vendor's IP system.

4. Configuring the AVPP

During initial setup of the AVPP the IP address is established and the maximum number of active calls per access point is set. Optionally, you may enter a hostname and a location for software updates via TFTP.

4.1 Connecting to the Avaya Voice Priority Processor

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 may be done via the network using Telnet. It is recommended that the basic setup actions occur while the serial connection is made.

Connect via the Serial Port

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. Press Enter to display the AVPP login screen.
4. Enter the default login: **admin** and default password: **admin**. These are case sensitive.
5. The **NetLink SVP-II System** menu will display.

Connecting Via Telnet

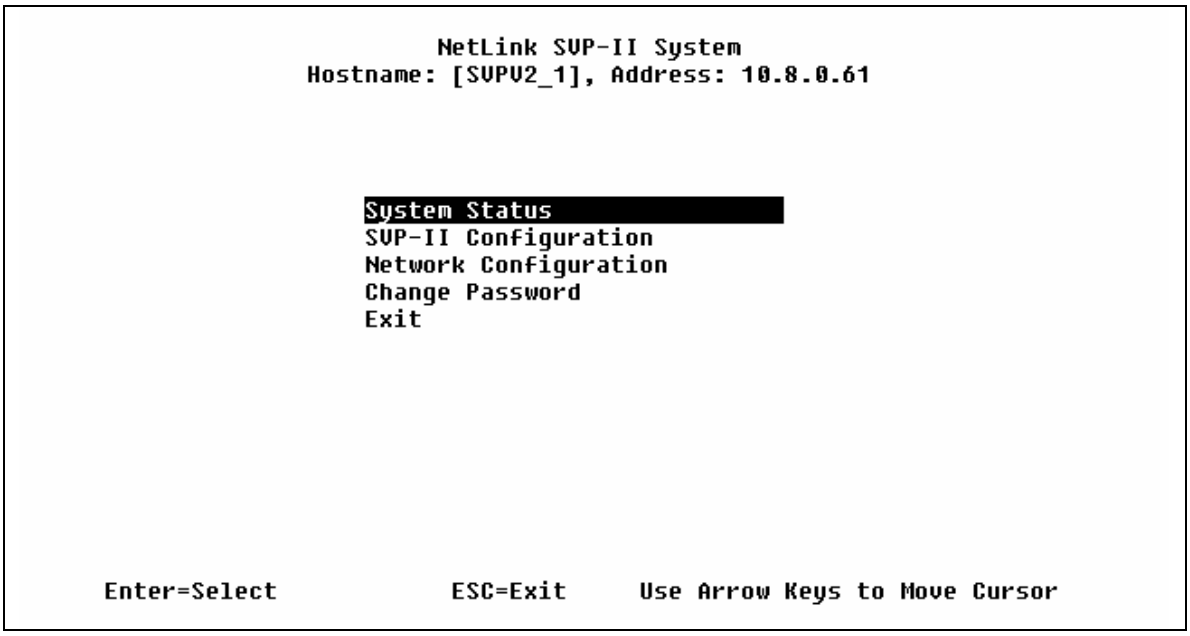
Telnet can only be used after the AVPP's IP address is configured.

The Telnet method of connection is used for routine maintenance of the Avaya Server for both local and remote administration, depending on your network.

To connect via Telnet, run a Telnet session to the IP address of the AVPP. Once you connect and log in, the **NetLink SVP-II System** menu displays.

4.2 The NetLink SVP-II [1]System Menu

The main menu displays as shown here:



System Status – menu for viewing error messages, status of operation and software code version. The 170 series software is required in the Alcatel IP environment. You can check the version currently installed on the AVPP through the **System Status** menu as described in section 7.3.

SVP-II Configuration – allows you to set the mode and reset the system.

Network Configuration – allows you to set network configuration options, including IP address and hostname.

