Welcome to

Avaya™ S8300 Media Server and Avaya™ G700 Media Gateway

555-234-200
Issue 1
May 2002

For best results, we recommend you download the latest **FREE** version of Acrobat 5.0 Reader® either from the Adobe website (http://www.adobe.com/products/acrobat/readstep2.html)

OR

Click on the icon below for a FREE copy and follow the installation instructions.

Get Acrobat Reader

Notice

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

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. The scope of your responsibilities is based upon 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
- Your Avaya-provided software applications, and their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products.

Preventing Toll Fraud

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

Avaya Fraud Intervention and how to get help

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, in the United States and Canada, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353. For additional support telephone numbers, see the Avaya website:

http://www.avaya.com

Click on Support, click on Escalation Lists US and International. This web site includes phone numbers for escalation within the United States. For escalation phone numbers outside the United States, click on Global Escalation List. This list contains the phone numbers for the Centers of Excellence in each Avaya-defined region.

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 is not 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 intrusions associated with your system and/or its networked equipment. Also realize than, 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).

Voice over Internet Protocol (VoIP)

If the equipment supports Voice over Internet Protocol (VoIP) facilities, you may experience certain compromises in performance, reliability and security, even when the equipment performs as warranted. These compromises may become more acute if you fail to follow Avaya's recommendations for configuration, operation and use of the equipment. YOU ACKNOWLEDGE THAT YOU ARE AWARE OF THESE RISKS AND THAT YOU HAVE DETERMINED THEY ARE ACCEPTABLE FOR YOUR APPLICATION OF THE EQUIPMENT. YOU ALSO ACKNOWLEDGE THAT, UNLESS EXPRESSLY PROVIDED IN ANOTHER AGREEMENT, YOU ARE SOLELY RESPONSIBLE FOR (1) ENSURING THAT YOUR NETWORKS AND SYSTEMS ARE ADEQUATELY SECURED AGAINST UNAUTHORIZED INTRUSION AND (2) BACKING UP YOUR DATA AND FILES.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the FCC Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.
The equipment described in this manual complies with standards of the following organizations and laws, as applicable:

- Australian Communications Agency (ACA)
- American National Standards Institute (ANSI)
- Canadian Standards Association (CSA)
- Committee for European Electrotechnical Standardization (EENELEC) - European Norms (EN's)
- Digital Private Network Signaling System (DPNSS)
- European computer Manufactures Association (ECMA)
- European Telecommunications Standards Institute (ETSI)
- FCC Rules Parts 15 and 68
- International Electrotechnical Commission (IEC)
- International Special Committee on Radio Interference (CISPR)
- International Telecommunications Union Telephony (ITU-T)
- ISDN PBX Network Specification (IPNS)
- National ISDN-1
- National ISDN-2
- Underwriters Laboratories (UL)

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international IMC standards and all relevant national deviations:
Limits and Methods of Measurement of Radio Interference of Information Technology Equipment, CISPR 22:1997 and EN55022:1998.
Information Technology Equipment - Immunity Characteristics - Limits and Methods of Measurement, CISPR 24:1997 and EN55024:1998, including:

- Electrostatic Discharge (ESD) IEC 61000-4-2
- Radiated Immunity IEC 61000-4-3
- Electrical Fast Transient IEC 61000-4-4
- Lightning Effects IEC 61000-4-5
- Conducted Immunity IEC 61000-4-6
- Mains Frequency Magnetic Field IEC 61000-4-8
- Voltage Dips and Variations IEC 61000-4-11
- Powerline Harmonics IEC 61000-3-2
- Voltage Fluctuations and Flicker IEC 61000-3-3

Ordering Information

Call: US Voice: 1 800 457 1235
US Fax: 1 800 457 1764
non-US Voice: +1 410 568 3680
non-US Fax: +1 410 891 0207

Write: Globalware Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA

Order: 555-234-200, Issue 1
May, 2002

Canadian Department of Communications (DOC)

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Industry Canada (IC) Interference Information

NOTICE: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indication that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

European Union Declaration of Conformity

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformité Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC, Class B) and Low Voltage Directive (73/23/EEC). This equipment has been tested to meet the CTR4 Primary Rate Interface (PRI) specification.
Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site:
http://support.avaya.com/elmodocs2/DoC/IDoC/index.jhtml/

Japan

This is a Class B product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Federal Communications Commission Statement

Part 15:
Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. 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. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Part 68: Answer-Supervision Signaling

Allowing this equipment to be operated in a manner that does not provide proper answer-supervision signaling is in violation of Part 68 rules. This equipment returns answer-supervision signals to the public switched network when:

- answered by the called station,
- answered by the attendant, or
- routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user.
- This equipment returns answer-supervision signals on all direct inward dialed (DID) calls forwarded back to the public switched telephone network. Permissible exceptions are:
- A call is unanswered.
- A busy tone is received.
- A reorder tone is received.

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.
This equipment complies with Part 68 of the FCC Rules. On the rear of this equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.
The REN is used to determine the quantity of devices which may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0. To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. REN is not required for some types of analog or digital facilities.

Means of Connection

Connection of this equipment to the telephone network is shown in the following table.

Manufacturer's Port Identifier	FIC Code	SOC/REN/ A.S. Code	Network Jacks
Ground start CO trunk	02GS2	0.5A	RJ11C
Loop start CO trunk	02LS2	0.5A	RJ11C
DID CO trunk	02RV2-T	AS.2	RJ11C
1.544 Mbit digital interface	04DU9-BN 04DU9-DN 04DU9-IKN 04DU9-ISN	6.0Y 6.0Y 6.0Y 6.0Y	RJ48C RJ48C RJ48C RJ48C
Primary Rate Interface	04DU9-ISN(PRI)	6.0Y	RJ48C
Basic Rate Interface	02IS5	6.0F	RJ49C

If the terminal equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.
The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.
If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242-2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved. It is recommended that repairs be performed by Avaya certified technicians.
The equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.
This equipment, if it uses a telephone receiver, is hearing aid compatible.

Contents

About this Book 1

Purpose . . . 1
Intended Audience . . . 1
Security Issues . . . 1
Safety Notices . . . 2
Admonishments . . . 2
Power Requirements . . . 2
Electrical Hazards . . . 2
Grounding . . . 3
LASER Product . . . 3
Rack-Mounting . . . 4
Technical Specifications . . . 4
Trademarks and Service Marks . . . 5
Where to Call for Technical Support . . . 6
How to View Documentation Online . . . 7
How to Order Documentation . . . 7
How to Comment on Documentation . . . 7

Overview 9

Introduction . . . 9
How to View Documentation Online . . . 9
Product Summary . . . 9
Feature Summary . . . 10
Applications Summary . . . 11

Access Procedures 13

Introduction . . . 13
Administration Tool and Access Summary . . . 13
S8300 and G700 interface and task summary . . . 15
General access guidelines . . . 16
Specific Access Procedures . . . 16
Accessing the G700 processors using a serial connection . . . 17
Hardware and software requirements . . . 17
Serial connection login procedure . . . 17
Media Gateway Processor (MGP) session . . . 18
Accessing a CLI using telnet . . . 18
Accessing the S8300 Media Server Web Interface and P330 Device Manager using an Ethernet interface . . . 20

Hardware and software requirements 20
S8300 Media Server login procedure. 20
P330 Device Manager login procedure 22
Accessing the S8300 Media Server using a dial-up connection. 22
Using a dial-up networking connection. 23
Setting up dial-up networking on Windows systems 23
Accessing Avaya MultiVantage software 25
Accessing Avaya Site Administration. 26
Accessing SAT from a CLI 26
Physical Connections to Media Gateways 27
Connecting directly to the G700 serial port. 27
Connecting a modem to a USB port 28
Connecting to an Ethernet interface 28
Corporate LAN remote access. 28
Corporate LAN direct connection 29
S8300 Services interface direct connection 29
Setting up a laptop for an S8300 Media Server direct Ethernet connection 30
General settings 30
Set TCP/IP properties on Windows systems 31
Disable proxies in browser 33

Supporting Library **35**

Introduction 35
MultiVantage Solutions Hardware Guide 35
S8300 and G700 Reference Library 35

About this Book

Purpose

This document introduces the Avaya™ S8300 Media Server and Avaya™ G700 Media Gateway IP-communications solution. It covers:

- An overview of this product including a product, feature, and application summary
- A guide to specific tools used to configure, administer, and maintain this product
- A guide to the document set that supports the S8300 Media Server and G700 Media Gateway

Intended Audience

The information in this document is intended to support all S8300 Media Server and G700 Media Gateway users, including Avaya technicians, provisioning specialists, business partners, and customers.

