



ASG Guard II
Setup/Integration Guide for
Linux-based S8X00 Servers

Version 5.2

11/7/2005

AVAYA, Inc.

211 Mt. Airy Rd.

Basking Ridge, NJ 07920

www.avaya.com

2005 Avaya Inc.
All Rights Reserved
Printed in U.S.A.

Notice

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

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 *suspect 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 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 may be a risk of unauthorized or malicious 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 system 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

To Get Help

If you need assistance with administration of the ASG Guard II call Avaya, Inc. at **1 800-242-2121**, or your local Authorized Dealer. Our technical support staff is available 24 hours. This call may be billable.

FCC Notices

United States Users

Part 15. Subpart A: 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.

Note: 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 operations. 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.

European Users

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Safety Warnings

1. Read and understand all instructions in the user's manual.
2. Observe all warnings and instructions marked on this product.
3. Unplug the product from wall outlets and telephone jacks before cleaning. Clean exposed parts with a soft, damp cloth. Do not use liquid or aerosol cleaners and never immerse in water.
4. Do not use the product near water or when you are wet. If the product comes in contact with any liquids, unplug the power and line cords immediately. Do not plug the product back in until it has been dried thoroughly.
5. Install this product securely on a stable surface. Damage may result if the product falls.
6. Install this product in a protected location, where no one can step on or trip over power and line cords. Do not place objects that may cause damage or abrasion on the cords.
7. Do not allow anything to rest on the power cord. Do not install this product where people walking on it will abuse the cord. Do not overload wall outlets, this can result in the risk of fire or electric shock.
8. Never push objects of any kind into this product through housing opening because they may touch dangerous voltage points or short out parts, resulting in possible fire or electric shock.
9. If this product does not operate normally, you cannot solve the problem, or if the product is damaged, report the trouble to

Avaya, Inc. Do not open the product; opening the product can expose you to dangerous voltage or other risks.

10. During thunderstorms, avoid using telephones, except cordless modes. There is a slight chance of electric shock from lightning.
11. Never install telephone wiring during a lightning storm.
12. Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
13. Never touch telephone wires, network wires, or terminals unless they have been disconnected from the service provider.
14. Use caution when installing or modifying telephone lines.
15. Do not use a telephone in the vicinity of a gas leak. If you suspect a gas leak, report it immediately, but use a telephone away from the area where gas is leaking.
16. This product should be operated from the power source indicated on the power transformer (see item 17 below). If you are not sure of the type of power supplied to your business or home, consult your local power company.

17. Use only a UL Listed wall plug-in power transformer that has the following characteristics:

Input Rating: 120 V AC \pm 10% 60 Hz

Output Rating: 16 V AC at 2063 milliamps

The power transformer supplied with this product has these characteristics.

Changes or modifications to the ASG Guard II and the devices that are not expressly approved by Avaya, Inc. will void the user's authority to operate the equipment.

Table of Contents

1	Introduction.....	7
1.1	Document Overview	7
1.2	Audience Assumptions	8
1.3	Related Reading Material	8
1.4	Getting Help.....	8
2	Hardware Overview	9
2.1	ASG Guard II Introduction.....	9
2.2	ASG Guard II Features	9
2.3	Package Contents	12
2.4	Supported Avaya Products	12
3	ASG Guard II Installation.....	13
3.1	Pre-Installation Checklist	13
3.2	Installation Checklist	15
3.3	ASG Guard II Physical Installation	16
3.4	Powering Up the ASG Guard II	16
3.5	Automatic Registration Tool (ART).....	17
3.6	Connecting to the AUX Port.....	17
3.7	Connect a Modem to a Telephone Line	18
3.8	International Modem Setup.....	18
3.9	Host Port Connectivity	18
3.10	Checking the Software Version – VER Command.....	19
3.11	Setting the Date and Time	19
4	ASG Guard II Configuration	21
4.1	Setting Network Parameters	21
4.2	Enabling Alarm Delivery.....	23
4.3	Configuring Avaya Device IP Addresses	24
4.4	Administering an Avaya IP Device	24
4.5	Set Network Services.....	25
4.6	Enabling Telnet on the ASG Guard II	26
4.7	Connecting to an IP Device.....	26
4.8	Saving and Loading Avaya IP Device Information.....	27
4.9	Provisioning the ASG Guard II	28
4.10	Modifying the Avaya S8X00 Platform to Work with the ASG Guard II.....	28
5	Additional Configuration.....	29
5.1	Adding a CMaster User.....	29
6	Additional Information.....	31
6.1	Using the ASG Guard II Configuration Wizard	31
6.2	How Automated Alarm Delivery Works	34
6.3	Aux and Host Port Pinouts	38
6.4	Standard Serial cables.....	39

List of Figures

Figure 1-1: ASG Guard II and S8700 Integration	8
Figure 2-1: ASG Guard II Front Panel.....	10
Figure 2-2: ASG Guard II 4-Port Rear Panel.....	10
Figure 2-3: ASG Guard II 16-Port Rear Panel.....	10
Figure 2-4: ASG Guard II 28-Port Rear Panel.....	10
Figure 3-1: AUX Port located on the rear of the ASG Guard II	17
Figure 3-2: Modem Port.....	18
Figure 3-3: Version Information.....	19
Figure 3-4: Set Date and Time.....	20
Figure 4-1: Set Network Parameters.....	22
Figure 4-2 Set Networking Services Screen.....	25
Figure 4-3: CONT Example	26
Figure 5-1: Add User Example.....	30
Figure 6-1: Secure Proxy.....	31
Figure 6-2: Setup Wizard.....	33
Figure 6-3: Secure Gateway	34
Figure 6-4: List Action Item Example	35
Figure 6-5: DOLIST Action Item.....	36
Figure 6-6: AINIT Action Item.....	36
Figure 6-7: TRAPTASK Action Item.....	37
Figure 6-8:PHONTRAP Action Item.....	37
Figure 6-9: XMLACK Action Item.....	38
Figure 6-10: RJ45 Interface Pinout	38

List of Tables

Table 2-1: ASG Guard II Features 9
Table 2-2: ASG Guard II Front Panel Features 10
Table 2-3: ASG Guard II 4/16/28-Port Rear Panel Features 11
Table 3-1: Installation Checklist 15
Table 4-1: Avaya Special Commands 24

1 Introduction

This section covers the following topics:

- [Document Overview](#)
 - [Audience Assumptions](#)
 - [Related Reading Material](#)
 - [Getting Help](#)
-

1.1 Document Overview

The purpose of this document is to:

- Present an easy-to-follow guide for installation of the ASG Guard II (referred to as the “Guard II” throughout this document).
- Provide integration procedures between the ASG Guard II and the Avaya S8x00 series media servers.

This document is an abbreviated guide. Additional information can be found in the *ASG Guard II Administrator Guide* and the *ASG Guard II Connectivity Guide*.

The Guard II provides both secure remote access and device monitoring of Avaya IP-enabled devices such as the S8x00 series media servers. Using a built-in firewall, the Guard II offers remote access to the management interfaces of IP-enabled devices, while limiting connectivity to any other device located on the same network. The Guard II provides a secure access path to the various management ports of the S8x00 through a PPP dialup session. Individuals who access the Guard II use a DES-based, two-factor authentication token called the ASG Key, which is available both as a software and hardware token.