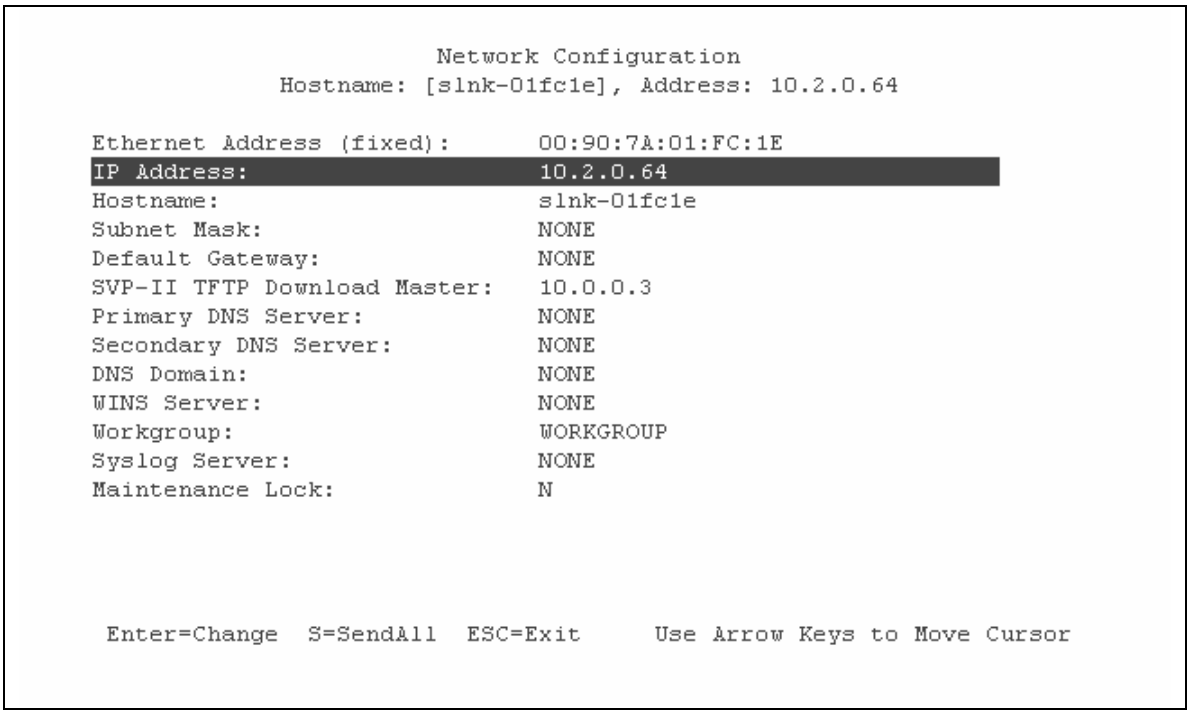
Change Password – allows you to change the password for AVPP access.

[1] SVP-II is a designation used internally by OEM Engineering.

4.3 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 you may obtain from Avaya. See section 5, the *Software Maintenance* section, of this document for more information about installing software updates via TFTP.

Scroll to **Network Configuration** and select by pressing Enter. A screen similar to the following appears:



- **IP Address –** enter the IP address of the AVPP, defined by your network administrator. Enter the complete address including digits and periods. **DHCP** may be entered.
- **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 spaces in this field.
- **SVP-II TFTP Download Master –** this entry indicates the source of software updates for the AVPP. See section 5, the *Software Maintenance* section, for more information.Valid source location entries are:
  - **NONE** – disables.
  - **IP Address** – the IP address of a 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 setting 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.

The AVPP must be reset in order to set the configuration options. If the AVPP is in **Maintenance Lock**, you will be prompted to reset the AVPP upon pressing Esc. Respond with a **Y** to the reset prompt.

The AVPP may be manually reset by selecting the **Reset** option in the **SVP-II Configuration** screen and then pressing **Y** (Yes).