Security Issues

To ensure the greatest security possible for customers, Avaya offers features such as toll-fraud protection and media encryption to reduce security-related liabilities. Contact your Avaya representative for more information.

Safety Notices

Admonishments

Admonishments used in the documentation for this product have the following meanings:

CAUTION:
Indicates the presence of a hazard that will or can cause minor personal injury or property damage if the hazard is not avoided.

WARNING:
Indicates the presence of a hazard that can cause death or severe personal injury if the hazard is not avoided.

DANGER:
Indicates the presence of a hazard which will cause death or severe personal injury if the hazard is not avoided.

SECURITY ALERT:
This sign is used to draw attention to possible toll-fraud issues.

Power Requirements

The G700 Media Gateway uses an auto-ranging 100-240 VAC power supply, 50 to 60 Hz, 5 A maximum at 100-120 VAC and 2 A maximum at 200-240 VAC. The AC power source is to be single phase, 3-conductor (Line, Neutral and Ground) with a 15 A circuit breaker for 100-120 VAC or a 10 A circuit breaker for 200-240 VAC.

WARNING:
Do not overload the power circuit.

Electrical Hazards

WARNING:
To prevent access to electrical hazards by unauthorized personnel and to ensure continued compliance to international radiated emissions requirements, all captive screws must be securely tightened such that they cannot be loosened without the use of a tool.

WARNING:
The Avaya G700 Media Gateway must not be operated with any slots open. Empty slots should be covered with the supplied blank plates.

Grounding

CAUTION:
System grounding must comply with the general rules for grounding provided in Article 250 of the National Electrical Code (NEC), National Fire Protection Agency (NFPA) 70, or the applicable electrical code in the country of installation.

WARNING:
If the installation location is greater than 50 feet (15 m) from an approved ground, do not install the Avaya G700 Media Gateway until a licensed electrician is present to install a Supplementary Ground Conductor.

WARNING:
Failure to install both grounds will void the Product Safety certifications (UL and the CE Mark) on the product and create a hazard that could result in death or severe personal injury.

LASER Product

The equipment described in the documentation for this product may contain Class 1 LASER Device(s). The LASER devices operate within the following parameters:

- Power output –9.5 dBm to -4 dBm
- Wavelength 1285 nm to 1343 nm

CLASS 1 LASER PRODUCT EN 60825-1:1994 + A11, EN60825-2:194, EN60950:1992 + A1 + A2 + A3.

Laser components used in the G700 are Class 1 Laser Products that comply with 21CFR 1040.10 and CFR 1040.11.

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure. Contact your Avaya representative for more laser product information.

Luokan 1 Laserlatte

Klass 1 Laser Apparat

Rack-Mounting

WARNING:
Warning: if the rack is not securely fixed in place, do not proceed with the installation.

WARNING:
Balancing the G700 Media Gateway requires two people. Use caution to avoid injury.

Technical Specifications

WARNING:
If the G700 Media Gateway is being mounted in a rack with other equipment already installed, the G700 Media Gateway must be positioned to avoid imbalance.

Table 1. Technical Specifications

Chassis Dimensions					
Height	2U (3.5 in)	88 mm	Depth	17.7 in	450 mm
Width	19 in	482.6 mm	Weight empty	22.25 lbs	10 kg
			Weight	34-27 lbs	16-12 kg
Required Clearances					
Front	12 in	30 cm	consistent with EIA 464 data rack standards		
Rear	18 in	45 cm			
Temperature Tolerances					
Recommended		65 to 85 deg Farenheit		18 to 29 deg Celsius	

WARNING:
Installation in a Restricted Access Location is required in Finland and Norway.

Trademarks and Service Marks

This document contains references to the following Avaya trademarked products:

- Avaya™ G700 Media Gateway
- Avaya™ S8300 Media Server and Avaya™ S8700 Media Server
- AUDIX®
- Cajun™ and CajunView™
- DEFINITY® and DEFINITY One™
- INTUITY™
- MultiVantage™
- Softconsole
- VisAbility™

The following are trademarked by their appropriate vendor:

- Adobe® and Adobe Acrobat® are registered trademarks of Adobe Systems Incorporated.
- Internet Explorer™ is a trademark of Microsoft® Corporation.
- Linux® is a registered trademark of Linus Torvalds.
- Microsoft® is a registered trademark of Microsoft Corporation.
- Netscape® is a registered trademark of Netscape Communications Corporation.
- Windows 95™, 98™, NT™, Millennium Edition™, and Windows 2000™ are trademarks, and Windows® is a registered trademark, of Microsoft® Corporation.
- Windows HyperTerminal™ is a trademark of Microsoft® Corporation.

Where to Call for Technical Support

If you need additional help, the following resources are available. You may need to purchase an extended service agreement to use some of these resources. See your Avaya representative for more information.

DEFINITY Helpline (for help with feature administration and system applications)	+1-800-225-7585
Avaya National Customer Care Center Support Line (for help with maintenance and repair)	+1-800-242-2121
Avaya Toll Fraud Intervention	+1-800-643-2353
Avaya Corporate Security	+1-800-822-9009 +1-925-224-3401
Avaya Centers of Excellence	
North America	1-800-248-1111
Central/Latin America, Caribbean (for dealers only)	Contact your local representative
Bahrain	+973-218-266
Budapest	+36-1238-8334
Moscow	+7095-363-6701
Saumur	+33-241-534-000
UK	+44-1483-308-000
Australia	+612-9352-9151
Hong Kong	+852-3121-6423
Japan	+813-5575-8800
Shanghai	+8621-5459-4590
Singapore	+65-872-8686
Canada	1-800-387-4268

How to View Documentation Online

You can view this document and other documentation on the Avaya website at:
http://www.avaya.com/support

This website may contain product information and documentation updates not covered in this document.

How to Order Documentation

You can order documentation from the Avaya Publications Center by calling or writing:

Call:	US Voice:	800 457 1235
	US FAX:	800 457 1764
	non-US Voice:	+1 410 568 3680
	non-US FAX:	+1 410 891 0207
Write:	Globalware Solutions	
	200 Ward Hill Avenue	
	Haverhill, MA 01835	

How to Comment on Documentation

Avaya welcomes your feedback on our documentation.

You can email comments to *document@avaya.com* or you can fax comments to 1-303-538-1741 or to your Avaya representative. Please mention name and number of the document.

Overview

Introduction

This document introduces the Avaya™ S8300 Media Server and Avaya™ G700 Media Gateway IP-communications solution. This section covers an overview of this product including:

- How to View Documentation Online
- Product Summary
- Feature Summary
- Applications Summary

How to View Documentation Online

You can view the most recent S8300 Media Server and G700 Media Gateway documentation and other product documentation on the Avaya website http://www.avaya.com/support

Product Summary

The S8300 Media Server and G700 Media Gateway solution seamlessly delivers a business's voice, fax, and messaging capabilities over an IP network. This unique solution converges the power of the Avaya MultiVantage™ Software feature set with the power of distributed switching from the Avaya™ P330 Stackable Switching System.

An S8300 Media Server and G700 Media Gateway solution is comprised of several elements:

- A G700 Media Gateway is always required. It can host an S8300 Media Server or various other media modules depending on the telephony needs at a particular location. Key components include the Avaya™ P330 stack processor, Media Gateway Processor (MGP), and Voice over IP (VoIP) engine on the MGP board.
- The S8300 Media Server is a special type of media module. If present, it supports the MultiVantage software that provides call-processing capabilities for the system. The S8300 can be configured as the primary call controller or as a Local Survivable Processor (LSP) standby server for an S8700 Media Server or for another S8300 Media Server in the configuration.

- Avaya MultiVantage™ Software provides the Avaya Call Processing (telephony) features. It resides on the S8300 Media Server, or on a remote S8700 Media Server if the G700 media gateway does not contain an S8300 media module.

Each of these components must be correctly configured in order to bring a new system into service. The different components also need ongoing administration and maintenance in order to upgrade or expand the system, or diagnose problems The methods and tools used to access each of these components are covered in Administration Tool and Access Summary.

Feature Summary

The S8300 Media Server and G700 Media Gateway solution will evolve over time. Table 2 summarizes key features that are available in the May 2002 release of this product, and the additional features that are expected in the next release.