The S8x00 Media Servers generate SNMP traps containing INADS alarms that are sent to the ASG Guard II. The ASG Guard II converts the SNMP traps to the Avaya alarm receiver format, and forwards the alarms to INADS via PSTN. Upon successful delivery and acknowledgement of the alarm, the Guard II sends a confirmation SNMP trap back to the originating S8x00 device.

Figure 1-1 illustrates an example of the integration of the S8700 and Guard II. The Guard II will proxy any incoming Telnet, SSH, Web (thru PPP) and FTP sessions to the target device.

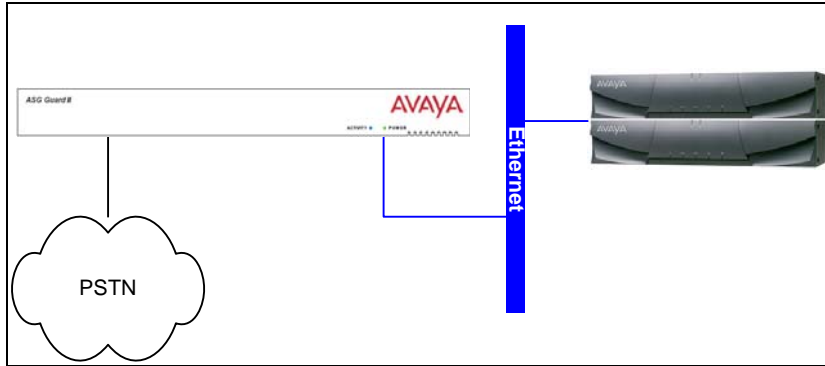


Figure 1-1: ASG Guard II and S8700 Integration

1.2 Audience Assumptions

This document is intended to assist Avaya field technicians and/or other authorized individuals who are responsible for the physical installation and configuration of ASG Guard II security appliances. Customer care and technical support associates should also refer to this document for assistance when working with field technicians to commission a customer site using ASG Guard II appliances.

1.3 Related Reading Material

ASG Guard II and Avaya product documentation are supplemental to this guide and can be found at the Avaya website: <http://www.avaya.com>.

1.4 Getting Help

For assistance with commissioning the ASG Guard II and the equipment it is protecting, contact the Avaya Customer Account Support Team at 1-800-248-1111 (US only).

Note: International sites should contact their regional Avaya Support Team.

2 Hardware Overview

This section covers the following topics:

- [ASG Guard II Introduction](#)
- [ASG Guard II Physical Features](#)
- [Package Contents](#)
- [Supported Avaya Products](#)

2.1 ASG Guard II Introduction

The ASG Guard II is the only Avaya-certified appliance that can securely access and manage S8700, S8500, and S8300 switches. The ASG Guard II is equipped with VPN access and a firewall for Avaya customers to define and restrict access to S8x00 switches. In addition to securing Avaya's IP switches, the ASG Guard II is certified to secure serially connected Definity, Octel, MAPD, CMS, etc. The ASG Guard II can also monitor environmental conditions surrounding infrastructure elements by using analog sensors that measure conditions such as temperature, humidity, and battery voltage.

2.2 ASG Guard II Features

There are three basic types of devices with the ASG Guard II family, differentiated by the number of host port connections (4, 16, or 28).

Table 2-1: ASG Guard II Features
Power button located on rear panel
"Power" and "Activity" LEDs located on front panel
IEC power connector
RJ-45 AUX port located on rear panel
RJ-45 host port connectivity: 4, 16, or 28 ports
One RJ-11 modem connector that supports two PCMCIA modems
One 10/100 "Internal" Ethernet connector that supports one LAN interface
One 10/100 "External" router interface
Five contact closure inputs
One analog sensor, 0-5 volts
Two temperature sensor inputs
Two mechanical relays: 1 latching/1 non-latching

Table 2-1: ASG Guard II Features
One RAM disk with up to 32 MB of memory
Integrated VPN router that securely carries administrative traffic through an intranet or public network from an administrator's desktop to each network connected device.

2.2.1 ASG Guard II 4/16/28 Port (RJ-45) Panel Diagrams



Figure 2-1: ASG Guard II Front Panel

Table 2-2: ASG Guard II Front Panel Features	
LEDs	The LEDs display power and activity status. When the unit is operating properly, the Power LED is steadily illuminated, and the Activity LED will pulse.



Figure 2-2: ASG Guard II 4-Port Rear Panel



Figure 2-3: ASG Guard II 16-Port Rear Panel



Figure 2-4: ASG Guard II 28-Port Rear Panel

Table 2-3: ASG Guard II 4/16/28-Port Rear Panel Features	
POWER INPUT	The ASG Guard II utilizes a standard PC cable to connect it to a 110/220 VAC outlet.
POWER BUTTON & LED	The Power button is located on the rear panel, adjacent to the power source input. When the Guard II is powered on, the green LED beneath the button is illuminated.
SENSOR INPUTS (Optional)	The Guard II provides three RJ45 sensor inputs: two temperature probes, and one 0-5V analog input. A 6-pin Terminal Block connector for the 2 simple relay outputs and a 10-pin Terminal Block connector for the 5 contact closure inputs are also supported. Note: Additional environmental monitoring options include an extended contact-closure wiring panel that increases contact closure density through the use of 12 host ports.
AUX PORT	The ASG Guard II provides an RJ-45 AUX port connector for local administrative access to the device. A standard 9-pin RS232 serial cable, with the enclosed modular RJ-45 adapter, is used to connect a PC or terminal to the Guard II.
HOST PORTS	The ASG Guard II provides an RJ-45 interface for up to 28 serially connected devices such as PBXs and routers. Host ports 1 through 4 are located directly beneath the contact closure inputs, while the remaining host ports are located on the right of the rear panel.
MODEMS	The Modems connector provides single RJ-11 connectivity for up to two internal PCMCIA modems.
INTERNAL	The Guard II provides one Internal port.
EXTERNAL	The Guard II provides one External port.

2.3 Package Contents

The ASG Guard II can be shipped with the following package contents:

One K003 Cable Kit (Material Code# 408122729), which includes:
One RJ-45 host port to DB-9 straight serial cable (for Intuity, Conversant, CMS)
One RJ-45 host port to DB-25 straight serial cable (for Definity INADS port, marked DCE)
One RJ-45 host port to DB-25 null serial cable (for Definity SAT terminal or MAPD)
One K002 Cable Kit includes:
Five DB9 Male to DB25 Female Cables with DB9F to RJ45 adapters attached
Three RJ45 to DB9 short serial cables
One RJ-11 “Y” cable
One temperature probe
One power cable

Note: The ASG Guard II may be shipped with additional adapter kits and cables. These cables are for connecting additional serially connected devices. The number of cables included will vary across different sites.