Send All

In an IP system with multiple AVPPs, 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 just the IP address and custom hostname (if desired) for each AVPP using the initial serial connection. Then connect via the LAN and use **SendAll** to set identical configuration options for all AVPPs.

If **SendAll** is to be utilized in your system, all passwords must be identical. DO NOT CHANGE THE PASSWORD AT THE INITIAL CONFIGURATION IF THE SEND ALL OPTION IS DESIRED. Use the default password and change it globally if desired after a LAN connection is established for all AVPP.

If independent administration of each AVPP is desired, the passwords may be set at initial configuration.

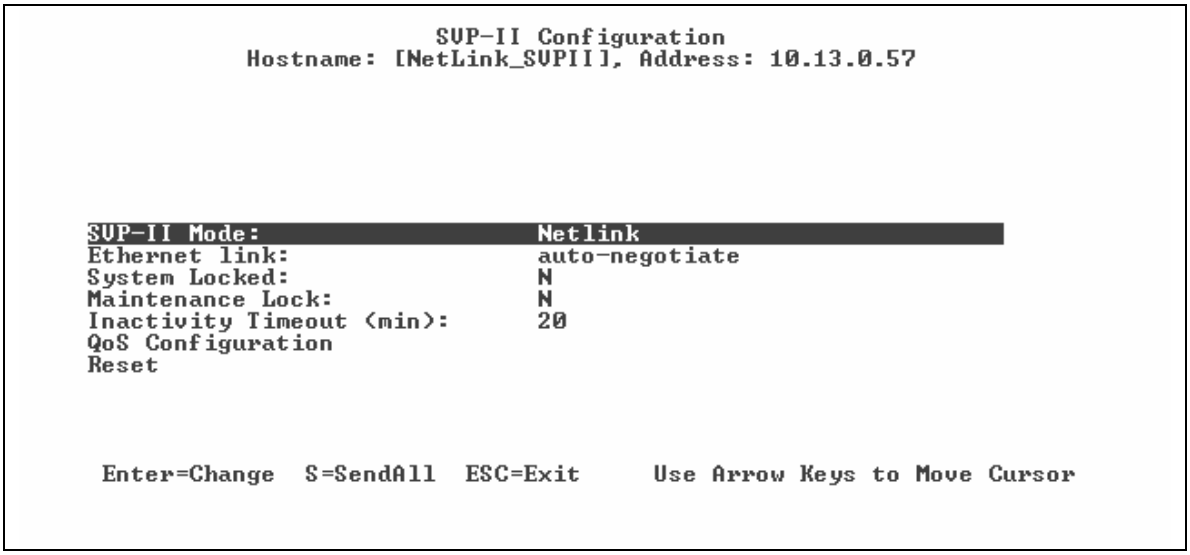
To change the IP address of the master AVPP, change it in this menu and reboot the system. Then you may change alias IP addresses in each of the other SVP Servers without error.