Table 2. May 2002 Release and Next Release Feature Comparison

May 2002 Release features	Next Release Features
One G700 media gateway with an S8300 media server can support up to 100 stations and 100 trunks, and must be installed at a single location	Up to 5 G700 media gateways with an S8300 media server can support up to a total of 250 stations and 250 trunks, and must be installed at a single location
Up to 5 G700 media gateways can be controlled by an S8700 External Media Server (EMS), if the S8700 is a multi-connect configuration	Up to 30 G700 media gateways can be controlled by an S8700 External Media Server (EMS), and the S8700 can be an IP-connect or a multi-connect configuration
One S8300 media server can operate as a Local Survivable Processor (LSP) standby call controller for an S8700 media server for multi-connect configuration (one LSP for each gateway that requires survivability)	One S8300 media server can operate as a Local Survivable Processor (LSP) standby call controller for an S8700 media server for either IP-connect or multi-connect configurations (one LSP for up to 5 gateways that require survivability)
Messaging is available through an externally connected or networked Messaging system	Messaging is available through an externally connected or networked Messaging system and optionally provided by an embedded Intuity AUDIX LX Messaging Application that may interact with other Intuity AUDIX Messaging systems (the embedded messaging application currently is *not* documented in the S8300/G700 document set)
Support for analog stations and trunks in the USA	Support for analog stations and trunks internationally
Simple Network Management Protocol (SNMP) agent on the G700	Simple Network Management Protocol (SNMP) agent on the G700 and S8300/S8700 call controllers

Applications Summary

The following programs support effective use of the S8300 Media Server and G700 Media Gateway:

- Avaya MultiService (formerly CajunView™) Network Manager: This optional product is a complete Network Management System (NMS) and is part of the VisAbility™ Management Suite. Services include:
  - viewing all network devices by type, subnet, or customized groupings
  - logging and viewing SNMP traps and events
  - launching and managing other applications including ASA
- Avaya VisAbility™ Management Suite: This set of software tools contains applications to manage a converged voice and data network including network management, fault and performance management, configuration management, directory management and policy management. Contact your Avaya representative for details about this extensive support system.
- Avaya Site Administration (ASA): used for telephony administration. ASA must be run on a compatible Microsoft Windows operating system. Versions currently supported include Windows 95, 98, NT 4.0, Millennium Edition, and Windows 2000. Typically one licensed copy is made available for every S8300 Media Server installation.
- Device Manager: also known as the P330 Embedded Web Manager, provides a browser-based graphical user interface (GUI) to assist with ongoing media gateway and P330 stack device administration. See the ***Avaya™ P330 Manager User Guide*** for complete information.
- File Transfer Protocol (FTP) program: used for uploading or downloading data files, announcements, license files, or software. Either a command-line interface version such as Trivial FTP (TFTP) may be used through a telnet connection, or an FTP graphical user interface (GUI) application may be used if available. Files *must* be transferred in binary mode. Refer to relevant published documentation for details on using these programs.
- NetSwitcher program: Avaya Services technicians use this internally available program to configure different network profiles so they can easily connect to a number of different systems. See General settings for details.
- Serial connection program: used to configure IP addresses for new G700 Media Gateway processors. Typically the Microsoft Windows® HyperTerminal program is used.
- System Access Terminal (SAT) program: uses a Command Line Interface (CLI) interface to administer telephony features. SAT is available through a telnet session or the ASA package.
- Telecommunications network (telnet) program: provides a command-line interface (CLI) for running server platform commands and applications such as FTP or TFTP and SAT. Refer to relevant published documentation for details on using a particular telnet program.
- Secure shell interface: A secure shell (SSH) remote interface utility can be used as an alternative to telnet. SSH commands and passwords are encrypted, and both ends of the client/server connection are authenticated through a digital certificate. The SSH suite includes a secure copy (SCP) program that can be used as an alternative to FTP. The SSH and SCP utilities provide greater security than FTP and telnet and should be used if available.

- VoIP Monitoring Manager: used to monitor network quality of service for Avaya IP endpoints using a graphical user interface. Currently it runs only on Windows 2000 systems. The VoIP Monitoring Manager program may be downloadable from some S8300 Media Servers. It is available as part of the Avaya VisAbility Management Suite.

Access Procedures

Introduction

This section is intended to be a guide to the various tools that are used to configure, administer, and maintain an S8300 Media Server or G700 Media Gateway. It covers:

- Administration Tool and Access Summary
- Specific Access Procedures
- Physical Connections to Media Gateways

Administration Tool and Access Summary

A variety of tools are used to access the different elements of the S8300 Media Server and G700 Media Gateway solution. A summary of key tools and their access methods is shown in Table 3.

A particular tool or access method may be preferred by one audience or another. This section is designed to provide a quick reference for accessing whatever tool you might need to perform a specific task, whether you are co-located with the G700 media gateway or accessing it remotely.

Table 3. Administration tool and access-method summary

Component	Task	Tool	Access methods
Media Gateway components:	**Initial configuration:** typically done by on-site Services technician or dealer partner		
Avaya™ P330 stack processor	- Set IP addresses for master and stack devices	- P330 stack command line interface (CLI)	- direct serial connection to master controller for media gateway or P330 stack
Media Gateway Processor (MGP), VoIP engine and optional VoIP Media Module	- Set IP address for MGP - Set IP address for VoIP engine on MGP board - Set IP addresses for VoIP Media Module if present	- MGP CLI	- session to MGP CLI from P330 stack CLI

1 of 2

Table 3. Administration tool and access-method summary *Continued*

Component	Task	Tool	Access methods
S8300 Media Server	- Configure media server - install license and call-processing software - do verification testing	- S8300 Media Server Web Interface	- direct Ethernet connection to the Services interface on S8300 media server
Media Gateway and software components:	**Ongoing administration and maintenance:** typically done remotely by system administrator, Services technician or dealer partner		
P330 stack processor	- Update configuration as needed	- P330 stack CLI - P330 Device Manager	- Ethernet connection over corporate LAN - direct connection to media gateway or P330 stack - remote PPP access
Media Gateway Processor (MGP), VoIP engine and media modules	- Update configuration as needed - Synchronize media gateway	- MGP CLI - P330 Device Manager	- Ethernet connection over corporate LAN - direct connection to media gateway or P330 stack - remote PPP access
S8300 Media Server	- Backup and restore data - Check server health - Update media server software and configuration as needed - synchronize G700 media modules as needed	- S8300 Media Server Web Interface	- Ethernet connection over corporate LAN - direct connection to the S8300 Services Ethernet interface - remote PPP access
MultiVantage software	- ongoing administration and maintenance of telephony features	- Avaya Site Administration (ASA) - System Access Terminal (SAT)	- launch ASA from desktop - launch ASA from another tool such as P330 Device Manager, S8300 web interface, or MultiService NMS - access SAT from CLI or ASA program

2 of 2

S8300 and G700 interface and task summary

A summary of the various interfaces and tools used to access the S8300 Media Server and G700 Media Gateway are shown in Figure 1.