2.4 Supported Avaya Products

In addition to Avaya S8x00 Media Servers, the ASG Guard II is certified to integrate with the following Avaya products:

- Definity G3r
- Definity G3si Prologix
- Intuity Audix RMB, including: Intuity Conversant, RMB, Avaya IR, UCS 1000, MMU
- Definity MAPD
- Definity SAT Terminal
- Octel Aria and Serenade
- Merlin Magix and Legend

3 ASG Guard II Installation

This section covers the following topics:

- [Pre-Installation Checklist](#)
- [Installation Checklist](#)
- [Physical Installation](#)
- [Powering Up the Guard II](#)
- [Automatic Registration Tool \(ART\)](#)
- [Connecting to the AUX Port](#)
- [Modem Setup](#)
- [International Modem Setup](#)
- [Host Port Connectivity](#)
- [Checking the Software Version](#)
- [Setting the Date and Time](#)

3.1 Pre-Installation Checklist

Obtain the following material and information prior to installation:

1. Determine where the GUARD II Will be installed, and obtain the appropriate rack mount equipment if necessary.
2. Ensure you have the appropriate cables required to connect the Guard II to the S8x00. This includes obtaining a Cat-5 Ethernet cable of appropriate length for the Guard II, as well as one for the S8x00, if necessary.
3. Provision one or two POTS lines at the site. Obtain the appropriate RJ-11 cable, depending on the number of POTS lines available. Refer to the table below:

Phone Line(s)	Cable
1 POTS Line, terminating at 1 RJ-11 Jack	One (2-conductor) RJ-11 cable
2 POTS Lines, terminating at 1 RJ-11 Jack	One (4-conductor) RJ-11 cable
2 POTS Lines, terminating at 2 RJ-11 Jacks	One RJ-11 "Y" cable

4. Obtain the modem phone number(s):

Modem #1 _____
 Modem #2 _____

5. Obtain network-provisioning information for the ASG Guard II. This information will be used to configure the External Address of the Guard II IP interface. The customer's network provisioning personnel typically provide this information.

IP Address _____
 Subnet Mask _____
 Gateway _____

6. Obtain the PPP address that Avaya has assigned to the Guard II. This information is obtained from Avaya.

PPP Address _____

7. Obtain AVAYA device IP address information for each device to be protected by the Guard II. (The first entry in the table below is for example purposes only.) The Avaya IP address is obtained by contacting Avaya, and the Customer IP Address is typically obtained from the customer's network provisioning personnel.

Note: When integrating a single S8x00 Media server with an ASG Guard II, you must actually establish connectivity between the Guard II and three separate Customer IP addresses. S8x00 Media Servers are deployed as a set of two servers for redundancy. Each server is assigned a real, unique IP address, as well as one virtual IP address that is used by the active server. Each address must be defined as a separate device. Refer to Section 4.

The Avaya IP table in the Guard II can support up to 30 IP devices.

	Device Name	Avaya IP Address	Customer IP Address
Ex.	S8700SRV1	10.1.1.37	192.1.1.4
1			
2			
3			
4			

8. Obtain a laptop with a terminal application such as HyperTerm AND AN APPROPRIATE CABLE to connect to the AUX port of the ASG Guard II. Connect at 9600 baud, 8 data bits, no parity, and 1 stop bit (9600, 8-N-1).

3.2 Installation Checklist

Table 3-1: Installation Checklist			
Number	Description	Completed	Technician Initials
1	Physical Installation of ASG Guard II Hardware		
2	Connect ASG Guard II to Laptop via AUX port		
3	Connect ASG Guard II to Ethernet port of customer Network (May be performed out of sequence)		
4	Connect Serial Equipment to the ASG Guard II (Where Necessary)		
5	Power on ASG Guard II		
6	Collect Information for ASG Guard II Configuration		
7	Access the Automatic Registration Tool (ART) for Product ID (PID)		
8	Connect to the ASG Guard via a Laptop and the AUX port		
9	Check ASG Guard II Version		
10	Set Date and Time		
11	Set Network Parameters		
12	Call Remote Technical Services Group for Registration of ASG Guard II		
13	Add Avaya IP Devices (S8x00)		
14	Set Network Services (SNS)		
15	Verify Connectivity of IP Devices		
16	Verify Connectivity of Serial Devices		
17	Set Alarming Configuration on S8X00 server		

3.3 ASG Guard II Physical Installation

To install the ASG Guard II:

1. Place the Guard II in the selected location.
Note: To rack-mount the unit:
2. Place a rack-mounting bracket on each side panel of the ASG Guard II, and secure it with three screws. The brackets are marked “L” and “R” to indicate left and right sides.
3. Place the Guard II in the rack and secure it with two screws in each rack-mounting bracket.
4. Connect the PC or terminal to the AUX port of the Guard II using the supplied RJ-45 to DB-9 serial cable. This connection is used to configure the Guard II and can be disconnected after the unit is installed. Refer to Section 3.6 for more information on connecting to the AUX port.
Note: Do not disconnect the AUX connection until you have verified the operation of the unit.
5. Connect the DB-9 end of the serial cable to a serial port (for example, COM1) on the terminal or computer.
6. Connect the RJ-45 end of the serial cable to the AUX port located on the rear panel of the ASG Guard II.
7. If you are serially connecting any protected equipment, refer to the *ASG Guard II Connectivity Guide* for the appropriate cabling and connection instructions. Serial connectivity is not related to the S8x00 Media Server integration, and is not covered in this document.
8. Connect one or two analog telephone lines to the RJ-11 modem port, as described in Section 3.1.
9. Connect a Cat-5 network cable to the “External” Ethernet port on the Guard II.
10. Connect the power cord.
Note: The ASG Guard II supports physical connectivity of networked devices to its internal Ethernet port. The ASG Guard II and S8x00 Media Server integration require VIRTUAL connections only. For more information on connecting networked devices to the Guard II internal Ethernet port(s), refer to Section 6.1.

3.4 Powering Up the ASG Guard II

ASG Guard II utilizes a standard IEC line cord to connect to an AC outlet. After connecting the power cord, press the “power” button located on the rear panel of the device. The “Power” LED located on the front panel lights whenever the Guard II is running. The “Activity” LED may flash briefly and go out while the Guard II initializes. It then flashes regularly during normal operation.

3.5 Automatic Registration Tool (ART)

Access the Automatic Registration Tool (ART) to receive the information required for ASG Guard II configuration (<http://ssdp.dr.avaya.com:7001/art/fwd/ARTstart.cgi?lang=en&country=US>)

You will need the Sold To (FL) for the location the ASG Guard II equipment will be associated with. You will also need the phone number for the maintenance line (“INADS”) connected to the ASG Guard II for remote maintenance purposes.

Use the S8x000, G350, CCS, CVLAN, IP Office, PG230, or ASG Guard link depending on the piece of equipment that you are registering.

** It is critical to use the ART tool to register any IP-connected device such as S8x00 prior to configuring the ASG Guard, in order to get the Product ID number. Product ID (PID) number will be used when setting up the equipment in the ASG Guard II. You must also get the PPP or RAS for S8700 Servers A and B, or the S8500.