4.4 Avaya Voice Priority Processor Configuration

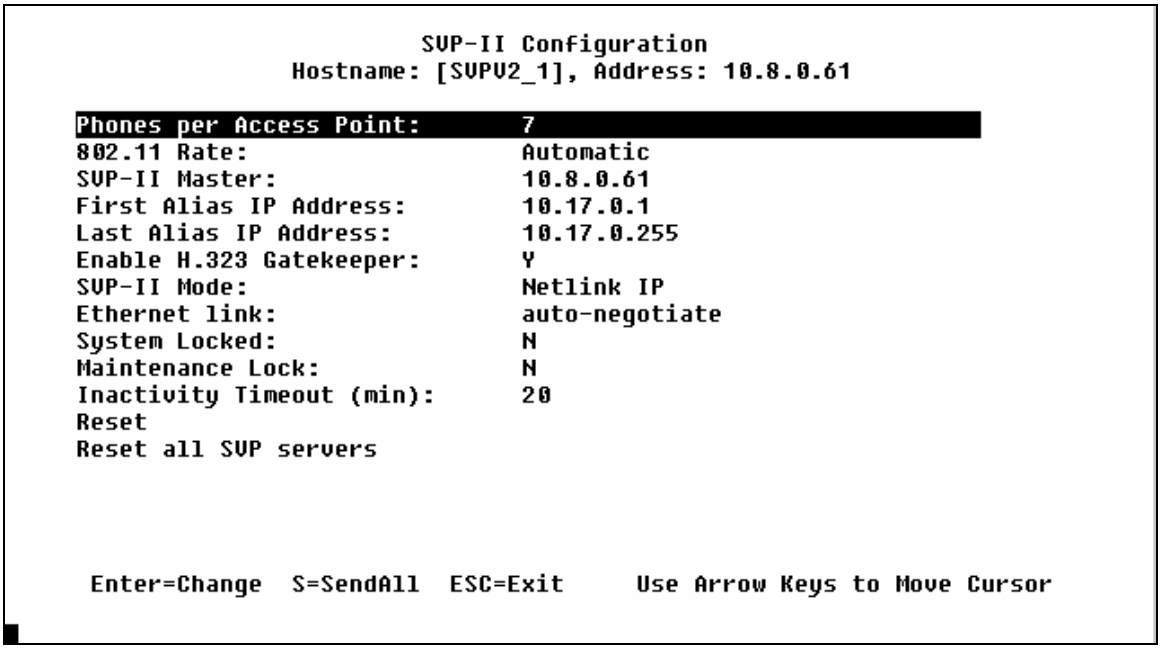
The **SVP-II Configuration** screen is where you set the mode of the AVPP for an IP environment. It is also where you can lock the AVPP for maintenance and reset the AVPP after maintenance.

The AVPP will automatically lock for maintenance if the IP address is changed. When this Maintenance Lock occurs, the AVPP must be reset upon exit. All active calls are terminated during a reset.

From the main menu, scroll to **SVP-II Configuration** and select by pressing Enter.



- **SVP-II Mode:** This option should be set to **AVAYA IP**.



Complete the configuration options:

- **Phones per Access Point**: Access point specifications are detailed in the *Configuration Notes* for each brand and type. Refer to these notes when entering the number of simultaneous calls supported for your type.
- **802.11 Rate**: Select 1MB/2MB to limit the transmission rate between the WTs and access points. Select **Automatic** to allow the WT to determine its rate (up to 11 Mb/s).
- **SVP-II Master**: The master AVPP must be identified in an IP system. Select one of the following identification options:
  - Statically configure the IP address of the master AVPP in each of the AVPPs. Enter the IP address.
  - Statically configure the IP address of the master AVPP in a DHCP server and configure each of the AVPPs to get the information from the DHCP server. Enter **DHCP**. If DHCP is used, the IP address of the master SVP Server must be configured in the DHCP server. See the WT interface document for your IP environment for more information about DHCP integration factors.
  - Statically configure the IP address of the master AVPP in a DNS server and configure the each of the AVPPs to retrieve this information from the DNS server. Enter **DNS**. If DNS is used, the IP address of the master SVP Server must be configured in the DNS server.

See the Overview section for an explanation of the master AVPP.

- **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 WTs.

All alias addresses must be on the same subnet as the SVP server and cannot be duplicated on other subnets or AVPPs. There is no limit to the number of addresses that can be assigned, but the capacity of each AVPP is 500 WTs.

Alias IP Addresses are not necessary in Avaya systems.

- **Enable H.323 Gatekeeper**: The Gatekeeper 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). Set it at **Y** (Yes) to prevent any new calls from starting. Return to **N** to restore normal operation.
- **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. Note that the

administrator cannot change this option. It is automatically set by the system. Reset the system at exit to clear Maintenance Lock.