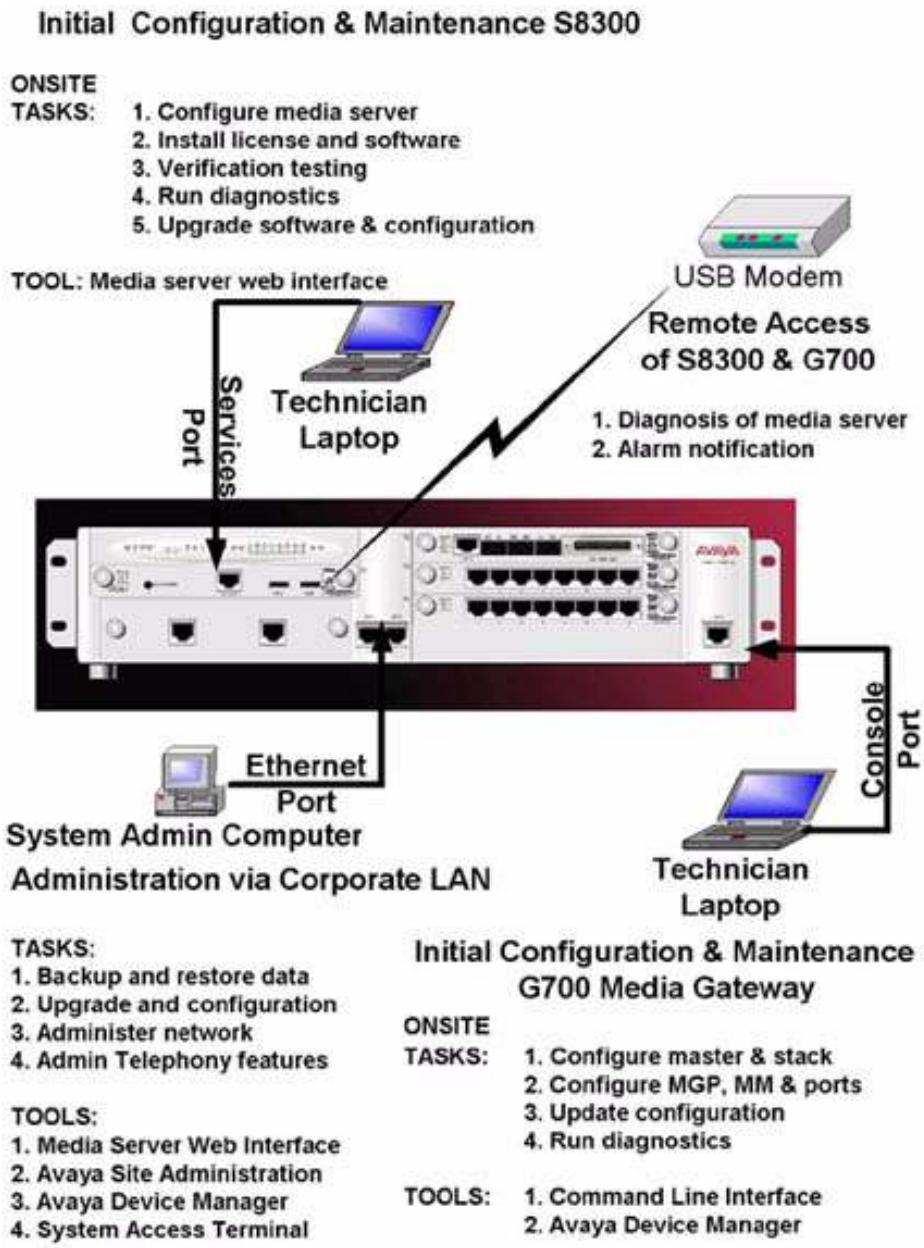

Figure 1. Summary of S8300 and G700 access methods and tasks

General access guidelines

The following considerations apply to the access procedures covered in this section.

- If a firewall is in place, you must access any IP devices such as the P330 stack processor, MGP, or media server from within the firewall boundary, or the firewall must grant the required access.
- Most corporate networks have one or more domain name service (DNS) servers that associate an IP address with a device's name. You can only access an IP device by name if the DNS server has been administered and is accessible for name resolution from the interface you are using. For example, direct connections from a laptop to the Services interface on the S8300 Media Server must use the server's IP address because DNS is disabled for this access method.
- Login service levels control access to the S8300 Media Server. These levels are specified through ASA or SAT. On the Login Administration screen, under Login Being Administered, the following service levels can be specified:
  - *super-user.* Logins assigned to this service level receive full access to the media server web interface. All screens are available.
  - *non-super-user.* Logins assigned to this service level receive a restricted level of access to the web interface. Only a few display-only screens are accessible.
  - *remote.* Logins assigned to this service level can use a PPP dial-up connection.

Specific Access Procedures

This section covers the following specific access procedures:

- Accessing the G700 processors using a serial connection
- Accessing a CLI using telnet
- Accessing the S8300 Media Server Web Interface and P330 Device Manager using an Ethernet interface
- Accessing the S8300 Media Server using a dial-up connection
- Accessing Avaya MultiVantage software

Accessing the G700 processors using a serial connection

This section covers how to access the P330 stack and G700 Media Gateway processors over a serial interface. Information includes:

- Hardware and software requirements
- Serial connection login procedure
- Media Gateway Processor (MGP) session

Hardware and software requirements

To successfully establish a serial connection, your computer must have:

- A physical serial connection to the master controller of the G700 Media Gateway or P330 stack. See Accessing the G700 processors using a serial connection for details.
- A serial-connection program such as Microsoft Windows® HyperTerminal installed.

Note: For a list of CLI commands, see the CLI Command Reference Pages.

Serial connection login procedure

1. Launch the terminal emulation program for a serial connection on your computer, such as HyperTerminal.
   - If your computer is directly connected to the serial port, access that port. For example, using HyperTerminal, choose **Call**.
   - If you are accessing the system remotely over a modem, you need to set up a profile to dial in to the Avaya P330 stack processor. See Setting up dial-up networking on Windows systems for guidelines on how to do this. Initiate the call when ready.
2. When the **Login** prompt appears, type the appropriate user name (such as **cust**).
3. When prompted, enter the appropriate password.
4. You are now logged in to the P330 stack processor CLI at the Supervisor level. The prompt appears as **P330-n(super)#** where *n* indicates the stack number of the device containing the master controller for the stack. If only one device is in the stack, the number appears as **P330-1**.
5. In order to use the commands necessary to configure the stack processor, you must reset to the Configure level of the CLI. Type `configure`
6. The prompt now appears as **P330-n(configure)#**. Enter commands as needed.
   - For example, you might type: `set interface inband 1 192.168.23.2 255.255.255.0` to assign IP address `192.168.23.2` to the stack processor (the fields before and after it are the VLAN group ID and the subnet mask).
   - To check the syntax of a command, type as much of the command as you know followed by `help`. For example, you could type: `set interface help`
7. From this interface, you can session to the Media Gateway Processor. See Media Gateway Processor (MGP) session.

Media Gateway Processor (MGP) session

Once you have logged in to the Avaya P330 stack processor, you can session over to the Media Gateway Processor (MGP) without having to log in again. From the MGP, you can session back to the P330 stack processor, or to the S8300 Media Server (if installed).

To session to the MGP from the P330 stack processor CLI:

1. You must be logged into the P330 stack processor. See Serial connection login procedure.
2. At the **P330-n(configure)#** prompt, type `session <module #> mgp` to reach the G700 Media Gateway processor, where `<module #>` is the number of the media gateway in the P330 stack (default is `1`).
3. You are now logged in to the MGP CLI at the view-only level. The prompt appears as **MG-???-n(super)#** where:
   - **MG** indicates Media Gateway
   - **???** indicates the media gateway number that is registered with the MultiVantage software. If the media gateway has not yet registered with a call-processing server, the number is replaced by question marks.
   - **n** indicates the media gateway module number in the P330 stack.
4. In order to use the commands necessary to configure the MGP, you must reset to the Configure level of the CLI. Type `configure`
5. The prompt now appears as **MG-???-n(configure)#** (or the equivalent administered name). Enter commands as needed.

   For example, you might type a `set mgp <vlan> <ip_address> <mask> <gateway>` command to assign an IP address to the G700 Media Gateway.
6. When finished, you can access other command line interfaces as follows:
   - To exit the MGP CLI and return to the P330 stack processor CLI, type `exit`. The **P330-n(configure)#** prompt appears.
   - To start a telnet session to an S8300 Media Server installed in slot 1 of this media gateway, type `telnet icc` (see Accessing a CLI using telnet for details about logging in to telnet).
   - To start a telnet session to any administered and accessible device in the network, type `telnet <ip_address>` (see Accessing a CLI using telnet for details).
     - Network routing information must be in place for a telnet connection to work.
     - Devices can be accessed by IP address only from this interface.

Accessing a CLI using telnet

A telecommunications network (telnet) program is a common way to access a command line interface (CLI). For example, you could access the Linux shell to run S8300 Media Server platform commands, or directly access the SAT program using a CLI connection. For a list of CLI commands, see the CLI Reference for the G700 Media Gateway Controller.

If you connect to a valid 10/100Base-T Ethernet interface and acquire a valid IP address either through Dynamic Host Configuration Protocol (DHCP) or static provisioning, you can telnet to any IP device administered on the network, provided that the firewall permits access.

Note: A secure shell (SSH) interface utility can be used as an alternative to telnet. SSH commands and passwords are encrypted, and both ends of the client/server connection are authenticated through a digital certificate. The SSH utility is more secure than telnet and should be used if available.

To run the telnet program:

1. Make sure you have a valid Ethernet or serial connection from your computer to the S8300 Media Server or the G700 Media Module (or its P330 stack).
2. Access the telnet program as follows:
   - If you already have a valid CLI connection in progress, go to step 3.
   - If you are not yet logged in, open a telnet program on your computer. For example, on a Windows system, go to the **Start** menu and select **Run**.
3. Type `telnet` to begin a telnet CLI session. Variations are:
   - Type `telnet <IP address>` to access any accessible, administered devices.
   - Type `telnet <name>` to access a device by name. This method only works for devices that are administered on a DNS that is accessible to the interface that you are using.

     Note: You can type `telnet <IP address> 5023` to log in directly to the SAT program. See Accessing SAT from a CLI for the SAT login procedure.
4. When the **login** prompt appears, type the appropriate user name (such as **cust** or **craft**).
5. When prompted, enter the appropriate password.
6. *If you log in as* ***craft****,* you are prompted to suppress alarm origination. Generally you should accept the default value (yes).
7. Enter your terminal type. Accept the default value, or enter the appropriate type for your computer.
8. If prompted for a high-priority session, typically answer **n**.
9. The telnet prompt appears. It may take the form <*username@devicename*>.
10. Enter the CLI commands appropriate for this interface. For example, you could:
    - Type Linux shell commands to set up Operations Support System (OSS) alarm notification on the S8300 Media Server.
    - Type `sat` or `dsat` to log in to the SAT program. See Accessing SAT from a CLI for this procedure.
    - Type `telnet <IP address>` to access another device, such as any other administered media gateway or P330 stack processor.