3.6 Connecting to the AUX Port

After physical installation is complete and the Guard II has initialized:

1. Connect your laptop to the AUX port (as shown in Figure 3-1) if you have not already done so. Do this with the supplied RJ-45 to DB-9 serial cable.
2. Insert the RJ-45 connector into the AUX port located on the rear of the Guard II and connect the DB-9 end of the cable to the COM port on your computer.
3. Start a terminal application, such as HyperTerminal or ProComm, which will allow you to communicate serially with the Guard II at 9600 baud, 8-N-1.
4. When prompted to connect as the Default User, use the <SPACE BAR> to select “YES.” The appliance prompt eventually displays.
Note: If you answer “NO” when prompted to connect as the default user, you must enter a valid user ID and authentication information.

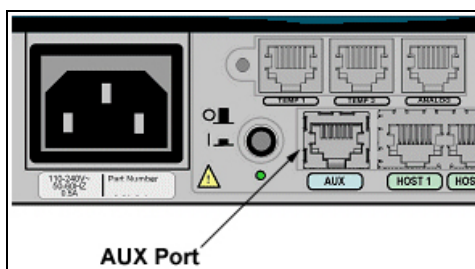


Figure 3-1: AUX Port located on the rear of the ASG Guard II

3.7 Connect a Modem to a Telephone Line

It will be necessary to use the supplied “Y” cable for connection to two analog lines. Plug the single connector end of the “Y” cable into the MODEMS port of the ASG Guard II as shown in Figure 3-2. The two-connector end of the “Y” cable should be plugged into the patch panel.

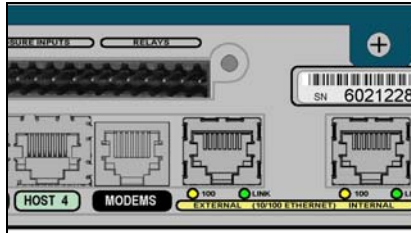


Figure 3-2: Modem Port

3.8 International Modem Setup

Installations in the domestic United States do not require modification to the modem settings. For international installations, you must set the modem to operate using the country codes that correspond to the location in which it is installed.

To configure a modem for international use:

1. Access the Guard II by connecting to the AUX port as described in Section 3.6.
2. At the system prompt type “SM” and the modem number and press <ENTER>. The Set Modem Port Parameters dialog displays.
3. Press <ENTER> to bypass each parameter that you are not modifying.
4. At the “Country” parameter, use the <SPACE BAR> to select the country in which the Guard II is located, or will be installed.
5. Press <ENTER> to bypass the rest of the parameters and accept your changes.
Note: For more information on configuring modem port parameters, refer to the *ASG Guard II Administrator Guide*.

3.9 Host Port Connectivity

Connectivity between the ASG Guard II host ports and other Avaya products (as listed in Section 2.4), is covered in detail in the *ASG Guard II Connectivity Guide*.

3.10 Checking the Software Version – VER Command

```
--- Version Information ---
ASG Guard II v5.2.0 (F/W 5.2.9)
Co-Processor Software Version 5.2.6-4
Flash Version: 5.2.3
Memory (DRAM) Size: 32 MB

Host ports:          4
Modem ports:         2
Telnet ports:        16
Expansion board 1:   Host Port Expansion

Modem 1:             Zoom V92 PC Card
Modem 2:             Zoom V92 PC Card

Site Name:           5010000000
Unit Serial Number: 042H113096

System Date/Time: 11/03/05 11:58:46

11/03/05 11:58:42 F41E {I} [T1:16] Version Information
5010000000>
```

Figure 3-3: Version Information

3.11 Setting the Date and Time

By default, ASG Guard II units are set to Eastern Time. It may be necessary to adjust time settings to match site settings.

To set the date and time:

The Set Date and Time (SDT) command allows you to set the date format to one of ten options and to set the time.

1. At the system prompt type “SDT” and press <ENTER>. The Set Date and Time screen displays as shown in Figure 3-4.

```

5010000000>sdt

--- Set Date and Time ---
Date Format                MM/DD/YY
Current Date              03/22/05
Current Time              16:45
GMT Offset (e.g.'-05:00') -05:00

03/22/05 16:45:51 C880 {I} [T2:120] Set Date and Time
03/22/05 16:46:08 A89C {I} [T2:120] Set Date and Time - O.K.

```

Figure 3-4: Set Date and Time

The default date format is shown in Figure 3-4. By using the <SPACE BAR>, you can change the format to one of ten date formats. All areas within the ASG GUARD II reflect the change in format. For example, if an action item is scheduled to occur (in the default format) on 05/23/05, and you change the format to a four-digit year, the Action Item date will contain a four-digit year.

2. Press the <SPACE BAR> at the Date Format prompt to show the next format. Continue pressing the <SPACE BAR> until the desired format is listed, then press <ENTER>.

The ten formats available in the ASG GUARD II are:

MM/DD/YY	MM-DD-YY
MM/DD/YYYY	MM-DD-YYYY
YYYY/MM/DD	YYYY-MM-DD
YY/MM/DD	YY-MM-DD
DD/MM/YYYY	DD-MM-YYYY

3. After setting the format, enter the current date and press <ENTER>.
4. Enter the current time using the 24-hour (Military) time format and press <ENTER>.
5. Enter the GMT Offset used for setting time zones.
The system responds with a confirmation.

4 ASG Guard II Configuration

This section covers the following topics:

- [Setting Network Parameters](#)
- [Enabling Alarm Delivery](#)
- [Configuring Avaya Device IP Addresses](#)
- [Administering an Avaya IP Device](#)
- [Set Network Services](#)
- [Enabling Telnet on the ASG Guard II](#)
- [Connecting to Avaya IP Devices](#)
- [Saving and Loading Avaya IP Device Information](#)
- [Provisioning the ASG Guard II](#)
- [Modifying the Avaya Platform to Work With the ASG Guard II](#)

4.1 Setting Network Parameters

In this section, you will learn how to manually set the basic network parameters needed to use the ASG Guard II. In some cases, ASG Guardian or PRIISMS management software may administer the Guard II. If this applies to you, refer to Section 6.1 Using the ASG Guard II Configuration Wizard.

As part of the installation process, you should have connected a PC or terminal to the AUX port of the appliance. You can also configure the appliance by connecting to it with a modem or via telnet. For the purpose of these instructions, configuration is performed through the Guard's AUX port.

To set network parameters:

1. At the system prompt type "SNP" (Set Network Parameters) and press <ENTER>. The Set Network Parameters screen displays as shown in Figure 4-1.

```

5010000000>snp

--- Set Network Params ---

1 = Network Initialization Params
2 = SNMP Manager Params
3 = FTP Params
4 = PPP Params
5 = Telnet Params
6 = HTTP Params

Select Group -->1
Restore Factory Defaults ?      No
Internal Address                10.23.55.1
      Mask                      255.255.0.0
      Gateway
External Address                10.21.55.1
      Mask                      255.255.0.0
      Gateway                  10.21.1.1
PPTP Local Address             192.168.1.1
      Remote Addresses          192.168.1.2-50
      Authentication Class      NONE
PPP Address                     192.9.200.3

```

Figure 4-1: Set Network Parameters

2. Select Group #1 “Network Initialization Params” and press <ENTER>.
3. Select NO when prompted to restore factory defaults and press <ENTER>.
4. Press <ENTER> to accept the defaults for *Internal Address*, *Mask*, and *Gateway*. Note that the *Gateway* field is typically blank, and can remain that way.
5. Enter the *External Address*, *Mask*, and *Gateway* you specified in Section 3.1, pressing <ENTER> after each entry. This is the actual LAN address of the Guard II.
6. Use one of the following methods to obtain the address used to establish a PPP session upon dialing into the Guard II.