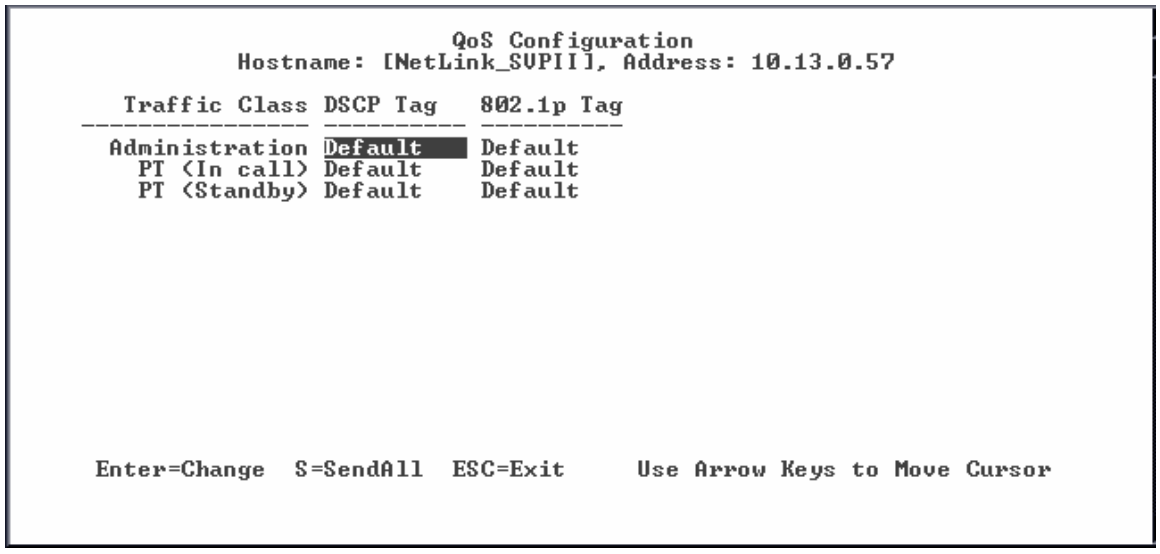
- **Inactivity Timeout (min):** Set the number of minutes the administrative module can be left unattended before the system closes it. This number can be from 1 to 100. If it is set to zero (0), the administrative module will not close due to inactivity.
- **QoS Configuration:** Select this option to set the DSCP tags and the 802.1p tags. See following section.
- **Reset System:** If this option is selected, you will be prompted to reset the AVPP upon exiting this screen.

Note that resetting the AVPP will terminate any calls in progress.

The AVPP should be reset at the end of any maintenance procedure that requires a reset either via **Maintenance Lock** or manually via **Reset System**.

4.5 QoS Configuration

Tags set packet priorities for QoS.