Accessing the S8300 Media Server Web Interface and P330 Device Manager using an Ethernet interface

This section covers how to access the S8300 Media Server Web Interface or the P330 Device Manager over an Ethernet interface. Information includes:

- Hardware and software requirements
- S8300 Media Server login procedure
- P330 Device Manager login procedure

Hardware and software requirements

To successfully access one of these browser-based tools, your computer must have:

- A valid physical connection to the S8300 Media Server (for the S8300 Media Server Web Interface), or to the G700 Media Gateway (for Device Manager). See Connecting to an Ethernet interface for details.
- A compatible Internet browser:
  - *P330 Device Manager:* supports Microsoft Internet Explorer 5.0 (or higher) and Netscape Navigator 4.7 and 6.2 browsers. The Java Plug-in 1.2.2 or 1.3.1 is required.
  - *S8300 Media Server:* requires either:
    - Microsoft Internet Explorer 5.x (5.5 is recommended). IE 6 is *not* currently supported. Internet Explorer 5.5 with Service Pack 2 (SP2) is required for initial configuration of the S8300 Media Server.
    - Netscape Navigator 4.7 or a later version of 4.x. Netscape 4.77 has been tested; other versions may work. Netscape 6 is *not* currently supported.

S8300 Media Server login procedure

To access the S8300 Media Server, you must log in as follows:

1. Establish a valid physical connection to the S8300 Media Server. See Connecting to an Ethernet interface for details.
2. Open a compatible Internet browser on your computer. Currently only Internet Explorer 5.x (5.5 with Service Pack 2 is recommended) and Netscape 4.7x are supported.
3. In the Address (or Location) field of your browser, type the IP address or name of the Avaya media server and press Enter.
   - *LAN access by IP address.* If you are logging into the administrative interface over the corporate local area network, you can type the media server's unique IP address in standard dotted-decimal notation, such as `http://192.152.254.201`
   - *LAN access by server name.* If the server has already been configured and if the corporate LAN includes a domain name service (DNS) server that has been administered with the servers' names, you can type the server's name into the address field instead of the IP address. Server names vary depending on local administration (such as `http://media-server1.mycompany.com`).

- *Laptop access by IP address.* If you are logging in to the services Ethernet interface from a directly connected laptop, the IP address on the server is always `192.11.13.6`. New servers that have not yet been configured can *only* be accessed in this way. Server-name login is *not* available through the services interface because this connection is a closed (private) network with no DNS.

Note: The S8300 media server's name and IP address are specified during initial media server configuration.

4. *If your browser does not have a valid security certificate,* you will see a warning screen and instructions to load the security certificate.
   - If you are certain your connection is secure, accept the server security certificate to access the Login screen.
   - If you plan to use this computer and browser to access this or other Avaya media servers again, click the main menu link to Install Avaya Root Certificate after you log in.
5. The Login screen appears.
   - In the Username field, type your user name (login ID), such as **cust**.
   - Click the **Login** button or press Enter.

Note: User names and passwords are case sensitive. Enter the login ID and confirmation information in upper- or lowercase as required.

6. Enter your login confirmation information as prompted:
   - *Password prompt.* Type your password in the Password field, and click Login or press Enter again.
   - *ASG challenge.* If your login is Access Security Gateway (ASG) protected, you will see a challenge screen. Enter the correct response and click Login or press Enter.
7. The server will match your login information against its authentication tables. If the information you entered is recognized as a valid login, the screen displays a two-frame window, with the main menu in the left panel and a usage-agreement notice in the right window.
   - If the main menu in the left panel has only about 10 links, you have accessed the server from a login ID that has restricted permissions. You can adjust the login service levels using the Login Administration screen in ASA or SAT.
   - If the server cannot recognize your user name or password, you receive an authentication failure message. Return to step 5. If you fail to enter the user name and login confirmation correctly 4 times within a few minutes, the Login screen will block further attempts to log in for a while.
8. When you successfully log in to the server, check the top of the left panel.
   - The Avaya media server you are logged into is identified by name and server number.
   - The S8300 media server number is always 1.

P330 Device Manager login procedure

To access the P330 Device Manager, you must:

1. Establish a valid physical connection to either the P330 stack processor or G700 Media Gateway processor. See Connecting to an Ethernet interface for details.
2. Open a compatible Internet browser on your computer. Currently this includes Internet Explorer 5.0 (or higher) and Netscape Navigator 4.7 and 6.2. The Java Plug-in 1.2.2 or 1.3.1 is required.
3. In the Address (or Location) field of your browser, type the IP address or name of the P330 stack processor and press Enter.
   - If you are accessing the Device Manager over a corporate LAN, and if the network includes a domain name service (DNS) server that has been administered with this IP device's name, you can type the processor's name into the address field instead of the IP address. For example, `http://P330-stack1.mycompany.com`
   - The Device Manager is *not* available through the S8300 Media Server. You must be connected to either the P330 stack processor or G700 Media Gateway processor through the corporate LAN interface (either by a directly connected cable or remote access).
4. A GUI rendering of the P330 stack P3xx devices appears. Proceed with media gateway or P330 device administration.

Accessing the S8300 Media Server using a dial-up connection

If an optional external modem is connected to the USB port on the S8300 Media Server, you can access the server over a dial-up connection. Issues include:

- Dial-up users must have a system configured for point-to-point protocol (PPP) access via modem.
- The remote connection should support a data speed of at least 33.6 kbps.

Note: A dial-up connection is typically used only for services support of the server, not for routine administration. If the server is administered to report OSS alarms, it uses this same line for alarm notification. The server cannot report any new alarms while this line is in use.

This section covers:

- Using a dial-up networking connection
- Setting up dial-up networking on Windows systems

Using a dial-up networking connection

To connect to the S8300 Media Server using a dial-up connection:

1. Your computer must have a modem that is connected to an analog line.
2. Launch the dial-up connection program. This varies from system to system. For example:
   - If you created an icon on your desktop for this connection, double-click the icon.
   - On a Windows NT 4.0 system: Open the Dial-Up Networking phonebook and click the **Dial** button. See Setting up dial-up networking on Windows systems for details.
   - *On a Windows 2000 or XP system:* Right-click My Network Places on your desktop or under the Start menu in XP. Select **Properties** to display the Network and Dial-up Connections window. Double-click the entry for the appropriate dial-up connection.
3. The appropriate Connect screen appears.
   a. The **User name** and **Password** fields are not validated (leave blank).
   b. *If a domain field appears,* leave it blank.
   c. If the **Dial** field is blank, enter the appropriate telephone number. Include special digits such as 9 or 1, or *70, if needed.
   d. Click the **Dial** button. (On some computers, you might click **OK**.)
4. Connection messages appear. When the media server's modem answers, the After Dial Terminal window appears.
   a. Enter your remote access login name and password.
   b. When the **Start PPP now!** message appears, click **Done**.
5. Your computer should now authenticate onto the network.
6. Open a telnet session to the IP address assigned to this S8300 Media Server during configuration.
   - To use Linux shell commands, see Accessing a CLI using telnet.
   - To access MultiVantage software directly, see Accessing SAT from a CLI.

Setting up dial-up networking on Windows systems

Administration of dial-up networking varies depending on your computer system and the dial-up program you use. Instructions for some Microsoft Windows systems are described below. Modify these as needed for your particular setup.

Windows 2000 or XP dial-up networking setup

1. Right-click My Network Places on your desktop or under the Start menu in XP.
2. Select **Properties** to display the Network and Dial-up Connections window.
3. Double-click **Make New Connection** in the window.
4. The Network Connection Wizard appears. Click **Next**.
5. In the Network Connection Type window, select the **Dial-up to private network** radio button Click **Next**.

6. Update the Phone Number to Dial window as follows:
   - To make this a general-purpose connection, leave the phone number blank.
   - To set up a connection for a specific location, enter the correct phone number for the media server's modem. Insert digits such as 9 and 1 or *70, if necessary.
   - Click **Next**.
7. In the Connection Availability window, select "For all users" or "Only for myself" as needed. Click **Next**.
8. Update the Completing the Network Connection Wizard window as follows:
   - Type a name for this dial-up connection. This name is used only by your computer to identify this connection.
   - Check the box to add the shortcut to your desktop if desired.
9. Click **Finish**.
10. *If a Connect screen appears,* click **Cancel**.
11. Return to the Network and Dial-up Connections window.
12. Right-click the entry you just created and select **Properties**.
13. On the connection's Properties screen, click the **Security** tab.
    - Select the **Advanced (custom settings)** radio button.
    - Check the **Show terminal window** checkbox.
14. Click the **Networking** tab.
    - In the Components box, verify that **Internet Protocol (TCP/IP)** and **Client for Microsoft Networks** are checked.
    - Select **Internet Protocol (TCP/IP)** and click the **Properties** button.
15. On the Internet Protocol (TCP/IP) Properties screen, click the **Advanced** button.
16. On the Advanced TIP/IP Settings screen, clear the **Use default gateway on remote network** checkbox.