For New Installations	The PPP address is included within the installation script provided by the ART registration system. The output will look like this: RAS IP address: 10.1.8.199
For Existing Installations	At one of the S8x00 media servers, execute the following command: Less /etc/ppp/ipaddrs The output will look like this: 10.1.1.37:10.1.1.38 Use the first IP address.

- Press <ENTER> through the rest of the parameters in the group.

NOTE: Use Ctrl+X to erase a line and Ctrl+A to abort a command.

4.2 Enabling Alarm Delivery

To enable alarm delivery from the S8x00 devices to Avaya Expert Systems, a “Home Phone Number” parameter must be specified.

Note: Refer to the *ASG Guard II Administrator Guide* for additional information on setting system parameters.

To specify a home phone number:

- At the system prompt type “SSP 3” and press <ENTER>. The Action Routine Parameters dialog displays.
- Enter the phone number for the Avaya Alarm Receiver. Ensure that the telephone number adheres to the proper format. Refer to the table below to determine which phone number to use:

EMEA COE	080012345679
USA	1-800-535-3573

Note: Other international sites should contact their regional Avaya Support Team.

The numbers listed below can be used to verify alarm reception. They are NOT the alarm receiver numbers.

U.S. 1-800-242-2121, prompt 3	Caribbean/Latin America: +786-331-0860
Australia - +612-9352-9151	Canada: +1 800 387-4268
Bahrain - +973-218-266	Moscow: +7-095-363-6780
Budapest +36-1238-8334	France: +33-241-534-000
Hong Kong +852-3121-6423	UK: +44 1483-308-000
Japan +813-5575-8800	Singapore +65-6872-8686

- Press <ENTER> through the remaining parameters to save your settings.

4.3 Configuring Avaya Device IP Addresses

The ASG Guard II contains a special set of commands and action routines that enable you to configure Avaya IP-connected devices like the S8x00 series.

To locate special commands:

1. At the system prompt type "N" and press <ENTER>. A list of "S8x00 Parameters" for the S8x00 displays.

Table 4-1 provides an overview of Avaya special commands.

Table 4-1: Avaya Special Commands	
Command	Description
CONT	Connect to Avaya IP devices via telnet.
CONHOST	Connect to Avaya device.
AAIP	Add an Avaya IP device. Note: Up to 30 IP devices can be added in the table.
XAIP	Delete an Avaya IP device.
SAIP	Change AAIP cmd access.
CAIP	Change an Avaya IP device.
LAIP	List all Avaya IP devices.
AINIT	An action routine that initializes proxy rules. This is part of the Guard II default configuration. No action is necessary.
ADDUMP	Download the table of Avaya IP devices.
ADCONFIG	Load the table of Avaya IP devices.
TRAPTASK	An action routine used to start or stop the SNMP Trap Proxy. It can also be invoked as a command using the following syntax: TRAPTASK START (or TRAPTASK STOP).
AVAYAPPP	Start a PPP session to the ASG Guard II.

4.4 Administering an Avaya IP Device

By default, both CMASTER and AMASTER users can configure the Avaya IP Table. However, a CMASTER user can issue the Block Avaya Administration (BAA) command to restrict an AMASTER user from accessing certain parameters related to the customer's network.

To add an S8x00 Avaya IP device:

1. At the system prompt type "AAIP" and press <ENTER>. The Add Avaya IP Device dialog begins.

2. Type a unique alphanumeric device name and press <ENTER>.
3. Enter the actual IP address of the S8x00. You should have already obtained this information from the customer's network provisioning personnel.
4. Enter the Avaya IP address. You should have already obtained this information from the Expert Systems staff. The Guard II will automatically translate the Avaya IP address into the actual IP address when Expert Systems connect using PPP.
5. Specify the ports that should be forwarded to the Avaya device. Port numbers can be comma or space delimited. By default, the following ports are specified: 23 and 5023 (telnet), 21 (FTP), 80 (HTTP), and 443 (HTTPS/SSL). These ports may need to be removed, as specified by the customer.

Note: After establishing a PPP session, the user may connect directly to Avaya IP devices, *except* on ports 23 and 5023. These ports are treated specially to prevent "telnet hopping." Attempts to telnet directly to these ports will be redirected back to the ASG Guard II login. Once authenticated into the Guard II, use the "CONT" command to connect to the Avaya IP devices.

Tip: Use the Change Avaya IP Device (CAIP) command to modify the parameters set when you added an IP device. Use the Delete Avaya IP Device (XAIP) command to remove the record for a particular IP device. Use the List Avaya IP Device (LAIP) command to list information for all Avaya IP devices that have already been defined.

4.5 Set Network Services

At this point, installation is nearly complete. It is now necessary to verify that the networking functions have been correctly configured in the Guard II.

To set networking services:

1. At the system prompt type "SNS" and press <ENTER>. The Set Networking Services with the default values displays as shown in Figure 4-2.
2. For each of the menu prompts use the <SPACE BAR> to toggle to the desired selection and press <ENTER>. Ensure that the configuration matches Figure 4-2.

```
5010000000>sns

--- Set Networking Services ---
Restore Factory Defaults ?      No

Telnet on Internal Port        Enable
Telnet on External Port        Enable
FTP on Internal Port           Disable
FTP on External Port           Enable
RIP                             Disable
PPTP Server                    Disable
SSH                            Enable
IPSec                          Disable
Ping                           Device and subnet
```

Figure 4-2 Set Networking Services Screen

4.6 Enabling Telnet on the ASG Guard II

Before you can telnet to devices protected by the ASG Guard II, you must first ensure that the telnet capability of the appliance is enabled.

To enable telnet:

1. At the system prompt type "SNP 5" and press <ENTER>. The Telnet Parameters dialog displays
2. At the "Telnet Service Type" prompt, use the <SPACE BAR> to select "Both" from the available options. This enables telnet on the Guard II as both a telnet client and telnet server.
3. Press <ENTER> to save your settings.

4.7 Connecting to an IP Device

To connect to an IP device:

1. At the system prompt type "CONT" and press <ENTER>. A list of IP devices accessible from the Guard II displays.
2. Type the name of the device and press <ENTER>.
3. Type the number of the port, or press <ENTER> to default to port 23 (telnet).

Note: The S8x00 requires users to connect via telnet using port 5023 instead of 23.

Note: If you already know the device name, you may issue the command, "CONT device,port" all on one line. For example, "CONT S8700SRV1,5023." Only ports administered for the device will be accessible; if you omit the port, it will default to 23 (telnet).