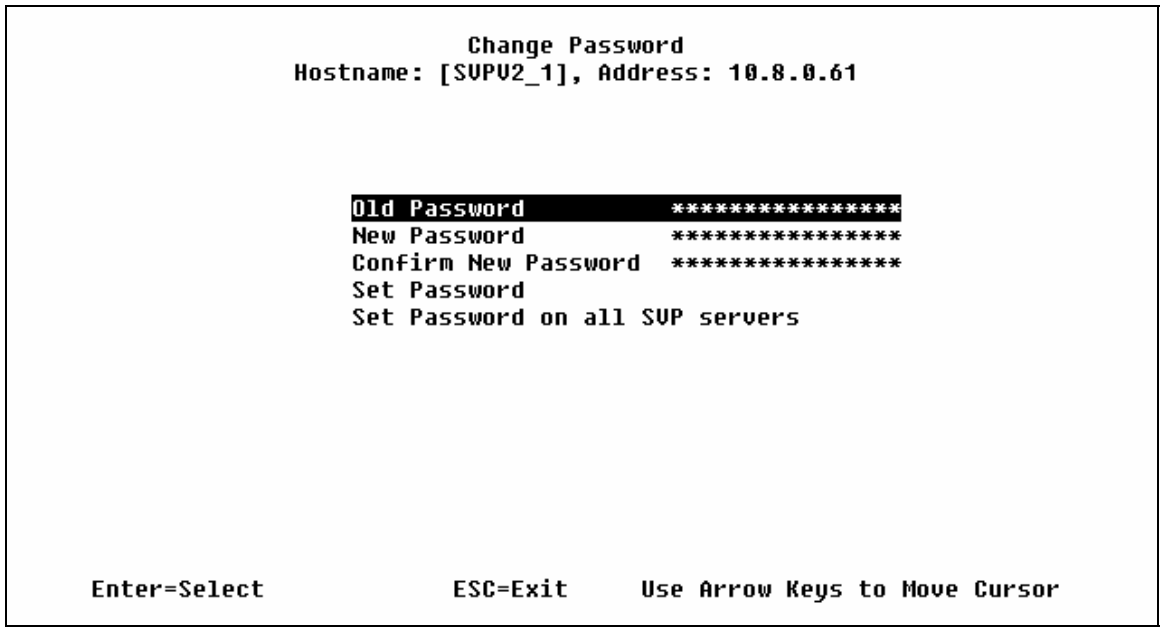


Either DSCP or 802.1p tags may be used. DSCP tags may be set to a number 0-255.

- **DSCP Tag** – (Differentiated Services Code Point) is a QoS mechanism for setting relative priorities. Packets are tagged with a DSCP field in the IP header for type of service. The value may be set as a number from 0-255 and may be different for administration and in call/not in call modes. The default value for the DSCP tags is 16.
- **802.11p Tag** –Packets are tagged with a 802.1p field in the Ethernet header for type of service. The value may be set as a number from 0-255 and may be different for administration and in call/not in call modes.

4.6 Change Password

If desired, the password to access the AVPP may be changed. Select **Change Password** from the main menu. A screen similar to the following will appear:



Enter the information and either select **Set Password** or press the **S** key to set the new password.

Password parameters:

- More than four characters,
- First character must be a letter,
- Other characters may be numbers or letters,
- No dashes, spaces, or punctuation marks, etc. (alphanumeric only).

If you forget a password, call Avaya Customer Service for assistance.

5. Swapping/Adding/Deleting Avaya Voice Priority Processors

Whenever an AVPP is removed from the system, WTs that are using the AVPP will be affected. If the removal of the AVPP is intentional, the administrator should lock and idle the system prior to removing an AVPP. Whenever an AVPP is added to the system, the change is seamless and does not affect WT calling functionality.

Adding an AVPP

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 WT not active in a call will immediately be forced to check-out and check-in again. Any WT 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 WT ends the call, it will be forced to checkout and checkin again.

Removing an AVPP

When an AVPP is removed from the system it is detected within two seconds. WTs not in calls are immediately forced to checkout and checkin again. For WTs active in calls, two possible scenarios can occur. If the AVPP that was removed was providing the "gateway" function for the WT, then the call is lost and the WT is forced to checkin again. If the AVPP that was removed was providing the "timing" function for the call, the call will switch to the AVPP that should now provide the "timing" function. Note that during the two seconds while the loss of the AVPP is being detected, the audio for the call will be lost.

Changing the Master AVPP

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

6. Software Maintenance

The AVPP uses proprietary software programs written and maintained by Avaya. The software versions that are running on the system components can be displayed via the **System Status** screen.

Avaya or its authorized dealer will provide information about software updates and how to obtain the software (for example, downloading from a web site).

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. See the *Setup and Administration* document for your vendor's IP system for more information about using TFTP.