    If you leave this box checked, all your network traffic will be routed to the media server. Your computer will act like it's been disconnected from the local network.
17. Click **OK** three times to exit and save the changes.
18. To access the remote server, see Using a dial-up networking connection.

Windows NT 4.0 dial-up networking setup

1. Open the Dial-Up Networking phonebook.
2. To create a new entry, click the **New** button. The New Phonebook Entry Wizard appears.
   a. In the New Phonebook Entry Wizard window, type a name for this dial-up connection. This name is used only by your computer to identify this entry.
   b. In the Server window, check only the third checkbox: "The non-Windows NT server I am calling expects me to type login information...".

c. In the Phone Number window, enter the phone number of the media server's modem. Insert digits such as 9 and 1 if necessary.

d. In the Serial Line Protocol window, select **Point-to-Point Protocol (PPP)**.

e. In the Login Script window, select "Use a terminal window".

f. In the next two windows (IP Address and Name Server Addresses), leave the various IP addresses set to all zeroes.

g. Click **Finish**.

3. Edit the just-created phonebook entry by clicking the **More** button.

   a. Select "Edit entry and modem properties".

   b. Select the Server tab and click the "TCP/IP Settings..." button.

   c. Uncheck the "Use default gateway on remote network" box.

      If you leave this box checked, all your network traffic will be routed to the media server. Your computer will act like it's been disconnected from the local network.

   d. When finished, close this window and save your entries.

Note: If you later want to connect to a different server, open the Dial-Up Networking phonebook, select an existing media server entry, and click on the **More** button. Next, select “Clone entry and modem properties”. Now you can change just the entry name and phone number without walking through the entire wizard.

4. To access the remote server, see Using a dial-up networking connection.

Accessing Avaya MultiVantage software

Avaya MultiVantage Software is an open, scalable, highly reliable and secure telephony application. MultiVantage software provides user and system management capability, intelligent call routing, application integration and extensibility, as well as enterprise communications networking. Tools used to administer MultiVantage software include:

- Avaya Site Administration (ASA): a telephony administration program that uses a graphical user interface (GUI). ASA must be run on a compatible Microsoft Windows operating system such as Windows 95, 98, NT 4.0, Millennium Edition, and Windows 2000.
- System Access Terminal (SAT) program: a version of the telephony administration software that uses a command line interface (CLI).

This section covers:

- Accessing Avaya Site Administration
- Accessing SAT from a CLI

Accessing Avaya Site Administration

The Avaya Site Administration (ASA) software must be installed on a compatible administration or Services laptop computer, in compliance with the ASA contract with Avaya Inc.

Note: A copy of the ASA package is available for download on every new Avaya media server. To download this copy, log in to the S8300 Media Server (see S8300 Media Server login procedure). When you access the main menu of the web interface, click the Download ASA link.

The Avaya Site Administration (ASA) software can be accessed in a variety of ways:

1. Make sure you have a valid physical connection from your computer to the S8300 Media Server, or another media server (such as the S8700) that is running MultiVantage software.
2. If ASA is installed on your computer, you can launch it in any of the following ways:
   - Click the Avaya Site Administration icon on your desktop.
   - From the S8300 Media Server Web Interface main menu, click the **Start ASA** link.
   - From the P330 Device Manager interface, select the **Launch ASA** toolbar button or menu item.
   - From the Avaya MultiService Network Manager, launch the ASA software.
3. Log in to the MultiVantage software. At the **Login** prompt, type the appropriate user name (such as **cust** or **craft**).
4. Enter your login confirmation information as prompted:
   - *Password prompt.* Type your password in the Password field, and click Login or press Enter again.
   - *ASG challenge.* If your login is Access Security Gateway (ASG) protected, you will see a challenge screen. Enter the correct response and click Login or press Enter.
5. The Avaya Site Administration package opens. You can administer telephony features in two main modes:
   - Using the Graphically Enhanced Interface user interface
   - Launching the System Access Terminal (SAT) program to use a CLI version

Accessing SAT from a CLI

The System Access Terminal (SAT) program can be accessed from a command line interface as follows:

1. Make sure you have a valid Ethernet or serial connection from your computer to the S8300 Media Server, or another media server (such as the S8700) that is running MultiVantage software.
2. *If you already have a valid CLI connection in progress,* access the SAT program by typing `sat` or `dsat`. Go to step 4.
3. *If you are not yet logged in,* open a telnet program on your computer. For example:
   - On a Windows system, go to the **Start** menu and select **Run**.
   - To log in directly to the SAT program, type `telnet <IP address> 5023`

4. Log in to the MultiVantage software. At the **Login** prompt, type the appropriate user name (such as **cust** or **craft**).
5. Enter your login confirmation information as prompted:
   - *Password prompt.* Type your password in the Password field, and click Login or press Enter again.
   - *ASG challenge.* If your login is Access Security Gateway (ASG) protected, you will see a challenge screen. Enter the correct response and click Login or press Enter.
6. Enter your terminal type. Accept the default value, or enter the appropriate type for your computer. For example, use type `ntt`.
7. The SAT interface appears. Enter SAT commands as appropriate.

Physical Connections to Media Gateways

This section describes how to physically connect a computer to the S8300 Media Server or G700 Media Gateway. See Figure 1 for an illustration of these physical connections. Setups covered include:

- Connecting directly to the G700 serial port
- Connecting a modem to a USB port
- Connecting to an Ethernet interface
- Setting up a laptop for an S8300 Media Server direct Ethernet connection

Connecting directly to the G700 serial port

A direct serial connection to the G700 Media Gateway is typically used for initial configuration.

To connect a laptop directly to the serial port on the G700 Media Gateway:

1. *For a stacked configuration:* locate the device that contains the master controller for the stack. Check the LED panel on the upper left of each G700 or P330 device in the stack as follows:
   - G700 Media Gateway: a lit **MSTR** LED indicates that this unit is the stack master.
   - P330 device: a lit **SYS** LED indicates that this unit is the stack master.
2. Use the RS-232 serial cable and DB-9 adapter cable provided with the G700 Media Gateway.
3. Attach one end of the RS-232 cable to the RJ-45 jack on the front of the unit that is the stack master. The serial port is on the lower right side of the chassis.
   - On a G700, this serial port is labeled **Console**.
   - The name of the serial port varies on P330 devices, but it is located on the lower right.
4. Plug the other end of the RS-232 cable into the RJ-45 jack on the DB-9 adapter cable.
5. Connect the other end of the DB-9 adapter cable to the 9-pin serial port on your laptop.

6. Use a serial-connection program such as HyperTerminal to access the P330 stack processor. See Serial connection login procedure.

Connecting a modem to a USB port

An optional external modem may be connected to the S8300 Media Server through a universal serial bus (USB) connection, providing dial-up access. The modem requires an analog line to the remote location.

To connect an external modem to a USB port on the S8300 Media Server:

1. Obtain an external modem and its required USB cabling.
2. Connect one end of the modem's USB cable to an available USB port on the S8300 Media Server's faceplate. Either USB1 or USB2 can be used.
3. Connect the other end of the cable to the external modem.
4. Connect the modem to an analog line.
5. Power up the modem and verify operation as instructed by the modem's documentation.

Connecting to an Ethernet interface

Types of Ethernet connections to an S8300 Media Server or G700 Media Gateway include:

- Remote access to the G700 from a computer over the corporate local area network (LAN). See Corporate LAN remote access.
- Direct connection from a laptop to the corporate LAN interface on the G700. See Corporate LAN direct connection.
- Direct connection from a laptop to the S8300 Media Server using a crossover cable. See S8300 Services interface direct connection.

Corporate LAN remote access

To physically connect the G700 Media Gateway (and S8300 Media Server if installed) to the corporate local area network (LAN) to support remote access:

1. Connect an Ethernet cable to one of the two 10/100Base-T Ethernet interfaces in the bottom center of the G700 chassis. Either port EXT 1 or EXT 2 can be used.
2. Connect the other end of the Ethernet cable to an Ethernet Layer 2 switch to connect the G700 and its media modules to the corporate network. LAN topology varies per location.
3. Complete administration of the S8300 and G700 components, including network routing.
4. From another location on the corporate LAN, connect your computer to the network. An Ethernet card in the computer is required.
5. Log in using the desired administration tool.