Once telnet is invoked, proceed with the login process on the Avaya IP device.

```
5010000000>cont

--- Telnet to Avaya device ---
  Name           Comment
  =====
  s8x00          Active Server

Device name           s8x00
Port (<Enter> for default = 23)  5023

Invoking telnet. Type ^A to exit
```

Figure 4-3: CONT Example

Note: CONT sessions are subject to session buffering, if that option is enabled in the user's profile. The session is also subject to command filter if enabled with the commands Set Host Command Filter

Parameters (SHFP) or Add Host Filter String (AHFS). Refer to the *ASG Guard II Administrator Guide* for more information on these additional commands.

4.8 Saving and Loading Avaya IP Device Information

The DUMPF command enables you to download configuration information from the ASG Guard II to a file, which you can then transfer to a PC. The CONFIG command enables you to load configuration information from a file into the ASG Guard II.

4.8.1 Using the DUMPF Command

To save a list of Avaya IP devices from an ASG Guard II to a file:

1. At the system prompt type "DUMPF" and press <ENTER>. The "Dump Configuration Details to File" dialog begins.
2. When prompted, specify a name for the file and press <ENTER>.
3. To save only the table of Avaya IP devices, press Ctrl+X to clear the line, then type "ROUT" and press <ENTER>. If you wish to save all of the configuration information from the ASG Guard II, press <ENTER> to accept the entire list of areas. The configuration file contents are saved to the file you specified.

Notes:

- The saved file is located in the root directory. At the system prompt, type "DIR" to locate the file. You can then transfer the file to your PC using either XMODEM or FTP. Refer to the *ASG Guard II Administrator Guide* for more information on sending files via XMODEM.
- When transferring the configuration file, ensure that Flow Control is set either to "Software" or "XON/XOFF." Other settings may corrupt the configuration file.
- A special command called **UDUMPF** downloads the user table ONLY. Follow the steps above, using the UDUMPF command to save the contents of the user table to a file. Authentication information contained within the user table is encrypted and therefore secure.

4.8.2 Using the ADCONFIG Command

To load a list of Avaya IP devices from a file into an ASG Guard II:

1. The predefined list of Avaya IP devices must reside in a text file on your PC. Use the "RCV" command to transfer the file from your PC to the ASG Guard II using the XMODEM protocol. Refer to the *ASG Guard II Administrator Guide* for more information on sending files via XMODEM.
2. At the system prompt type "ADCONFIG" and press <ENTER>. The contents of the file are loaded onto the ASG Guard II.
3. Type "LAIP" to list the Avaya IP devices you just loaded onto the Guard II.

4.8.3 Importing a Configuration File to the ASG GUARD II

Once you have transferred a configuration file to the Guard II, you can execute the CONFIG command to import it.

Note: The file must be located within the same directory from which you are executing the CONFIG command. If necessary, verify the location of the configuration file using the DIR command.

To import a configuration file:

1. At the system prompt, type "CONFIG <filename>" and press <ENTER>. The filename must match the name that was used when you transferred the file to the Guard II. The "Upload Configuration Details" banner displays, and commented contents of the configuration file may scroll by as the file is being imported.

Note: It is not necessary to restart the Guard II after a configuration file is loaded.

4.9 Provisioning the ASG Guard II

Once you have physically installed the ASG Guard II and either physically or virtually connected the protected equipment, you must contact the TSO/COE at 1-800-248-1111 to provision the Guard II. Follow the prompts to reach a member of the Account Support Team.

As part of the provisioning process, the TSO/COE will perform such functions as:

- Building the customer's Equipment and Guard II records in proprietary Avaya systems.
- Dialing into the Guard II and installing a standard configuration script.
- Adding a default TSO/COE user table to the Guard II for remote support.
- Setting specific system parameters.

4.10 Modifying the Avaya S8X00 Platform to Work with the ASG Guard II

In some cases you may need to modify particular settings on the protected platform to ensure proper functionality. Use the chart below to determine whether or not the platform you are connecting requires additional modifications.

Product	Modification
S8300	The "SNMP Manager" should be set to the external IP address of the ASG Guard II. (ASG Guard II Proxy Mode)
S8500	
S8700	

TIP: Access to S8x00 can be restricted, allowing only direct access from the ASG Guard II by using the available access list option in S8x00. This requires users to authenticate to the ASG Guard II prior to S8x00 connectivity being achieved, and forces users to proxy connections through the ASG Guard II.

5 Additional Configuration

This section covers the following topics:

- [Adding a CMaster user](#)
-

5.1 Adding a CMaster User

This section provides basic instructions for adding a CMASTER access level user. Refer to the *ASG Guard II Administrator Guide* for additional information on modifying the user database.

Note: A CMASTER user may issue the Block Avaya Administration (BAA) command to restrict Avaya users from administering the customer user table. If this restriction is in effect, you will not be able to add a CMASTER user.

To add a CMASTER user:

1. At the system prompt type "AU" (Add User) and press <ENTER>.
2. When prompted, type the user "name" (or use the one line command AU "name") and press <ENTER>.
3. Use the <SPACE BAR> to select the CMASTER access level. Refer to the *ASG Guard II Administrator Guide* for a definition of the various types of access levels.
4. Press <ENTER> to bypass the Block Access, Sessions Allowed, and User Expiration Date parameters.
5. Use the <SPACE BAR> to select from one of the following Primary Authentication Methods: *ASG Key, Pager, or Password/Callback*.
6. Press <ENTER> to bypass the Secondary Authentication Method, Auto Execute Command, Comments, and Options parameters.
7. When prompted, enter the additional information required for the authentication method you chose. Press <ENTER> after each entry until complete. A log will display above the prompt indicating that the user was added successfully. Your screen should look similar to Figure 5-1.

Note: When adding a customer user, remember to advise the user of his/her user ID and authentication information.

```
Ser#2090114746>au
--- Add User ---
User Name                Guard-CMaster
Access Class             CMaster
Block Access             No
Sessions Allowed (blank=unlimited)
User Expiration Date     MM/DD/YY
Primary Authentication Method ASG Key
Secondary Authentication Method None
Auto Execute Command
Comments:
Options:

-- ASGKey Details --
Encryption Key Source    Randomly Generated
Enter These Digits as Key1 or Key2: 6576 4334 = 3520 4215 = 4040 =
Test Challenge: 1234567 ...Reply: 421-7876

Press <ENTER> to Continue
06/04/03 10:32:14 4B33 [T1] User: GUARD-CMASTER Added - O.K.
Ser#2090114746>
```

Figure 5-1: Add User Example

6 Additional Information

This section covers the following topics:

- [Using the ASG Guard II Configuration Wizard](#)
- [How Automated Alarm Delivery Works](#)
- [Aux and Host Port Pinouts](#)
- [Standard Serial cables](#)

6.1 Using the ASG Guard II Configuration Wizard

The ASG Guard II provides a Configuration Wizard that enables you to quickly configure the appliance's network settings. For the purposes of configuring ASG Guard II network parameters for use with ASG Guardian software, you can select the "Secure Proxy" or "Secure Gateway" configuration option.

Note: Throughout these instructions and the prompts on the appliance, PRIISMS is synonymous with ASG Guardian.