6.1 Software Updates

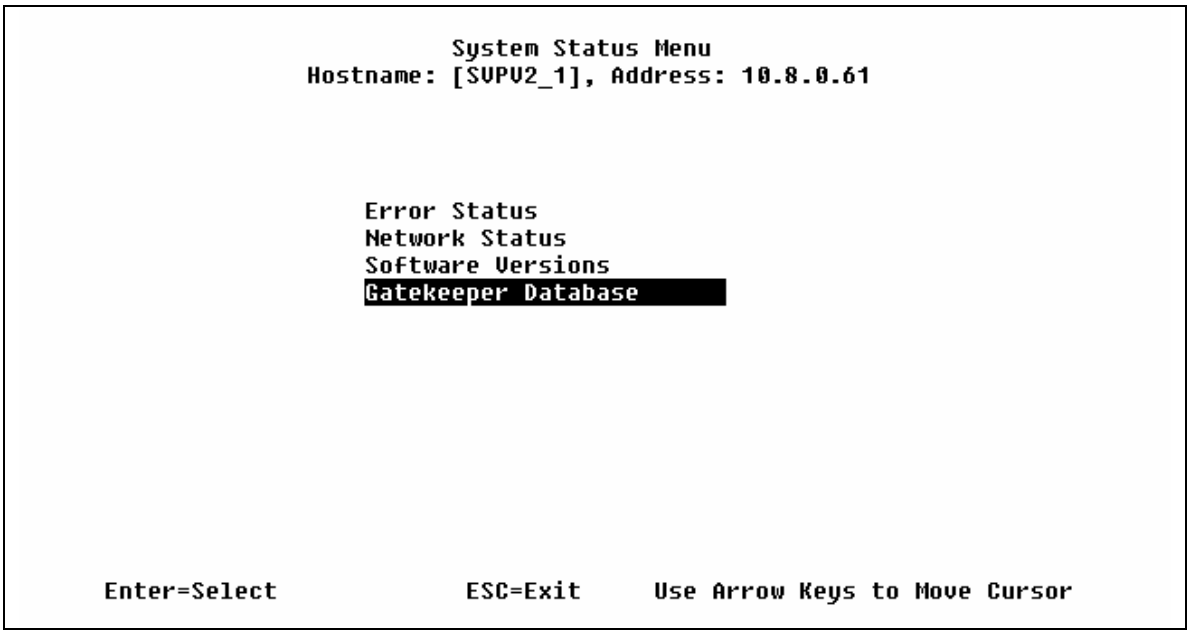
After software updates are obtained from Avaya, they must be transferred to the TFTP location in the LAN to update the code used by the AVPP.

Lock the AVPP in the **SVP-II Configuration** screen prior to updating the software.

Note that locking the AVPP will prevent new calls from starting. All calls in progress will be terminated when the AVPP is reset.

7. Troubleshooting via System Status Menu

Information about system alarms, and network status displays on various screens accessed through the **System Status Menu** screen, opened from the main menu of the AVPP. See the previous sections for directions on how to connect to the AVPP and navigate to the **System Status Menu**.



Error Status – displays alarm and error message information.

Network Status – displays information about the Ethernet network to which the AVPP is connected.

Software Versions – lists the software version for each Avaya component.

Gatekeeper Database – not used.

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 trouble.

7.1 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 Department.

From the **System Status Menu**, select **Error Status**. 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

Press C to clear all clearable alarms.

7.2 Network Status

The AVPP is connected to the Ethernet network, referred to as the LAN or Local Area Network. The information about that connection is provided through the **Network Status** screen.