Corporate LAN direct connection

To connect a laptop directly to a G700 Media Gateway Ethernet interface:

1. Your laptop must be assigned an IP address compatible with this subnet of the corporate LAN. The IP address may be assigned statically or through a Dynamic Host Configuration Protocol (DHCP) service on the customer's LAN.
2. Connect an Ethernet cable to one of the two 10/100Base-T Ethernet interfaces in the bottom center of the G700 chassis. Either port EXT1 or EXT2 can be used if available.

   If both corporate LAN Ethernet interfaces on the G700 are in use, and if the G700 is in a stacked configuration, another Ethernet interface can be used if available on one of the P330 devices.
3. Connect the other end of the Ethernet cable to the 10/100 BaseT Ethernet network interface card (NIC) on your laptop. (Do *not* use a crossover Ethernet cable for this connection.)
4. Log in to the desired administration tool.

S8300 Services interface direct connection

To connect a laptop directly to the S8300 Media Server:

1. Make sure your laptop meets the hardware and software requirements.
2. Plug an Ethernet crossover cable (MDI to MDI-X) into the 10/100 BaseT Ethernet network interface card (NIC) on your laptop.
   - Crossover cables of various lengths are commercially available.
   - See Table 4 for pinout connections if needed. Crossover of the transmit and receive pairs (as shown) is required
3. Connect the other end of the laptop's Ethernet cable to the Services Ethernet interface on the front of the S8300 media server.
4. If your laptop is already configured with the correct network settings, you can now open your Internet browser and log in.
   - When accessing the server from a directly connected laptop, always type the following IP address in the browser's Address or Location field to access the server: `192.11.13.6`
   - If you have never connected this laptop directly to an Avaya media server before, see Setting up a laptop for an S8300 Media Server direct Ethernet connection.

Table 4. Crossover cable pinout chart

Pin to Avaya S8300 Media Server's Services Ethernet interface	connects to	Pin to laptop's Ethernet card
8		8
7		7
6		2
5		5
4		4

1 of 2

Table 4. Crossover cable pinout chart *Continued*

Pin to Avaya S8300 Media Server's Services Ethernet interface	connects to	Pin to laptop's Ethernet card
3		1
2		6
1		3
		2 of 2

Setting up a laptop for an S8300 Media Server direct Ethernet connection

A laptop connected directly to the Services Ethernet interface on the S8300 Media Server requires a specific setup. This section covers:

- General settings
- Set TCP/IP properties on Windows systems
- Disable proxies in browser

General settings

On any operating system, the network settings need to reflect the following:

- *TCP/IP properties.* Set the laptop's TCP/IP properties as follows:
  - IP address: 192.11.13.5
  - Subnet mask: 255.255.255.252
- *Browser settings.* Configure the browser for a direct connection to the internet. Do *not* use proxies.
- *Server address.* Access the media server using the URL `http://192.11.13.6`

The names of the dialog boxes and buttons vary on different operating systems and browser releases. Use your computer's help system if needed to locate the correct place to enter this information.

Note: Avaya Service technicians can use the NetSwitcher program to configure alternate network profiles so they can easily connect to a number of different systems. NetSwitcher configures a profile for each type of system for easy future access without requiring you to reset TCP/IP properties or browser settings manually. NetSwitcher is available from an Avaya Services CTSA.

The S8300 Media Server uses the same access configuration as an Avaya S8100 Media Server with CMC1 Media Gateway. If you already have a NetSwitcher profile for the S8100 Media Server (formerly called DEFINITY One), try using that profile first before configuring a new one.

Set TCP/IP properties on Windows systems

TCP/IP administration varies among Windows systems as described below.

Note: Make a record of any IP addresses, DNS servers, or WINS entries that you change when you configure your services computer. Unless you use the NetSwitcher program or an equivalent, you will need to restore these entries to connect to other networks.

Change TCP/IP Properties and Network Settings (Windows 2000 and XP)

1. Right-click My Network Places on your desktop or under the Start menu in XP.
2. Select **Properties** to display the Network and Dial-up Connections window.

   Windows should have automatically detected the Ethernet card in your system and created a LAN connection for you. More than one connection may appear.
3. Right-click the correct **Local Area Connection** from the list in the window.
4. Select **Properties** to display the Local Area Connection Properties dialog box.
5. Select **Internet Protocol (TCP/IP)**
6. Click the **Properties** button. The Internet Protocol (TCP/IP) Properties screen appears.
7. On the General tab, select the radio button **Use the following IP address**. Enter the following:
   - IP address: 192.11.13.5
   - Subnet mask: 255.255.255.252

   Note: Record any IP addresses, DNS settings, or WINS entries that you erase. You may need to restore them later to connect to another network.

8. **Disable DNS service as follows:**
   a. Click the radio button labeled **Use the following DNS server addresses**. The entries for Preferred DNS server and Alternate DNS server should both be blank.
   b. Click the **Advanced** button at the bottom of the screen. The Advanced TCP/IP Settings screen appears.
   c. Click the **DNS** tab. Verify that no DNS server is administered (the address field should be blank).
9. Disable WINS Resolution as follows:
   a. Click the **WINS** tab. Make sure WINS is not administered (the address field should be blank).
   b. Click **OK**. If warned about an empty primary WINS address, click **Yes** to continue.
10. Click **OK** twice to accept the address information and close the TCP/IP and Local Area Connection Properties dialog boxes.
11. Reboot the system if directed to do so.

After you have made these changes to your computer's network configuration information, the Network and Dial-up Connections window shows the status of the Local Area Connection:

- Enabled appears when the laptop's Ethernet cable is connected to the server.
- Disabled or unplugged appears if the NIC is not connected to anything.

Change TCP/IP properties (Windows 95, 98, NT 4.0, and Millennium Edition [Me])

1. Access your computer's network information. On your desktop:
   - *Windows 95, 98, and NT:* Right-click Network Neighborhood.
   - *Windows Me:* Right-click My Network Places.
2. Select **Properties** to display the Network dialog box.
3. Locate the TCP/IP properties as follows:
   - *Windows 95, 98, and Me:* On the **Configuration** tab, scroll through the installed network components list to the TCP/IP part of the devices list. Select the TCP/IP device that corresponds to your Ethernet card.
   - *Windows NT:* On the Protocols tab, select **TCP/IP** in the installed network components list.
4. Select the **Properties** button.
5. In the TCP/IP Properties box., click the **IP Address** tab.
6. Click the radio button to **Specify an IP address**, and enter the following:
   - IP address: 192.11.13.5
   - Subnet mask: 255.255.255.252

   Note: Record any IP addresses, DNS settings, or WINS entries that you erase. You may need to restore them later to connect to another network.

7. **Disable DNS service as follows:**
   - *Windows 95, 98, and Me:* Click the **DNS Configuration** tab. Verify that the **Disable DNS** radio button is selected.
   - *Windows NT:* Click the **DNS** tab.
     - If any IP addresses appear under DNS Service Search Order, make a note of them in case you need to restore them later.
     - Select each IP address in turn and click the **Remove** button.
8. Disable WINS Resolution as follows:
   - *Windows 95, 98, and Me:* Click the **WINS Configuration** tab. Verify that the **Disable WINS Resolution** radio button is selected.
   - *Windows NT:* Click the **WINS Address** tab.
     - If any IP addresses appear for the Primary and Secondary WINS servers, make a note of them in case you need to restore them later.
     - Clear each server entry.

- Clear the checkbox for **Enable DNS for WINS Resolution**.

9. Click OK twice to accept the address information and close the Network dialog box.
10. Reboot the system if directed to do so.

Disable proxies in browser

If you are connecting a laptop directly to the Services Ethernet interface on the S8300 Media Server faceplate, you must disable proxies as described below.

Note: You may not have to disable using a proxy server if you instruct your browser to not use the proxy server when accessing address 192.11.13.6 from a directly connected laptop. Otherwise, you need to remember to turn proxy usage on or off as needed.

To check or change proxy settings:

1. Open your Internet browser.
2. Verify that you have a direct connection with no proxies as follows:

- **Internet Explorer**
  - a. Select **Tools > Internet Options**.
  - b. Click the **Connections** tab
  - c. Click the **LAN Settings** button.
  - d. Deselect **proxy server** if selected, and click **OK**.
  - e. Click **OK** again to close the Internet Options dialog box.
- **Netscape**
  - a. Select **Edit > Preferences**.
  - b. Under Category, click **Advanced**.
  - c. Click **Proxies**.
  - d. Make sure **Direct connection to the Internet** is selected.
  - e. Click **OK**.