6.1.1 Configuring the ASG Guard II for Secure Proxy

The Secure Proxy connection is where the ASG Guard II and the S8x00 switches reside on the corporate network. To restrict a user's direct access into the S8x00, the access list option on the S8x00 can be turned ON.

1. At the system prompt type "WIZARD" and press <ENTER>. The Initial Setup Wizard displays.
2. Press the <SPACE BAR> to select "Secure Proxy," and press <ENTER>. The Wizard prompts you for the external IP address (*IP Address*), network mask (*Mask*) and *Default Gateway* as shown in Figure 6-1.

IP Address	10.50.20.20
Mask	255.255.0.0
Default Gateway	10.50.1.1
PPP Address	192.9.200.3

Figure 6-1: Secure Proxy

3. Enter the addresses you noted in Section 3.1, pressing <ENTER> after each entry.
4. Next, you are prompted whether or not to accept the default PRIISMS IPsec key. If you select NO you will be prompted to select an authorization type and enter the corresponding key. If you want to specify your own PRIISMS IPsec key, you must select the "Secret" authorization type, and then enter the secret key.
5. Select YES when asked to use the default PRIISMS IPsec Key. If you answer NO you must ensure that PRIISMS is configured with the same Secret Key you created for the ASG Guard II.

6. Select YES to add a default PRIISMS user. If you select NO, then you must ensure that PRIISMS has a user to authenticate into the ASG Guard II.
7. Specify the date and time format, pressing <ENTER> after each entry.
8. After the last date entry option, you will be informed that the new settings will be applied. If you are ready to proceed, answer "YES" when prompted. A "Configuration Successful" prompt displays when the process is complete.

```

08/23/2005 12:19:49 69AB {I} [T1:8] Initial setup Wizard
5010000000>wizard

--- Initial setup Wizard ---

Initial setup Wizard

The Setup Wizard will guide you through the
configuration process. Select a mode of operation to determine
the parameters that will be set.

1. Secure Proxy - The device is used as a secure proxy to local devices.

2. Secure Gateway- The device allows network traffic to local devices
on the internal subnet through a tunnel only.

3. Custom - Advanced configuration:
All features can be customized; internal and external
interface parameters can be set independently.

Select mode of operation          Secure Proxy
IP Address                       10.22.99.3
Mask                             255.255.0.0
Default Gateway                  10.22.1.1
PPP Address                      192.9.200.3

Up to three units can be cascaded at the following IP addresses:

                                192.168.0.3
                                192.168.0.4
                                192.168.0.5

Telnet to this unit will be available only through IPsec.
Set encryption parameters for the default IPsec tunnel:

Use default PRIISMS IPsec key?   Yes
Add default user for PRIISMS?    Yes

```

```

Date Format                MM/DD/YYYY
Current Date              08/23/2005
Current Time              12:32
GMT Offset (e.g.'-05:00') -05:00

The new networking settings will be applied.
You might have to reconnect.

Proceed?                  Yes
Applying new settings...
Creating IPsec tunnel 'default_tunnel'
Notifying PRIISMS servers
Deleting PRIISMS IPsec tunnels
Setting up default user...
Setting IP addresses...
Reconfiguring commands...
Restarting Co-Processor ...
... it will take several minutes for the Co-Processor to restart

08/23/2005 12:31:01 ACA3 {I} [T1:8] Initial setup Wizard
08/23/2005 12:32:38 CDE9 {I} [T1:8] User: ADMIN Added - O.K.
08/23/2005 12:32:44 F503 {I} [T1:8] Wizard - OK, restarting Co-Processor
5010000000>

```

Figure 6-2: Setup Wizard

TIP: Access to S8x00 can be restricted to only the ASG Guard II by using the available access list option in S8x00. This requires users to authenticate to the ASG Guard II for s8x00 connectivity.

6.1.2 Configuring the ASG Guard II for Secure Gateway

The Secure Gateway mode is where the ASG Guard II sits on the corporate network and the S8x00 switch is connected to internal port of the ASG Guard II. The S8x00 is segregated from the corporate network for security. To access the S8x00 switch the customer users have to authenticate into ASG Guard II.

1. At the system prompt type "WIZARD" and press <ENTER>. The Initial Setup Wizard displays.
2. Press the <SPACE BAR> to select "Secure Gateway," and press <ENTER>. The Wizard prompts you for the external IP address (*IP Address*), network mask (*Mask*) and *Default Gateway* as shown in Figure 6-3.

Internal Address	192.168.0.1
Mask	255.255.255.0
Gateway	
External Address	10.50.20.20
Mask	255.255.0.0
Gateway	10.50.1.1
PPP Address	192.9.200.3

Figure 6-3: Secure Gateway

3. The Internal address allows you to create a protected network behind the ASG Guard II. Specify an appropriate IP address for the Guard II on the protected network, or accept the default. Note that the Gateway field is typically blank, and can remain that way.
4. Enter the information for the External network that you noted in Section 3.1, pressing <ENTER> after each entry.
5. Next, you are prompted whether or not to accept the default PRIISMS IPsec key. If you select NO, you will be prompted to select an authorization type and enter the corresponding key. If you want to specify your own PRIISMS IPsec key, you must select the "Secret" authorization type, and then enter the secret key.
6. Select YES when asked to use the default PRIISMS IPsec Key. If you answer NO you must ensure that PRIISMS is configured with the same secret key you created for the ASG Guard II.
7. Enter the PRIISMS IP address as the Home IP Address. This is generally used for alarming purposes.
8. Select YES to add a default PRIISMS user. If you select NO, then you must ensure that PRIISMS has a user to authenticate into the ASG Guard II.
9. Specify the date and time format, pressing <ENTER> after each entry.
10. After the last date entry option, you will be informed that the new settings will be applied. If you are ready to proceed, answer "YES" when prompted. A "Configuration Successful" prompt displays when the process is complete.

6.2 How Automated Alarm Delivery Works

The ASG Guard II is pre-configured with action items that automate the delivery of SNMP alarms generated by the S8x00 media server to Avaya Expert Systems. Action Items utilize specific Action Routines to respond to events that are triggered on the ASG Guard II.

The S8x00 Media Server generates SNMP traps that contain alarms and sends them to the ASG Guard II. The Guard IIs trap proxy receives the alarms and stores the IP address, timestamp, and alarm message in a file and generates the event #SENDALL <filename>.

The PHONTRAP action routine runs when this event is generated and delivers the alarm to Expert Systems.

Upon receipt of the alarm, Expert Systems sends a delivery acknowledgment to the Guard II, which generates an .ACKTRAP <filename> event.

The XMLACK action routine runs when this event is generated, which sends a delivery confirmation to the S8x00 Media Server.

If delivery confirmation is not received from Expert Systems, a .NACKTRAP event is generated. In both cases, these events are logged on the Guard II.