From the **System Status Menu**, select **Network Status**. The screen displays information about the Ethernet network. This information can help troubleshoot network problems. A sample screen is displayed here.

```
                        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 utilized. See SVP100 Capacity for more information.

Data is transmitted over Avaya components by proprietary technology developed by Avaya. The Avaya Radio Protocol (SRP) packets and bytes can be differentiated from other types of transmissions and are used to evaluate system functioning by Avaya customer support and engineering personnel.

RX – Ethernet statistics concerning the received packets during System Uptime.

bytes – bytes received

packets – packets received

errors – sum of all receive errors (long packet, short packet, CRC, overrun, alignment)

drop – packets dropped due to insufficient memory

fifo – overrun occurred during reception

alignment – nonoctet-aligned packets (number of bits NOT divisible by eight)

multicast – packets received with a broadcast or multicast destination address

TX – Ethernet statistics concerning the transmitted packets during System Uptime.

bytes – bytes transmitted

packets – packets transmitted

errors – sum of all transmit errors (heartbeat, late collision, repeated collision, underrun, carrier)

drop – packets dropped due to insufficient memory

fifo – underrun occurred during transmission

carrier – carrier lost during transmission

collisions – packets deferred (delayed) due to collision

SVP-II Access Points in Use – access points in use by WTs, 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 WTs in a call

SVP-II Telephones in Use – WTs in standby or in a call

SVP-II Telephones in Calls – WTs in a call

SVP-II SRP Audio (Delay) – SRP audio packets whose transmission was momentarily delayed

SVP-II SRP Audio (Lost) – SRP audio packets dropped due to insufficient memory resources

7.3 Software Version

The AVPP and WTs utilize Avaya's proprietary software that is controlled and maintained through versioning. 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.

From the **System Status Menu**, select **Software Version**. A sample screen is displayed here.

```
                    Software Version Numbers
              Hostname: [SVPV2_1], Address: 10.8.0.61


   Hardware Versions:       32/02 ENG
   Factory Page:            230.008
   Downloader:              230.157 (5ea5a4cc)
   Table of Contents:       173.001 (ddb366ac)
   Functional Code:         174.001 (c0942c06)
   File System:             175.001 (cce2b488)









                              ESC to Exit
```

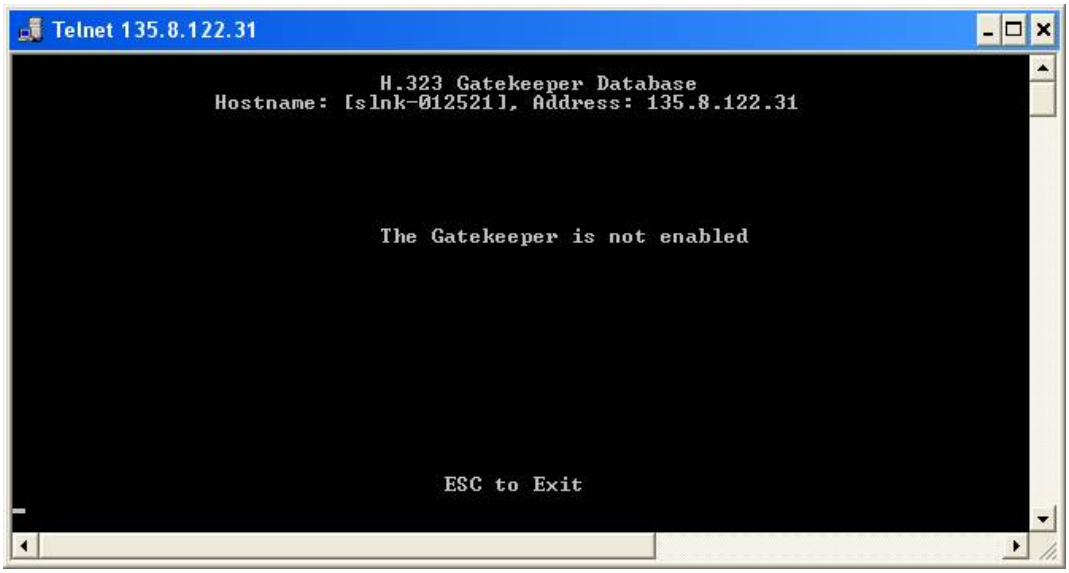
Note that the software versions on your system will be different from the versions displayed in the above sample screen.

The 170 series software is required in certain IP environments.

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

7.4 Gatekeeper Database

The **Gatekeeper Database** screen lists the registered extension numbers and the IP address currently being used by each. The Gatekeeper is not enabled.



Index