Supporting Library

Introduction

This section describes the document set that supports the Avaya S8300 Media Server and Avaya G700 Media Gateway. This section covers:

- MultiVantage Solutions Hardware Guide
- S8300 and G700 Reference Library

MultiVantage Solutions Hardware Guide

This document provides a detailed description of the S8300 Media Server and G700 Media Gateway. It should be used in conjunction with the other documents in the library set. See Table 5 for a list of key documents that support the S8300 Media Server and G700 Media Gateway.

S8300 and G700 Reference Library

Table 5 lists the documents that support the S8300 Media Server and G700 Media Gateway.

Table 5. S8300 Media Server and G700 Media Gateway library

S8300/G700 Core Document Set

Welcome to Avaya™ S8300 Media Server and Avaya™ G700 Media Gateway, 555-234-200

Purpose:

This document provides and brief summary of the S8300 and G700 IP-communications solution, describes its features and applications, and provides a guide to the supporting documentation library. It also provides a detailed description of the access procedures used to configure, administer, and maintain the S8300/G700 solution.

Audience:

Users of the S8300/G700 documentation library.

Avaya MultiVantage™ Solutions Hardware Guide, 555-233-200

Purpose:

This guide provides descriptions of the Avaya's IP-based Media Server and Media Gateway hardware components as well as the Avaya™ DEFINITY servers, and Avaya™ SCC1 Media Gateway, Avaya™ MCC1 Media Gateway, Avaya™ CMC1 Media Gateway, and Avaya™ G600 Media Gateway. It also provides example configurations of these components that provide a variety of telecommunication solutions.

Audience:

Sales and Pre-Sales personnel, Design Engineers, Technicians, Customers

Installation and Upgrades for the Avaya™ G700 Media Gateway controlled by an Avaya™ S8300 Media Server or an Avaya™ S8700 Media Server, 555-234-100

Purpose:

This document provides procedures to install, upgrade, or add to an S8300 or S8700 with an Avaya™ G700 Media Gateway and other communication controllers and to establish initial access to the full range of Avaya MultiVantage™ capabilities.

Audience:

Field technicians, Support personnel

Table 5. S8300 Media Server and G700 Media Gateway library *Continued*

Installation Quick Reference for the Avaya™ S8300 Media Server and the Avaya™ G700 Media Gateway, 555-234-201

Purpose:

This guide contains the steps with pictures explaining how to set the system up, including:

- Mounting in the rack
- Inserting the S8300 Media Server
- Inserting media modules
- Connecting the units
- Assigning IP addresses
- Configuring the media server
- Connecting to the LAN

Audience:

Field technicians

Maintenance for the Avaya™ G700 Media Gateway controlled by an Avaya™ S8300 Media Server or an Avaya™ S8700 Media Server, 555-234-101

Purpose:

This document provides procedures to monitor, test, and maintain a G700 Media Gateway controlled by an S8300 or S8700 Media Server. It covers many of the faults and troubles that can occur in the system.

Audience:

Field technicians, Support personnel

Network Reference for the Avaya™ S8300 Media Server with an Avaya™ G700 Media Gateway, 555-234-600

Purpose:

This document provides reference information needed to install, monitor, test, and maintain a G700 Media Gateway controlled by an S8300 or S8700 Media Server.

Audience:

Design Engineers, System Administrators, Field technicians

Table 5. S8300 Media Server and G700 Media Gateway library *Continued*

Key supporting documents: Avaya™ P330 devices

Avaya™ P330 Manager User Guide

Purpose:

The Avaya P330 manager provides full management capabilities for Avaya P330 devices. This includes the ability to view four aspects of P330 management:

- Device Manager
- Routing Manager
- Device SMON
- Any Layer SMON

Audience:

Field technicians, Design Engineers, Telecommunications managers

Avaya™ P333T User's Guide

Purpose:

This guide tells you how to connect up to 10 Avaya™ P330 switches in a stack.

Audience:

Field technicians, Design Engineers

Key supporting documents: MultiVantage software

Administrator's Guide for Avaya MultiVantage™ Software, 555-233-506

Purpose:

This document provides procedures to set up and administer network connectivity for media servers and DEFINITY servers with MulitVantage software.

Audience:

Network administrators

Reports for Avaya MultiVantage™ Software, 555-233-505

Purpose:

This document provides a description of the performance reports available with Avaya MultiVantage™ software.

Audience:

System Administrator's

Table 5. S8300 Media Server and G700 Media Gateway library *Continued*

Avaya MultiVantage™ Little Instruction Box, 555-233-908

Purpose:

These three documents provide descriptions of commonly used basic and advanced administration procedures and how to solve common problems.

Audience:

Network administrators

Administration for Network Connectivity for Avaya MultiVantage™ Software, 555-233-504

Purpose:

This document provides procedures to set up and administer network connections for media servers and DEFINITY servers with MulitVantage software.

Audience:

Design Engineers, Network administrators, Technicians, Support personnel

Dial Plan Expansion Job Aid for Avaya MultiVantage™ Software, 555-233-782

Purpose:

This job aid provides an overview for converting an Avaya MultiVantage Solutions system from a 4/5-digit dial plan to a 6/7-digit dial plan.

Audience:

System Administrators, Software Specialists

Maintenance for the Avaya™ S8700 Media Server for Multi-Connect Configurations, 555-233-143

Purpose:

This document provides procedures to monitor, test, and maintain an S8700 Media Server for multiconnect configurations. It covers many of the faults and troubles that can occur in the system.

Audience:

Field technicians and support personnel

Maintenance for the Avaya™ S8700 Media Server for IP-Connect Configurations, 555-233-142

Purpose:

This document provides procedures to monitor, test, and maintain an S8700 Media Server for IP-connect configurations. It covers many of the faults and troubles that can occur in the system.

Audience:

Field technicians and support personnel

Table 5. S8300 Media Server and G700 Media Gateway library *Continued*

Maintenance for Avaya DEFINITY® Server R, 555-233-117

Purpose:

This document provides procedures to monitor, test, and maintain DEFINITY servers. It covers many of the faults and troubles that can occur in the system.

Audience:

Field technicians and support personnel

Additional Supporting Documents

4600 Series IP Telephone LAN Administration, 555-233-507

Purpose:

This guide provides a description of Voice over IP, how to administer DHCP and TFTP servers, and how to troubleshoot operational problems with the 4600 Series IP Telephones and servers.

Audience:

System Administrators, Network Administrators, Design Engineers

INTUITY™ AUDIX® LX Release 1.0 LAN Integration with S8300 and DEFINITY® Systems

Purpose:

This document provides procedures set up a LAN connection from the S8300 with a G700 to an INTUITY™ AUDIX LX messaging system.

Audience:

Field Technicians, System Administrators

DEFINITY® Communications System G2.2 and G 3 V2 DS1/CEPT1/ISDN PRI Reference, 555-025-107

Purpose:

This document describes narrowband switching using digital facilities based on the digital signal level 1 (DS1), 1.544 Mbps, and Conference of Postal and Telecommunications (CEPT1), 2.048 Mbps, rates.

Audience:

Network Engineers, Network Administrators

Avaya Products Security Handbook, 555-025-600

Purpose:

This guide tells you how to protect your telecommunications network from a variety of security risks.

Audience:

Network security personnel

Table 5. S8300 Media Server and G700 Media Gateway library *Continued*

Avaya™ G700 Media Gateway Security White Paper

Purpose:

This guide tells you how to protect your network from outside exposure when remote access to the S8300 and G700 system is supported.

Audience:

System Administrators, Network Security personnel

Avaya™ Voice over IP Monitoring Manager

Purpose:

This is a voice over IP (VoIP) quality of service monitoring tool. It enables you to monitor and review the quality of a call, in an easy to use interface. With the information this manager provides, you can begin to troubleshoot and isolate problems.

Audience:

Telecommunications maintenance personnel

Avaya MultiVantage™ CallVisor® ASAI Technical Reference, 555-230-220

Purpose:

This document describes ASAI (Adjunct/Switch Applications Interface) services in terms of function sets or capability groups, which enable applications to monitor and control switching resources.

Audience:

System Administrators, Application Designers and Programmers

Documentation Library CDs

You can order the following documentation Library CDs from the Avaya Publications Center; see How to Order Documentation.

Avaya DEFINITY® Servers and Avaya™ S8100 Media Server Library CD, 555-233-823

Avaya™ S8700 Media Server Library CD, 555-233-824

Avaya™ S8300 Media Server and Avaya™ G700 Media Gateway Library CD, 555-234-800

INTUITY™ AUDIX® LX Release 1.0 Documentation CD, 555-313-818

Avaya MultiVantage™ Release 11 CallVisor® ASAI Documents CD, 555-246-801