To view the list of predefined action routines on the Guard II:

1. At the system prompt type "LA" and press <ENTER>. The List Action Items screen displays as shown in Figure 6-4.

```

5010000000>la
--- List Action Items ---
  Alarm:           Routine: Parameters:
                   Severity: Comments:

1) #SENDALL       PHONTRAP
                   Info
2) #SENDERR       LOG
                   E
3) .ACKTRAP       XMLACK
                   Info
4) .COPROC.INITOK DOLIST
                   Info
5) .COPROC.INITOK.1 AINIT
                   Info      Initialize rules for Avaya
6) .COPROC.INITOK.2 TRAPTASK START
                   Info      Start trap capture

-- End of List --

06/30/03 16:16:29 57B9 {I} [T1:26] List Action Items
5010000000>

```

Figure 6-4: List Action Item Example

6.2.1 AINIT – Initialize Rules for Avaya Devices

The AINIT action routine initializes the IP rules for all defined Avaya IP devices. This includes rules for forwarding IP ports, redirecting telnet ports to the ASG Guard II, and forwarding SNMP traps for dialup delivery to Avaya Expert Systems.

Note: Both the AINIT and TRAPTASK action routine (discussed in Section 6.2.2) should run when the .COPROC.INITOK event is generated.

To generate the .COPROC.INITOK event:

1. At the system prompt type "AA" and press <ENTER>. The Add Action Item screen displays.
2. Specify the event .COPROC.INITOK.1 in the "Alarm" parameter and press <ENTER>.
3. Type "DOLIST" in the Action Routine parameter and press <ENTER>.
4. Leave the "Routine Parameters" field blank.

5. Enter comments if desired and press <ENTER>.
6. Use the <SPACE BAR> to select Info for the “Severity” parameter. Refer to Figure 6-5.

```
ASG_GuardII>aa
--- Add Action Item ---

Alarm                .COPROC.INITOK
Action Routine       DOLIST
Routine Parameters
Comment
Severity             Info
```

Figure 6-5: DOLIST Action Item

To create an action item that utilizes the AINIT action routine:

1. At the system prompt type “AA” and press <ENTER>. The Add Action Item screen displays.
2. Specify the event .COPROC.INITOK.1 in the “Alarm” parameter and press <ENTER>.
3. Type “AINIT” in the Action Routine parameter and press <ENTER>.
4. Leave the “Routine Parameters” field blank.
5. Enter comments if desired.
6. Use the <SPACE BAR> to select Info for the “Severity” parameter. Refer to Figure 6-6.

```
ASG_GuardII>aa
--- Add Action Item ---

Alarm                .COPROC.INITOK.1
Action Routine       AINIT
Routine Parameters
Comment              Initialize IP Rules
Severity             Info
```

Figure 6-6: AINIT Action Item

6.2.2 TRAPTASK - Start/Stop SNMP Trap Proxy

The TRAPTASK action routine is used to start or stop the SNMP Trap Proxy. SNMP traps are generated by the S8x00 Media Server, received by the ASG Guard II, and written to a file. Like the AINIT action routine discussed in Section 6.2.1, TRAPTASK should be scheduled to run on the .COPROC.INITOK event.

To create an action item that utilizes the TRAPTASK action routine:

1. At the system prompt type "AA" and press <ENTER>. The Add Action Item screen displays.
2. Specify the event .COPROC.INITOK.2 in the "Alarm" parameter and press <ENTER>.
3. Type "TRAPTASK" in the Action Routine parameter and press <ENTER>.
4. Type "Start" in the "Routine Parameters" field.
5. Enter comments if desired. Refer to Figure 6-7.

```
ASG_GuardII>aa
--- Add Action Item ---

Alarm                .COPROC.INITOK.2
Action Routine       TRAPTASK
Routine Parameters   START
Comment Start/stop SNMP Trap Proxy
Severity             Info
```

Figure 6-7: TRAPTASK Action Item

Note: This action item can also be invoked as a command by using the following syntax: TRAPTASK START (or STOP).

6.2.3 PHONTRAP – Deliver S8x00 Alarms

The PHONTRAP action routine dials the Avaya Expert Systems server and delivers the S8x00 alarm with the message specified in the filename field. The Avaya Expert Systems phone number is specified using the Set System Parameter (SSP) command. (See Section 4.2 of this document, "Enabling Alarm Delivery.") An .ACKTRAP <filename> event is generated upon successful alarm delivery, and a .NACKTRAP <filename> event is generated if alarm delivery has failed. When scheduling an action item that utilizes the PHONTRAP action routine, specify the event #SENDALL and select "Info" for the Severity parameter. Refer to Figure 6-8.

```
ASG_GuardII>aa
--- Add Action Item ---

Alarm                #SENDALL
Action Routine       PHONTRAP
Routine Parameters
Comment
Severity             Info
```

Figure 6-8:PHONTRAP Action Item

6.2.4 XMLACK – Sends Alarm Delivery Confirmation

Upon successful delivery of an alarm to Avaya Expert Systems, an .ACKTRAP event and a response SNMP trap are generated. The XMLACK action routine runs when the .ACKTRAP event is generated, and delivers the SNMP trap back to the S8x00, confirming successful alarm delivery. Refer to Figure 6-9.

```
ASG_GuardII>aa
--- Add Action Item ---

Alarm                .ACKTRAP
Action Routine       XMLACK
Routine Parameters
Comment
Severity             Info
```

Figure 6-9: XMLACK Action Item

6.3 Aux and Host Port Pinouts

The serial ports (AUX and Host) on the ASG Guards are all RS232 DCE.

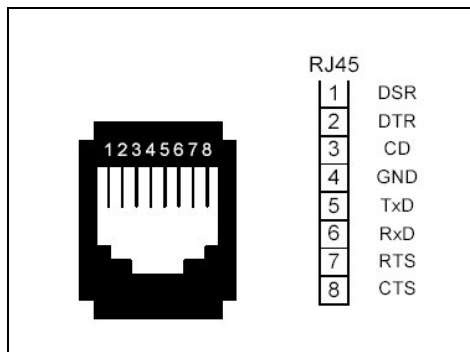


Figure 6-10: RJ45 Interface Pinout

6.4 Standard Serial cables

RJ45 Host to DB9		
RJ45	DCE Signal	DB9
1	DSR	6
2	DTR	4
3	CD	1
4	GND	5
5	TxD	3
6	RxD	2
7	RTS	7
8	CTS	8

RJ45 Host to DB25 (Straight)		
RJ45	DCE Signal	DB25
1	DSR	6
2	DTR	20
3	CD	8
4	GND	7
5	TxD	2
6	RxD	3
7	RTS	4
8	CTS	5

RJ45 Host to DB25 (Null)		
RJ45	DCE Signal	DB25
1	DSR	
2	DTR	8
3	CD	20
4	GND	7
5	TxD	3
6	RxD	2
7	RTS	5
8	CTS	4

DB9 Host to DB9		
DB9	DCE Signal	DB9
1	CD	1
2	RxD	2
3	TxD	3
4	DTR	4
5	GND	5
6	DSR	6
7	RTS	7
8	CTS	8
9	RI	9

DB9 Host to DB25 (Short)		
DB9	DCE Signal	DB25
1	CD	8
2	RxD	3
3	TxD	2
4	DTR	20
5	GND	7
6	DSR	6
7	RTS	4
8	CTS	5
9	RI	22